MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY

VOLUME **18** | NUMBER **2** | FALL **2024** | ISSN **1802-5943**

PEER REVIEWED

CONTENTS:

www.mujlt.law.muni.cz

Masaryk University Journal of Law and Technology
issued by Institute of Law and Technology
Faculty of Law, Masaryk University
www.mujlt.law.muni.cz

Official Partner (Czech Republic)
ROWAN LEGAL, advokátní kancelář s.r.o. (https://rowan.legal)
Na Pankráci 127, 14000 Praha 4

Subscriptions, Enquiries, Permissions
Institute of Law and Technology, Faculty of Law, MU (cyber.law.muni.cz)

listed in HeinOnline (www.heinonline.org)
listed in Scopus (www.scopus.com)
reg. no. MK ČR E 17653

MASARYK UNIVERSITY JOURNAL OF
LAW AND TECHNOLOGY

VOLUME **18** | NUMBER **2** | FALL **2024**

LIST OF ARTICLES

DOI 10.5817/MUJLT2024-2-1

PEOPLE'S REPUBLIC OF CHINA AND THE ADEQUACY – WHY CHINESE DATA PROTECTION LAW IS NOT ADEQUATE WITHIN THE MEANING OF THE GDPR

by

WOJCIECH PANEK *

Chinese data protection seems to be problematic. On the one hand, it does exist, at least formally, especially after the reform initiated by the adoption of the Cybersecurity Law and finished by the Personal Information Protection Law entering into force. However, the mere adoption of personal data protection regulations does not guarantee that they provide personal data protection at an appropriate level. For EU law, the adequacy standard is the reference point for verifying personal data protection in a third country. Therefore, it is necessary to meet specific criteria summarising the term of essential equivalence, as introduced by the Court of Justice of the European Union. This article discusses the three most critical problems that result from comparing the provisions of the Chinese Cybersecurity Law, the Civil Code, the Data Security Law and the Personal Information Protection Law with the EU's adequacy standard. The article consists of the introduction, four parts and closing remarks. The first part explains the methodology of research on Chinese data protection law and criteria applied to its examination. The second, third and fourth parts discuss the complicated relationships between the laws related to the protection of personal data, the status of state authorities as data controllers and multi-stakeholder supervision over personal data protection.

KEY WORDS

GDPR, Adequacy, Personal Data Transfers, China, Data Protection in China.

* At the time of writing this paper, the Author was a PhD student at Doctoral School at the University of Silesia in Katowice. ORCID: 0000-0003-3264-986x. For correspondence: wojciech.panek@us.edu.pl

1. INTRODUCTION

Is there any data protection in the People's Republic of China[1]? The answer to that question is not as straightforward as one might expect. Through several recent reforms, the Chinese legal system of data protection has undergone far-reaching changes. It all started in October 2017 and – probably – finished in October 2021. The first date refers to the adoption of the Cybersecurity Law[2], a cybersecurity-oriented regulation. The fact that it included data protection provisions led to the doctrine declaring it a milestone in developing contemporary data protection law in China.[3] The second date is when the Personal Information Protection Law[4] came into force. In the meantime, some other data-protection-related regulations were enacted[5]. Hence, the Chinese data protection law currently comprises the Cybersecurity Law and the Personal Information Protection Law[6], supplemented by the Chinese Civil Code[7] and the Data Security Law[8].

The mere existence of data protection law does not necessarily amount to actual data protection. The latter depends on the quality of that law. The uncertain effectiveness of Chinese data protection legislation[9] stems from purpose of the reform clearly set out by the Chinese authorities.

1 Hereinafter referred to as China

2 Zhonghua Renmin Gonghegup Wanglup Anquan Fa (中华人民共和国网络安全法) [Cybersecurity Law of the People's Republic of China] (issued by the Standing Committee of the National People's Congress on 11 July 2016, came into force on 1 June 2017, bilingual version accessed via PKU Law database).

3 Pernot-Leplay, E. (2020) China's Approach on Data Privacy Law: A Third Way between the U.S. and the EU? *Penn State Journal of Law and International Affairs*, 8(1), p. 71.

4 Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [Personal Information Protection Law of the People's Republic of China] (issued by the Standing Committee of the National People's Congress on 20 August 2021, came into force on 1 November 2021, bilingual version accessed via PKU Law database).

5 These are: Zhonghua Renmin Gongheguo Minfa Dian (中华人民共和国民法典) [Civil Code of of the People's Republic of China] (issued by the National People's Congress on 28 May 2020, came into force on 1 January 2021, bilingual version accessed via PKU Law database) and Zhonghua Renmin Gongheguo shuju Anquan Fa (中华人民共和国数据安全法) [Data Security Law of the People's Republic of China] (issued by the Standing Committee of the National People's Congress on 10 June 2021, came into force on 1 September 2021, bilingual version accessed via PKU Law database).

6 Guangping, W. (2021) Challenges and Responses to the Protection of Workers' Personal Information in the Context of Human-Computer Interaction. *China Legal Science*, 9(139), pp. 144-145.

7 Gao, R. Y. (2020) Personal Information Protection under Chinese Civil Code: A Newly Established Private Right in the Digital Era. *Tsinghua China Law Review*, 13 (1), p. 183.

8 Cai, P., Chen, L. (2022) Demystifying data law in China: a unified regime of tomorrow. *International Data Privacy Law*, 12(2), p. 78; Chen, J. Sun, J. (2021) Understanding the Chinese Data Security Law. *International Cybersecurity Law Review*, 2, p. 218.

9 Cai, P., Chen, L. Demystifying data law in China: a unified regime of tomorrow. *International Data Privacy Law*, 12(2), p. 92; Zheng, G. (2021) Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S. and China. *Computer Law & Security Review*, 43, p. 6.

The overarching purpose was to diminish the influence of lacking data protection laws on economic relations with Western entities, yet with Chinese specificity.[10] Consequently, the protection of the data subject, well-known from the GDPR and EU legislation, was not the central theme of the reform and abovementioned regulations.[11] Instead the focus was primarily on business needs, mainly the need for undisturbed technological development, combined with political factors.[12]

With this background in mind, it would not be shocking to say that the reform brought nothing to data subjects. However, the overall impression of the Chinese data protection law[13] suggests something different as the legislation encompasses data protection principles, data subject's rights, sanctions for data controllers and establishes some data authorities.

EU data protection law takes a strict attitude[14] towards personal data transfers outside the EU[15]. Though, any remarks concerning the content of a third country's data protection law automatically bring about the

[10] See: Creemers, R. (2021) China's Emerging Data Protection Framework. *Journal of Cybersecurity*, 8(1), p. 14.

[11] Creemers, R. (2021) China's Emerging Data Protection Framework. *Journal of Cybersecurity*, 8(1), p. 14; Zhao, B., Feng, Y. (2021) Mapping the development of China's data protection law: Major actors, core values, and shifting power relations. *Computer Law & Security Review*, 40, p. 11.

[12] Feng, Y. (2019) The future of China's personal data protection law: challenges and prospects. *Asia Pacific Law Review*, 27 (1), p. 64.; Zhao, B. (2021) Connected Cars in China: Technology, Data Protection and Regulatory Responses. In: Alexander Roßnagel, Gerrit Hornung (eds.). *Grundrechtsschutz im Smart Car. DuD-Fachbeiträge*. Wiesbaden: Springer Vieweg, p. 21.; Liu, J. (2020) China's data localization. *Chinese Journal of Communication*, 13 (1), p. 91.; Trakman, L., Walters, R., Zeller, B. (2020) Digital consent and data protection law – Europe and Asia-Pacific experience. *Information & Communications Technology Law*, 29 (2), p. 233.; Creemers, R. (2021) China's Emerging Data Protection Framework. *Journal of Cybersecurity*, 8(1), p. 14; Zhao, B., Feng, Y. Mapping the development of China's data protection law: Major actors, core values, and shifting power relations. *Computer Law & Security Review*, 40, pp. 6; 12.; You, C. (2022) Half a loaf is better than none: The new data protection regime for China's platform economy. *Computer Law & Security Review*, 45, p. 16.

[13] The Cybersecurity Law, the Personal Information Protection Law, supplemented by the provisions of the Chinese Civil Code and the Data Security Law, hereinafter referred to as the Chinese data protection law.

[14] Schantz, P. (2023) Article 44 GDPR. In: Spiecker gen. Döhmann et al. (eds.). *General Data Protection Regulation: Article-by-Article Commentary*. Nomos, p. 777; Kuner, C. (2020) Article 44 GDPR. In: Christopher Kuner et al. (eds.). *The EU General Data Protection Regulation (GDPR). A commentary*. Oxford University Press, p. 757.

[15] By virtue of Article 44, the GDPR only allows personal data to be transferred to a third country which has demonstrated it provides for an acceptable level of data protection. If there is an adequate level of data protection, then under Article 45 GDPR, the European Commission is entitled to issue an adequacy decision. In that case personal data can be transferred to a third country without limitations. If not, there should be no transfer of personal date to that country, unless the data controller implements appropriate safeguards of Article 46 GDPR or relies on one of derogation of Article 49 GDPR.

concept of adequacy, as set out in the GDPR[16]. Reflecting the EU's attitude towards personal data transfers outside the EU, the adequacy standard sets a benchmark for assessments of similarities or differences between EU and third countries' laws.[17] In a nutshell, the adequacy standard requires the third-country data protection law to offer a level of data protection equivalent to that arising from EU law, particularly from the GDPR[18]. As further explained by the Court of Justice of the European Union in Schrems I and Schrems II cases, the third-country's legal system must be essentially equivalent, which means there is no need for the third-country legal system to be the same as that of the EU. Nevertheless, a third country must provide data subjects with fundamental rights that are enforceable and must organise the data processing activities in line with the data protection principles under the supervision of an independent data protection authority.[19]

In this paper, I discuss the level of data protection stemming from the Chinese data protection law. The paper presents partial result of my research project on Chinese data protection law.[20] While conducting research, I answered the following research question: does Chinese data protection law meets the criteria derived from the adequacy concept? The analysis proved that Chinese data protection law[21] does not meet the adequacy criteria, and as a result, falls short compared to the GDPR and EU law. Due to the limited volume of this paper, which makes it impossible to present an in-depth description of the results, I decided to focus on three main disparities of Chinese data protection law from the EU law model namely:

---

[16] Schantz, P. (2023) Article 44 GDPR. In: Spiecker gen. Döhmann et al. (eds.). *General Data Protection Regulation: Article-by-Article Commentary*. Nomos, p. 777-778; Kuner, C. (2020) Article 45 GDPR. In: Christopher Kuner et al. (eds.). *The EU General Data Protection Regulation (GDPR). A commentary*. Oxford University Press, p. 775.

[17] Thoughts on the expected level of data protection in a third country are presented, among others, by Schwartz P.M. (1995) European Data Protection Law and Restrictions on International Data Flows. *Iowa Law Review,* 80(3), p. 471, 473, 487; Blume P. (2015) EU Adequacy Decisions: The Proposed New Possibilities. *International Data Privacy Law*, 5(1), p. 34; also: Gulczyńska Z. (2021) A certain standard of protection for international transfers of personal data under the GDPR. *International Data Privacy Law*, 11(4), p.34.

[18] Schantz, P. (2023) Article 45 GDPR. In: Spiecker gen. Döhmann et al. (eds.). *General Data Protection Regulation: Article-by-Article Commentary*. Nomos, p. 789-790.

[19] Judgement of 6 October 2015 *Maximillian Schrems v Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650, hereinafter referred to as Schrems I; Judgement of 16 July 2020 *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems*, C-311/18, ECLI:EU:C:2020:559, hereinafter referred to as Schrems II.

[20] Devoted to the problem of data transfers between China and European Union

[21] The Cybersecurity Law, the Personal Information Protection Law, supplemented by the provisions of the Chinese Civil Code and the Data Security Law, hereinafter referred to as the Chinese data protection law.

- the complicated structure of personal data protection law landscape,
- the doubtful application of data controller definition to state bodies,
- the lack of a dedicated data protection authority in China.

Nevertheless, there are also other problems, in particular the interpretative concerns related to the rights of data subjects granted by the Cybersecurity Law, the Civil Code, the Data Security Law and the Personal Information Protection Law, or the data protection principles they mention[22]. In addition, the overall level of personal data protection in China is also affected by the widely cited cases of surveillance of individuals by state authorities and the associated access to personal data by state authorities[23].

The paper consists of four parts. In the first part, I briefly describe the methodology of the assessment of the Chinese data protection law. The second, third and fourth parts discuss in detail the drawbacks of the Chinese data protection law, to end with concluding remarks.

2. ASSESSING A THIRD COUNTRY'S LEGAL SYSTEM – THE INFLUENCE OF THE GDPR'S ADEQUACY STANDARD ON THE ASSESSMENT OF THE CHINESE DATA PROTECTION LAW

I analysed the Chinese data protection law with the following criteria:

- Criterion of core data principles,
- Criterion of a data subject's enforceable rights,
- Criterion of a competent, independent supervisory authority,
- Criterion of a data subject's remedies in the event of a data breach,
- Criterion of access to data by public authorities in the third country.

[22] See inter alia: Pernot-Leplay, E. (2020) China's Approach on Data Privacy Law: A Third Way between the U.S. and the EU? *Penn State Journal of Law and International Affairs*, 8(1), p. 53-54, 77-78; Wang Han, S. Munir, A.B. (2018) Information Security Technology – Personal Information Security Specification: China's Version of the GDPR? *European Data Protection Law Review*, (4) 4, p. 535.

[23] See inter alia: Shao, Y. (2021) Personal Information Protection: China's Path Choice. *US-China Law Review*, 18(5), p. 236; Pernot-Leplay, E. (2020) China's Approach on Data Privacy Law: A Third Way between the U.S. and the EU? *Penn State Journal of Law and International Affairs*, 8(1), p. 107;

The choice of criteria included in the assessment was based on comprehensive analysis of adequacy concept.[24] Although the adequacy assessment procedure is still not transparent enough[25], the doctrine explained that content of the adequacy assessment arises from four elements[26]:

1) Article 45 of GDPR and with its assessment criteria.

2) The European Data Protection Board guidelines[27].

It is worth emphasising that the guidelines issued by the European Data Protection Board and its predecessor[28] are the only official comment on the adequacy assessment. Consequently, the assessment debate often amounts to mostly a discussion of these guidelines

3) The jurisprudence of Court of Justice of the European Union[29].

Since 2015, the Court of Justice of the European Union has played a significant role in the third-country assessment. For the purpose of this article, it is enough to say that the Schrems I judgement explains the required level of data protection in the third country by introducing the essential equivalence concept. Moreover, it creates an additional criterion for assessing adequacy, namely the access to personal data by third countries' authorities.

[24] More detailed description of this part of my research I present in the following paper: Panek, W (2024) The European Commission's adequacy decisions' content as a guide for applying the adequacy assessment criteria. The paper awaits publication in the Privacy Symposium Proceedings 2024 (Springer).

[25] Kuner, C. (2009) Developing an Adequate Legal Framework for International Data Transfers. In: Serge Gutwirth, et al. (eds.). *Reinventing Data Protection?* Springer Science+Business Media B.V., p. 268.; Makulilo, A. B. (2013) Data Protection Regimes in Africa: too far from the European 'adequacy' standard? *International Data Privacy Law*., 3(1); Kuner, C. (2017) Reality and Illusion in EU Data Transfer Regulation Post Schrems. *German Law Journal*, 18 (4), pp. 900–901. Also, see: Czerniawski, M. (2021) Rola Komitetu Art. 93 RODO w procedurze oceny adekwatności państw trzecich. *Gdańskie Studia Prawnicze*, 25(4), pp. 106-126.

[26] See: Blume, P. (2015) EU Adequacy Decisions: The Proposed New Possibilities. *International Data Privacy Law*, 5(1); Gulczyńska, Z. (2021) A certain standard of protection for international transfers of personal data under the GDPR. *International Data Privacy Law*, 11(4); Kuner, C. (2009) Developing an Adequate Legal Framework for International Data Transfers. In: Serge Gutwirth, et al. (eds.). *Reinventing Data Protection?* Springer Science+Business Media B.V., p. 268.; Makulilo, A. B. (2013) Data Protection Regimes in Africa: too far from the European 'adequacy' standard? *International Data Privacy Law*., 3(1); Kuner, C. (2017) Reality and Illusion in EU Data Transfer Regulation Post Schrems. *German Law Journal*, 18 (4), pp. 900–901.

[27] European Data Protection Board (2017) Adequacy Referential (WP 254 Rev.01, 28 November 2017) hereinafter referred to as a WP254.

[28] Article 29 Working Party (1998) Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive (WP12, 24 July 1998) hereinafter referred to as WP12.

[29] Schrems I and Schrems II.

The Schrems II judgment sustains and confirms both concepts.[30] At the same time, it expands on using the Charter of Fundamental Rights as the assessment criterion.

4) The adequacy decisions issued to date[31].

The analysis of four elements mentioned above allowed me to reconstruct the list of criteria that are crucial when assessing a third country's legal system. When it comes to the content of each criterion, the doctrine and the European Commission is highly influenced by its understanding propose by the EDPB[32]. Consequently, the meaning of core data principles' criteria, data subject's enforceable rights, competent, independent supervisory authority and data subject's remedies in the event of a data breach is derived from EDPB guidelines WP254. For the criterion of data access by public authorities in a third country, the EDPB created
a separate document which in detail explains the meaning of that criterion.[33]

Before commencing the discussion on the subject matter, I would like to draw the reader's attention to another detail. The abovementioned criteria, used for assessing Chinese data protection law, do not address the criterion of human rights protection. Surprising as it might be, this attitude reflects the vague nature of adopting human rights criterion, which is part and parcel of all the adequacy decisions issued so far.[34] Under Article 45 GDPR, the European Commission is obliged to verify human rights protection and respect for rules of law in the examined third country.[35] However, in practice, none of the adequacy decisions referred to these criteria in their content.[36] The same might be said about the European Data Protection Board

[30] However, Bradford et. al. claim that Schrems II judgement has made the adequacy much stricter – see Bradford L., Aboy M., Liddell K. (2021) Standard Contractual Clauses for Cross-Border Transfers of Health Data after Schrems II. *Journal of Law and the Biosciences*, 8 (1), p. 11 - 17

[31] Past decisions are relevant because they show which criteria apply and to what extent.

[32] Stemming from WP254.

[33] European Data Protection Board (2020) Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

[34] Another example is the criterion of international commitments. Within GDPR-based adequacy decisions, only the UK's decision contains the European Commission's affirmation of ratification of the Council of Europe Convention No 108 and mentions the Convention for the Protection of Human Rights and Fundamental Freedoms.

[35] Kuner, C. (2021) The Path to Recognition of Data Protection in India: The Role of the GDPR and International Standards. *National Law Review of India*, 33(1), p. 80; Wittershagen, L. (2023) Transfer of Personal Data to Third Countries under the European Data Protection Law. In: Leonie Wittershagen (ed.) *The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit*. De Gruyter, p. 59,

[36] The doctrine has noticed the inconsistent approach of the European Commission when assessing third countries in this respect – see Wolf C. (2013) Delusions of Adequacy -

guidelines, where no reference was made to the criterion of human rights protection.

This attitude might be explained by political background involvement. C. Kuner believes that the adequacy assessment is also related to background political pressure, not only the protection of personal data as such.[37] Bradford explains the political background by referring to trade or cultural relationships, or strategic objectives that stand behind the need for continuous data flow.[38] Therefore, the political background sometimes amounts to the criterion of supporting business relations between the European Union and the examined third country. First and foremost, this is the case in the EU – USA transfers. Graham Greenleaf finds justification for an imperfect adequacy standard arising from the Safe Harbour decision in American economic power and its influence on Europe.[39] Other third countries are in a different position because, as Greenleaf says, 'other countries do not have the economic muscle of the US.'[40] Economic relations are often mentioned during discussions about the adequacy of Israel or Argentina. Some authors say that these countries are adequate as they can be found among the close trading partners of the European Union.[41] For that reason, despite identified shortcomings, they were granted adequacy

Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers. *Washington University Journal of Law & Policy*, 43, p. 240-241.

37 Kuner, C. (2009) Developing an Adequate Legal Framework for International Data Transfers. In: Serge Gutwirth, et al. (eds.). *Reinventing Data Protection?* Springer Science+Business Media B.V., p 267. The problem of considering the political background is also mentioned by: Makulilo, A.B, (2013) Data Protection Regimes…, p. 49; Blume, P. (2000) Transborder Data Flow: Is There a Solution in Sight. *International Journal of Law and Information Technology*, 8(1), p. 69

38 Bradford, L., Aboy, M., Liddell, K. (2021) Standard Contractual Clauses for Cross-Border Transfers of Health Data after Schrems II. *Journal of Law and the Biosciences*, 8 (1), p. 14.

39 Greenleaf, G. (2000) Safe Harbor's low benchmark for 'adequacy': EU sells out privacy for US$. *Privacy Law and Policy Reporter*, 7(3), p. 45.

40 Ibid.

41 Roth P. (2017) Adequate level of data protection' in third countries post-Schrems and under the General Data Protection Regulation. *Journal of Law, Information and Science,* 25(1), p. 49; Blackmore N. (2019) Feeling inadequate? Why adequacy decisions are rare (and may get rarer) in Asia-Pacific. *Kennedys* 26 March, available from: `https://kennedyslaw.com/thought-leadership/article/feeling-inadequate-why-adequacy-decisions-are-rare-and-may-get-rarer-in-asia-pacific/` [accessed 17 October 2022].

decisions[42], while for other countries same shortcomings somehow made it impossible to find those third countries adequate.[43]

Interestingly, the political background discussed above finds support of European Parliament. In its resolutions referring to data transfers to the USA, the European Parliament emphasised the importance of economic relations and their influence on the subject matter.[44]
A similar view can be found in a paper related to data transfers between the European Union and China. Here, economic relations were used as an argument for a less strict, more practical, and realistic attitude to assessing the Chinese legal system.[45]

In my opinion, business relations should have no sway in terms of turning a blind eye to human rights infringements. I agree with Drechsler and Kamara that violations of human rights and a disrespect for the rule of law should disqualify any country from being found adequate within meaning of the GDPR.[46] Therefore, it seems evident that human rights infringement in China are still a major obstacle to the adequacy decision being granted. In next part of this paper, I elaborate on the identified shortcomings of Chinese data protection law. Their existence has a significant influence on the standard of data protection in China. Nevertheless, even the best data

[42] In case of Israel it is said that the assurances of its representatives were considered sufficient guarantees of adequate level of data protection – Tene, O.(2022) Data transfer theatre: The US and Israel take the stage. *Privacy Perspectives*, 4 October, available from: https://iapp.org/news/a/data-transfer-theater-the-us-and-israel-take-the-stage/ [accessed 17 October 2022]; similar view expressed by Yablonko, Y. (2020) Israel's outdated privacy laws jeopardize relations with EU. *Globes*, 23 July, available from: https://en.globes.co.il/en/article-israels-outdated-privacy-laws-jeopardize-relations-with-eu-1001337077 [accessed 17 October 2022].

[43] As in the case of Burkina Faso – see Wolf C. (2013) Delusions of Adequacy - Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers. *Washington University Journal of Law & Policy*, 43, p. 240-241.

[44] Resolution of European Parliament (2016) Transatlantic data flows. Official Journal (C 76/82) 26 May. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A52016IP0233; the European Parliament refers to one of the communications of the European Commission - European Commission Communication (2013) Rebuilding Trust in EU-US Data Flows. COM 846 final, 23 November. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013DC0846.

[45] de Hert, P. Papakonstantinou, V. (2015) The data protection regime in China. In-depth analysis. European Union, p. 8. Available from: https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA\%282015\%29536472_EN.pdf.

[46] Drechsler, L., Kamara, I. (2022) Essential equivalence as a benchmark for international data transfers after Schrems II. In: Eleni Kosta, Ronald Leenes, Irene Kamara (eds.). *Research Handbook on EU Data Protection Law*. Edward Elgar Publishing, p. 235.

protection legislation means nothing in a legal system where human rights are violated[47].

3. WHICH LAW APPLIES? THE COMPLICATED STRUCTURE OF THE CHINESE DATA PROTECTION LAW SYSTEM

Chinese data protection legislation is composed of many different laws and regulations. That was the most discussed feature of Chinese law before the enactment of the Cybersecurity Law, where data-protection-related provisions were scattered among various laws, such as criminal law or consumer protection law, with no regulation of the general scope and application[48]. The reform was supposed to change this, as a specific complete data protection law was highly desired.

Initially, it was the Cybersecurity Law to be described as an example of general and comprehensive data protection law.[49] Nevertheless, some of the authors explained that personal data protection within the Cybersecurity Law was only an additional element and the legislation refers primary to cybersecurity in China.[50] Also, the Cybersecurity Law does not cover the processing of analogue personal data.[51] Hence, when the Personal Information Protection Law came into force, the doctrine changed its views

[47] It also must be noted that before the Cybersecurity Law came into force, the main obstacle to recognising Chinese legal system as adequate within the meaning of EU data protection law was the numerous problems with the state's approach to protecting human rights. However, the adoption and subsequent implementation of the Cybersecurity Law, Civil Code, Data Security Law, and Personal Information Protection Law caused the discussion on the adequacy of Chinese law within the meaning of the GDPR to no longer be limited to broadly understood issues of protecting fundamental rights. What matters now is also the quality of the provisions introduced by these laws, as these provisions should implement effective data-protection-oriented solutions that will meet the adequacy criteria referred to above.

[48] Gao, R. Y. (2020) Personal Information Protection under Chinese Civil Code: A Newly Established Private Right in the Digital Era. *Tsinghua China Law Review*, 13(1), p. 183; Duoye, X. (2020) The Civil Code and the Private Law Protection of Personal Information. *Tsinghua China Law Review*, 13(1), p. 188.

[49] Qi, A., Shao, G., Zheng, W. (2018) Assessing China's Cybersecurity Law. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 34(6), p. 7; Yuexin, Z. (2019) Cyber Protection of Personal Information in a Multi-Layered System. *Tsinghua China Law Review*, 12(1), p. 167,169.; Shao, Y. (2021) Personal Information Protection: China's Path Choice. *US-China Law Review*, 18 (5), p. 239; Tiwari, A. (2022) The Comparison between Indian Personnel and PRC New Civil Code, Cyber Laws, and Privacy. *Jus Corpus Law Journal*, 3, p. 367, 368, 377.

[50] Vecellio Segate, R. (2020) Litigating Trade Secrets in China: An Imminent Pivot to Cybersecurity? *Journal of Intellectual Property Law & Practice*, 15(8), p. 649, 650

[51] Wang Han S., Munir A.B. (2018) Information Security Technology – Personal Information Security Specification: China's Version of the GDPR? *European Data Protection Law Review*, (4) 4, p. 53.

and started to see the latter as general and comprehensive data protection law.[52]

At the same time, the role of the Data Security Law started to clarify.[53] According to Article 3 Data Security Law, the data protected by the law amounts to any information recorded, notwithstanding its form[54]. Although it covers a much broader scope of data[55] for some authors, it became evident that the Personal Information Protection Law refers to the processing of personal data, while the Data Security Law deals with the rest.[56] Thus, the link between the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law became clearer.[57]

However, one should also remember those provisions of the Chinese Civil Code that touch upon the issue of data protection. These include Articles 111 and 1034 - 1039. According to Zhou, the Civil Code, the Personal Information Protection Law and the Data Security Law present a comprehensive view of personal data protection in China.[58] This is because it is through the provisions of the Civil Code the principles of personal data protection, discussed only partially in the Cybersecurity Law, along with specific definitions given there, became universally applicable law.[59]

---

[52] Yan Wang, C. (2022) Governing Data Markets in China: From Competition Litigation and Government Regulation to Legislative Ordering. *George Mason International Law Journal*. 13(1), p. 39.

[53] Dorwart, H. (2021) Platform regulation from the bottom up: Judicial redress in the United States and China. *Policy & Internet*, 14(2), p. 377.

[54] That is because motives of cyberspace sovereignty and the protection of national security stand behind the Data Security Law.

[55] Personal data are not excluded from the definition of data.

[56] Cai, P., Chen, L. (2022) Demystifying data law in China: a unified regime of tomorrow. *International Data Privacy Law*, 12(2), p. 78. Interestingly, for relations between the Data Security Law and the Cybersecurity Law, it was the national security protection to be the explanation - Guangping, W. (2021) Challenges and Responses to the Protection of Workers' Personal Information in the Context of Human-Computer Interaction. *China Legal Science*, 9(139), p. 146; Cai, P., Chen, L. (2022) Demystifying data law in China: a unified regime of tomorrow. *International Data Privacy Law*, 12(2), p. 90.

[57] Chaskes, W. (2022) The Three Laws: The Chinese Communist Party Throws down the Data Regulation Gauntlet. *Washington and Lee Law Review*, 79(3), p. 1173.

[58] Zhou, Q. (2023) Whose data is it anyway? An empirical analysis of online contracting for personal information in China. *Asia Pacific Law Review*, 31 (1), p. 74.

[59] Berti, R. (2020) Data Protection Law: A Comparison of the Latest Legal Developments in China and European Union. *European Journal of Privacy Law & Technologies*, 1, p. 51..; Gao, R. Y. (2020) Personal Information Protection under Chinese Civil Code: A Newly Established Private Right in the Digital Era. *Tsinghua China Law Review*, 13(1), p. 174.; Duoye, X. (2020) The Civil Code and the Private Law Protection of Personal Information. *Tsinghua China Law Review*, 13(1), p. 188; Guangping W (2021) Challenges and Responses to the Protection of Workers' Personal Information in the Context of Human-Computer Interaction. *China Legal Science*, 9(139),, pp. 141–142.; Shao, Y. (2021) Personal Information Protection: China's Path Choice. *US-China Law Review*, 18 (5), p. 239.

The concise description of the various data protection laws in China, presented above, suggests that the reform's principal effect was to further complicate an already perplexing legal system.[60] Although the legislator established the applicability of the Cybersecurity Law, the Civil Code, the Data Security Law and the Personal Information Protection Law in addition to the existing provisions, it is in vain to find provisions in any of these laws clarifying the scope of their application. What is lacking is the lawmaker's clearly expressed intention regarding the scope of application of Chinese data protection laws[61]. As Greenleaf points out, the Personal Information Protection Law – the most advanced personal data protection law – does not by itself repeal the previously binding provisions related to the same issues, which means, among other things, the duplication of obligations or slightly different wording of the same obligations.[62] For other authors the Cybersecurity Law the Data Security Law and the Personal Information Protection Law have similar background[63]. Because of that, all three laws should apply to every personal data processing activity within Chinese jurisdiction, whilst only factual analysis of the case might lead to exclusion of one of them[64]. Such an interpretation means that under the threat of sanctions provided by the Cybersecurity Law, Data Security Law, and Personal Information Protection Law it is data subject or controller to decide which law they should abide, by accurately construe their current situation[65]. In such a situation, it is common to have doubts about the leading role of one of these laws, the existing catalogue of data protection principles that absolutely must be implemented and complied with, or the interplay between the different principles under the various laws.

---

[60] The expected streamlining and unification of legal data protection in China has yet to arrive.

[61] General and ambiguous provisions of data protection laws are not helpful too.

[62] Greenleaf, G. (2020) China issues a comprehensive draft data privacy law. *Privacy Laws & Business International Report*, 1, p. 12.

[63] Belli L., Doneda D. (2023) Data protection in the BRICS countries: legal interoperability through innovative practices and convergence. *International Data Privacy Law*, 13 (1), p. 82, 86, 87

[64] Cai P., Chen L. (2022) Demystifying data law in China: a unified regime of tomorrow. *International Data Privacy Law*, 12(2), p. 78-79; also: Greenleaf G. (2020) China issues a comprehensive draft data privacy law. *Privacy Laws & Business International Report*, 1, p. 12; Dorwart H. (2021) Platform Regulation from the Bottom up: Judicial Redress in the United States and China. *Policy & Internet*, 14(2), p. 379; Chaskes W. (2022) The Three Laws: The Chinese Communist Party Throws down the Data Regulation Gauntlet. *Washington and Lee Law Review*, 79(3), p. 1173; Xing H. (2023) Government Data Sharing and Personal Information Protection. *Administrative Law Research*, 2, p. 72; Zhou Q. (2023) Whose data is it anyway? An empirical analysis of online contracting for personal information in China. *Asia Pacific Law Review*, 31 (1), p. 74.

[65] While the interpretation of Chinese law will pose less of a challenge for local market players, the position of foreign players is far worse.

In conclusion, the coexistence of the Cybersecurity Law, Civil Code, Data Security Law, and Personal Information Protection Law means that the Chinese personal data protection is too complicated for the average recipient to understand. Theoretically, this is not such a severe defect as one might expect but in practice the complexity of China's personal data protection regulations results in a lack of transparency regarding the protection this system should provide. In other words, the individual, i.e. the entity whose rights and freedoms are to be protected, is not entirely sure where the protection they can invoke comes from. As a result, especially on daily basis, an individual may face a refusal to comply with a request under Law X because, according to the data controller, it is actually Law Y that covers this case, and Law Y does not include the right that the individual is invoking. Therefore, it is dubious to discuss the effective protection of personal data expected by the EU adequacy standard.

4. THE SCOPE OF CONTROLLER DEFINITION - IS A STATE BODY A DATA CONTROLLER?

From the perspective of the GDPR, state authorities that determine purposes and means of data processing are data controllers. This interpretation is not in doubt. However, based on China's data protection laws, no such statement is apparent.

The Personal Information Protection Law is the only law that contains a definition of data controller. As in the GDPR, what makes an entity a data controller within the Chinese definition is determining the means and purposes of personal data processing. The doctrine has no clear position regarding the possibility of considering a state authority as a data controller. Some authors automatically limit themselves to purely theoretical considerations when discussing the concept of the state authority as a data controller.[66] The justification for this approach is supposed to be a pragmatic approach to the surrounding reality[67] – a reality in which it is highly questionable to consider a state authority as a data controller. The reason why the state authorities would not fall within the definition of controller are consequences. As Bethany Allen-Ebrahimian once said, "Privacy, in the

[66] Ibid.; Dorwart, H. (2021) Platform regulation from…, p. 379; Chaskes. W. (2022) The Three Laws: The Chinese Communist Party Throws down the Data Regulation Gauntlet. *Washington and Lee Law Review*, 79(3), p. 1173.; Xing, H. (2023) Government data sharing and personal information protection. *Administrative Law* Research, 2.; Zhou, Q. (2023) Whose data is it anyway? An empirical analysis of online contracting for personal information in China. *Asia Pacific Law Review*, 31 (1), p. 74.

[67] Duoye, X. (2020) The Civil Code and the Private Law Protection of Personal Information. *Tsinghua China Law Review*, 13(1), p. 191.; Cai P., Chen L. (2022) Demystifying data law in China: a unified regime of tomorrow. *International Data Privacy Law*, 12(2), p. 92.

Chinese government's eyes, means privacy from other non-state actors — not privacy from the government."[68] A positive answer and application would imply a complete change in the approach to processing personal data by state bodies, which then should act in accordance with the law and thus comply with the obligations addressed to controllers. This is not what Chinese authorities need. More broadly, their status is necessary and convenient for the state authorities to still be able to carry out their surveillance activities.[69] In particular, such an approach allows the powers of the state authorities to access personal data to remain unhindered.[70]

The above considerations confirm that the approach to data protection amounts to another manifestation of the peculiar Chinese nature. State organs are de facto excluded from the qualification as data controllers[71]. As a result, changes to the legislation were made while the status quo of state bodies was maintained.[72] It is a glaring example of the incompleteness of Chinese law, whether intended or not. The consequences of promoting and accepting such an approach hit the data subject first. It leads to a situation where the same processing activities undertaken by a state authority and a private sector entity entail different obligations and remarkably different restrictions, if any at all. Also, doubts regarding the qualification of any entity processing personal data as a data controller mean that the data subject does not know what is happening with their data. That is a severe problem because, the data controller is another leading actor in the processing of personal data. Specific obligations are imposed on the controller, who should

[68] Allen-Ebrahimian, B. (2022) China makes genetic data a national resource. *Axios*. 29 May. Available from https://www.axios.com/2022/03/29/china-makes-genetics-data-national-resource [accessed 30 November 2023].

[69] Greenleaf, G. (2020) China issues a comprehensive draft data privacy law. *Privacy Laws & Business International Report*, 1, p. 12.

[70] Gold, A. (2021) China's new privacy law leaves U.S. behind. *Axios*. 23 November. Available from: https://www.axios.com/2021/11/23/china-privacy-law-leaves-us-behind [accessed 30 March 2023].

[71] Creemers, R. (2021) China's Emerging Data Protection Framework. *Journal of Cybersecurity*, 8(1), p. 19.; Chen, Y-J., Lin C-F., Liu H-W. (2018) "Rule of Trust": The Power and Perils of China's Social Credit Megaproject. *Columbia Journal of Asian Law*, 32(1), p. 27; Duan, Y. (2019) Balancing the Free Flow of Information and Personal Data Protection. 3 April. Available from: https://ssrn.com/abstract=3484713 [accessed 26 April 2023], p. 11–12; Yu L., Ahl B. (2021) China's Evolving Data Protection Law and the Financial Credit Information System: Court Practice and Suggestions for Legislative Reform. *Journal Hong Kong Law Journal*, 51(1), p. 292

[72] Gold, A. (2021) China's new privacy law leaves U.S. behind. *Axios*. 23 November. Available from: https://www.axios.com/2021/11/23/china-privacy-law-leaves-us-behind [accessed 30 March 2023]; Yang, Z. (2022) The Chinese surveillance state proves that the idea of privacy is more "malleable" than you'd expect. *MIT Technology Review*. 10 October. Available from: https://www.technologyreview.com/2022/10/10/1060982/china-pandemic-cameras-surveillance-state-book/[accessed 28 March 2023].

handle the data appropriately. Moreover, the data controller is the addressee of the data subject's requests or complaints. Thus, if an entity that processes personal data, having defined the purposes and means of their processing, may not be considered
a controller, then such a legal system provides at least illusory protection of personal data. Therefore, the lack of clarity regarding the qualifications of state authorities as data controllers significantly reduce the level of personal data protection resulting from the entirety of Chinese law.

5. (NO) DATA AUTHORITY IN CHINA

As already mentioned, for EU law, the theoretical protection of personal data is less relevant than its actual level. Thus, a vital element of any third country's data protection regime should be adequate compliance supervision carried out by a supervisory authority. The provisions of the GDPR indicate that it is not about any public authority. It should be a body equipped with appropriate powers and resources. Moreover, the independence of such a body in performing the tasks entrusted to it must be guaranteed. However, it is difficult to say that such a supervisory authority has been established by Chinese law.

The Cybersecurity Law, Data Security Law, and Personal Information Protection Law devote some provisions to the supervision carried out by the supervisory authority. However, they operate with highly general terms, making identifying the entity considered a supervisory authority challenging.[73] The implication of the construction adopted is that there is a multi-stakeholder supervisory authority in China.[74] In other words, the functions of the supervisory authority are performed by various authorities. Consequently, there is no single, dedicated, specialised data protection authority. Instead, there are several public authorities in China. Among the tasks carried out by these authorities is the supervision of personal data protection, although this is not their primary task.[75] Such bodies include the Cyberspace Administration of China, the People's Bank of China, the

[73] Creemers, R. (2021) China's Emerging Data Protection Framework. *Journal of Cybersecurity*, 8(1), p. 14.

[74] Dorwart, H. (2021) Platform regulation from the bottom up: Judicial redress in the United States and China. *Policy & Internet*, 14(2), p. 383.; Liu, Y. et al. (2022) Privacy in AI and the IoT: The privacy concerns of smart speaker users and the Personal Information Protection Law in China. *Telecommunications Policy*, 46(7), p. 6–7.; Yin, Y. (2023) Conflict and Balance Between Private Information Protection and Public Interests Against the Background of Normalization of Epidemic Prevention and Control. *Hebei Law Science*, 3.

[75] You, C. (2022) Half a loaf is better than none: The new data protection regime for China's platform economy. *Computer Law & Security Review*, 45,,p. 22.

Ministry of Industry and Information, Technology and the Ministry of Public Security.[76]

The Cyberspace Administration of China is mostly identified as the data protection authority in China. This comes from the fact that a significant part of the powers or duties are addressed precisely to the entity identified as the Cyberspace Administration of China.[77] Nevertheless, this does not alter the fact that its jurisdiction is much broader, as it concerns network security issues.[78] Furthermore, doubts about recognising the Cyberspace Administration of China as a GDPR-compliant supervisory authority in China are compounded by its position towards other state authorities. The existing relationship prevents the Cyberspace Administration of China from being granted the characteristic of independence. It is pointed out that data protection-related institutions in China are closely linked to the state apparatus, including the political one.[79] As Creemers and You explain, despite the separation of the Cyberspace Administration of China from the State Council, it is still not clear that the Cyberspace Administration of China is an independent body.[80] Hence, multi-agency supervision would not be a problem as long as we could attribute the feature of independence[81] to each of these authorities. Independence guarantees that the authority will perform the tasks imposed on it freely, supervising all the other entities. Moreover, its actions will be based on objective criteria, detached from political preferences or suggestions from other authorities.

The most vivid example of politically driven action by the Cyberspace Administration of China is the case of DiDI Chuxing Technology. Under the cover of data-protection-related control, the Cyberspace Administration of

[76] Greenleaf, G., Livingston, S. (2016) China's New Cybersecurity Law – Also a Data Privacy Law? *Privacy Laws & Business International Report*, 144, p. 8.; Creemers, R. (2021) China's Emerging Data Protection Framework. *Journal of Cybersecurity*, 8(1), p. 10.; Chaskes, W. (2022) The Three Laws: The Chinese Communist Party Throws down the Data Regulation Gauntlet. *Washington and Lee Law Review*, 79(3), p. 1175.; Wang, C. et al. (2022 Privacy Protection in Using Artificial Intelligence for Healthcare: Chinese Regulation in Comparative Perspective. *Healthcare*, 10(10), p. 4.; You, C. (2022) Half a loaf is better than none: The new data protection regime for China's platform economy. *Computer Law & Security Review*, 45, p. 21.

[77] Creemers. R. (2021) China's Emerging Data Protection Framework. *Journal of Cybersecurity*, 8(1), p. 14.

[78] Dorwart, H. (2021) Platform regulation from the bottom up: Judicial redress in the United States and China. *Policy & Internet*, 14(2), p. 383–384.

[79] Pyo, G. (2021) An Alternate Vision: China's Cybersecurity Law and Its Implementation in the Chinese Courts. *Columbia Journal of Transnational Law*, 60(1), p. 236.

[80] You, C. (2022) Half a loaf is better than none: The new data protection regime for China's platform economy. *Computer Law & Security Review*, 45, p. 21.; Creemers, R. (2021) China's Emerging Data Protection Framework. *Journal of Cybersecurity*, 8(1), p. 14.

[81] Mentioned in the GDPR and indicated by the adequacy standard.

China pursued the state's goal of stopping DiDi's preparation of an initial public offering on the New York Stock Exchange against the state's will.[82]

Therefore, since one cannot speak of the independence of the state authorities to which the Cybersecurity Law, Data Security Law and Personal Information Protection Law address specific obligations, no competent supervisory authority can be said to exist in China. The systemic position of the supervisory authority in China raises the issue of the powers granted to the authority. The provisions of the Personal Information Protection Law (and, at times, the Cybersecurity Law, and the Data Security Law) do not deviate significantly from the catalogue of powers referred to in Articles 57 and 58 of the GDPR. Unfortunately, even the most advanced powers lose their meaning when it is unclear who would exercise them and when.

6. CONCLUDING REMARKS

hina's reformed data protection legislation has attracted the attention of many commentators. Without a doubt, the changes introduced can be described as advanced, considering the state of legislation before the Cybersecurity Law entered into force. However, there is no cause for excessive optimism, as has been proven by the three features of Chinese data protection law.

When it comes to the complicated structure of Chinese data protection legislation, the effect of the reform is to fundamentally deepen its existing fragmentation. The doctrine is unconvinced on how to treat the Cybersecurity Law, Data Security Law and Personal Information Protection Law. Some authors claim these laws are regulations of cyberspace and its safety, rather than personal data protection.[83] At the same time, others see the Personal Information Protection Law in particular as being a GDPR-like law or containing some GDPR-derived similarities.[84] Evidently,

[82] See among others: DigiChina (2022) Chinese Authorities Announce $1.2B Fine in DiDi Case, Describe 'Despicable' Data Abuses. *DigiChina*, 21 July. Available from https://digichina.stanford.edu/work/translation-chinese-authorities-announce-2b-fine-in-didi-case-describe-despicable-data-abuses/ [accessed 14. 11. 2023]; Dou, E., Wu, P.-L. (2022) China fines Didi $1.2 billion for breaking data-security laws. *The Washington Post*, 21 July. Available from: https://www.washingtonpost.com/world/2022/07/21/china-didi-fine-data-security/; Huld, A. (2022) How Did Didi Run Afoul of China's Cybersecurity Regulators? Understanding the US$1.2 Billion Fine. *China Briefing*, 2 August. Available from: https://www.china-briefing.com/news/didi-cyber-security-review-which-laws-did-didi-break/

[83] Liu, Y. et al. (2022) Privacy in AI and the IoT: The privacy concerns of smart speaker users and the Personal Information Protection Law in China. *Telecommunications Policy*, 46(7),, p. 12.; You, C. (2022) Half a loaf is better than none: The new data protection regime for China's platform economy. *Computer Law & Security Review*, 45, p. 24.

[84] Zheng, W. (2020) Comparative Study on the Legal Regulation of a Cross-Border Flow of Personal Data and Its Inspiration to China. *Frontiers of Law in China*, 15(3), p. 7; Pyo, G.

the Cybersecurity Law, the Civil Code, the Data Security Law, and the Personal Information Protection Law have been added to the sectoral regulations.

Such an unclear structure of Chinese data protection law weakens the protection it provides. The main consequence is that neither the data subject, nor the data controller or data processor are in a certain position. The data controller and the data processor will not find out whether they have applied the data protection legislation properly until one of authorities decides to check their activity. The same is true for data subjects, but here the convoluted relations within Chinese data protection law also becomes an opportunity to refuse the data subject's request by claiming it is based on the wrong law.

Another reason for finding the Chinese data protection law to be problematic is the status of state bodies. This is primarily influenced by the fact that the scope of the provisions of data protection law can easily be contested when it comes to state bodies. Moreover, even acknowledging with absolute certainty that the provisions in question apply and the state body is a data controller, this does not mean that the expected interpretation will prevail. As long as there is a state authority on the other side, the data subject should not count on being in the same situation as if a private sector entity had processed their data.

Lastly, there is also no dedicated data protection authority in China. It cannot be said that there is any competent supervisory authority in China, bearing in mind the standard of supervision set out in the GDPR. Instead, there are several bodies for which data protection is just an additional task. The functional shape of data protection supervision does not improve the situation, and nor did politically driven supervisory actions carry out recently.

With all this in mind, and even without considering the aspects of human rights protection in China that also affect personal data protection, as mentioned above,[85] I fall firmly into the part of the doctrine that considers the protection of personal data provided by Chinese law, including the Cybersecurity Law, the Civil Code, the Data Security Law, and the Personal

(2021) An Alternate Vision: China's Cybersecurity Law and Its Implementation in the Chinese Courts. *Columbia Journal of Transnational Law*, 60(1), p. 232; Calzada, I. (2022) Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL). *Smart Cities*, 5(3), p. 1130, 1140.; You. C (2022) Half a loaf is better than none: The new data protection regime for China's platform economy. *Computer Law & Security Review*, 45, p. 12.; Xixin, W. (2022) The Bundle of Personal Information Rights from the Perspective of State Protection. *Social Sciences in China*, 43(2), p. 47–48.

[85] Of course, bearing in mind the fact that a profound obstacle for China to be found adequate under the GDPR is its attitude towards human rights protection.

Information Protection Law, to be a long way short of the standard of adequacy under the GDPR.

LIST OF REFERENCES

[1] Allen-Ebrahimian, B. (2022) China makes genetic data a national resource. Axios. 29 May. Available from https://www.axios.com/2022/03/29/china-makes-genetics-data-national-resource [accessed 30 November 2023].

[2] Article 29 Working Party (1998) Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive (WP12, 24 July 1998),

[3] Belli L., Doneda D. (2023) Data protection in the BRICS countries: legal interoperability through innovative practices and convergence. International Data Privacy Law, 13 (1).

[4] Berti, R. (2020) Data Protection Law: A Comparison of the Latest Legal Developments in China and European Union. European Journal of Privacy Law & Technologies, 1.

[5] Blackmore N. (2019) Feeling inadequate? Why adequacy decisions are rare (and may get rarer) in Asia-Pacific. Kennedys 26 March, Available from: https://kennedyslaw.com/thought-leadership/article/feeling-inadequate-why-adequacy-decisions-are-rare-and-may-get-rarer-in-asia-pacific/[accessed 17 October 2022].

[6] Blume P. (2015) EU Adequacy Decisions: The Proposed New Possibilities. International Data Privacy Law, 5(1).

[7] Blume, P. (2000) Transborder Data Flow: Is There a Solution in Sight. International Journal of Law and Information Technology, 8(1).

[8] Bradford L., Aboy M., Liddell K. (2021) Standard Contractual Clauses for Cross-Border Transfers of Health Data after Schrems II. Journal of Law and the Biosciences, 8 (1).

[9] Cai P., Chen L. (2022) Demystifying data law in China: a unified regime of tomorrow. International Data Privacy Law, 12(2).

[10] Chen, J. Sun, J. (2021) Understanding the Chinese Data Security Law. International Cybersecurity Law Review, 2.

[11] Cai, P., Chen, L. (2022) Demystifying data law in China: a unified regime of tomorrow.

[12] International Data Privacy Law, 12(2).

[13] Calzada, I. (2022) Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL). Smart Cities, 5(3).

[14] Chaskes W. (2022) The Three Laws: The Chinese Communist Party Throws down the Data Regulation Gauntlet. Washington and Lee Law Review, 79(3).

[15] Chen, Y-J., Lin C-F., Liu H-W. (2018) "Rule of Trust": The Power and Perils of China's Social Credit Megaproject. Columbia Journal of Asian Law, 32(1).

[16] Creemers, R. (2021) China's Emerging Data Protection Framework. Journal of Cybersecurity, 8(1).

[17] Zhao, B., Feng, Y. (2021) Mapping the development of China's data protection law: Major actors, core values, and shifting power relations. Computer Law & Security Review, 40.

[18] Czerniawski, M. (2021) Rola Komitetu Art. 93 RODO w procedurze oceny adekwatności państw trzecich. Gdańskie Studia Prawnicze, 25(4).

[19] de Hert, P. Papakonstantinou, V. (2015) The data protection regime in China. In-depth analysis. European Union, Available from: https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA%282015%29536472_EN.pdf

[20] DigiChina (2022) Chinese Authorities Announce $1.2B Fine in DiDi Case, Describe 'Despicable' Data Abuses. DigiChina, 21 July. Available from https://digichina.stanford.edu/work/translation-chinese-authorities-announce-2b-fine-in-didi-case-describe-despicable-data-abuses/ [accessed 14. 11. 2023].

[21] Dorwart H. (2021) Platform Regulation from the Bottom up: Judicial Redress in the United States and China. Policy & Internet, 14(2).

[22] Dou, E., Wu, P.-L. (2022) China fines Didi $1.2 billion for breaking data-security laws. The Washington Post, 21 July. Available from: https://www.washingtonpost.com/world/2022/07/21/china-didi-fine-data-security/

[23] Drechsler, L., Kamara, I. (2022) Essential equivalence as a benchmark for international data transfers after Schrems II. In: Eleni Kosta, Ronald Leenes, Irene Kamara (eds.). Research Handbook on EU Data Protection Law. Edward Elgar Publishing.

[24] Duan, Y. (2019) Balancing the Free Flow of Information and Personal Data Protection. 3 April. Available from: https://ssrn.com/abstract=3484713 [accessed 26 April 2023].

[25] Duoye, X. (2020) The Civil Code and the Private Law Protection of Personal Information. Tsinghua China Law Review, 13(1).

[26] European Commission Communication (2013) Rebuilding Trust in EU-US Data Flows. COM 846 final, 23 November. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013DC0846.

[27] European Data Protection Board (2017) Adequacy Referential (WP 254 Rev.01, 28 November 2017).

[28] European Data Protection Board (2020) Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

[29] Feng, Y. (2019) The future of China's personal data protection law: challenges and prospects. Asia Pacific Law Review, 27 (1).

[30] Gao, R. Y. (2020) Personal Information Protection under Chinese Civil Code: A Newly Established Private Right in the Digital Era. Tsinghua China Law Review, 13(1).

[31] Gold, A. (2021) China's new privacy law leaves U.S. behind. Axios. 23 November. Available from: https://www.axios.com/2021/11/23/china-privacy-law-leaves-us-behind [accessed 30 March 2023].

[32] Greenleaf G. (2020) China issues a comprehensive draft data privacy law. Privacy Laws & Business International Report, 1.

[33] Greenleaf, G., Livingston, S. (2016) China's New Cybersecurity Law – Also a Data Privacy Law? Privacy Laws & Business International Report, 144.

[34] Guangping W. (2021) Challenges and Responses to the Protection of Workers' Personal Information in the Context of Human-Computer Interaction. China Legal Science, 9(139).

[35] Gulczyńska Z. (2021) A certain standard of protection for international transfers of personal data under the GDPR. International Data Privacy Law, 11(4). , A. (2022) How Did Didi Run Afoul of China's Cybersecurity Regulators? Understanding the US$1.2 Billion Fine. China Briefing, 2 August. Available from: https://www.china-briefing.com/news/didi-cyber-security-review-which-laws-did-didi-break/

[36] Judgement of 16 July 2020 Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559.

[37] Judgement of 6 October 2015 Maximillian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650.

[38] Kuner, C. (2009) Developing an Adequate Legal Framework for International Data Transfers. In: Serge Gutwirth, et al. (eds.). Reinventing Data Protection? Springer Science+Business Media B.V.

[39] Kuner, C. (2017) Reality and Illusion in EU Data Transfer Regulation Post Schrems. German Law Journal, 18 (4).

[40] Kuner, C. (2020) Article 44 GDPR. In: Christopher Kuner et al. (eds.). The EU General Data Protection Regulation (GDPR). A commentary. Oxford University Press.

[41] Kuner, C. (2020) Article 45 GDPR. In: Christopher Kuner et al. (eds.). The EU General Data Protection Regulation (GDPR). A commentary. Oxford University Press.

[42] Kuner, C. (2021) The Path to Recognition of Data Protection in India: The Role of the GDPR and International Standards. National Law Review of India, 33(1).

[43] Liu, J. (2020) China's data localization. Chinese Journal of Communication, 13 (1).

[44] Liu, Y. et al. (2022) Privacy in AI and the IoT: The privacy concerns of smart speaker users and the Personal Information Protection Law in China. Telecommunications Policy, 46(7).

[45] Makulilo, A. B. (2013) Data Protection Regimes in Africa: too far from the European 'adequacy' standard? International Data Privacy Law., 3(1).

[46] Panek, W (2024): The European Commission's adequacy decisions' content as a guide for applying the adequacy assessment criteria. The paper awaits publication in the Privacy Symposium Proceedings 2024 (Springer).

[47] Pernot-Leplay, E. (2020) China's Approach on Data Privacy Law: A Third Way between the U.S. and the EU? Penn State Journal of Law and International Affairs, 8(1).

[48] Pyo, G. (2021) An Alternate Vision: China's Cybersecurity Law and Its Implementation in the Chinese Courts. Columbia Journal of Transnational Law, 60(1).

[49] Qi, A., Shao, G., Zheng, W. (2018) Assessing China's Cybersecurity Law. Computer Law & Security Review: The International Journal of Technology Law and Practice, 34(6).

[50] Resolution of European Parliament (2016) Transatlantic data flows. Official Journal (C 76/82) 26 May. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016IP0233;

[51] Roth P. (2017) Adequate level of data protection' in third countries post-Schrems and under the General Data Protection Regulation. Journal of Law, Information and Science, 25(1).

[52] Schantz, P. (2023) Article 44 GDPR. In: Spiecker gen. Döhmann et al. (eds.). General Data Protection Regulation: Article-by-Article Commentary. Nomos.

[53] Schwartz P.M. (1995) European Data Protection Law and Restrictions on International Data Flows. Iowa Law Review, 80(3).

[54] Shao, Y. (2021) Personal Information Protection: China's Path Choice. US-China Law Review, 18 (5).

[55] Tene, O.(2022) Data transfer theatre: The US and Israel take the stage. Privacy Perspectives, 4 October, available from: https://iapp.org/news/a/

data-transfer-theater-the-us-and-israel-take-the-stage/ [accessed 17 October 2022].

[56] Tiwari, A. (2022) The Comparison between Indian Personnel and PRC New Civil Code, Cyber Laws, and Privacy. Jus Corpus Law Journal, 3.

[57] Trakman, L., Walters, R., Zeller, B. (2020) Digital consent and data protection law – Europe and Asia-Pacific experience. Information & Communications Technology Law, 29 (2).

[58] Vecellio Segate, R. (2020) Litigating Trade Secrets in China: An Imminent Pivot to Cybersecurity? Journal of Intellectual Property Law & Practice, 15(8).

[59] Wang Han S., Munir A.B. (2018) Information Security Technology – Personal Information Security Specification: China's Version of the GDPR? European Data Protection Law Review, (4) 4.

[60] Wang, C. et al. (2022) Privacy Protection in Using Artificial Intelligence for Healthcare: Chinese Regulation in Comparative Perspective. Healthcare, 10(10).

[61] Wittershagen, L. (2023) Transfer of Personal Data to Third Countries under the European Data Protection Law. In: Leonie Wittershagen (ed.) The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit. De Gruyter.

[62] Wolf C. (2013) Delusions of Adequacy - Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers. Washington University Journal of Law & Policy, 43.

[63] Xing H. (2023) Government Data Sharing and Personal Information Protection. Administrative Law Research, 2.

[64] Zhou Q. (2023) Whose data is it anyway? An empirical analysis of online contracting for personal information in China. Asia Pacific Law Review, 31 (1).

[65] Xixin, W. (2022) The Bundle of Personal Information Rights from the Perspective of State Protection. Social Sciences in China, 43(2).

[66] Yablonko, Y. (2020) Israel's outdated privacy laws jeopardize relations with EU. Globes, 23 July, available from: https://en.globes.co.il/en/article-israels-outdated-privacy-laws-jeopardize-relations-with-eu-1001337077 [accessed 17 October 2022].

[67] Yan Wang, C. (2022) Governing Data Markets in China: From Competition Litigation and Government Regulation to Legislative Ordering. George Mason International Law Journal. 13(1).

[68] Yang, Z. (2022) The Chinese surveillance state proves that the idea of privacy is more "malleable" than you'd expect. MIT Technology Review. 10 October. Available from: https://www.technologyreview.com/2022/

10/10/1060982/china-pandemic-cameras-surveillance-state-book/[accessed 28 March 2023].

[69] Yin, Y. (2023) Conflict and Balance Between Private Information Protection and Public Interests Against the Background of Normalization of Epidemic Prevention and Control. Hebei Law Science, 3.

[70] You, C. (2022) Half a loaf is better than none: The new data protection regime for China's platform economy. Computer Law & Security Review, 45.

[71] Yu L., Ahl B. (2021) China's Evolving Data Protection Law and the Financial Credit Information System: Court Practice and Suggestions for Legislative Reform. Journal Hong Kong Law Journal, 51(1).

[72] Yuexin, Z. (2019) Cyber Protection of Personal Information in a Multi-Layered System. Tsinghua China Law Review, 12(1).

[73] Zhao, B. (2021) Connected Cars in China: Technology, Data Protection and Regulatory Responses. In: Alexander Roßnagel, Gerrit Hornung (eds.). Grundrechtsschutz im Smart Car. DuD-Fachbeiträge. Wiesbaden: Springer Vieweg.

[74] Zhao, B., Feng, Y. Mapping the development of China's data protection law: Major actors, core values, and shifting power relations. Computer Law & Security Review, 40.

[75] Zheng, G. (2021) Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S. and China. Computer Law & Security Review, 43.

[76] Zheng, W. (2020) Comparative Study on the Legal Regulation of a Cross-Border Flow of Personal Data and Its Inspiration to China. Frontiers of Law in China, 15(3).

[77] Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [Personal Information Protection Law of the People's Republic of China] (issued by the Standing Committee of the National People's Congress on 20 August 2021, came into force on 1 November 2021, bilingual version accessed via PKU Law database).

[78] Zhonghua Renmin Gongheguo Minfa Dian (中华人民共和国民法典) [Civil Code of of the People's Republic of China] (issued by the National People's Congress on 28 May 2020, came into force on 1 January 2021, bilingual version accessed via PKU Law database)

[79] Zhonghua Renmin Gongheguo shuju Anquan Fa (中华人民共和国数据安全法) [Data Security Law of the People's Republic of China] (issued by the Standing Committee of the National People's Congress on 10 June 2021, came into force on 1 September 2021, bilingual version accessed via PKU Law database).

[80] Zhonghua Renmin Gonghegup Wanglup Anquan Fa (中华人民共和国网络安全法) [Cybersecurity Law of the People's Republic of China] (issued by the Standing Committee of the National People's Congress on 11 July 2016, came into force on 1 June 2017, bilingual version accessed via PKU Law database).

[81] Zhou, Q. (2023) Whose data is it anyway? An empirical analysis of online contracting for personal information in China. Asia Pacific Law Review, 31 (1).

DOI 10.5817/MUJLT2024-2-2

OF HACKERS AND PRIVATEERS: THE POSSIBLE EVOLUTION OF THE PROBLEM OF CYBER-ATTRIBUTION *

by

JAKUB VOSTOUPAL † KATEŘINA UHLÍŘOVÁ ‡

The escalating severity of the cyber-attribution problem (a problem with attributing cyberattacks to states that ordered them) poses a significant challenge to international law and cyberspace security. However, amidst worsening international relations, a viable solution remains elusive. To address this predicament, the authors turn to a historical echo of the contemporary practice of employing hacker groups – namely, privateering. After an in-depth examination of this analogy's suitability, they focus mainly on the factors that contributed to the decline of privateering. Their goal is to uncover parallels potentially applicable to mitigating modern challenges posed by state-sponsored cyberattacks and the exploitation of cyber-attribution problem. Among the key identified factors, the most crucial were the emergence of professional cyber-capacities (akin to post-Napoleonic emergence of professional navies) and the disruption of hackers' safe havens. The paper concludes by introducing three prospective scenarios reflecting potential pathways for the future of the cyber-attribution challenges.

KEY WORDS

Cybersecurity, Cyber-attacks, Cyber-attribution, Hacker Groups, Non-state Actor, Privateers

* This article was supported by ERDF project "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

† Jakub Vostoupal is a researcher at Institute of Law and Technology at the Faculty of Law, Masaryk University. For correspondence: jakub.vostoupal@law.muni.cz

‡ Kateřina Uhlířová is an assistant professor at the Department of International and European Law at the Faculty of Law, Masaryk University. For correspondence: Katerina.Uhlirova@law.muni.cz

1. INTRODUCTION

The creation of cyberspace and the almost absolute integration of information and communication technologies into our lives marked the beginning of a new era. It provided us with tools to boost the effectiveness of many processes, whether waste disposal, nuclear programs, or healthcare, and therefore, it became an essential part of the worldwide community. However, as a former US President Obama aptly pointed out in the 2010 USA National Security Strategy, "*the very technologies that empower us to lead also empower those who would disrupt and destroy.*"[1]

At first, many states underestimated the perils posed by cyber threats, often attributing them to risks confined primarily to individuals and private companies.[2] However, the cyberattacks on the Estonian government in 2007 debunked this myth and demonstrated that certain types of cyber-attacks can also pose a substantial security threat to states.[3] Moreover, the asymmetric nature of cyberspace does not keep this danger just between the states but also allows non-state actors, primarily hacker groups, to mount successful attacks against otherwise much stronger targets (states).[4] The Colonial Pipeline ransomware attack in 2021 serves as a striking example, highlighting the potential for such entities to disrupt critical infrastructure with relatively minimal skills and resources.[5]

The fact that these attacks pose more than just an opportunity for an academic debate is reflected in both the official positions of states (e.g., the official mandate of the Czech Security and Information Service[6] or of

---

[1] Obama, B. (2010) *US National Security Strategy*. The White House, Washington, p. 27. https://obamawhitehouse.archives.gov/sites/default/files/rss\viewer/national\security\strategy.pdf

[2] Banks, W. (2021) Cyber Attribution and State Responsibility. *International Law Studies* 1039(97), pp. 1040–1041.; Kolouch, J., Zahradnický, T., Kučínský, A. (2021) Cyber Security: Lessons Learned From Cyber-Attacks on Hospitals in the COVID-19 Pandemic. *Masaryk University Journal of Law and Technology* 15(2), pp. 303–309.

[3] Pamment, J. et al. (2019) *Hybrid Threats: 2007 Cyber Attacks on Estonia*. NATO Strategic Communications Centre of Excellence, pp. 66–68. https://stratcomcoe.org/cuploads/pfiles/cyber\attacks\estonia.pdf

[4] Boebert, W. E. (2010) A Survey of Challenges in Attribution. In: *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, D.C.: The National Academies Press, pp. 42–43. http://www.nap.edu/catalog/12997.html

[5] Turton, W., Riley, M., Jacobs, J. (2021) Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom. *Bloomberg.com*. https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom; Kolouch, J. et al. Cybersecurity: Notorious, but Often Misused and Confused Terms. (2023) *Masaryk University Journal of Law and Technology* 17(2), pp. 282–285.

[6] This intelligence service actively participates on investigations of various electronic attacks safeguarding, inter alia, critical infrastructure entities. This involves assessing information related to *"threats and risks associated with the operation of strategic information and communication*

the American Cybersecurity and Infrastructure Security Agency[7]) as well as international organisations. For instance, the North Atlantic Treaty Organization (NATO) has incorporated mitigation of cyber threats into its alliance doctrines as well as into its military strategy.[8] Notably, NATO has actively developed cyber warfare capabilities, formally acknowledging "cyberspace" as a fourth domain of warfare during the 2016 Warsaw Summit.[9]

Similarly, the European Commission has issued a Joint Communication to the European Parliament, the European Council, and the Council, aiming to enhance resilience and strengthen capabilities to counter hybrid threats. The rationale behind this initiative lies in recognising that "*hybrid activities by state and non-state actors continue to pose a serious and acute threat to the EU and its Member States. From cyber-attacks that disrupt economies and public services to targeted disinformation campaigns and aggressive military actions*."[10]

Cyberspace did not just challenge the factual power of states and the stability of international society; it also challenged the rule of international law and its application.[11] Even though it is primarily of a customary nature and thus quite flexible and capable of adaptation, the introduction of cyberspace presented a crucial question of whether the current international law can be applied in this global domain or whether a cyber-specific regulation is needed.[12] The *UN Group of Governmental Experts* (UN GGE) concluded in their 2013 report that no substantial reason would preclude the application of international law in cyberspace – a stance acknowledged

systems, the destruction or disruption of which could have a serious impact on the security or economic interests of the Czech Republic." See BIS. Kybernetická bezpečnost. `https://www.bis.cz/kyberneticka-bezpecnost/`

7 See About CISA [online]. *Cybersecurity & Infrastructure Security Agency*. 2024 [accessed 8.1.2024]. `https://www.cisa.gov/about`

8 NATO Standard, AJP-6, Applied Joint Doctrine for Communication and Information Systems, February 2017 `https://www.coemed.org/files/stanags/01\AJP/AJP-6\EDA\V1\E\2525.pdf`

9 NATO Summit Warsaw 2016, 9 July 2016. `https://www.nato.int/cps/en/natohq/events\132023.htm`

10 Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response JOIN/2016/018 final, 6 April 2016.

11 Schmitt, M., Watts, S. (2015) The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare. *Texas International Law Journal*, 50(2–3), pp. 220–222.; Svantesson, D. et al. (2023) On sovereignty. *Masaryk University Journal of Law and Technology*, 17(1), pp. 34–40.

12 *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/68/98*. UN, 2013. `https://digitallibrary.un.org/record/753055`; Osula, A.-M., Kasper, A. and Kajander, A. (2022) EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology*, 16(1), pp. 94–100.

and endorsed by the General Assembly.[13] However, the ill-received UN GGE report of 2015[14] that sought to restrain the irresponsible use of states' cyber capabilities demonstrated that some states are not yet ready to give up this newfound power nor to clear out the legal uncertainty that currently favours those who exploit it.[15]

This reluctance is particularly evident in the context of one of the key points from the 2013 UN GGE report: "*States must not use proxies to commit internationally wrongful acts*."[16] This refers to the practice of exploiting the inherent anonymity and asymmetricity of cyberspace by using non-state actors to attack and destabilise rivals while at the same time being protected by a plausible deniability from the legal consequences as the link between the non-state actor and a state is very hard to find and prove in cyberspace.[17] In other words, the exploitation of the cyber-attribution problem.[18]

In the context of the law of international responsibility, attribution is one of two constitutive aspects of an international wrongful act and describes a procedure and a set of requirements through which such an act may be linked to a particular state.[19] Identifying the perpetrator then unlocks the possibility of legal repercussions, making attribution a crucial part of the deterrence strategy.[20] Yet, applying the existing rules proved somewhat inefficient in the case of cyberattacks,[21] as the attribution procedure did not account for the

[13] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/68/98*, 2013.

[14] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/150*. UN, 2015. `https://digitallibrary.un.org/record/799853`

[15] Schmitt, Watts. (2015) *The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare*, pp. 220–222.; Spáčil, J. (2022) Plea of Necessity: Legal Key to Protection against Unattributable Cyber Operations. *Masaryk University Journal of Law and Technology*, 16(2), pp. 216–218.

[16] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/68/98*, 2013.

[17] Banks, W. (2021) Cyber Attribution and State Responsibility. *International Law Studies* 1039(97), pp. 1040–1041.

[18] Edwards, B. et al. (2017) Strategic Aspects of Cyberattack, Attribution, and Blame. *Proceedings of the National Academy of Sciences*, 114(11), pp. 2825–2827.

[19] See Article 2 of the Draft Articles on State Responsibility for Internationally Wrongful Acts: Elements of an internationally wrongful act of a State: There is an internationally wrongful act of a State when conduct consisting of an action or omission: (a) is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State.

[20] Baliga, S., Bueno De Mesquita, E., Wolitzky, A. (2020) Deterrence with Imperfect Attribution. *American Political Science Review*, 114(4), pp. 1155–1157.

[21] As of now, there is no universally agreed definition of cyberattack nor its potential consequences. Cyberattacks can range over a wide spectrum, causing less significant damage, but also damage more than comparable to attacks with conventional weapons, including loss of life (e.g., WannaCry, Stuxnet or the instances of the so-called killware). Nevertheless, as Giles and Hartmann point out, the emerging state practice shows, that the extent of the cyber-attack is not really a predeterminant of attribution (supported by the attribution of

specifics of cyberspace.[22] The sources of the problem may be explicitly found in the requirements on forensic capabilities necessary to identify a responsible individual,[23] the unclear legal requirements on the attribution procedure itself,[24] the impact of extra-legal aspects (mainly political and strategic),[25] and the uncertainty linked with the unspecified standard of proof[26] and evidence disclosure[27]. The combination of these factors has prevented several early major cyber-attacks (e.g., Estonia in 2007,[28] Russia-Georgian War in 2008,[29] Stuxnet in 2010/2012[30]) from ever being attributed. Unsurprisingly, some states, such as the Russian Federation, the People's Republic of China or even the United States of America, have quickly utilised the potential presented by the cyber-attribution problem and began recruiting or at least cooperating with hackers and cybercriminal groups to use them as means of projecting power.[31] Some states even offer those actors "*safe harbours*" – leniency from law enforcement and monetary incentives to take on a mission for the benefit of the said state.[32] These cooperations may be kept at some level of secrecy

cyberattacks against Albania in 2022), and therefore the abstract term cyberattack in its wide meaning is sufficient for the purposes of this paper. See Giles, K., Hartmann, K. (2019) 'Silent Battle' Goes Loud: Entering a New Era of State-Avowed Cyber Conflict. In: Minárik, T. et al. (eds.). *11th International Conference on Cyber Conflict: Silent Battle*. Tallinn: NATO CCD COE Publications, p. 26.; Attack (International Humanitarian Law) [online]. *International Cyber Law: Interactive Toolkit*. 28. 7. 2023 [accessed 10. 1. 2024]. `https://cyberlaw.ccdcoe.org/wiki/Attack\(international\humanitarian\law)`

22 Berghel, H. (2017) On the Problem of (Cyber) Attribution. *Computer - IEEE Computer Society*, 50(3), pp. 84–85.

23 Rid, T., Buchanan, B. (2015) Attributing Cyber Attacks. *Journal of Strategic Studies* 38(1–2).

24 Eichensehr, K. E. (2019) The Law and Politics of Cyberattack Attribution. *UCLA Law Review*, 67(3).

25 Egloff, F. J., Smeets, M. (2021) Publicly attributing cyber attacks: a framework. *Journal of Strategic Studies*. 2021.

26 Davis, J. K. (2022) *Tallinn Paper No. 13 - Developing Applicable Standards of Proof for Peacetime Cyber Attribution*. NATO CCD COE Publications.

27 Aravindakshan, S. (2021) Cyberattacks: A Look at Evidentiary Thresholds in International Law. *Indian Journal of International Law*, 59(1–4).

28 Pamment, J. et al. *Hybrid Threats: 2007 Cyber Attacks on Estonia*. NATO Strategic Communications Centre of Excellence, 2019. `https://stratcomcoe.org/cuploads/pfiles/cyber\attacks\estonia.pdf`

29 Connel, M., Vogler, S. (2017) *Russia's Approach to Cyber Warfare*. CNA. `https://www.cna.org/archive/CNA\Files/pdf/dop-2016-u-014231-1rev.pdf`

30 Connect the Dots on State-Sponsored Cyber Incidents – Stuxnet [online]. *Council on Foreign Relations* [accessed 26. 12. 2023]. `https://www.cfr.org/cyber-operations/stuxnet`

31 APTs & Adversary Groups List - Malware & Ransomware [online]. *Crowdstrike Adversary Universe* [accessed 27. 8. 2023]. `https://adversary.crowdstrike.com/en-US/`

32 Harašta, J., Bátrla, M. (2022) 'Releasing the Hounds?' Disruption of the Ransomware Ecosystem Through Offensive Cyber Operations. In: Jančárková, T., Visky, G., Winther, I. (eds.). *14th International Conference on Cyber Conflict: Keep Moving*. Tallinn, Estonia: CCDCOE Publications, pp. 99–100.

to allow for plausible deniability of the state, e.g., Iran has tried to mask its involvement in the cyberattacks against Albania in 2022 in such a way.[33]

And even though there has been a significant progress in the forensic capabilities of states allowing for better identification of the perpetrators[34] and the consequent rise in the number of public cyber-attributions since the WannaCry and NotPetya cyberattacks in 2017, these attributions still refrain from using legal terminology and invoking state responsibility.[35] States are, therefore, willing to attribute politically but not apply current customary attribution rules. This reluctance may suggest a profound lack of confidence in the evidence-gathering procedures or even in the legal attribution process as a whole. Some scholars[36] have already criticized the central aspect of the attribution process for the non-state actors controlled by states, the so-called *effective control test*, as being unrealistically stringent and "unsatisfiable" within the context of cyberspace.[37]

However, the focus should not solely be on whether this test is "unsatisfiable" (and Mačák's claim about this is clearly supported by the data from the EuRepoC' and Council on Foreign Relations' Datasets[38]) but also to explore the underlying reasons for its perceived inadequacy. The *effective control doctrine* was established by the International Court of Justice (ICJ) in the 1986 Nic*aragua v. USA case* and reaffirmed in the 2007 *Bosnian Genocide case*.[39] In both instances, the conflicts were primarily land-based,

[33] Microsoft Threat Intelligence. Microsoft investigates Iranian attacks against the Albanian government [online]. *Microsoft Security Blog*. 8. 9. 2022 [accessed 31. 7. 2023]. https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/

[34] Eichensehr, K. E. (2019) The Law and Politics of Cyberattack Attribution. *UCLA Law Review*, 67(3), pp. 520–598.

[35] Eichensehr, K. E. (2017) Three Questions on the WannaCry Attribution to North Korea [online]. *Just Security*. [accessed 31. 10. 2023]. https://www.justsecurity.org/49889/questions-wannacry-attribution-north-korea/; Roguski, P. (2020) Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace [online]. *Just Security*. [accessed 8. 1. 2024]. https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/

[36] E.g., Mačák, K. (2016) Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law*, 21(3), pp. 420–428.

[37] Roguski, P. (2020) Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace [online]. *Just Security*. [accessed 8. 1. 2024]. https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/

[38] Attribution Tracker [online]. *EuRepoC: European Repository of Cyber Incidents*. 2024 [accessed 18. 5. 2024]. https://eurepoc.eu/attribution-tracker/; Tracking State-Sponsored Cyberattacks Around the World [online]. *Council on Foreign Relations*. 2024 [accessed 7. 2. 2024]. https://www.cfr.org/cyber-operations

[39] *Judgement of the International Court of Justice in the Case concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America) - Merits*. 1986.

an environment where states have historically held significant power.[40] The strictness of the attribution test is therefore understandable in these contexts, as states can exert greater control over non-state actors and forensic evidence can be more readily examined.

We contend that the primary cause of the *effective control doctrine's* ineffectiveness and unsuitability in cyberspace lies in the fundamental differences between land and cyber domains. Specifically, the symmetric nature of land-based conflicts[41] contrasts sharply with the asymmetric nature of cyberspace, and the actors involved in these domains differ significantly. Rather than attempting to apply land-based procedures to cyberspace, we should seek more appropriate analogies—environments where state control is similarly challenged. We propose that the most fitting analogy to cyberspace, one with a sufficient historical legal precedent, is the sea. In this analogy, the practice of states using non-state hacker groups to obscure their involvement in cyberattacks (or to conduct them when the state lacks the necessary capabilities) parallels the historical practice of privateering and the issuance of Letters of Marque in the absence of professional navies.

If this analogy proves to be more suitable, it could offer valuable insights into mitigating the exploitation of cyber-attribution issues by states and predicting the future development of state-sponsored cyberattacks. This is particularly relevant given the current improbability of establishing a cyber-specific treaty or the emergence of a new general customary rule through state practice. Therefore, this article undertakes a thorough examination of this analogy and focuses on the following research questions:

- Are there similarities between the state practices of utilising privateers and non-state hacker groups that would allow drawing inspiration from the historical development as to the evolution of the cyber-attribution problem?
- If so, then based on this analogy, what factors could lead to the resolution or mitigation of the cyber-attribution problem and the exploitative practice of state-sponsored cyberattacks?

`https://www.icj-cij.org/case/70/judgments`; *Judgement of the International Court of Justice in the Case of Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*. 2007. `https://www.icj-cij.org/case/91/judgments`

[40] Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4).

[41] Many states struggle to effectively control cyberspace and the actors within it, whereas these non-state actors find it significantly easier to launch attacks against state interests in the digital realm compared to the physical world.

To offer a comprehensive response, our first step involves thoroughly analysing the compatibility between the historical functioning of the state responsibility and attribution regimes pertinent to privateering practices and the contemporary law of international responsibility. Within both frameworks, we focus on the problems of attributing the acts of non-state actors used by states as proxies. Should our analysis reveal no significant obstacles to employing this analogical comparison, we proceed to explore the parallels between non-state hacker groups and privateers/pirates, specifically focusing on four distinctive areas: the parallels in the subject, the environment, the purpose, and the effect.

Upon confirming that both the legal regimes and relevant subjects are sufficiently similar to warrant working with this analogy and drawing experience from it, we delve into examining key historical milestones of privateering. Our attention is particularly directed towards aspects that contributed to the decline of this once-widely accepted practice that could help us determine the possible future development of the cyber-attribution problem and its exploitation. It is important to add that our focus in this paper does not extend to addressing whether the practice of employing non-state hacker groups should fall under the same legal regime as privateers, as it would diverge from the attribution aspect and delve into a much wider issue, that was already addressed by others.[42]

2. THE RULES OF ATTRIBUTION IN THE ERA OF PRIVATEERS

The law of sovereign responsibility existed for a long time (there are recounts older than 3000 years mentioning these rules from Egypt[43]) and underwent many fundamental changes.[44] In the Roman period (under the *Jus Gentium*), the sovereign responsibility was not unlike the modern due diligence principle – it was constructed as a strict responsibility of the

[42] For more detailed treatise on this matter, see Egloff, F. (2017) Cybersecurity and the Age of Privateering. In: Perkovich, G., Levite, A. E. (eds.). *Understanding Cyber Conflict: Fourteen Analogies*. Washington, DC: Georgetown University Press.; and Still, J. L. (2013) *Resurrecting Letters of Marque and Reprisal to Address Modern Threats*. United States Army War College - Defense Technical Information Center. http://www.dtic.mil/docs/citations/ADA590294

[43] Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4). p. 265.

[44] Crawford, J. (2013) *State Responsibility: The General Part*. Cambridge University Press, chap. 1. https://www.cambridge.org/core/product/identifier/9781139033060/type/book

collective.[45] The perfect example of its functioning can be found in the consequences of "kidnapping" Helen of Sparta, which served as a *casus belli* for the Trojan War, thus making a whole nation responsible for the act of a prince.[46] The state and its subjects in this period were not understood as separate units, which would allow for the non-attribution of some acts (there was no non-state actor) but a single collective.[47] Moreover, the invoked responsibility could have had only a single output – a reason for war (*casus belli*). The *Jus Gentium* strongly affected the medieval period, especially in the tribal environment.[48] Basically, "*had one member of the tribal entity killed or injured a member of another entity, the whole first entity was responsible and subject to retribution.*"[49] The principle of collective responsibility remained for quite a long time and was not softened until the late Middle Ages (15th century),[50] which meant that it also influenced the rising early practice of privateering[51].[52]

The attempts to stabilise international society caused the strict responsibility (which gave many states excuses to wage war) to decline and give way to a more modern approach based on the fault of the sovereign (about the 17th century).[53] Therefore, the responsibility for the acts of the non-state actors and the consequent procedure of attribution became much more relevant. One of the first authors to introduce this approach was Alberico Gentili, who argued that the casus belli exist only "*in instances in which a private individual has done wrong, and his sovereign or nation has failed to atone for his fault.*"[54]

---

[45] Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4), p. 278.

[46] Hayes, A. (1925) Private Claims against Foreign Sovereigns. *Harvard Law Review*, 38(5), p. 606.

[47] Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4), p. 278.

[48] Berman, H. J. (1983) *Law and Revolution: the Formation of the Western Legal Tradition*. Cambridge (Mass.) London: Harvard university press, p. 52.

[49] Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4), p. 280.

[50] Ibid., p. 281.

[51] The definition and delineation of the terms privateer and pirate and presented in Section 4. For the purposes of sections 2 and 3, even the general understanding of those terms will suffice.

[52] Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), pp. 566–567.

[53] Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4), p. 281.

[54] Gentili, A. (1612) *De Iure Belli Libri Tres*. Oxford: The Clarendon Press, p. 104. https://archive.org/details/threebooksonlawo0002ayal/page/n3/mode/2up

This was then further elaborated by one of the most influential authors, thinkers, and philosophers of this period – Hugo Grotius. He completely severed the remaining attachments to the collective responsibility and limited the reach of sovereign responsibility over the non-state actors, as in his view, the primary aspect of international responsibility was fault.[55] As such, acts *ultra vires* were not attributable to the kings, neither were the acts of privateers that "*had seized the property of friends, had abandoned their native land and were wandering at sea without returning even when recalled…*" because the kings "*themselves had not been the cause of the wrongful freebootery and they had not had any share in it…*".[56] By *argumentum a contrario,* the contraction of a privateer (or issuing the *Letter of Marque*[57]) created a bond between the sovereign and the privateer, which made the king responsible for the actions of the privateer as long as he had some degree of power over them.[58]

Grotian take on international responsibility (also in combination with the due diligence principle[59], as in this era, both regimes were somewhat intertwined) is based on two principles: *patientia* and *receptus*.[60] The first term means that "*responsibility ensues if a community or its rulers know of a crime committed by a subject but fail to prevent it if they can and should do so.*"[61] This is one of the reasons why renegade privateers are out of the scope of sovereign responsibility, because if the sovereign "*had also forbidden by laws that friends should be harmed*"[62], he would have taken a stance against the harming act. The *receptus* principle required the king to "*either punish or extradite those who have taken refuge from justice in his realm if he wants to avoid responsibility for their crimes.*"[63] This would be especially grave for rogue privateers, who would lose all safe harbours and risk extradition and execution. If the receptus

[55] Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4), p. 283.

[56] Groot, H. de. (2004) *De Iure Belli ac Pacis*. Whitefish, MT: Kessinger, pp. 433–437.

[57] Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), pp. 55–56.

[58] Compare with Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4), pp. 283–284.

[59] It is important to note that Grotian take on the due diligence principle is based on the link between the sovereign and his subjects, not territory (that is a modern post-Westphalian approach to due diligence). See Ibid., p. 287.

[60] Groot, H. de. (2004) *De Iure Belli ac Pacis*. Whitefish, MT: Kessinger, pp. 433–437.

[61] Ibid., p. 523.

[62] Ibid., p. 526.

[63] Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4), p. 284.

principle was breached, the king would be held responsible for the crimes of individuals.[64]

During the age of absolutism (the age that witnessed the rise of the Golden Age of Piracy and privateering), the position of a sovereign was said to hold absolute power. With the premise of absolute power over his subjects, such a king should be responsible for any transgressions in light of Grotian ideas. However, this was impractical and unrealistic, as no sovereign had complete control over his lands and subjects, and the concept that a king or a state could not be held responsible for the acts of individuals they did not control grew stronger.[65]

The 18th century (the final period of the Golden Age of Piracy) marked the rise of state responsibility and a slight decline in the doctrine of fault.[66] One of the most influential authors of this period was Christian Wolff, who modified the Grotian concept of the due diligence principle to the point where no sovereign should allow any of its subjects to harm or injure other sovereigns or foreigners.[67] If the ruler fails to uphold this duty, he should punish the offender or compel the perpetrator to repair the loss.[68] He also reflected upon the growing distinction between states and non-state actors in terms of sovereign responsibility and laid down the foundations of the modern take on the attributability of the acts done by non-state actors, as he emphasised that "*the acts of a private citizen are not the acts of the nation to which he is subject, since they are not done as by a subject or so far as he is a subject… The situation is different if he acts by order of the ruler of the state, whom he obeys as a superior.*"[69] Therefore, the concept of control became crucial for the attribution, even though it remained largely unspecified.[70]

2.1. THE SOVEREIGN'S RESPONSIBILITY FOR THE PRIVATEERS' ACTIONS – SUMMARY

To conclude this Section, we find it helpful to briefly summarise the key aspects related to the responsibility for actions carried out by non-state actors, specifically privateers. A privateer's commission (usually cemented by granting the Letter of Marque and Reprisal) creates a bond of responsibility between the state and a non-state actor. The privateers then act as an

64 Ibid.
65 *op. cit.*, pp. 286–287.
66 *op. cit.*, p. 288.
67 Wolff, C. (1995) *Jus Gentium Methodo Scientifica Pertractatum*. Buffalo, NY: Hein, § 317. `https://archive.org/details/jusgentiummethod0002wolf`
68 *op. cit.*, § 318.
69 *op. cit.*, § 315.
70 As demonstrated by the practice of utilization of privateers, see Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), pp. 568–571.

extension of the sovereign's power as long as they are loyal and the sovereign has control over them. This control was never entirely clarified by the state practice and thus remained within the limits of an abstract overall control.[71] For instance, a sovereign commissioned a privateer, he could recall the privateer, could unleash him, could name preferred targets, could specify requirements on the conduct of privateers[72], but could not exercise any control over the execution of the privateer's actions on the sea (at best, he could denounce these acts afterwards).[73] Also, should the privateer break the limitations set down by a sovereign, it would not lead to a sovereign responsibility (unless the sovereign has retained control over the privateer and just did not act).[74]

However, the bond between a privateer and a state was not always apparent to an outside observer. In fact, the only times it could be examined was during the sale of his prize (which was usually done in a friendly or at least neutral harbour and thus not entirely helpful for the sake of attribution), when he earned himself a reputation (often interpreted as insufficient), or upon the capture of the said privateer.[75] Typically, a privateer would reveal the Letter of Marque to his adversary only if captured, as it was the only thing distinguishing him from a pirate and thus saving him from quite a gruesome death reserved for pirates (privateers were granted the status of prisoners of war under the law of nations and the consequent protection[76]).[77] In the end, the reputation and the self-interest of privateers themselves allowed for attribution, nothing else.

---

[71] Reminiscing the so-called *overall control* test invoked in the Tadić case by the International Criminal Tribunal for the Former Yugoslavia, see Section 3.1.

[72] In the later times (the turn of the 18th and 19th century), the conduct of privateers was strictly regulated via national laws and under supervision of the national courts. It was also still a highly respected position and the privateer commissions were accepted throughout the world.

[73] Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), pp. 56–58.; Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), pp. 570–571.

[74] Groot, H. de. (2004) *De Iure Belli ac Pacis*. Whitefish, MT: Kessinger, pp. 433–437.

[75] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 6. `https://lthj.qut.edu.au/article/view/1583`; Anderson, J. L. (1995) Piracy and World History: An Economic Perspective on Maritime Predation. *Journal of World History*, 6(2), pp. 178–181.; Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), pp. 570–571.

[76] Even though the extent of the protection differed greatly throughout the history.

[77] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 6. `https://lthj.qut.edu.au/article/view/1583`; Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), p. 56.

Therefore, the main problem with the responsibility for the privateers' actions was of an evidentiary and enforcing nature. While lacking professional navies, it was problematic at best for many countries to hunt the privateers down and seize them (or kill them in battle) to attribute their actions to any sovereign.[78] At the same time, privateers were the only hope for smaller states to project their power against maritime superpowers such as England and Spain.

3. THE CONTEMPORARY RULES OF ATTRIBUTION

After exploring the relevant parts of the historical development of the sovereign responsibility and attribution rules, it is now imperative to compare them with the contemporary set of attribution rules with an accent on the attribution of non-state actors' acts in cyberspace to find whether these regimes are compatible for the analogy to work with, or not.

The modern state is, de facto, only an abstract construct which has no choice but to act through its organs and individuals, whose actions are then attributed to it according to specific rules. While these rules are primarily customary in nature, their system and function are captured in detail in the codification prepared by the UN Commission on International Law – the Draft Articles on State Responsibility for Internationally Wrongful Acts ("Draft Articles" or "ARSIWA").[79] Experts have no consensus on whether the state responsibility is currently strict or subjective in nature.[80] The Draft Articles do lean towards the strict concept, but the historical idea of fault is not entirely abandoned.[81]

The contemporary conception of international responsibility is based upon the commission of an international wrongful act.[82] That consists

[78] Anderson, J. L. Piracy and World History: An Economic Perspective on Maritime Predation. *Journal of World History*. 1995, vol. 6, no. 2, pp. 175–199; pp. 186–188.; Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 6 - 7. https://lthj.qut.edu.au/article/view/1583

[79] Despite the fact that it is only a "Draft", these Articles are widely recognized as binding capture of customary international law, see *Responsibility of States for Internationally Wrongful Acts - Comments and information received from Governments and Report of the Secretary-General (A/71/79)*. General Assembly of the United Nations, 2016. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/112/74/PDF/N1611274.pdf?OpenElement

[80] Haataja, S. (2021) Autonomous Cyber Capabilities and Attribution in the Law of State Responsibility. In: Liivoja, R., Väljataga, A. (eds.). *Autonomous Cyber Capabilities under International Law*. Tallinn, Estonia: NATO CCD COE Publications, pp. 265–266.

[81] *Op. cit.*, pp. 265–266.; Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4), pp. 290–292.

[82] Pellet, A. (2010) The Definition of Responsibility in International Law. In: Crawford, J., Olleson, S., Parlett, K. (eds.). *The Law of International Responsibility*. Oxford: Oxford University Press, p. 9.; *Draft articles on Responsibility of States for Internationally Wrongful Acts*.

of a breach of an international primary rule (sometimes inappropriately called the objective element of the state responsibility) and the attributability (inappropriately called the subjective element).[83] However, due to the problems with the interpretation and application of both of these elements in the cyber-context (e.g., there is no consensus on what primary rules may be breached by cyber means nor on how intense the breach must be[84,85]), some authors[86] propose to use the due diligence principle (which is nowadays, as opposed to the Grotian era, entirely distinguishable from the traditional "direct" attribution) as a mean of bypassing the controversial aspects of state responsibility.[87] This is caused by the fact that the due diligence principle is not a procedure of assigning responsibility to a state but more of a primary rule of international law, which mitigates the attribution problem.[88] This principle obligates states to prevent events (as it is called in Article 23 of ARSIWA) that could cause harm to other subjects or sovereigns.[89] Therefore, it is not necessary to find any linkage between the state and the act as with

International Law Commission – United Nations, 2001, arts. 1–2. https://legal.un.org/ilc/texts/instruments/english/commentaries/9\6\2001.pdf

83 Brigitte, S. (2010) The Elements of An Internationally Wrongful Act. In: Crawford, J. et al. (eds.). *The Law of International Responsibility*. Oxford: Oxford University Press, pp. 200–202.

84 The prevailing view, which is also reflected by the Tallinn Manual 2.0, is the requirement of equivalence of consequences between a cyberattack and a kinetic attack in terms of the use of force. See Schmitt, M., NATO Cooperative Cyber Defence Centre of Excellence (eds.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017, pp. 84–86. https://doi.org/10.1017/9781316822524

85 The controversy over the breach of primary rule of international law in cyberspace is, however, beyond the limits of this article, and for the remainder of this paper, we will consider this aspect to be fulfilled. See Crawford, J. (2013) *State Responsibility: The General Part*. Cambridge University Press, p. 113.https://www.cambridge.org/core/product/identifier/9781139033060/type/book; Schmitt, M., NATO Cooperative Cyber Defence Centre of Excellence (eds.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2017, pp. 84–86.; Schmitt, M. In Defense of Sovereignty in Cyberspace [online]. *Just Security*. 8. 5. 2018 [accessed 28. 6. 2023]. https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/

86 E.g., Chircop, L. (2018) A Due Diligence Standard of Attribution in Cyberspace. *International and Comparative Law Quarterly* 67(3); Jensen, E. T. (2020) Due Diligence in Cyber Activities. In: Krieger, H., Peters, A., Kreuzer, L. (eds.). *Due Diligence in the International Legal Order*. UK: Oxford University Press. https://doi.org/10.1093/oso/9780198869900.003.0015; Liu, I. Y. (2017) *State Responsibility and Cyberattacks: Defining Due Diligence Obligations*. Rochester, NY. https://papers.ssrn.com/abstract=2907662

87 There is also another way and that is the Plea of Necessity. Same as with the Due Diligence Principle, it has yet to reach a sufficient level of state practice, but nevertheless remains an interesting proposal. See more at Spáčil, J. (2022) Plea of Necessity: Legal Key to Protection against Unattributable Cyber Operations. *Masaryk University Journal of Law and Technology*, 16(2).

88 Chircop, L. (2018) A Due Diligence Standard of Attribution in Cyberspace. *International and Comparative Law Quarterly*, 67(3), pp. 645–648.

89 Crawford, J. (2013) *State Responsibility: The General Part*. Cambridge University Press, pp. 226 - 227. https://www.cambridge.org/core/product/identifier/9781139033060/type/book

the attribution procedure; it is only necessary to find that the state failed in its obligation to "*frustrate the occurrence of the event as far as lies within its power*".[90] Because of the missing linkage, it is sometimes called indirect responsibility. Any state may demand fulfilment of this obligation from another if it has knowledge about an act in preparation or execution that could compromise its security and originates from a domain of the said state (for example, IT infrastructure).[91]

However, as the application of this principle in cyberspace currently faces not insignificant problems (the lack of the state practice has been called out by several major cyber-powers, who rejected the applicability of this principle in cyberspace, among others the USA[92] and Israel[93]), we shall mainly focus on the process of attribution.[94]

3.1. THE LINK TO ATTRIBUTE

The Draft articles delineate three fundamental constellations of actors concerning attributability. Initially, the focus is on the conduct of state authorities (Article 4) and individuals or entities exercising state power (Article 5)[95]. Actions undertaken by any state organ, whether representative of state power or local government[96], when performed within their official capacity, are attributable to the respective state.[97] The purview of official capacity is extended by Article 7 of ARSIWA, establishing attributability of State organs' actions even in instances of *ultra vires* acts. The same principle

[90] This is not an absolute responsibility, therefore the failure to prevent an undesired outcome is in itself insufficient to conclude the breach of the state's due diligence. See par. 6 Article 23 ARSIWA Commentary.

[91] Crawford, J. (2013) *State Responsibility: The General Part*. Cambridge University Press, pp. 227–229. https://www.cambridge.org/core/product/identifier/9781139033060/type/book ; Svantesson et al. *On sovereignty*, pp. 40–43.

[92] *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies*. General Assembly of the United Nations, 2021, p. 141. https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf

[93] Schöndorf, R. (2021) Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations. *International Law Studies*, 97(1). https://digital-commons.usnwc.edu/ils/vol97/iss1/21

[94] For a general overview of issues connected with state responsibility, attribution, or the use of force in cyberspace, see e.g. Osula, A.-M., Kasper, A. and Kajander, A. (2022) EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology*, 16(1), pp. 94–100; or Osula, A. M., Svantesson, D., J. B., Vostoupal, J., Uhlířová, K., et al. (2021) *Cybersecurity Law Casebook 2020*. Brno: Masaryk University.

[95] According to the Tallinn Manual, this could be, for example, a private company in charge of cyber-espionage. See Schmitt, M., NATO Cooperative Cyber Defence Centre of Excellence (eds.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2017, pp. 89–90.

[96] To illustrate, it may be an act of the court, the military or the intelligence service.

[97] This has been confirmed several times by the International Court of Justice, e.g., in the judgments of *Salvador Commercial Company* and *Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights*.

applies to individuals and entities vested with State power (see Articles 5 and 7 of ARSIWA). Only when the individual in question pursues purely private interests are the relevant acts not attributable to the State. In the *Bosnian Genocide Judgment*, the International Court of Justice (ICJ) further broadened the concept of state organs and persons exercising state power to encompass entities that, while de jure non-state actors, operate in complete dependence and under the absolute control of the relevant state.[98]

In contrast to actors vested with state power, the actions of non-state actors represent a distinct (second) category. The historical development mentioned above, illustrating a gradual lowering of the standard of state responsibility for the non-state actors' actions, resulted in the contemporary principle whereby the actions of non-state actors are typically not attributable to states.[99]

Between these positions lies a more intricate level involving non-state actors operating in dependence on the state[100], with ex-post recognition and adoption of activities by the state (attribution by adoption) or actions of parastatals in cases of fallen governments or the establishment of new states. Such actions are attributable to the states in question under conditions stipulated in ARSIWA, with Article 8 being particularly pertinent. This article states that "*(t)he conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is, in fact, acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.*"

It is this very article which emerged as the focal point of the attribution problem, particularly concerning the terms "*instructions*", "*direction*", and "*control*".[101] While the Draft Articles explicitly differentiate between these

[98] *Responsibility of States for Internationally Wrongful Acts - Comments and information received from Governments and Report of the Secretary-General (A/71/79)*, 2016.

[99] Crawford, J. (2013) *State Responsibility: The General Part*. Cambridge University Press, p. 113. https://www.cambridge.org/core/product/identifier/9781139033060/type/book

[100] It is important to add, that when considering private individuals, with or without ties to the state, the Tallinn Manual specifically addresses so-called hacktivists or hackers attacking for patriotic reasons (patriotic hackers). Rule 6 of the Tallinn Manual 1.0 appropriately draws upon Article 8 of ARSIWA, demanding evidence that the individuals in question acted on the instructions of the State or that the State directed their conduct. See Schmitt, M., NATO Cooperative Cyber Defence Centre of Excellence (eds.). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge ; New York: Cambridge University Press, 2013, pp. 35–38.

[101] Mačák, K. (2016) Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law*, 21(3), pp. 407–408.; Crawford, J. (2002) *The International Law Commission's Articles on State Responsibility: Introduction, Text, and Commentaries*. Cambridge, U.K. New York: Cambridge University Press, pp. 110–113.

three categories[102], the practical application often blurs the distinction between the concepts of *direction* and *control*.[103] According to Crawford, *instructions* involve a specific scenario where a state authorises, instructs, and mandates a non-state actor to conduct a particular operation as a de facto "*auxiliary*" – for instance, a private company mandated to support ongoing military operations[104].[105] In contrast, *direction* and *control* encompass broader relationships, with the degree of control over a non-state actor's actions determining an act's attributability.

The ICJ addressed (and tried to clarify) the definition of sufficient control for the attribution of an internationally wrongful act in the case of *Military and Paramilitary Activities in and against Nicaragua*.[106] The ICJ established a stringent *test of effective control*, emphasising that mere support for the activities is insufficient.[107] Instead, the state must actively participate in the planning (beginning), execution, and conclusion of the operation, retaining the ability to terminate the operation itself at all times.[108]

The Tallinn Manual 2.0, aligning with the ICJ's *effective control test* from the Nicaragua case, employs this standard to assess the attributability of cyber-attacks committed by private parties.[109] However, the Nicaragua test is rather old (1986) and does not account for the specifics of cyberspace, making it demand a rather high evidentiary standards and an unrealistic link between hackers and a state.[110] The ICJ had a chance to "update" its approach in 2007 during the Bosnian Genocide case, but it reaffirmed *the effective control*

[102] See par. 7, Article 8 *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries - 2001*. International Law Commission – United Nations, 2001. `http://legal.un.org/ilc/texts/instruments/english/commentaries/9\6\2001.pdf`

[103] Crawford, J. (2013) *State Responsibility: The General Part*. Cambridge University Press, p. 145. `https://www.cambridge.org/core/product/identifier/9781139033060/type/book`

[104] See Schmitt, M. (2017) NATO Cooperative Cyber Defence Centre of Excellence (eds.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, pp. 95–96.

[105] Crawford, J. (2002) *The International Law Commission's Articles on State Responsibility: Introduction, Text, and Commentaries*. Cambridge, U.K. New York: Cambridge University Press, p. 110.

[106] *Judgement of the International Court of Justice in the Case concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America) - Merits*, 1986, para. 109.

[107] *Op. cit.*, paras 109–110.

[108] Mačák, K. (2016) Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law*, 21(3), pp. 413.

[109] Schmitt, M. (2017) NATO Cooperative Cyber Defence Centre of Excellence (eds.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, pp. 94–99.

[110] Mačák, K. (2016) Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law*, 21(3), pp. 423–426.

instead[111] and thus gave "*States the opportunity to carry out criminal policies through non-state surrogates without incurring direct responsibility.*"[112]

Except for the unfortunate factual consequences of these judgements, Talmon[113] and Cassese[114] directly criticise the ICJ's research work in examining the state practice (as the ICJ should according to its own rules on the identification of international customary law). Cassese specifically stresses that *"had the Court undertaken a close perusal of such practice, it would have concluded that it indeed supported the 'effective control' test but solely with regard to instances where single private individuals act on behalf of a state, (. . .) international practice uses another test, that of 'overall control', for the attribution to states of acts of organised armed groups acting on behalf of such states."*[115]

The *overall control test*, mentioned by Cassese, was explicitly laid down by the International Criminal Tribunal for the former Yugoslavia in the *Tadić* case.[116] This test is sometimes favoured as a more suitable tool for the digital age. It also better reflects the requirements of control over privateers. Nevertheless, except its rejection by the ICJ,[117] there are also several major impediments to its potential general applicability.[118]

In contrast to the attribution of ultra vires acts of state power permitted by Article 7 of ARSIWA, Article 8 does not extend the same application to non-state actors. Crawford notes that states typically do not assume the risk of non-state actors exceeding their instructions, and such acts then "escape" the reach of attribution.[119] Nevertheless, if the transgression was

[111] *Judgement of the International Court of Justice in the Case of Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, 2007, arts. 391–393.

[112] An exempt of the Dissenting Opinion of Vice-President Al-Khasawneh. See *op. cit.*, p. 217.

[113] Talmon, S. (2015) Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion. *European Journal of International Law*, 26(2).

[114] Cassese, A. (2007) The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia. *European Journal of International Law*. 18(4).

[115] *Op. cit.*, p. 654.

[116] Condorelli, L., Kress, C. (2010) The Rules of Attribution: General Considerations. In: Crawford, J. et al. (eds.). *The Law of International Responsibility*. Oxford: Oxford University Press, pp. 229–231.

[117] The rejection by itself may not be devastating for the possibility of application of overall control test, as article 59 of the Statute of the International Court of Justice states that "*the decision of the Court has no binding force except between the parties and in respect of that particular case*". Nevertheless, it is apparent that the ICJ consider its finding as (at least) argumentatively binding and therefore, it is improbable that it would deviate from its reasoning in those cases.

[118] *Judgement of the International Court of Justice in the Case of Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, 2007, articles 391–393.

[119] Crawford, J. (2002) *The International Law Commission's Articles on State Responsibility: Introduction, Text, and Commentaries*. Cambridge, U.K. New York: Cambridge University Press, p. 110.

not accidental or the state continued to exert *effective control* over the non-state actor, the act in question can be attributed to the state.[120]

3.2. RESPONSIBILITY FOR THE ACTS OF THE NON-STATE HACKER GROUPS

The contemporary law of state responsibility represents a logical endpoint in the historical development outlined in Section 2. The separation of responsibility regimes governing the actions of representatives of state power and those of non-state actors has been completed, and the prevailing principle nowadays asserts that states, in general, are not held responsible for the actions of non-state actors. The specific rules outlined in Article 8 and subsequent provisions of ARSIWA serve as an exemption and, consequently, demand a strict interpretation. However, should a state commission or contract a hacker group for a cyberattack, the extent of control it exercises over it may still give rise to the state's responsibility for this group's actions. Therefore, the rule of control remained a primary indicator of attributability, akin to earlier phases delineated in Subsection 2.1). The significant shift lies in the introduction of *the effective control test* and the clear demarcation of the due diligence principle as the way of "indirect" responsibility, distinct from attribution mechanisms.

The effective control test sets a much more rigorous standard compared to the connection required between a sovereign and a privateer. The requirements of this test (especially on factual control and evidence) are probably completely unrealistic for the purposes of attributing cyberattacks to states, and its reaffirmation by the ICJ in the Bosnian Genocide case has provided states with a means to conceal adversarial activities in cyberspace through proxies. Consequently, the problem of cyber-attribution concerning non-state hacker groups extends beyond issues of evidence and enforcement, as was the case of privateers, but also encompasses a fundamental legal challenge. Coupled with the unspecified standard of proof[121] and uncertain requirements on evidence disclosure, legal attribution of cyberattacks orchestrated by hacker groups cooperating with or controlled by the state becomes nearly impossible.[122]

Therefore, after the comparison of said legal regimes, although there are obvious differences, we find no discrepancies serious and complex enough that they would preclude the analogical comparison between the fates of

[120] *Op. cit.*, p. 113.

[121] Eichensehr, K. E. (2019) The Law and Politics of Cyberattack Attribution. *UCLA Law Review*, 67(3), p. 563

[122] Banks, W. Cyber Attribution and State Responsibility. *International Law Studies*. 2021, vol. 1039, no. 97, pp. 1042–1045.;Eichensehr, K. E. (2019) The Law and Politics of Cyberattack Attribution. *UCLA Law Review*, 67(3), pp. 563–566.

privateers and hackers. On the contrary, the parallels between the extent of control necessary for attribution and the nature of the attribution problem in the case of both subjects support the relevance of this comparison, as well as the already proclaimed unsuitability of comparing the land-based and cyber-based regimes of attribution.

4. OF HACKERS AND PRIVATEERS

Having assessed the suitability of the respective responsibility regimes for the purposes of analogical comparison, we proceed to the examination of factual and legal parallels between the sea and cyberspace. But apart from the analysing the similarities between the domains themselves, it is also necessary to delve into the state practices involving the commissioning of privateers and hacker groups. The primary focus of this comparative analysis therefore revolves around several distinct categories – purpose and effect, environment and subject. This categorisation enables a detailed comparison that extends beyond the legal status of both non-state actors. It incorporates considerations of the factual attributes of their respective environments, the geopolitical context, and the specific needs of states employing these techniques.

Before delving further into the subject, it is essential to clarify the terms privateer and pirate. Both terms refer to private individuals employing predatory tactics, attacking commercial targets with armed vessels upon the seas, and sharing similar aims and methods. Consequently, throughout history, these terms have often been conflated.[123] Nonetheless, the primary distinction lies in the fact that privateering was a process sanctioned by a sovereign, which imposed limitations and rules on the conduct of privateers (such as restricting targets to the ships of an enemy nation), whereas piracy was universally recognised as an international crime, posing a threat to international commerce and generally disapproved by all states (pirates were a force uncontrolled by any sovereign, without bounds or loyalties).[124,125]

[123] Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press, pp. 19–20. http://www.jstor.org/stable/10.2307/j.ctv2nxkpmw

[124] Ibid.

[125] This can be demonstrated in the interpretation of Com. Still, who refers to piracy as: "a *robbery or forcible depredation on the high seas, without lawful authority, done animo furandi, in the spirit and intention of universal hostility.*" See Still, J. L. (2013) *Resurrecting Letters of Marque and Reprisal to Address Modern Threats*. United States Army War College - Defense Technical Information Center, p. 4 http://www.dtic.mil/docs/citations/ADA590294

However, this theoretical distinction was not consistently reflected in practice until the 17th century.[126]

With the development of maritime law, rules against piracy became clearer and more rigorously enforced. Simultaneously, privateering underwent a transformation, initially being formalised as a tool of international relations and ultimately abolished as an outdated form of warfare.[127,128] Consequently, there is no universally accepted and contemporary legal definition of a privateer[129], while the definition of piracy can be found within Article 101 of the United Nations Convention on the Law of the Sea.[130]

4.1. THE PURPOSE AND THE EFFECT

The first category of comparison focuses on the motivations behind the deployment of privateers and hackers. In the case of privateers, this aspect also serves as an additional distinguishing factor between privateers and pirates, as their purpose significantly impacts their legal status. Privateers were typically commissioned during times of war as a form of supportive measures to intensify attrition against enemies and disrupt their economies.[131] The fact that these activities were "*considered a legitimate*

[126] Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press, pp. 19–20. http://www.jstor.org/stable/10.2307/j.ctv2nxkpmw

[127] The Hague Peace Convention VI officially declared armed merchant ships to be in the same category as warships, which ended the special position of privateers.

[128] Ibid.

[129] This means that the practice of privateering has been extinguished, merely transformed (and renamed). The private military companies played a pivotal role in a number of conflicts (e.g., Sierra Leone, Kosovo or Iraq) and are frequently utilized by many states, for instance the USA. See Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), p. 575.

[130] Article 101 reads: Piracy consists of any of the following acts:

> *(a) any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed: (i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft; (ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;*
>
> *(b) any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;*
>
> *(c) any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b).*

[131] Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), pp. 566–567.

form of a war-like activity conducted by non-state actors"[132] notably influenced the treatment of those captured. While a captured pirate would almost certainly face trial and execution, a captured privateer was recognised as a prisoner of war under the law of nations [133](and their bond to the sovereign, therefore, protected them).[134,135] Although the rights of the prisoners of war varied significantly throughout history, their legal status was generally more favourable.[136] This contrast was starkly demonstrated in 1582 when nearly 400 combatants from a French raiding party were executed for failing to provide evidence of commission by the French Crown.[137]

While privateers played a pivotal role during times of war, their significance also extended into peacetime through the issuance of "*Letters of Marque*."[138] These private individuals represented a valuable asset not only due to their cost-effectiveness compared to a professional navy (further elaborated in Subsection 4.2)[139] but also because their deployment "*made possible minor acts of war without breaking the general peace existing between nations*,"[140] partly due to the more complicated evidentiary situation for

[132] Still, J. L. (2013) *Resurrecting Letters of Marque and Reprisal to Address Modern Threats*. United States Army War College - Defense Technical Information Center, p. 4. http://www.dtic.mil/docs/citations/ADA590294

[133] The expression „the law of nations" has historically more meanings. The older meaning can be understood as „the common law of all nations", and thus „goes back to Jewish, Greek, and Roman Law". The notion „ the law regulating the mutual relations between States" is nowadays expressed in the term „International Law", as coined by the English philosopher Jeremy Bentham. In Idelson, V. R., et al. The Law of Nations and the Individual. *Transactions of the Grotius Society*, vol. 30, Problems of Peace and War, Transactions for the Year 1944, Cambridge University Press, 1944, p. 50.

[134] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 6. https://lthj.qut.edu.au/article/view/1583; Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), p. 56.

[135] This is also the reason why privateers were motivated to provide the means of attribution – their commission.

[136] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 6. https://lthj.qut.edu.au/article/view/1583; Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), p. 56.

[137] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 6. https://lthj.qut.edu.au/article/view/1583

[138] Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press, p. 20. http://www.jstor.org/stable/10.2307/j.ctv2nxkpmw

[139] Tabarrok, A. (2007) *The Rise, Fall, and Rise Again of Privateers*, p. 566.

[140] Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press, p. 20 http://www.jstor.org/stable/10.2307/j.ctv2nxkpmw

the purposes of the attribution.[141] Although the term "*Letters of Marque and Reprisal*" is often used interchangeably with privateering, these letters were originally issued only during peacetimes, providing employment for privateers who would otherwise be idle during times of peace.[142]

The primary purpose of privateers during peacetimes is captured in the very name of the legal instrument commissioning their services, as it stems from two traditional laws – marque and reprisal. The law of *Marque* allowed a private individual to cross the border between two sovereigns and their domains, and the law of *Reprisal* gave the right to seek retribution or restitution for perceived harm that would be otherwise unsatisfied.[143] Therefore, by issuing letters combining these two rights, states authorised private individuals "*to take recompense from the citizens of another* (state) *for a legally recognised grievance.*"[144]

Hence, for sovereigns, privateers presented a relatively cost-effective tool, deployable against adversaries during both times of war and peace, offering a means to project sovereign power without overtly violating the general peace. For several states, privateers also represented the sole means of naval warfare, considering professional navies were prohibitively expensive and challenging to monitor for an extended part of history.[145] And while controlling privateers, similar to managing mercenary companies on land, typically posed quite a few challenges, they proved to be a pragmatic choice during the absence of professional navies.

The primary purpose of privateers was to intensify the attrition and disrupt adversarial economies, trade, international relations, and overall power projection. However, it would be a mistake to downplay the economic impact of their deployment, as privateers shared a percentage of their loot with the sovereign and thus often provided states with much-needed income.[146]

---

[141] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 4 - 5. https://lthj.qut.edu.au/article/view/1583

[142] Cooperstein, T. M. (2009) *Letters of Marque and Reprisal: The Constitutional Law and Practice of Privateering*. Rochester, NY, pp. 223–225. https://papers.ssrn.com/abstract=1406677

[143] *Op. cit.*, p. 223.; Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press, p. 20. http://www.jstor.org/stable/10.2307/j.ctv2nxkpmw

[144] Still, J. L. (2013) *Resurrecting Letters of Marque and Reprisal to Address Modern Threats*. United States Army War College - Defense Technical Information Center, p. 5. http://www.dtic.mil/docs/citations/ADA590294

[145] Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), p. 575.

[146] Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press, pp. 21 - 24. http://www.jstor.org/stable/10.2307/

Comparing these historical aspects with the contemporary employment of Advanced Persistent Threat (APT) and other hacker groups reveals striking similarities in their goals and effects. Given the significant understaffing and high costs associated with professional cyber-capacities,[147] hacker groups offer a viable means of projecting power in cyberspace during both times of war[148] and peace[149]. Furthermore, numerous instances of cyberattacks demonstrate their use for asset destruction,[150] economic disruption,[151] destabilisation of countries and international relations,[152] espionage,[153] support for military operations,[154] and general power projection.[155] The WannaCry attack also exemplifies the second face of cyberattacks' economic importance, showcasing how they can generate income for the responsible state.[156]

j.ctv2nxkpmw; Rodger, N. A. M. The Law and Language of Private Naval Warfare. *The Mariner's Mirror*. 2014, vol. 100, no. 1, pp. 11–13.

147 The Urgency of Tackling Europe's Cybersecurity Skills Shortage [online]. *Microsoft: EU Policy Blog*. 23. 3. 2022 [accessed 17. 2. 2023]. https://blogs.microsoft.com/eupolicy/2022/03/23/the-urgency-of-tackling-europes-cybersecurity-skills-shortage/; (ISC)2. *Cybersecurity Workforce Study*. 2022. https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx; Svantesson et al. *On sovereignty*, pp. 52–63.

148 E.g., the cyberattack on Georgian governmental infrastructure during the Russia-Georgian war of 2008. See Connel, M., Vogler, S. (2017) *Russia's Approach to Cyber Warfare*. CNA. https://www.cna.org/archive/CNA\Files/pdf/dop-2016-u-014231-1rev.pdf

149 The majority of other attacks, e.g., Estonian cyberattacks of 2007, Stuxnet, WannaCry or NotPetya.

150 E.g., Stuxnet and NotPetya.

151 E.g., WannaCry and Petya.

152 E.g., the cyberattacks against Estonia in 2007, the cyberattacks against Albania in 2022 or the ransomware campaign against hospitals during COVID-19 pandemics. See e.g., Kolouch, J., Zahradnický, T., Kučínský, A. (2021) Cyber Security: Lessons Learned From Cyber-Attacks on Hospitals in the COVID-19 Pandemic. *Masaryk University Journal of Law and Technology* 15(2).

153 E.g., SolarWinds.

154 The cyberattacks against Georgian governmental infrastructure during the Russia-Georgian war of 2008 and the KASAT hack (hacks against Ukraine in 2022).

155 This aspect is especially apparent in the work of the Equation Group (USA) or in the cyberattacks mounted under the control of the Russian Federation, as these attacks sometimes need to remind their targets of the cyber-capabilities of the aggressor. See e.g., Connel, M., Vogler, S. (2017) *Russia's Approach to Cyber Warfare*. CNA. https://www.cna.org/archive/CNA\Files/pdf/dop-2016-u-014231-1rev.pdf

156 Bossert, T. Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea – The White House [online]. *The White House - Press Briefings*. 19. 12. 2017 [accessed 22. 11. 2023]. https://trumpwhitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/; Bendiek, A., Schulze, M. Attribution: A Major Challenge for EU Cyber Sanctions: An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW. *SWP Research Paper*. 2021, pp. 20–23. https://www.swp-berlin.org/10.18449/2021RP11/; Global Research and Analysis Team of Kaspersky Lab. WannaCry and Lazarus Group – the missing link? [online]. *Kaspersky*

And while hacker groups also pose challenges in terms of control, they stand as the next best alternative in the absence of professional expert capacities. Therefore, it is evident that in the category of purpose and effect, the practices of deploying privateers and hackers are analogous.

4.2. THE ENVIRONMENT – THE RISE TO POWER

In the second subsection, our focus shifts to a comparative analysis of the distinctive characteristics of high seas and cyberspace, elucidating the factors contributing to the ascendancy of both privateers and hackers to power.

In contrast to land, both the high seas and cyberspace present environments that defy easy governance and border demarcation. Non-state actors can relatively easily access both domains (both skill- and resource-wise), which both guarantee a certain degree of anonymity. These aspects hinder the states' monitoring and enforcement capabilities, thus amplifying the demands on effective governance. Consequently, states exert a much weaker presence in these environments, creating opportunities for private individuals and organisations (such as East India Company or Google and Facebook).

These dynamics are aptly illustrated by the factors leading to the zenith of privateering during its golden age in the 18th century (also known as the Golden Age of Piracy). While the importance and respectability of the privateering practice grew throughout history (mainly in the Middle Ages), it was the surge in maritime trade, particularly with the exploration of America and the East Indies, that catapulted privateering to unprecedented heights.[157] The competition among European powers, particularly Spain and England, for dominance in the New World pushed many naval powers to augment their naval capabilities beyond their national arsenals (especially after the defeat of the Spanish Armada in 1588) and lesser powers, that lacked the resources and capabilities to deploy a respectable navy, to employ at least private contractors to extend their power projection and impede the hegemonic progress of colonial powers.[158]

The constant conflicts between naval superpowers during the wars to control East and West Indies presented lucrative opportunities for

- *SecureList*. 15. 5. 2017 [accessed 7. 1. 2024]. https://securelist.com/wannacry-and-lazarus-group-the-missing-link/78431/

[157] Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press, pp. 35–41. http://www.jstor.org/stable/10.2307/j.ctv2nxkpmw

[158] Rodger, N. A. M. The Law and Language of Private Naval Warfare. *The Mariner's Mirror*. 2014, vol. 100, no. 1, pp. 11–13.; Anderson, J. L. (1995) *Piracy and World History: An Economic Perspective on Maritime Predation*, pp. 189–194.

privateers.[159] The abundance of lucrative prizes, coupled with diminishing naval threats (as the navies were either shattered, weary or preoccupied with the conflict), resulted in an influx of privateers so vast that it was impossible to employ all of them even during the peacetimes, which prompted many of them to turn to piracy (e.g., after the end of the Spanish Succession Wars in 1713, there was an evident upsurge in pirate activity in the Caribbean).[160] And despite draconian law enforcement attempts by the English in the 1720s (mass hangings in the Atlantic ports), piracy persisted due to states' inability to sustain such efforts for longer periods of time and target safe havens.[161]

As noted in the previous subsection, a pivotal aspect of the environment fostering privateer activity was the absence of professional forces capable of opposing and bringing them to justice.[162] As Still points out, "*for the better part of human history, the primary method for dealing with maritime pirates and privateers was individual avoidance and self-defence.*"[163] States, unable to effectively address the issue, adopted a laissez-faire approach to maritime trade, and many either paid foreign privateers to spare their ships or employed their own to redirect the problem towards their enemies.[164]

Considering all these factors within the broader geopolitical context, it becomes evident that states played a crucial role in ushering in the golden age for both privateers and pirates through their laissez-faire approach or outright utilisation.[165] As the alternatives and solutions appeared either too costly or in direct contradiction with the strategic goals of a sovereign, most states were somewhat reluctant to refrain from the practice of privateering.[166] And because most of the naval powers used these private individuals to bolster their strength at sea, abolishing this practice would disadvantage any

[159] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 6. https://lthj.qut.edu.au/article/view/1583

[160] Kraska, J. (2011) *Contemporary Maritime Piracy: International Law, Strategy, and Diplomacy at Sea*. Santa Barbara, Calif: Praeger, p. 30.

[161] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 7. https://lthj.qut.edu.au/article/view/1583

[162] Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), pp. 575–576.

[163] Still, J. L. (2013) *Resurrecting Letters of Marque and Reprisal to Address Modern Threats*. United States Army War College - Defense Technical Information Center, p. 3. http://www.dtic.mil/docs/citations/ADA590294

[164] Anderson, J. L. (1995) Piracy and World History: An Economic Perspective on Maritime Predation. *Journal of World History*, 6(2), p. 187.

[165] Cooperstein, T. M. (2009) *Letters of Marque and Reprisal: The Constitutional Law and Practice of Privateering*, pp. 223–224.

[166] Ibid.

state that would do so.[167] Thus, the equation was relatively simple – states tolerated the suffering of their subjects as long as others suffered more.

Therefore, it is evident that the environments of the sea and cyberspace have much in common. The presence of states, their power, and their capacity to monitor and enforce their will within both of these environments was/is much weaker compared to their power over land.[168] Both promise a certain degree of anonymity, they both are problematically divided by borders that would directly limit states' interests (resulting in the direct conflict of those interests), and they are both relatively easy to access for individuals. Both of these also exhibit a certain degree of asymmetry, enabling private individuals to challenge the power of other sovereigns to some extent.[169]

As states recognised their lack of skills and professional capacities even in cyberspace, some collaborated with cybercriminal hacker groups. These partnerships, promising safe haven and preferential treatment from law enforcement, impeded the prosecution of cyber-criminals from specific countries.[170] Consequently, many states, even in cyberspace, adopted a regime of *avoidance* and *self-defence* (meant generally, not in the sense of UN Charter), which severely lowered the threat level faced by hacker groups.[171] Moreover, collaborations with hacker groups, even among permanent UN Security Council members, hinder discussions and the political will to effect meaningful changes and enhance security in cyberspace.[172,173]

---

[167] Rodger, N. A. M. The Law and Language of Private Naval Warfare. *The Mariner's Mirror*. 2014, vol. 100, no. 1, pp. 9–13.

[168] In case of limitations of sovereigns' power within cyberspace, see Polčák, R., Svantesson, D. J. B. (2017) *Information Sovereignty: Data Privacy, Sovereign Powers and the Rule of Law*. Cheltenham: Edward Elgar Publishing.

[169] Spector, P. (2017) In Defense of Sovereignty, in the Wake of Tallinn 2.0. *AJIL Unbound*, 111, pp. 219–222.

[170] Harašta, J., Bátrla, M. (2022) 'Releasing the Hounds?' Disruption of the Ransomware Ecosystem Through Offensive Cyber Operations. pp. 96–99.

[171] This is further worsened by the inefficient sanctions aimed at the individual hackers, that can be easily avoided should the hackers refrain from travelling into extraditing countries. See Goldsmith, J. (2017) The Strange WannaCry Attribution [online]. *Lawfare*. [accessed 21. 11. 2023]. https://www.lawfaremedia.org/article/strange-wannacry-attribution; Eichensehr, K. E. (2017) Three Questions on the WannaCry Attribution to North Korea [online]. *Just Security*. [accessed 31. 10. 2023]. https://www.justsecurity.org/49889/questions-wannacry-attribution-north-korea/

[172] Analogically, see keynote by Johanna Weaver for the CyCon 2022 Conference, accessible here: https://www.youtube.com/watch?v=O8eFiJaNzRU\&list=PLV8RTnZwQxcmajmJOMBlXByxJpzy9qD3c\&index=29

[173] The similarity of both environments may be of analogical significance even at this point, as it is crucial to understand that it was the states who exploited the privateering practices the most, that brought forth the golden age of the privateers and pirates through safe havens, preferential treatments and laissez-faire approach. It is likely that utilising cybercriminal groups may have similar consequences. See Osula, A.-M., Kasper, A. and Kajander, A. (2022)

As previously discussed, both cyberspace and the maritime environment are well-suited for projecting power anonymously and destabilizing rivals without crossing the threshold of war. The nature of the relationship between a state and non-state actors such as hacker groups and privateers, which we will explore in the following subsection, differs qualitatively from that with entities like mercenary companies on land. Unlike mercenaries, these non-state actors do not require extensive support and control to achieve significant levels of damage or power projection; in some cases, merely unleashing them is sufficient. Additionally, the inherent characteristics of these environments (i.e., the relatively limited state presence) further complicate the process of gathering evidence, particularly for states with weaker intelligence capabilities.

The fact that there are states aware of this complexity is aptly illustrated by the varying levels of state involvement in cyberattacks as outlined by Jason Healey in his 2012 article.[174] He categorizes state involvement on a spectrum: "*State-prohibited, State-prohibited-but-inadequate, State-ignored, State-encouraged, State-shaped, State-coordinated, State-ordered, State-rogue-conducted, State-executed and State-integrated.*"[175] For instance, the 2007 cyberattacks against Estonia likely fell between the State-shaped and State-coordinated levels, both of which are insufficient to meet *the effective control test* for legal attribution. It is evident that if states can execute a sufficiently damaging cyberattack with a level of control that does not meet the threshold for legal attribution, they are likely to pursue such tactics. Alternatively, they may integrate private hacker groups into the state apparatus to further complicate attribution.[176] Overall, due to the asymmetric natures of the environments (cyberspace and sea), states find it unnecessary to exert the same level of control and support as in traditional cases, such as the *Nicaragua* case.

EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology*, 16(1).

[174] Healey, J. (2012) *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*. Atlantic Council – Cyber Statecraft Initiative. `https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212\ACUS\NatlResponsibilityCyber.PDF`

[175] Ibid.

[176] The State-integrated level by Healey is specific in this matter as the level of control and support are relatively high but the states involvement is still hidden by the obscurity provided by the integration, because the integration is seldom made on a legal level (e.g., the actor behind the WannaCry attack or APT 28 and 29 were once probably stand-alone hacker groups, but later integrated into the state apparatus, effectively obscuring the level of control the state has over them).

4.3. THE SUBJECT – A PRIVATE INDIVIDUAL WITH MEANS AND MOTIVATION

The final comparative category between hackers and privateers focuses on the subject aspect.

Privateers were typically recruited from among private individuals possessing the requisite resources, such as an armed vessel with a crew, a specific skill set, and a particular motivation driven by the desire for wealth.[177] Typically, they had already established a reputation for themselves, distinguishing them in the eyes of state representatives and proving their value as an asset for the state. This reputation might have been gained through various means, even including harassing the state's subjects, which in turn motivated the state to bribe or employ them against its enemies instead, especially if it lacked the power to bring such an individual to justice.[178]

Privateers were primarily motivated by financial gains[179], often compensated by piece (captured or sunk ships and cargo), ransom from prisoners, and a portion of the loot (with a percentage going to the commissioning sovereign).[180] Nonetheless, the privateering profession, even in the absence of professional navies, was inherently risky and a loyalty to a sovereign offered some crucial benefits, primarily the guaranteed safe havens, which reduced the threat level privateers faced and offered a place to repair and regroup.[181,182] The rise of the pirates and privateers would have been impossible without these bases of operations throughout the Caribbean, Mediterranean or East Indies.[183] These bases of operation also severely

[177] Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press, pp. 19–24, 35–39 and 59–66. http://www.jstor.org/stable/10.2307/j.ctv2nxkpmw

[178] Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), pp. 567–570.

[179] Even though some also pursued this profession from a sense of patriotic duty or a sadistic pleasure.

[180] Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press, pp. 59–66. http://www.jstor.org/stable/10.2307/j.ctv2nxkpmw

[181] The safe havens or harbours were not an exclusive aspect of privateering, pirates also used these bases, nevertheless, privateers' access to the safe harbours of their master were guaranteed. See Cartwright, M. (2021) Pirate Havens in the Golden Age of Piracy [online]. *World History Encyclopedia*. [accessed 14. 1. 2024]. https://www.worldhistory.org/article/1844/pirate-havens-in-the-golden-age-of-piracy/

[182] Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press, pp. 59–66. http://www.jstor.org/stable/10.2307/j.ctv2nxkpmw

[183] Cartwright, M. (2021) Pirate Havens in the Golden Age of Piracy [online]. *World History Encyclopedia*. [accessed 14. 1. 2024]. https://www.worldhistory.org/article/1844/pirate-havens-in-the-golden-age-of-piracy/

diminished the effectiveness of deterrence.[184] From the criminological and psychological point of view, people are deterred from anti-social acts mainly because of the fear of punishment or the high probability of failure.[185] Therefore, the effectiveness of punitive deterrence is primarily influenced by the probability of arrest and conviction and the severity of punishment.[186] Therefore, the combination of a relatively low risk of arrest guaranteed by the existence of safe havens with high monetary gains could not serve as a capable deterrence.[187]

In comparison, hackers are usually also recruited from among the private individuals already organised with like-minded colleagues and typically with a cybercriminal background and reputation, akin to privateers.[188,189] These groups possess the necessary skills, knowledge, and equipment, with their own techniques, tactics, and processes, and while primarily motivated by financial gains, some hackers may also harbour a sense of patriotism or destructive tendencies.[190] States cooperating with such actors may establish specific rules of conduct, promising leniency from law enforcement as long as the hacker groups avoid targeting the citizens of the cooperating states[191] and offering a safe haven against foreign law enforcement and intelligence agencies in exchange for occasional execution of cyberattacks more or less specified by the government or intelligence services.[192]

[184] This aspect is crucial for the factors impacting cyber-deterrence.

[185] Jervis, R. et al. (1989) *Psychology and deterrence*. Baltimore (Ma.) London: The John Hopkins university press, pp. 34–37.

[186] Baliga, S., Bueno De Mesquita, E., Wolitzky, A. (2020) Deterrence with Imperfect Attribution. *American Political Science Review*, 114(4), pp. 1155–1157.

[187] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 8. `https://lthj.qut.edu.au/article/view/1583`

[188] That is apparent with most of the top 20 APT listed by CrowdStrike, see *APTs & Adversary Groups List - Malware & Ransomware*.

[189] The relationship between privateers and pirates is essentially analogous to the one between state-sponsored hacker groups and cybercriminal groups.

[190] Horsley, E. (2020) State-Sponsored Ransomware Through the Lens of Maritime Piracy. *Georgia Journal of International & Comparative Law*, 47(3), pp. 671–673.; Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure [online]. *Cybersecurity and Infrastructure Security Agency*. 9. 5. 2022 [accessed 15. 1. 2024]. `https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a`

[191] Harašta, J., Bátrla, M. (2022) 'Releasing the Hounds?' Disruption of the Ransomware Ecosystem Through Offensive Cyber Operations. In: Jančárková, T., Visky, G., Winther, I. (eds.). *14th International Conference on Cyber Conflict: Keep Moving*. Tallinn, Estonia: CCDCOE Publications, pp. 96–99.

[192] Holt, T. J. et al. (2023) Assessing nation-state-sponsored cyberattacks using aspects of Situational Crime Prevention. *Criminology & Public Policy*, 22(4), pp. 826–828; Osawa, J. (2017) The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem? *Asia-Pacific Review*, 24(2), pp. 114–118.

Both non-state actors typically engage in activities below the threshold of war, aiming to cause harm without disrupting the general peace.[193] However, hackers and privateers differ in an essential aspect – the physical risks of their endeavours. Privateers had to be physically present (ergo, not in the safe haven) during raids, increasing the likelihood of capture or harm (consequently increasing also the motivation of presenting valid commission and thus attributing their activities to a sovereign). In contrast, hackers do not need to compromise their security in such a way. Should they refrain from travelling, they are relatively safe from most targeted sanctions.[194] Yet, most of them still travel, which may present the aggrieved state with the possibility of apprehension, such as in the case of Roman Seleznev, who was apprehended by the USA in Maldives in 2013.[195] Nevertheless, the effectiveness of safe harbours is undeniably higher for hackers (inter alia due to the anonymous and global nature of the internet), complicating attribution more than in the case of privateers.

Based on the analogies found throughout the examined categories, it is reasonable to assume that the practice of utilising hacker groups is sufficiently similar to the practice of commissioning privateers (effectively making the practice of utilising hacker groups "cyber-teering"). Even though we have found differences (such as the extent and effectivity of the safe haven in case of hackers), which may further complicate the evolution of the cyber-attribution problem, analysing factors that contributed to the decline of privateering may offer valuable insights into addressing, mitigating, and potentially resolving the cyber-attribution problem associated with "state-sponsored" hacker groups[196]. Therefore, we now proceed to analyse these factors in the next section, where we also examine their potential relevance for the modern age analogy.

[193] Horsley, E. (2020) State-Sponsored Ransomware Through the Lens of Maritime Piracy. *Georgia Journal of International & Comparative Law* 47(3), pp. 671–673.

[194] Eichensehr, K. E. (2017) Three Questions on the WannaCry Attribution to North Korea [online]. *Just Security*. [accessed 31. 10. 2023]. https://www.justsecurity.org/49889/questions-wannacry-attribution-north-korea/.

[195] Layne, N. (2017) Russian Lawmaker's Son gets 27 Years Prison in U.S. hacking case. *Reuters*. https://www.reuters.com/article/idUSKBN17N2GZ/; Russian Cyber-Criminal Sentenced to 14 Years in Prison for Role in Organized Cybercrime Ring Responsible for $50 Million in Online Identity Theft and $9 Million Bank Fraud Conspiracy [online]. *United States Department of Justice, Office of Public Affairs*. 30. 11. 2017 [accessed 29. 12. 2023]. https://www.justice.gov/opa/pr/russian-cyber-criminal-sentenced-14-years-prison-role-organized-cybercrime-ring-responsible

[196] We use this term to encompass more than just APT groups – there are also groups, who are not as advanced or who cooperate only rarely. Unfortunately, we know of no term that would describe such a subject.

5. HIC SUNT DRACONES

The 19th century marked the decline of the privateering practice, initially apparent in shifting policies around the turn of the century[197] and later, in 1856, also legally, with the enactment of the Paris Declaration Respecting Maritime Law.[198]

It is crucial to emphasise that privateering was a widely employed practice by the end of the Golden Age, and piracy was a necessary and somewhat tolerated complement. The initial crack in this paradigm emerged during the American conflicts with the Barbary States in 1801, coupled with a general weariness and dissatisfaction with paying tributes to these states.[199] This development shattered the idealised view of privateers and exposed the inadequacy of suppressing their activities. Following America's lead, other European powers adopted similar strategies to deal with foreign corsairs and privateers, collectively bringing an end to the dominance of Barbary privateering in the Mediterranean.[200] Additionally, the French colonisation of key strongholds for the Barbary states in the 1830s further contributed to the cessation of the Barbary privateer threat.[201]

Although the American-Barbary conflicts served as a guide for Europe, the transformative shift did not come until the Napoleonic Wars, albeit in an ironic fashion. The conflict's extent and intensity forced most participating powers to equip professional navies, thus lowering the demand for privateers.[202] Furthermore, following the wars, the British Royal Navy found itself with surplus capacity and a newfound role of a naval hegemon. Leveraging their considerable naval strength, the British Royal Navy found, for the first time in history, that it was powerful enough to counter the threat of pirates and foreign privateers and thus enforced the so-called *Pax Britannica*.[203] In this endeavour, the Royal Navy actively participated in global anti-piracy and anti-slavery initiatives to safeguard international

[197] Rubin, A. P. (1988) *The Law of Piracy*. Honolulu.: University Press of the Pacific Hunolulu, p. 216. https://archive.org/details/lawofpiracy63rubi

[198] Stark, F. R. (1987) *The Abolition of Privateering and the Declaration of Paris*. New York: Columbia University.

[199] Kraska, J. (2011) *Contemporary Maritime Piracy: International Law, Strategy, and Diplomacy at Sea*, pp. 25–26.

[200] *Op. cit.*, pp. 26–27.

[201] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 7. https://lthj.qut.edu.au/article/view/1583

[202] Kraska, J. (2011) *Contemporary Maritime Piracy: International Law, Strategy, and Diplomacy at Sea*, p. 31.

[203] Ibid.

trade.[204] Dwan et al. also add that during this era, "*the British treated international law more like guidelines than actual rules, as best demonstrated by their practice in counter piracy operations. Further, this period in which British naval dominance ended piracy is significant because of the way in which it blurred British Imperial Law with international law.*"[205]

The cornerstone of British success lay in strategically targeting and blockading safe pirate anchorages and notorious safe havens, effectively nullifying the primary security feature for both pirates and privateers.[206] Moreover, legal mechanisms supporting privateers' income, such as the rights of ransom and parole, gradually eroded, eventually leading to their outlawing.[207] As governmental capacities strengthened, including heightened capabilities for monitoring the high seas, the privateering system became increasingly perceived as inefficient (and unprofitable for the privateers).[208] It is crucial to emphasise that throughout history, privateering has never been an ideal solution. Due to fiscal constraints, it had served as a makeshift alternative to professional navies, being a cheaper yet more challenging-to-control option that rarely aligned precisely with government objectives.[209] To add insult to injury, in the 19th century, privateers also emerged as direct competitors with states' navies in hiring sailors (and were typically more proficient in that, worsening their relations with professional capacities).[210]

The rise of professional navies, both in strength and professionalism, coupled with their growing animosity toward privateers, increased risks of apprehension and death in the era of *Pax Britannica*, the destruction of safe

[204] Anderson, J. L. (1995) Piracy and World History: An Economic Perspective on Maritime Predation. *Journal of World History*, 6(2), p. 189.; Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 7. https://lthj.qut.edu.au/article/view/1583

[205] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 7 - 8. https://lthj.qut.edu.au/article/view/1583

[206] Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), pp. 572–573;Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2), p. 8. https://lthj.qut.edu.au/article/view/1583

[207] Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), pp. 572–573.

[208] Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), pp. 57–58.

[209] Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), p. 575.; Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), p. 59.

[210] Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), p. 59.

havens, and a decline in potential financial gains[211], collectively rendered the privateer practice obsolete and unprofitable for states and privateers alike.[212] The formal abolition of this practice in 1856 through the Paris Declaration was already more of a declaratory in nature.[213]

6. LESSONS OF THE PAST

As established in Section 4.2, most sovereign powers still lack sufficient capabilities to manage the cybercrime problem entirely.[214] Instead of addressing it directly, certain states, such as the Russian Federation, attempt to exploit the situation by harnessing these individuals against rivals, leveraging their capabilities within cyberspace's weakly monitored and governed environment.[215] However, drawing from the historical example of privateers, this exploitative approach, combined with the laissez-faire approach of many other states, could potentially lead to a golden age of cybercriminals and cyberattacks. Such a scenario can potentially severely destabilise not only cyberspace but also international relations.[216] Moreover, contemporary society is even more dependent on the availability of cyberspace[217] than it was on the high seas and maritime trade.

The utilisation of hacker groups exploits the cyber-attribution problem to detrimentally impact the interests of strategic rivals, causing harm to their assets and crippling economies, all while avoiding a disturbance to general peace. This situation is relatively unlikely to change in the foreseeable future, as although the frequency of attributions is increasing, states hesitate to invoke international responsibility and enforce relevant consequences.[218]

---

[211] Not only because of the abolition of the rights to ransom and parole, but also because of the rising percentage of the loot that was supposed to be sent to the commissioning sovereign. See Kraska. *Contemporary Maritime Piracy: International Law, Strategy, and Diplomacy at Sea*, p. 30.

[212] Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review*, 11(4), pp. 575–576.; Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), pp. 59–60.

[213] Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), pp. 55–56.

[214] For example, the cybersecurity of the public and private sectors in the Czech Republic is far from ideal. It is so because of many reasons, one being the inability of the public sector to draw experts into their fold. However, these problems are beyond the scope of this paper.

[215] *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022.

[216] Spáčil, J. (2022) Plea of Necessity: Legal Key to Protection against Unattributable Cyber Operations. *Masaryk University Journal of Law and Technology*, 16(2), pp. 216–222.; Kolouch et al. *Cybersecurity: Notorious, but Often Misused and Confused Terms*, pp. 291–298.

[217] Evident, e.g., in Kolouch, J., Zahradnický, T., Kučínský, A. (2021) Cyber Security: Lessons Learned From Cyber-Attacks on Hospitals in the COVID-19 Pandemic. *Masaryk University Journal of Law and Technology* 15(2), pp. 305–321.

[218] Roguski, P. (2020) Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace [online]. *Just Security*. [accessed 8. 1. 2024]. `https:`

Furthermore, exploiting the cyber-attribution problem typically lies in the hard-to-prove link between hackers and the state in question. Akin to privateers, state-sponsored hackers may only disclose this link if captured. However, their motivation to do so is much lower than in the case of privateers providing valid *Letters of Marque*, as mere cybercriminals do not face death sentences (unlike pirates). The situation's complexity is further compounded by the global reach of cyberattacks and the extensive safe haven protection afforded to state-sponsored hacker groups.

The historical excursion presented above illustrates that the attribution problem in the case of privateers was not resolved directly, nor was the solution of a legal nature. Instead, the relevance of the privateers' attribution problem diminished together with the factual decline of the privateering practice. Considering current developments, it is rather unlikely that history would not repeat itself in the case of state-sponsored hacker groups, despite the increasing frequency of political attributions since 2017.[219,220]

However, the historical analogy effectively highlights that as long as there are safe havens for hackers, cybercrime and state-sponsored cyberattacks are likely to persist and even grow.

Therefore, based on the historical parallels, the future development of the cyber-attribution problem and "cyber-teering" practice appears to be heading in one of three potential directions:

1) **Unification of the State Practice Leading to a Cyber-specific Customary Rule of Attribution**: The trend of political attributions of cyberattacks may persist, gradually contributing to the reformation of the unused rules of the attribution (i.e., *the effective control test*). The unification of state practices could lead to the formation of cyber-specific customary rules along the lines of maritime attribution standards, which would be better tailored to the unique needs of states in cyberspace. This renewed applicability might result in more

//www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/; Osula, A.-M., Kasper, A. and Kajander, A. (2022) EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology*, 16(1), pp. 94–100.

[219] Eichensehr, K. E. (2019) The Law and Politics of Cyberattack Attribution. *UCLA Law Review*, 67(3), pp. 530–533.

[220] That is closely related to the geopolitical context, as political attributions utilizing naming and shaming strategy are relatively meaningless in the relationship of strategic rivals (such as North Korea and the USA). See Goldsmith. *The Strange WannaCry Attribution*.; Eichensehr, K. E. (2017) Three Questions on the WannaCry Attribution to North Korea [online]. *Just Security*. [accessed 31. 10. 2023]. https://www.justsecurity.org/49889/questions-wannacry-attribution-north-korea/

frequent invocations of state responsibility, potentially stabilising the international situation.

2) **Emergence of Sufficient Professional Cyber-capabilities**: The current practice of political attributions may remain too diverse and thus fail to create a cyber-specific customary rule due to varying state interests. The number (and severity of consequences) of state-sponsored cyberattacks could increase, further destabilising cyberspace and international relations. This scenario could lead to a conflict or a major cyber-incident with catastrophic consequences, which might force states to invest in the preparation of professional cyber-capacities[221], improving their capabilities to monitor and govern cyberspace. The possibility of not only identifying the perpetrator but also striking back could then serve as a basis for cyber-deterrence. With the emergence of such capabilities on a sufficient level[222], the need to employ hacker groups could diminish, akin to the decline observed in privateering.[223]

3) **Stabilisation through Destabilisation**: As mentioned in Section 3, not every state desires the cyber-attribution problem to be resolved. There are those who exploit it and benefit from the more restrained approach of (primarily) Western states.[224] However, with the worsening of these problems of applied cyber legalism and overall security situation, even Western states may abandon the high road and adopt the same tactics (exploitation of the cyber-attribution problem).[225] The ensuing worsening of international relations, stability of international society and security in cyberspace (*the destabilisation aspect*) could eventually

[221] There are already many projects trying to improve the education of cybersecurity expert capacities, such as the project SPARTA (see `https://www.sparta.eu/`), however, the capabilities of the states to produce a sufficient number of those experts and employ them in the public sector are still rather limited.

[222] Many states have already a cyber-capacities within their armies and intelligence services, nevertheless, similarly to the relationship between navies and privateers, their numbers are not yet sufficient to deter and effectively fulfil any of the states' goals.

[223] These official capacities could either accept and adapt to cyber-attribution problem (and thus create a new state practice), or completely resign on it and leave the attribution only in the political level without legal constrains (paradoxically also creating new state practice).

[224] Schmitt, M. Three International Law Rules for Responding Effectively to Hostile Cyber Operations [online]. *Just Security*. 13. 7. 2021 [accessed 16. 1. 2024]. `https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations/`

[225] Kello, L. (2021) Cyber Legalism: Why It Fails and What to do about It. *Journal of Cybersecurity*, 7(1), pp. 2–3; Schmitt, M. Three International Law Rules for Responding Effectively to Hostile Cyber Operations [online]. *Just Security*. 13. 7. 2021 [accessed 16. 1. 2024]. `https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations/`.

lead to a consensus among states on the need for regulation, reminiscent of the Paris Declaration, bringing the cyber-attribution back within the scope of the law and constraining the use of cyberattacks (*the stabilisation aspect*). To minimise the risks of full escalation, it might be necessary to implement a particular set of rules balancing this destabilising campaign, such as the multi-level attribution-cyberteering concept and reinstitution of Letters of Marque proposed by Still.[226] A vital component of this destabilisation campaign should also involve targeting and "blockading" (DDoS and infrastructure destruction) hackers' safe havens and the states supporting them, as Harašta and Bátrla suggested.[227] By doing so, such a campaign could not only disrupt the cybercriminal environment but also influence the most relevant states. This scenario is based upon the premise that the political will to improve the situation may only emerge when the *general annoyance* becomes too substantial to ignore.

7. CONCLUSION

In this article, we have argued that the inadequacies of contemporary cyber-attribution legal procedures stem from the misguided attempt to apply standards developed for land-based conflicts to an environment that more closely resembles the high seas, primarily due to the lower level of control that states exert over these domains. This perspective offers a compelling parallel to the practice of obscuring states' involvement[228] in cyberattacks by employing hacker groups – privateering. To explore this analogy, we examined the historical practices of employing privateers and hackers, aiming to derive insights into the challenges posed by state-sponsored cyberattacks and the exploitation of the cyber-attribution problem. Our analysis revealed significant parallels across various dimensions, including purpose, effect, environment, and the nature of non-state actors, supporting the validity of drawing comparisons between cyberspace and the high seas, and justifying the application of historical analogy for inspiration. Consequently, we analysed the factors that led to the decline of privateering, seeking insights that could be applied to mitigate the issues associated

[226] Still, J. L. (2013) *Resurrecting Letters of Marque and Reprisal to Address Modern Threats*. United States Army War College - Defense Technical Information Center, p. 3. `http://www.dtic.mil/docs/citations/ADA590294`, pp. 24–25.

[227] Harašta, J., Bátrla, M. (2022) 'Releasing the Hounds?' Disruption of the Ransomware Ecosystem Through Offensive Cyber Operations. In: Jančárková, T., Visky, G., Winther, I. (eds.). *14th International Conference on Cyber Conflict: Keep Moving*. Tallinn, Estonia: CCDCOE Publications, pp. 99–100.

[228] Or utilizing capabilities that would otherwise be inaccessible for the said state.

with cyber-attribution and the modern-day equivalent of privateers – "cyber-teers."

Our analysis revealed that the resolution of the privateering problem (and associated attribution problems) was not achieved by means of law but by the change of doctrine, which is unfortunately the probable course even in the case of cyber-attribution.[229] The factors instrumental to the decline of privateers that could also potentially mitigate the practice of state-sponsored cyberattacks and exploitation of cyber-attribution problem involve the emergence of professional state capacities (rendering the use of hard-to-control and unreliable privateers or hackers less necessary and profitable), destruction, disruption or denial of safe havens and the consequent decline of the risk/gain profitability for the non-state actors. In combination with technological advancements like the thorough implementation of *security by design and default* approaches throughout the market, these factors may cause or at least contribute to the decline of the cyber-teering practice.

Concluding our exploration, we introduced three prospective scenarios based on contemporary developments and historical analogies. These scenarios encompass the emergence of cyber-specific rules of attribution and the enhancement of legal aspects of cyber-deterrence, the development of professional cyber-capacities of states following a major cyber-incident or even a conventional conflict (such as in the case of the post-Napoleonic era) enhancing the factual aspects of cyber-deterrence, and stabilisation through destabilisation. These scenarios or their combination reflect potential pathways for the evolution of the current situation, offering a perspective on addressing the challenges in the realm of state-sponsored cyberattacks and cyber-attribution.

LIST OF REFERENCES

[1] Anderson, J. L. (1995) Piracy and World History: An Economic Perspective on Maritime Predation. *Journal of World History*, 6(2), pp. 175–199.

[2] Aravindakshan, S. (2021) Cyberattacks: A Look at Evidentiary Thresholds in International Law. *Indian Journal of International Law*, 59(1–4), pp. 285–299.

[3] Baliga, S., Bueno De Mesquita, E., Wolitzky, A. (2020) Deterrence with Imperfect Attribution. *American Political Science Review*, 114(4), pp. 1155–1178.

[4] Banks, W. (2021) Cyber Attribution and State Responsibility. *International Law Studies*, 1039(97), pp. 1040–1072.

[229] Kello, L. (2021) Cyber Legalism: Why It Fails and What to do about It. *Journal of Cybersecurity*, 7(1), pp. 2–3.

[5] Bendiek, A., Schulze, M. (2021) Attribution: A Major Challenge for EU Cyber Sanctions: An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW. *SWP Research Paper*. https://www.swp-berlin.org/10.18449/2021RP11/

[6] Berghel, H. (2017) On the Problem of (Cyber) Attribution. *Computer - IEEE Computer Society*, 50(3), pp. 84–89.

[7] Berman, H. J. (1983) *Law and Revolution: the Formation of the Western Legal Tradition*. Cambridge (Mass.) London: Harvard university press.

[8] Boebert, W. E. (2010) A Survey of Challenges in Attribution. In: *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, D.C.: The National Academies Press, pp. 41–52. http://www.nap.edu/catalog/12997.html

[9] Bossert, T. (2017) Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea – The White House [online]. *The White House - Press Briefings*. [accessed 22. 11. 2023]. https://trumpwhitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/

[10] Brigitte, S. (2010) The Elements of An Internationally Wrongful Act. In: Crawford, J. et al. (eds.). *The Law of International Responsibility*. Oxford: Oxford University Press. Oxford Commentaries on International Law.

[11] Cartwright, M. (2021) Pirate Havens in the Golden Age of Piracy [online]. *World History Encyclopedia*. [accessed 14. 1. 2024]. https://www.worldhistory.org/article/1844/pirate-havens-in-the-golden-age-of-piracy/

[12] Cassese, A. (2007) The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia. *European Journal of International Law*, 4, pp. 649–668.

[13] Chircop, L. (2018) A Due Diligence Standard of Attribution in Cyberspace. *International and Comparative Law Quarterly*, 67(3), pp. 643–668.

[14] Condorelli, L., Kress, C. (2010) The Rules of Attribution: General Considerations. In: Crawford, J. et al. (eds.). *The Law of International Responsibility*. Oxford: Oxford University Press. Oxford Commentaries on International Law.

[15] Connel, M., Vogler, S. (2017) *Russia's Approach to Cyber Warfare*. CNA. https://www.cna.org/archive/CNA\Files/pdf/dop-2016-u-014231-1rev.pdf

[16] Cooperstein, T. M. (2009) *Letters of Marque and Reprisal: The Constitutional Law and Practice of Privateering*. Rochester, NY. https://papers.ssrn.com/abstract=1406677

[17] Crawford, J. (2013) *State Responsibility: The General Part*. Cambridge University Press. https://www.cambridge.org/core/product/identifier/9781139033060/type/book

[18] Crawford, J. (2002) *The International Law Commission's Articles on State Responsibility: Introduction, Text, and Commentaries*. Cambridge, U.K. New York: Cambridge University Press.

[19] Davis, J. K. (2022) *Tallinn Paper No. 13 - Developing Applicable Standards of Proof for Peacetime Cyber Attribution*. NATO CCD COE Publications.

[20] Dwan, J. H., Paige, T. P., McLaughlin, R. (2022) Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers. *Law, Technology and Humans*, 3(2). https://lthj.qut.edu.au/article/view/1583

[21] Edwards, B. et al. (2017) Strategic Aspects of Cyberattack, Attribution, and Blame. *Proceedings of the National Academy of Sciences*, 114(11), pp. 2825–2830.

[22] Egloff, F. (2017) Cybersecurity and the Age of Privateering. In: Perkovich, G., Levite, A. E. (eds.). *Understanding Cyber Conflict: Fourteen Analogies*. Washington, DC: Georgetown University Press, pp. 231–247.

[23] Egloff, F. J., Smeets, M. (2021) Publicly attributing cyber attacks: a framework. *Journal of Strategic Studies*, pp. 1–32.

[24] Eichensehr, K. E. (2019) The Law and Politics of Cyberattack Attribution. *UCLA Law Review*, 67(3), pp. 520–598.

[25] Eichensehr, K. E. (2017) Three Questions on the WannaCry Attribution to North Korea [online]. *Just Security*. [accessed 31. 10. 2023]. https://www.justsecurity.org/49889/questions-wannacry-attribution-north-korea/

[26] Gentili, A. (1612) *De Iure Belli Libri Tres*. Oxford: The Clarendon Press. Carnegie Classics of International Law. https://archive.org/details/threebooksonlawo0002ayal/page/n3/mode/2up

[27] Giles, K., Hartmann, K. (2019) 'Silent Battle' Goes Loud: Entering a New Era of State-Avowed Cyber Conflict. In: Minárik, T. et al. (eds.). *11th International Conference on Cyber Conflict: Silent Battle*. Tallinn: NATO CCD COE Publications, pp. 23–36.

[28] Global Research and Analysis Team of Kaspersky Lab. WannaCry and Lazarus Group – the missing link? [online]. *Kaspersky - SecureList*. 15. 5. 2017 [accessed 7. 1. 2024]. https://securelist.com/wannacry-and-lazarus-group-the-missing-link/78431/

[29] Goldsmith, J. (2017) The Strange WannaCry Attribution [online]. *Lawfare*. [accessed 21. 11. 2023]. https://www.lawfaremedia.org/article/strange-wannacry-attribution

[30] Groot, H. de. (2004) *De Iure Belli ac Pacis*. Whitefish, MT: Kessinger.

[31] Haataja, S. (2021) Autonomous Cyber Capabilities and Attribution in the Law of State Responsibility. In: Liivoja, R., Väljataga, A. (eds.). *Autonomous Cyber Capabilities under International Law*. Tallinn, Estonia: NATO CCD COE Publications, pp. 260–290. NATO CCDCOE Publications.

[32] Harašta, J., Bátrla, M. (2022) 'Releasing the Hounds?' Disruption of the Ransomware Ecosystem Through Offensive Cyber Operations. In: Jančárková, T., Visky, G., Winther, I. (eds.). *14th International Conference on Cyber Conflict: Keep Moving*. Tallinn, Estonia: CCDCOE Publications, pp. 93–115.

[33] Hayes, A. (1925) Private Claims against Foreign Sovereigns. *Harvard Law Review*,38(5), pp. 599–621.

[34] Healey, J. (2012) *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*. Atlantic Council – Cyber Statecraft Initiative. https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212\ACUS\NatlResponsibilityCyber.PDF

[35] Hessbruegge, J. (2004) The Historical Development of the Doctrines of Attribution and Due Diligence in International Law. *New York University Journal of International Law and Politics*, 36(4), pp. 265–306.

[36] Holt, T. J. et al. (2023) Assessing nation-state-sponsored cyberattacks using aspects of Situational Crime Prevention. *Criminology & Public Policy*, 22(4), pp. 825–848.

[37] Horsley, E. (2020) State-Sponsored Ransomware Through the Lens of Maritime Piracy. *Georgia Journal of International & Comparative Law*, 47(3), p. 669.

[38] (ISC)2. *Cybersecurity Workforce Study*. 2022. https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

[39] Jensen, E. T. (2020) Due Diligence in Cyber Activities. In: Krieger, H., Peters, A., Kreuzer, L. (eds.). *Due Diligence in the International Legal Order*. UK: Oxford University Press, p. 0. https://doi.org/10.1093/oso/9780198869900.003.0015

[40] Jervis, R. et al. *Psychology and deterrence*. Baltimore (Ma.) London: The John Hopkins university press, 1989. Perspectives on security.

[41] Kello, L. (2021) Cyber Legalism: Why It Fails and What to do about It. *Journal of Cybersecurity*, 7(1), pp. 1–15.

[42] Kolouch, J. et al. (2023) Cybersecurity: Notorious, but Often Misused and Confused Terms. *Masaryk University Journal of Law and Technology*, 17(2), pp. 281–305.

[43] Kolouch, J., Zahradnický, T., Kučínský, A. (2021) Cyber Security: Lessons Learned From Cyber-Attacks on Hospitals in the COVID-19 Pandemic. *Masaryk University Journal of Law and Technology*, 15(2), pp. 301–341.

[44] Kraska, J. (2021) *Contemporary Maritime Piracy: International Law, Strategy, and Diplomacy at Sea*. Santa Barbara, Calif: Praeger. Contemporary Military, Strategic, and Security Issues.

[45] Layne, N. (2017) Russian Lawmaker's Son gets 27 Years Prison in U.S. hacking case. *Reuters*. https://www.reuters.com/article/idUSKBN17N2GZ/

[46] Liu, I. Y. (2017) *State Responsibility and Cyberattacks: Defining Due Diligence Obligations*. Rochester, NY. https://papers.ssrn.com/abstract=2907662

[47] Mačák, K. (2016) Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law*, 21(3), pp. 405–428.

[48] Microsoft Threat Intelligence. (2022) Microsoft investigates Iranian attacks against the Albanian government [online]. *Microsoft Security Blog*. [accessed 31. 7. 2023]. https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/

[49] Obama, B. (2010) *US National Security Strategy*. The White House, Washington. https://obamawhitehouse.archives.gov/sites/default/files/rss\viewer/national\security\strategy.pdf

[50] Osawa, J. (2017) The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem? *Asia-Pacific Review*. 24(2), pp. 113–131.

[51] Osula, A.-M., Agnes Kasper, Aleksi Kajander. (2022) EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology*, 16(1), pp. 89–123.

[52] Pamment, J. et al. (2019) *Hybrid Threats: 2007 Cyber Attacks on Estonia*. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/cuploads/pfiles/cyber\attacks\estonia.pdf

[53] Pellet, A. (2010) The Definition of Responsibility in International Law. In: Crawford, J., Olleson, S., Parlett, K. (eds.). *The Law of International Responsibility*. Oxford: Oxford University Press. Oxford Commentaries on International Law.

[54] Polčák, R., Svantesson, D. J. B. (2017) *Information Sovereignty: Data Privacy, Sovereign Powers and the Rule of Law*. Cheltenham: Edward Elgar Publishing.

[55] Rid, T., Buchanan, B. (2015) Attributing Cyber Attacks. *Journal of Strategic Studies*, 38(1–2), pp. 4–37.

[56] Rodger, N. A. M. (2014) The Law and Language of Private Naval Warfare. *The Mariner's Mirror*, 100(1), pp. 5–16.

[57] Roguski, P. (2020) Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace [online]. *Just Security*. [accessed 8. 1. 2024]. https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/

[58] Rubin, A. P. (1988) *The Law of Piracy*. Honolulu.: University Press of the Pacific Hunolulu. https://archive.org/details/lawofpiracy63rubi

[59] Schmitt, M. (2018) In Defense of Sovereignty in Cyberspace [online]. *Just Security*. [accessed 28. 6. 2023]. https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/

[60] Schmitt, M. (2021) Three International Law Rules for Responding Effectively to Hostile Cyber Operations [online]. *Just Security*. [accessed 16. 1. 2024]. https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations/

[61] Schmitt, M. (2017) NATO Cooperative Cyber Defence Centre of Excellence (eds.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316822524

[62] Schmitt, M. (2013) NATO Cooperative Cyber Defence Centre of Excellence (eds.). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge ; New York: Cambridge University Press.

[63] Schmitt, M., Watts, S. (2015) The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare. *Texas International Law Journal*, 50(2–3), pp. 189–232.

[64] Schöndorf, R. (2021) Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations. *International Law Studies* 97(1). https://digital-commons.usnwc.edu/ils/vol97/iss1/21

[65] Spáčil, J. (2022) Plea of Necessity: Legal Key to Protection against Unattributable Cyber Operations. *Masaryk University Journal of Law and Technology*, 16(2), pp. 215–239.

[66] Spector, P. (2017) In Defense of Sovereignty, in the Wake of Tallinn 2.0. *AJIL Unbound*, 111, pp. 219–223.

[67] Stark, F. R. (1897) *The Abolition of Privateering and the Declaration of Paris*. New York: Columbia University.

[68] Starkey, D. J. (1990) *British Privateering Enterprise in the Eighteenth Century*. Exeter, Devon, UK: University of Exeter Press. http://www.jstor.org/stable/10.2307/j.ctv2nxkpmw

[69] Still, J. L. (2013) *Resurrecting Letters of Marque and Reprisal to Address Modern Threats*. United States Army War College - Defense Technical Information Center. http://www.dtic.mil/docs/citations/ADA590294

[70] Svantesson, D. et al. (2023) On sovereignty. *Masaryk University Journal of Law and Technology*, 17(1), pp. 33–85.

[71] Tabarrok, A. (2007) The Rise, Fall, and Rise Again of Privateers. *The Independent Review* 11(4), pp. 565–577.

[72] Tabarrok, A., Nowrasteh, A. (2015) Privateers: Their History and Future History. *Fletcher Security Review*, 2(1), pp. 55–62.

[73] Talmon, S. (2015) Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion. *European Journal of International Law*, 26(2), pp. 417–443.

[74] Turton, W., Riley, M., Jacobs, J. (2021) Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom. *Bloomberg.com*. https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom

[75] Wolff, C. (1995) *Jus Gentium Methodo Scientifica Pertractatum*. Buffalo, NY: Hein. The Classics of International Law 13. https://archive.org/details/jusgentiummethod0002wolf

[76] APTs & Adversary Groups List - Malware & Ransomware [online]. *Crowdstrike Adversary Universe* [accessed 27. 8. 2023]. https://adversary.crowdstrike.com/en-US/

[77] (2023) Attack (International Humanitarian Law) [online]. *International Cyber Law: Interactive Toolkit*. 28. 7. 2023 [accessed 10. 1. 2024]. https://cyberlaw.ccdcoe.org/wiki/Attack(international_humanitarian_law)

[78] (2024) Attribution Tracker [online]. *EuRepoC: European Repository of Cyber Incidents*. [accessed 18. 5. 2024]. https://eurepoc.eu/attribution-tracker/

[79] Connect the Dots on State-Sponsored Cyber Incidents – Stuxnet [online]. *Council on Foreign Relations* [accessed 26. 12. 2023]. https://www.cfr.org/cyber-operations/stuxnet

[80] (2001) *Draft articles on Responsibility of States for Internationally Wrongful Acts*. International Law Commission – United Nations. https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

[81] (2001) *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries - 2001*. International Law Commission – United Nations. http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

[82] (2013) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/68/98*. https://digitallibrary.un.org/record/753055

[83] (2015) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/150*. UN. https://digitallibrary.un.org/record/799853

[84] *Judgement of the International Court of Justice in the Case concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America) - Merits*. 1986. https://www.icj-cij.org/case/70/judgments

[85] *Judgement of the International Court of Justice in the Case of Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*. 2007. https://www.icj-cij.org/case/91/judgments

[86] (2021) *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies*. General Assembly of the United Nations. https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf

[87] (2016) *Responsibility of States for Internationally Wrongful Acts - Comments and information received from Governments and Report of the Secretary-General (A/71/79)*. General Assembly of the United Nations. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/112/74/PDF/N1611274.pdf?OpenElement

[88] (2017) Russian Cyber-Criminal Sentenced to 14 Years in Prison for Role in Organized Cybercrime Ring Responsible for $50 Million in Online Identity Theft and $9 Million Bank Fraud Conspiracy [online]. *United States Department of Justice, Office of Public Affairs*. 30. 11. 2017 [accessed 29. 12. 2023]. https://www.justice.gov/opa/pr/russian-cyber-criminal-sentenced-14-years-prison-role-organized-cybercrime-ring-responsible

[89] (2022) Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure [online]. *Cybersecurity and Infrastructure Security Agency*. 9. 5. 2022 [accessed 15. 1. 2024]. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a

[90] (2022) The Urgency of Tackling Europe's Cybersecurity Skills Shortage [online]. *Microsoft: EU Policy Blog*. 23. 3. 2022 [accessed 17. 2. 2023]. https://blogs.microsoft.com/eupolicy/2022/03/23/the-urgency-of-tackling-europes-cybersecurity-skills-shortage/

[91] (2024) Tracking State-Sponsored Cyberattacks Around the World [online]. *Council on Foreign Relations*. [accessed 7. 2. 2024]. https://www.cfr.org/cyber-operations

DOI 10.5817/MUJLT2024-2-3

SHROUDED IN SECRECY – DOES THE COMITOLOGY PROCEDURE FOR GDPR ADEQUACY DECISIONS FIT ITS PURPOSE?

by

MICHAL CZERNIAWSKI *

With the entry into force of Directive 95/46/EC, the EU based its approach toward data transfers on adequacy decisions, unilateral acts of the European Commission, issued as implementing acts. The EU co-legislators subsequently copied this model into the GDPR and the LED. Since the very beginning, the adequacy procedure involves a comitology phase in which a committee consisting of representatives of Member States expresses its opinion about the Commission's draft implementing act. I argue that adequacy, designed as a technical process, evolved into a tool in which politics, including economic relations and commercial interests, play an ever-greater role. This goes against the concept of comitology, the legitimacy of which is built on denying the political nature of what is delegated. Taking into account the above, as well as other shortcomings of the EU adequacy model, I argue that it is the right time to rethink it. There is also the need for a separate discussion regarding the role of the Article 93 Committee in the adequacy procedure, to be conducted together with the debate on the role and accountability of the European Commission.

KEY WORDS

General Data Protection Regulation (GDPR), Law Enforcement Directive (LED), Data Transfers, Adequacy Decisions, Comitology.

* Affiliated Researcher, Research Group on Law, Science, Technology & Society (LSTS), Vrije Universiteit Brussel (VUB). Pleinlaan 2, 1050, Brussels, Belgium. For correspondence: michal.czerniawski@vub.be. The views and opinions expressed in this paper are mine and do not reflect the opinions or positions of any entity, in particular the European Parliament. I would like to thank Laura Drechsler for her useful input and feedback during the writing process. Any errors or mistakes are my own.

1. INTRODUCTION

The European Union's approach towards regulating transfers of personal data in both the General Data Protection Regulation (hereinafter: GDPR),[1] and the Law Enforcement Directive (hereinafter: LED)[2] is determined by the dual objective of enabling, on the one hand, internal data flows between EU Member States, while, on the other hand, restricting international data transfers to third countries or international organisations. In accordance with Article 45 GDPR, the European Commission may issue an adequacy decision and decide that the third country, a territory or one or more specified sectors within that third country, or the international organisation ensures an adequate level of protection. This provision also establishes a list of elements, which the Commission needs to take into account when assessing the adequacy of the level of protection. A similar provision can be found in the LED (Article 36 thereof). Adequacy decision allows for an unrestricted flow of personal data between the EU and a third country a territory or one or more specified sectors or an international organisation, without any further safeguard being necessary. This makes it the most important instrument for legalising transfers of personal data from the EU,[3] a "holy grail" for third countries that want to achieve a free flow of data with the EU. Only in the absence of an adequacy decision, data transfers to third countries can be based on appropriate safeguards, and as a last resort on derogations, as provided by the GDPR and the LED.

While there is a lot of discussion about how to interpret different adequacy requirements, in particular, the concept of "essential equivalence",[4] **much less**

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88. Available from: `https://eur-lex.europa.eu/eli/reg/2016/679/oj` [Accessed 1 July 2024].

[2] See Article 36 of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A32016L0680` [Accessed 1 July 2024]. For a detailed analysis of the assessment under the LED, see: Drechsler, L. (2020) Comparing LED and GDPR Adequacy: One Standard Two Systems, *Global Privacy Law Review*, 1(2), pp. 93-104.

[3] For information about other instruments, such as Standard Contractual Clauses or Binding Corporate Rules, see the official Commission's webpage: `https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection\_en` [Accessed 1 July 2024].

[4] See for example, Drechsler, L. and Kamara, I. (2022) Essential equivalence as a benchmark for international data transfers after Schrems II, [in:] Kosta, E. and Leenes, R. (eds), *Research Handbook on EU data protection law*. Cheltenham/Northampton: Edward Elgar Publishing

attention is dedicated to the procedure of granting adequacy itself. The adequacy model based on implementing acts, which puts the Commission in charge of the assessment procedure, was proposed by the EU legislator in 1990, with the publication of the first legislative proposal of what was known as Directive 95/46/EC.[5] It relies on the comitology procedure, introduced in the EU legal system to relieve some of the burden from the European intergovernmental negotiating process, and allow negotiators not to discuss matters that would be too detailed and time-consuming.[6] Since its very beginning, **the comitology procedure has been considered as a technical and not political process**.

The comitology in data protection was introduced more than 30 years ago,[7] in a totally different geopolitical, technological and societal reality. Let me just mention that it took place one year after the fall of communism in several countries that are now EU Member States, something that back in 1990 was unimaginable. Since then, the data protection laws have changed significantly, European data protection has become a benchmark at the global level, and data transfers have become one of the key elements of our societies and economy. In the recent GDPR evaluation, the Commission correctly states that "[d]ata flows have become integral to the digital transformation of society and to the globalisation of the economy".[8]

I believe that there are four reasons why the model based on the committee procedure stayed in place for such a long time. **First**, due to the motives

2022; pp. 314-352, Wagner, J. (2018) The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection? *International Data Privacy Law*, 8(4), pp. 318-337, Lindsay, D. (2017) The role of proportionality in assessing trans-atlantic flows of personal data, [in:] Svantesson, D.J.B. and Kloza, D. (eds.), *Trans-Atlantic data privacy relations as a challenge for democracy*, Cambridge: Intersentia, pp. 49-84, Gulczynska, Z. (2021) A certain standard of protection for international transfers of personal data under the GDPR. *International Data Privacy Law*, 11(4), pp. 360-374.

5 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31. Available from: `https://eur-lex.europa.eu/eli/dir/1995/46/oj` [Accessed 1 July 2024].

6 Robert, C. (2019) The political use of expertise in EU decision-making: The case of comitology. *Research report*, p. 15. Available from: `https://dumas.ccsd.cnrs.fr/SCIENCESPO\_LYON/halshs-03021131v1` [Accessed 1 July 2024].

7 See Commission Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security /* COM/90/314FINAL */, 13 September 1990. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM\%3A1990\%3A0314\%3AFIN` [Accessed 1 July 2024].

8 European Commission, Communication from the Commission to the European Parliament and the Council, Second Report on the application of the General Data Protection Regulation, COM(2024) 357 final, Brussels, 25 July 2024, p. 19. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM\%3A2024\%3A357\%3AFIN` [Accessed 1 July 2024].

described in this paper, the Commission is against any changes to it, with a strong preference towards maintaining the *status quo*; **second**: during the GDPR negotiations, i.e. the moment when the adequacy procedure was discussed, there were more important issues linked to data transfers, in particular the so-called "Snowden provision" prohibiting transfers not authorised by the EU law;[9] **third**: comitology constitutes a procedure that is widely used in the EU, relying on it allowed to avoid lengthy discussion regarding the possible way forward; **fourth**: use of comitology, which involves representatives of Member States, ensured that Member States would respect the Commission's adequacy decisions.

At the same time, there should be no doubt that the current model of issuing adequacy decisions is **lengthy and inefficient** - it takes years to negotiate a single decision. One of the reasons for this is the lack of any continuous monitoring of the Commission's actions and of any milestones or deadlines the Commission needs to meet. The following sentence by Kuner can serve as a summary of all the problems with adequacy procedure raised by its critics: "[t]he procedure for having third countries declared "adequate" by the European Commission is (...) a triumph of bureaucracy and formalism over substance, and has been criticized as inefficient, untransparent, and subject to political influence."[10] For the reasons explained below, I believe that the procedure, as it stands now, seems **not to fit its purpose in the digital age**. There are several reasons for that. The pace of work on adequacy decisions might be among the factors deterring third states from engaging in talks with the EU. In addition, for the first time, we can observe the emergence of mechanisms aimed at facilitating cross-border data transfers competing with the EU standard and being faster and less bureaucratic. In this context, let me just mention the Asia-Pacific Economic Cooperation and Privacy (APEC) Cross Border Privacy Rules (CBPR).[11] APEC includes countries with adequacy decisions such as the USA, Japan or Canada and the number of its members is growing faster than the number of third countries covered with adequacy decisions.[12] While APEC rules do not involve the

[9] See Article 48 GDPR.

[10] Kuner, C. (2017) Reality and Illusion in EU Data Transfer Regulation Post Schrems. *German Law Journal*, 18(4), p. 911.

[11] Asia-Pacific Economic Cooperation, APEC Privacy Framework. Available from: `https://www.apec.org/publications/2005/12/apec-privacy-framework` [Accessed 1 July 2024].

[12] At the same time, it should be noted that the APEC approach is not compliant with the essential equivalence requirement. See: European Commission, Commission Staff Working Document accompanying the document: Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decision for Japan' SWD (2023) 75 final, 3 April 2023. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A52023SC0075` [Accessed 1 July 2024]. "The

process of making adequacy determination,[13] we can observe third countries such as Japan or the United Kingdom establish their own adequacy models for data transfers and grant the EU their adequacy findings. Finally, the adequacy decisions now constitute a piece of a broader EU strategy[14] and the Commission uses them as a part of trade negotiations. As the best example in this case serves Japan, which received an adequacy decision ahead of the agreement between the EU and Japan for an economic partnership.[15] It seems that the Commission is extending the reach of EU's data protection standards in parallel with international trade agreement negotiations.[16]

Another issue is the fact the Commission undertakes the adequacy assessment, with very far-reaching consequences for the EU, being at the same time the guardian of the treaties i.e. an institution, which is supposed to

APEC CBPR system is a self-certification system based on the principle of accountability. Its main weakness, at least from an EU perspective, is that it lacks tools to make it binding and thus operates essentially on a voluntary basis", Drechsler, L. and Matsumi, H. (2024) Caught in the middle: the Japanese approach to international personal data flows. *International Data Privacy Law*, 14(2), p. 143.

13 Wolf, C. (2014) Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers. *Washington University Journal of Law and Policy*, 227(43), p. 232.

14 European Commission, Communication from the Commission to the European Parliament and the Council, Exchanging and Protection Personal Data in a Globalised World, COM(2017) 7 final. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM\%3A2017\%3A7\%3AFIN` [Accessed 1 July 2024].

15 EU Council, EU-Japan: the Council approves a protocol to facilitate free flow of data, Press release, 29 April 2024. Available from: `https://www.consilium.europa.eu/en/press/press-releases/2024/04/29/eu-japan-the-council-approves-a-protocol-to-facilitate-free-flow-of-data/` [Accessed 1 July 2024].

16 Voss, W. G. (2020) Cross-border data flows, the GDPR, and data governance. *Washington International Law Journal*, 29(3), p. 517. As revealed by the Commission, in deciding which nations to target, the Commission looks at:

- the extent of the EU's (actual or potential) commercial relations with a given third country, including the existence of a free trade agreement or ongoing negotiations;
- the extent of personal data flows from the EU, reflecting geographical and/or cultural ties;
- the pioneering role the third country plays in the field of privacy and data protection that could serve as a model for other countries in its region; and
- the overall political relationship with the third country in question, in particular with respect to the promotion of common values and shared objectives at the international level.

See: European Commission, Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World Questions and Answers, COM(2017) 7 final (19 January 2017), p. 8. Available from: `http://ec.europa.eu/newsroom/document.cfm?doc\_id=41157` [Accessed 1 July 2024].

check whether the assessment aligns with EU primary law.[17] This leads to a situation where, **in the case of adequacy decisions**, **the Commission cannot be considered an honest broker and independent assessor**, as it is interested in a particular outcome of the procedure and, as I argue in this paper, might be politically motivated in its actions. The consecutive attempts to ensure the adequacy of EU-U.S. transfer mechanisms, which required a significant effort and political will, might be the best example of using adequacy as a political tool. Over the period of several years, the Commission dedicated significant resources to EU-U.S. negotiations while at the same time, it has not explored the possibility of adequacy decisions e.g. for EU neighbouring countries or international organisations. Finally, the recent controversies regarding the review of decisions issued under Directive 95/46/EC,[18] could also be seen as another proof of the role politics plays during the adequacy assessment. A decision-making process based on politics would go against the core of the comitology model. As pointed out by Robert, the idea underlying this procedure "is that some matters may be delegated because they are basically only reliant on technical competence as opposed to the exercise of political responsibility".[19] In the adequacy context, such a situation may have significant implications as it creates risks for data subjects' rights. **If the adequacy is based on a Commission's assessment, which is incorrect or politically motivated, it might be undermining the protection of the EU's fundamental rights**.

2. FUNCTIONING OF THE ARTICLE 93 COMMITTEE

2.1. GENERAL RULES ON ADEQUACY DECISIONS AND THE COMITOLOGY PROCEDURE

In the information society, while data subjects remain in one geographical location, their data can be processed in many different places and jurisdictions. The objective of the transfer rules established in the GDPR (and the LED) is to ensure that the level of protection for natural persons is not undermined no matter where their data are processed. At the foundation of the EU model lies the principle that protection accompanies personal

[17] European Commission, What the European Commission does in law. Available from: https://commission.europa.eu/about-european-commission/role-european-commission/law_en [Accessed 1 July 2024].

[18] EDRi European Digital Rights et al. (2024) Concerns Regarding European Commission's Reconfirmation of Israel's Adequacy Status in the Recent Review of Adequacy Decisions, a letter sent on 22 April 2024. Available from: https://edri.org/wp-content/uploads/2024/04/Concerns-Regarding-European-Commissions-Reconfirmation-of-Israels-Adequacy-Status-in-the-Recent-Review-of-Adequacy-Decisions-updated-open-letter-April-2024.pdf [Accessed 1 July 2024].

[19] Robert, C. (2019) op.cit., p. 19.

data during their whole "life-cycle".[20] While there are also other means of legalising data transfers, adequacy decisions are the most convenient ones. They do not require any actions on the controller's or processor's side - an adequacy decision confirms that a third country (or an international organisation) has a standard of essential equivalence regarding the protection of the fundamental rights and freedoms in connection with personal data and covers all entities within its territory.[21] In the absence of an adequacy decision, as indicated in Article 46 GDPR, organisations may also transfer personal data either where appropriate safeguards *vis-a-vis* the organisation receiving the personal data can be provided (in particular - standard data protection clauses (SCCs) and binding corporate rules (BCRs)). Besides the adequacy decision or appropriate safeguards, subject to specific conditions, one may still be able to transfer personal data based on a derogation listed in Article 49 GDPR (and respectively - Article 38 LED), such as the necessity to protect the vital interests of the data subject or of other persons.[22] However, if there is an adequacy decision in place that would cover the intended transfer, it has to be used for the transfer. Only in the absence of an adequacy decision, exporters can rely on appropriate safeguards and only as a last resort on derogations, as provided by the GDPR and the LED.

In line with Article 45(1) GDPR, it is up to the Commission to decide that the third country, a territory or one or more specified sectors within that third country, or the international organisation ensure an adequate level of protection. Moreover, **the Commission is in full control of the assessment process**. It conducts a detailed analysis of third-country legal regime; however, these documents are never made public.[23] Besides legal analysis, before issuing an adequacy decision, the Commission always holds detailed discussions with a third country. As a part of this process, Kuner identifies a stage called "agreement in principle",[24] which means a phase where a political deal has been reached, but is to be yet followed by the

[20] Padova, Y. (2016) The Safe Harbour is invalid: what tools remain for data transfers and what comes next? *International Data Privacy Law*, 6(2), p. 142.

[21] Article 45(1) and recital 104 GDPR.

[22] For a comprehensive overview of different transfer tools, see the European Data Protection Board, The EDPB data protection guide for small business. Available from: `https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers\_en` [Accessed 1 July 2024].

[23] Kuner, C. (2024) International data transfers and the EDPS: current accomplishments and future challenge. In Van Alsenoy B. et al. (eds.), *Two decades of personal data protection. What next? EDPS 20th Anniversary*, Luxembourg: Publications Office of the European Union, p. 90.

[24] Ibid., p. 89.

agreement on the working level. This term was used when announcing the Data Privacy Framework.[25]

As adequacy decisions are adopted in the form of implementing acts, there are two ways of controlling the Commission's actions:

(i) *ex-post*, by the Court of Justice of the European Union (CJEU) - so far the Court has invalidated two of the Commission's adequacy decisions;[26]

(ii) *ex-ante* - by the "Article 93 Committee", competent to prevent the Commission from adopting an adequacy decision. [27]

The comitology procedure has formed a part of the adequacy decisions since its very beginning and the entry into force of Directive 95/46/EC. In line with Article 291(1) TFEU,[28] it is for the Member States to adopt all measures of national law necessary to implement legally binding Union law. However, when uniform conditions of implementation are needed, implementing powers are granted to the Commission (and, in specific cases, to the Council). Within the framework of the comitology procedure, a committee issues a formal opinion on a draft implementing act, in this case - a draft implementing decision of the European Commission recognising an adequate level of protection of personal data. The comitology procedure established in Article 93 GDPR is governed by Regulation 182/2011,[29] which contains the rules and general principles regarding the Commission's exercise of implementing powers. These rules are supplemented by the committee's rules of procedures, which specify the provisions of Regulation 182/2011.

The committee itself, despite its important role in the process of issuing adequacy decisions and other implementing acts to the GDPR, the LED and

[25] The White House, Remarks by President Biden and European Commission President Ursula von der Leyen in Joint Press Statement, 25 March 2022. Available from: https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/03/25/remarks-by-president-biden-and-european-commission-president-ursula-von-der-leyen-in-joint-press-statement/ [Accessed 1 July 2024].

[26] See Judgment of 6 October 2015 Maximillian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650 and Judgment of 16 July 2020 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559.

[27] In accordance with Recital 167 GDPR, "[i]n order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011. In that context, the Commission should consider specific measures for micro, small and medium-sized enterprises".

[28] Consolidated version of the Treaty on the Functioning of the European Union, O J 115, 09/05/2008 P. 0173 - 0173. Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF [Accessed 1 July 2024].

[29] Regulation (EU) 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers, OJ L 55, 28.2.2011, p. 13–18. Available from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX\%3A32011R0182 [Accessed 1 July 2024].

Regulation 1725/2018,[30] remains shrouded in secrecy. The information on its meetings, provided by the European Commission in the comitology register, is **very laconic and is only accessible through a general register of all committee procedures, often with significant delay**. While this approach may help in protecting the EU decision-making process, at the same time it hinders access to even the most basic information concerning the discussions on transnational flows of personal data.

2.2. FROM THE ARTICLE 31 COMMITTEE OF DIRECTIVE 95/46/EC TO THE ARTICLE 93 GDPR COMMITTEE

When adopting implementing acts, the Commission relies on competencies entrusted to it by the Member States. Therefore, the Member States should be able to execute control over how the Commission uses these powers. The Member States exercise control through a committee composed of their representatives. Adequacy decisions are subject to the examination procedure, i.e. a procedure, which allows Member States to review the proposal and, if needed, prevent the Commission from adopting an implementing act - in this case, an adequacy decision.

Despite having an official name,[31] the committee dealing with issues relating to the protection of personal data is traditionally identified by the number of the article that constitutes the legal basis for its functioning. If we look at the statistics of the work of the committee established in accordance with Article 31 of Directive 95/46/EC, [32] it has been quite active - it has held a

[30] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39–98. Available from: https://eur-lex.europa.eu/eli/reg/2018/1725/oj [Accessed 1 July 2024].

[31] The official name of both the Article 31 Committee and the Article 93 is: Committee on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[32] The Article stated: Article 31 The Committee 1. The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission. 2. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit, which the chairman may set according to the urgency of the matter. The opinion shall be delivered by the qualified majority, as laid down in Article 148 (2) of the Treaty. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article. The chairman shall not vote. The Commission shall adopt measures which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. In that event: - the Commission shall defer the application of the measures which it has decided for a period of three months from the date of communication, - the Council, acting by a qualified majority, may take a different decision within the time limit referred to in the first indent.

total of 73 meetings; the last meeting took place on 15 November 2016.[33] The Article 31 Committee ceased to operate on 25 May 2018, the date on which the GDPR became applicable, and was replaced by the Committee referred to in Article 93 GDPR. The three main EU legal acts on data protection: the GDPR, the LED and Regulation 2018/1725 all refer to this committee in their provisions. As of July 2024, the Article 93 Committee held 22 meetings.[34]

The comitology procedure shall be seen as an attempt to put in place a control mechanism over the Commission's actions when it implements EU law, in particular in light of its constantly increasing competence. The aim of the comitology is protecting the interests of the Member States. At the same time, **the Commission executes a relatively high level of influence over the committees' works**, in particular by chairing the meetings, setting the timeframe for the committees' activities and preparing agendas for the meetings. The role of the committees is to assess drafts prepared by the Commission; thus, by assisting in their works, **the Commission is assisting in the assessment of its own proposals**. During the GDPR negotiations not only the European Parliament but also Member States criticized the scope of powers granted to the Commission in the GDPR proposal.[35] Although the co-legislators limited some of the Commission's powers foreseen in the initial GDPR draft, this did not affect adequacy. The issue of the comitology in adequacy decisions was briefly discussed between the European Parliament and the EU Council, with the Parliament suggesting to have adequacy decisions adopted in the form of delegated acts.[36] However, in the final text the co-legislators kept the approach known from Directive 95/46/EC.

2.3. RULES GOVERNING THE ARTICLE 93 COMMITTEE

The Article 93 Committee applies the examination procedure referred to in Article 5 Regulation 182/2011 – in certain situations, it is also able to apply the

[33] See the European Commission's website on this comitology procedure. Available from: https://ec.europa.eu/transparency/comitology-register/screen/committees/C27000/consult?lang=en [Accessed 1 July 2024].

[34] Ibid.

[35] Note from General Secretariat to Working Group on Information Exchange & Data Protection, Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (18 July 2012). Available from: http://www.statewatch.org/news/2012/jul/eu-council-dp-reg-ms-positions-9897-rev2-12.pdf [Accessed 1 July 2024].

[36] Position of the European Parliament adopted at first reading on 12 March 2014 with a view to the adoption of Regulation (EU) No .../2014 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A52014AP0212 [Accessed 1 July 2024].

emergency procedure. In accordance with Article 5(1) Regulation 182/2011 and Article 4(1) of its Rules of Procedure, the opinions of the Committee shall be adopted by a qualified majority.[37] If the committee delivers a positive opinion, the Commission is obliged ("shall") to adopt the draft implementing act; in case of a negative opinion, the Commission cannot ("shall not") adopt the draft implementing acts, and in case of a "no opinion", i.e. a situation where none of the options got the required number of votes, the Commission has the choice to decide ("may") whether to adopt it or not. In practice, an abstention by a committee member has a similar effect to a vote against, as it counts towards the *quorum* but not towards the qualified majority, which is required for a draft implementing act to be adopted. Where the opinion of the committee is positive (i.e. a qualified majority of Member States voted in favour of the adoption of an implementing act), the Commission shall adopt the draft implementing act. In accordance with Article 4(3) of the Committee's rules of procedure, it is possible to issue a positive opinion by consensus, i.e. without a formal vote. For example, this was the case when the committee was deciding on the level of protection of personal data afforded by Japan.[38]

If the opinion of the committee is negative (i.e. a qualified majority of Member States opposed the adoption of the implementing act), the Commission shall not adopt the draft act. **The Article 93 Committee, therefore, has the power to prevent the Commission from issuing an implementing act**. In such a case, if the Commission deems an implementing act necessary, the chair of the committee, i.e. the Commission, may submit a revised version of the draft implementing act within two months of the negative opinion or submit a draft implementing act to the appeal committee for further discussion within one month of the delivery of such an opinion.[39]

---

[37] Article 16(4) of the Treaty on European Union stipulates that, as of 1 November 2014, a qualified majority shall be defined as at least 55 % of the members of the Council, comprising at least fifteen of them and representing Member States comprising at least 65 % of the population of the Union. A blocking minority must include at least four Council members, failing which the qualified majority shall be deemed attained.

[38] According to the report of the Committee meeting of 15 January 2019, the Committee delivered a positive opinion on the implementing measure by consensus. See: European Commission, Comitology Register, Minutes of the fifth meeting of the Committee on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available from: `https://ec.europa.eu/transparency/comitology-register/screen/documents/060401/1/consult?lang=en` [Accessed 1 July 2024].

[39] With respect to adequacy decisions, the Commission has never triggered an appeal procedure. For more information about this procedure see Tosoni, L. (2019) Commentary on Article 93. In Kuner, C., Bygrave, L.A., Docksey, C., *The EU General Data Protection Regulation (GDPR). A Commentary*. New York: Oxford Academics, pp. 1285-1286.

Where the committee delivers no opinion, i.e. where no qualified majority has been obtained either in favour of or against the draft implementing act, the Commission may adopt the act or submit a revised new version thereof. However, in accordance with Article 5(4)(c) of Regulation 182/2011, the Commission may not adopt a draft implementing act where a simple majority of the committee members has objected to its adoption. Where an implementing act is deemed to be necessary, the chair may either submit an amended version of that act to the same committee within 2 months of the vote, or submit the draft implementing act within 1 month of the vote to the appeal committee for further deliberation.

The chair may use the written procedure to obtain the opinion of the committee, in particular where the draft implementing act has already been the subject of its deliberations. This procedure is convenient for the Commission, as - in line with Article 3(5) of Regulation 182/2011 - in such a case it is assumed that any member of the committee who does not oppose or expressly abstain from voting on the draft implementing act before the expiry of the prescribed period gives their tacit agreement with regard to the draft implementing act. In the course of the work of the Article 93 Committee, the written procedure was used e.g. to assess the adequacy of UK law – both under the GDPR and the LED,[40] when issuing an opinion on a new set of standard contractual clauses[41] or more recently - to vote on the EU-U.S. Data Privacy Framework.[42] The Article 93 Committee may also apply the emergency procedure referred to in Article 8 Regulation 182/2011, which concerns immediately applicable implementing acts. This procedure will only apply in the situation referred to in Article 45(5) GDPR, i.e. where available information reveals that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection.

[40] See Comitology Register, Written vote on the draft Commission Implementing Decisions on the adequate protection of personal data by the United Kingdom pursuant to Regulation (EU) 2016/679 and pursuant to Directive (EU) 2016/680. Available from: https://ec.europa.eu/transparency/comitology-register/screen/meetings/CMTD\%282021\%291032/consult?lang=en [Accessed 1 July 2024].

[41] See Comitology Register, Written vote on Draft Implementing Decision on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 and Article 29(7) of Regulation (EU) 2018/1725 and on Draft Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679. Available from: https://ec.europa.eu/transparency/comitology-register/screen/meetings/CMTD\%282021\%29817/consult?lang=en [Accessed 1 July 2024].

[42] See Comitology Register, Written vote on the draft adequacy decision on the EU-US Data Privacy Framework. Available from: https://ec.europa.eu/transparency/comitology-register/screen/meetings/CMTD\%282023\%291164/consult?lang=en [Accessed 1 July 2024].

Finally, it should be noted that the Commission's failure to adopt an implementing act or the failure to find a compromise with the Member States is not challengeable before the Court[43] and the Commission cannot be held accountable in this respect.

2.4. FUNCTIONING OF THE ARTICLE 93 COMMITTEE

The Article 93 Committee adopted the Rules of Procedure at its meeting on 21 September 2018.[44] As mentioned above, it is composed of one representative from each EU Member State,[45] who are accountable to their respective Member States and bound by the instructions agreed upon at the national level. Therefore, **members of the committee, even if they are experts in the field of data protection, cannot be considered independent in their actions**. The Secretariat of the Committee is provided by the European Commission – the Directorate-General for Justice and Consumers (DG JUST) and chaired by a Commission official. The Commission drafts minutes from the Committee's meetings (Rule 10 of the Committee's rules of procedure). Members of the committee shall have the right to request their position to be recorded in the minutes. The Chair shall also be responsible for drawing up summaries of each meeting for the Commission's register of the work of all committees **- these summaries constitute the only publicly available record of the committee's activities**. Importantly, they do not state the individual position

[43] Dordi, C., Forganni, A. (2003) The Comitology Reform in the EU: Potential Effects on Trade Defence Instruments, *Journal of World Trade*, 47 (2), p. 370.

[44] In comparison to the Rules of Procedure of the Article 31 Committee, the new rules introduce several important changes:

1. Article 2 (2)(b) RoP: Committee members removed the written form requirement for new items to be added by them to the meetings' agendas. In practice, this should allow for a possible change of a meeting agenda even just before the start of a committee meeting, which was not possible under the Rules of Procedure of the Article 31 Committee;
2. Article 3(1) RoP: Committee members clarified that substantial modifications of the draft implementing acts that require in-depth analysis, such as draft adequacy decisions, should be submitted no later than three calendar days before the date of the meeting during which they will be discussed. This provision is intended to prevent the Commission from sharing new versions of documents just before the meetings and to provide Member States with sufficient time to assess the documents submitted by the Commission;
3. Article 7 (1) RoP: Committee members added the provision on inviting representatives of Iceland, Norway, Liechtenstein and Switzerland to the meetings of the Article 93 Committee.

[45] In accordance with Article 5(1) of the Committee's rules of procedure, each Member State shall be treated as one member of the Committee. In addition to representatives of the EU Member States, representatives of Iceland, Liechtenstein and Norway are also invited to attend the meetings of the Committee.

of each Member State. **There is no written justification for the committee's decision and no explanation of the reasoning behind its actions**.

The committee meets in Brussels (during the COVID-19 pandemic and also more recently it held several meetings remotely). The Commission shares an invitation, agenda and draft implementing act with Member States no later than fourteen calendar days before the date of the meeting. It is important to emphasise the need for the Commission to comply with these requirements – in the case of comitology procedure, failure to comply with "essential procedural requirements" may lead to invalidity of the implementing act.[46] The Commission drafts meeting agendas; it convenes meetings of the committee either on its own initiative or at the request of a simple majority of the members of the committee.

In accordance with Article 3(3) Regulation 182/2011, the committee shall deliver its opinion on the draft implementing act within a time limit set by the chair, according to the urgency of the matter. The time limits should be proportionate and enable the members of the committee to examine the draft implementing act in an early and effective manner and to express their views. It should be stressed that **Member States are not involved in the preparation of draft implementing acts, including draft adequacy decisions**. In the case of adequacy, this means that the assessment of a third country's legal system and drafting of the implementing act are conducted solely by the Commission. Once the draft is shared with the Member States, within the comitology procedure, they are allowed to propose changes to it. However, **these changes need to be accepted by the Commission - as it is the Commission that decides on the shape of the document it puts to the vote**. This situation leads to the question of what constitutes the actual content of the committee's opinion. In Case T-254/99 the Commission argued that a committee's opinion does not consist in a text, but only in a vote on the measure, merely 'yes' or 'no'.[47] Assuming this interpretation is correct; it confirms the limited role played in practice by Member States in the whole procedure and the strong position of the European Commission.

3. WE KNOW THAT WE DO NOT KNOW ANYTHING (ABOUT PENDING ADEQUACY DECISIONS)

Draft adequacy decisions are prepared solely by the Commission. It is Commission's competence and not an obligation to issue them. Civil society,

[46] See Tosoni, L. (2019) op.cit., p. 1280. See also Judgment of the Court of Justice of 20 September 2017, C-183/16 P, *Tilly-Sabco SAS*, ECLI:EU:C:2017:704, paragraph 114.

[47] See Judgment of 12 March 2003, Case T-254/99 Maja Srl v Commission of the European Communities, ECLI:EU:T:2003:67, paragraph 67.

Member States, the EU Council and the European Parliament lack not only access to specific documents on the basis of which the adequacy was assessed but also some basic information about, for example, the methodology used and the way the Commission determines its priorities. Moreover, they learn about a possible new adequacy decision only when a relevant draft implementing act is made public in order to be sent by the Commission to Member States. The lack of transparency seems to be a conscious choice of the Commission, which on one hand, protects the EU decision-making process, but on the other - **limits the Commission's accountability** to the level that seems difficult to accept when taking into account the European Union's aspiration as a global standard setter in the area of data protection, as well as potential risks for data subjects' rights if the Commission's assessment is incorrect.

We lack information about which states were subject to the evaluation by the Commission, when the Commission ordered relevant studies on third countries, and what are the strategic priorities. For example, in its 2017 document, the Commission mentioned adequacy negotiations with India and Latin America, in particular Mercosur.[48] The most recent communication from the Commission mentions Kenya and Brazil.[49] For the first time, it mentions negotiations with an international organisation - the European Patent Organisation.[50] What is the status of negotiations with India and Mercosur countries other than Brazil? When did the Commission launch negotiations with Kenya? When the Commission engaged in negotiations with international organisations? Nobody knows the answers to these rather basic questions, as **there is no public information on these matters**. Moreover, there is no reporting obligation on the Commission in this regard. In addition, the Commission's strategy regarding adequacy decisions remains unclear, all we know, based on facts, is that the EU prioritised US adequacy,[51] at the same time marginalising some other topics, such as the adequacy of international organisations or the adequacy of EU neighbouring countries, including, for example, Ukraine. Why this is happening and what

[48] European Commission, Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, COM/2017/07 final, point 3.1. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM\%3A2017\%3A7\%3AFIN` [Accessed 1 July 2024].

[49] European Commission, Communication from the Commission to the European Parliament and the Council, Second Report on the application of the General Data Protection Regulation, COM(2024) 357 final, Brussels, 25 July 2024, p. 20. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM\%3A2024\%3A357\%3AFIN` [Accessed 1 July 2024].

[50] Ibid., p. 21.

[51] By issuing three consecutive adequacy decisions for EU-U.S. transfer schemes - i.e. Safe Harbour, Privacy Shield, Data Privacy Framework.

are the exact reasons behind it - we do not know, as all decisions remain at the discretion of the European Commission. In this context, broader transparency would allow Member States or the European Parliament to have more impact on the Commission's priorities. The dissatisfaction with the current model has been reflected in official documents. In its contribution to the GDPR evaluation, the Council "invites the European Commission to increase the transparency of its assessment process and present a comprehensive and coherent strategy for future adequacy decisions".[52] Similar comments were made for example by Kuner, who points out that "[t]he secretive nature of such [adequacy - MC] negotiations, together with the fact that adequacy decisions are based on legal studies that are never made public, illustrates the lack of transparency surrounding much data transfer regulation".[53] Analysis of the few available documents may lead to a conclusion that there seems to be no strategy regarding adequacy decisions, and the priorities seem to constantly change and evolve. The negotiations, of course, require involvement from the third state, something the EU has no control over. At the same time, making the Commission plans public would impose pressure on governments of such third countries, e.g. from a side of businesses interested in free flows of data with the EU. Finally, another argument in favour of higher transparency could be the fact that **the assessment conducted by the Commission is not always correct and could benefit from increased scrutiny**. The Commission not only does not publish any documents but also has never made public information about the methodology it relies on. Taking into account that out of thirteen adequacy decisions issued under Directive 95/46 /EC, the Court of Justice invalidated two, this puts the invalidation ratio at 15%. It is not only academics, who point out at mistakes made by the Commission in the Safe Harbour and Privacy Shield's adequacy assessment process,[54] for example, in his opinion in case Case C-311/18 Schrems II, Advocate General Saugmandsgaard Øe

[52] European Commission, Communication from the Commission to the European Parliament and the Council, Second Report on the application of the General Data Protection Regulation, COM(2024) 357 final, Brussels, 25.7.2024, p. 19. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM\%3A2024\%3A357\%3AFIN` [Accessed 1 July 2024].

[53] Kuner, C. (2024) International data transfers and the EDPS: current accomplishments and future challenge [in:] Van Alsenoy B. et al. (eds.), *Two decades of personal data protection. What next? EDPS 20th Anniversary*, Luxembourg: Publications Office of the European Union, p. 90.

[54] Cohen, N. (2015) The Privacy Follies: A Look Back at the CJEU's Invalidation of the EU/US Safe Harbor Framework. *European Data Protection Law Review*, 240 (3), p. 243.

presented a very detailed critique of the analysis of the Privacy Shield mechanism conducted by the Commission.[55]

4. ON THE NEED FOR A DEDICATED PROCEDURE FOR ASSESSING ADEQUACY

4.1. ARE IMPLEMENTING ACTS SUITABLE FOR ADEQUACY DECISIONS?

Formally, adequacy findings are decisions based solely on the objective assessment of a specific legal regime and take into account criteria established in Article 45(2) GDPR and Article 36(2) LED; in practice, however, they nowadays became also political decisions. Therefore, some reflection might be needed on the future of the adequacy procedure; in particular, what is the role of politics in it. If we conclude that the procedure is political, this would put the whole mechanism in question and place it beyond Article 16 TFEU - the GDPR's legal basis. On the other hand, the conclusion that the adequacy decisions are not purely technical but have a political component could **justify the higher level of scrutiny over the Commission's actions by both Member States and the European Parliament**. Currently, the European Parliament and the EU Council may challenge Commission only if they believe that a draft implementing act exceeds the implementing powers provided for in the GDPR.[56] Max Schrems, when commenting on the invalidation of the Safe Harbour and what happened next, stated that "[f]irst, I would like to voice my frustration with the weakness of the political level in the European Commission that lead to the absolutely laughable proposal for a new EU-US data sharing agreement called 'Privacy Shield'",[57] therefore making it clear that in his opinion the adequacy procedure was a political process in which the Commission made concessions towards the US. The view that adequacy decisions constitute a political instrument, among others influenced by economic relations and commercial interests, was expressed by

[55] Opinion of Advocate General Saugmandsgaard Øe delivered on 19 December 2019. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Case C-311/18, paragraph 196-342.

[56] In line with Article 11 Regulation 182/2011 "[w]here a basic act is adopted under the ordinary legislative procedure, either the European Parliament or the Council may at any time indicate to the Commission that, in its view, a draft implementing act exceeds the implementing powers provided for in the basic act. In such a case, the Commission shall review the draft implementing act, taking account of the positions expressed, and shall inform the European Parliament and the Council whether it intends to maintain, amend or withdraw the draft implementing act".

[57] Schrems, M. (2016) The Privacy Shield is a Soft Update of the Safe Harbor. *European Data Protection Law Review*, 2(2), p. 148.

authors such as Greenleaf,[58] Wolf[59] and Panek.[60] The Commission's view on adequacy decisions that "[b]y enabling the free flow of personal data, these decisions have opened up commercial channels for EU operators, including by complementing and amplifying the benefits of trade agreements, and eased collaboration with foreign partners in a broad range of fields, from regulatory cooperation to research"[61] puts adequacy decisions in **the context that goes beyond data protection**. As I have already mentioned, the political dimension of the adequacy decisions can be also observed in cases where a decision is followed by a trade agreement, which includes provisions on data transfers.

Since the adoption of Directive 95/46/EC, the EU data protection framework has evolved and its importance increased. The EU Council has recently stated that "the GDPR has been instrumental in positioning the European Union as an international benchmark and reference standard for data protection and privacy beyond EU borders".[62] From the fundamental rights perspective, the verification of whether a third country's legal order meets this benchmark should be based solely on impartial criteria, and while politicians may take certain strategic decisions, we have to make sure that the process of assessing adequacy "on the ground" is objective, conducted by experts and protected from any external influence. This brings us to the issue of the lack of transparency embedded in the current model of assessing adequacy. **The sole actor in charge of the whole adequacy mechanism is the European Commission,** and as described above, this mechanism does not provide tools that would allow Member States to influence the Commission's actions in a meaningful way. If we conclude that adequacy decisions, while requiring certain objective criteria to be met, became also

[58] Greenleaf, G. (2000) Safe Harbor's low benchmark for 'adequacy': EU sells out privacy for US$. *Privacy Law and Policy Reporter*, 32.

[59] Wolf, C. (2014) op.cit., p. 241-242.

[60] Panek, W. (forthcoming) The European Commission's adequacy decisions' content as a guide for applying the adequacy assessment criteria, [in:] Hoepman, J.H., Jensen, M., Porcedda, M.G., Schiffner, S., Ziegler, S., (eds.). *Privacy Symposium 2024 - Data Protection Law International Convergence and Compliance with Innovative Technologies (DPLICIT)*. Cham: Springer Nature Switzerland. Available from: `https://kau.app.box.com/s/jn8zb7ntesoafs1rqm6igt9tljfu1k5x` [Accessed 1 July 2024].

[61] European Commission, Communication from the Commission to the European Parliament and the Council, Second Report on the application of the General Data Protection Regulation, COM(2024) 357 final, Brussels, 25 July 2024, p. 20. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM\%3A2024\%3A357\%3AFIN` [Accessed 1 July 2024].

[62] EU Council, Council position and findings on the application of the General Data Protection Regulation (GDPR), adopted on 17 November 2023, document 15507/2, point 16. Available from: `https://data.consilium.europa.eu/doc/document/ST-15507-2023-INIT/en/pdf` [Accessed 1 July 2024].

a political instrument, then the argument that they should be granted *via* a separate, dedicated procedure **becomes much stronger**.

4.2. TOWARDS RETHINKING OF THE CURRENT ADEQUACY PROCEDURE

The lack of transparency regarding the Commission's actions in the area of data transfers may give reasons to worry - we do not know with which third countries or international organisations the Commission is engaged in talks, we do not know the status of these talks, we do not know what are the Commission's plans and strategy as regards adequacy decisions. At the same time, we see growing concerns from academics[63] and NGOs[64] regarding the way the Commission is handling these matters. One of the ways of improving the current adequacy procedure could be **a separate regulation on data transfers, a *lex specialis* to the GDPR and the LED, similar to the Commission's proposal on harmonisation of the GDPR enforcement procedures**.[65] A dedicated procedure could allow, among others, to enhance transparency of the Commission's actions as well as to increase its accountability, e.g. by specifying the elements the Commission needs to take into account when conducting its assessments, introducing certain reporting obligations, increasing transparency of the procedure and imposing deadlines. It could also balance the Commission's role and allow for it to be held accountable by Member States or the European Parliament. Currently, the Member States scrutinize the Commission's work *via* a comitology procedure. However, as described above, **this mechanism does not provide tools that would allow Member States to influence the Commission's actions in a meaningful way**. The role of the European Parliament is limited to non-binding resolutions it can adopt. The discussion about the adequacy procedure is not new. The lack of a detailed procedure for adequacy decisions was criticised already during the GDPR negotiations.[66] Schweighofer argues that in order to address

[63] "The EU has focused disproportionately on data transfers to US companies and law enforcement authorities, and neglected other important strategic issues, such as how EU data transferred to authoritarian and non-democratic countries can be protected" Kuner C., International data transfers and the EDPS: current accomplishments and future challenge [in:] Van Alsenoy B. et al. (eds.), *Two decades of personal data protection. What next? EDPS 20th Anniversary*, Luxembourg: Publications Office of the European Union, p. 89.

[64] EDRi European Digital Rights, et. al. (2024) op. cit.

[65] See Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, COM/2023/348 final. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A52023PC0348` [Accessed 1 July 2024];

[66] "[t]he Draft GDPR does not discuss the logistics of how adequacy decisions are to be issued" Weber, R. H. (2013) Transborder data transfers: concepts, regulatory approaches and new legislative initiative, *International Data Privacy Law*, 3(2), p. 130.

the shortcomings, adequacy decisions should be replaced by international treaties signed by the EU.[67] However, this approach would result in replacing a non-transparent procedure with secret negotiations.

The importance of adequacy decisions has significantly increased since the early 1990s, i.e., the time when the procedure was drafted. At the same time, assessing adequacy still remains highly non-transparent. Given the importance of data transfers for society, the current model of assessing adequacy seems not to be sustainable and futureproof. The Commission makes decisions on the adequacy of third countries, which bear significant legal implications and affect the EU citizens' fundamental rights, behind closed doors. We all learn about new draft adequacy decisions only at the very moment the Commission makes them public ahead of sending the drafts to Member States. There are no updates regarding the status of ongoing works or even a list of states with which the Commission is currently negotiating the decisions. There are no deadlines for the Commission, no milestones, no body towards which it could be held accountable. In light of the above, the question that needs to be asked is whether matters of such importance as adequacy decisions, which have broad impacts on the EU citizens' fundamental rights, should be decided in the procedure that is currently in place. This question is even more relevant if we consider the length of the actual assessment procedure and the fact that the Commission granted adequacy to two transfer mechanisms, the Safe Harbour and the Privacy Shield, which did not meet the EU requirements and were subsequently invalidated by the CJEU.

We are dealing with a procedure where the **first phase** consists of non-transparent negotiations with third countries conducted by the Commission. As I have pointed out, it is already difficult to establish with which countries the Commission engages in talks - the lack of transparency reached the level where, without any explanation, the Commission stops mentioning in its documents certain states that it had mentioned previously as being assessed. The **second phase** consists of an actual assessment and preparations of a draft adequacy decision - both done in secrecy by the Commission. These are followed by the **third phase**, which is a non-transparent comitology procedure. The only publicly available assessment of draft adequacy decisions comes from the European Data Protection Board and its opinions. This situation should make us ask several questions. In the first place, we should ask ourselves why adequacy

[67] Schweighofer, E. (2017) Principles for US–EU Data Flow Arrangements [in:] Svantesson, D.J.B., Kloza, D. (eds.), *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*, Cambridge: Intersentia, pp. 44-46.

decisions are adopted *via* implementing acts. **The comitology procedure was chosen by the EU co-legislators more than 30 years ago** and was aimed at addressing different issues than the ones we are facing nowadays, such as how to ensure a harmonised approach inside the EU and how to guarantee that all Member States will recognise adequacy decisions adopted under Directive 95/46/EC. These were the challenges of the first years of the EU data protection laws, resolved a long time ago. In the meantime, the world has moved forward, data protection as an area of law has significantly developed and its importance has increased beyond the level the authors of Directive 95/46/EC could foresee.

Today we have mechanisms alternative to comitology aimed at achieving harmonisation on the EU level; in the case of the GDPR let me just mention the guidelines and recommendations of the EDPB, which are followed by all the EU data protection authorities. The EDPB recommendations on supplementary measures, developed in the aftermath of Schrems II judgment and applicable in all the EU Member States, could serve as an example of such soft-law harmonisation.[68] As regards Member States and the European Parliament, the information they receive is limited to two documents. When sending the draft implementing act to the Article 93 Committee, the Commission is obliged to share it with the European Parliament and the EU Council.[69] However, this obligation does not apply to any revisions of the initial text. Therefore, the Commission shares with the Parliament and the EU Council **only the first and the final version of the implementing act**. This means that both institutions lack information about drafting suggestions made during the comitology phase that were not included in the final document, which could for example help them in identifying the most problematic issues. While in practice Member States can receive relevant information from their representatives in the Article 93 Committee, the Parliament has no means of obtaining it.

When it comes to the Article 93 Committee, for almost thirty years, **the activities of it and its predecessor, the Article 31 Committee, have always been shrouded in secrecy**. Taking into account the significance of transfers of personal data to third countries, I argue that there is a need for a separate

[68] European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Available from: `https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en` [Accessed 1 July 2024].

[69] See Article 10(5) Regulation 182/2011. The Commission also shares the draft adequacy decision with the European Data Protection Board and asks it to issue an opinion (see Article 70(1)(s) GDPR).

discussion regarding the committee's role, to be conducted together with the discussion about the role and accountability of the European Commission.

5. CONCLUSION

With the entry into force of Directive 95/46/EC, the EU based its approach toward data transfers outside the Union on adequacy decisions,[70] unilateral acts of the Commission, issued in the form of implementing acts. This model was subsequently copied into the GDPR and the LED. Since the very beginning, the adequacy procedure involves a comitology phase in which a committee consisting of representatives of Member States expresses its opinion about the Commission's draft implementing act. As mentioned above, what makes the difference between opinions issued by the Article 93 Committee and the EDPB opinions or resolutions of the European Parliament is that the opinions of the committee are binding for the Commission. At the same time, in principle, they are limited to a vote on a draft decision, either "yes" or "no", which significantly reduces their impact.

The Commission would be in favour of keeping the *status quo* as the current procedure puts its actions beyond the scope of any meaningful scrutiny. The Commission plays a crucial role in the works of the Article 93 Committee by (i) conveying and chairing the meetings, (ii) providing its secretariat, (iii) setting the timeframe for the committee's activities, (iv) preparing agendas for the meetings; (v) deciding on the final wording of documents put to the vote; and (vi) deciding on when these documents will be voted. **As regards the adequacy procedure, the Commission is dominating it at every and each of its stages**, as it: (i) engages in negotiations with a third country; (ii) conducts the initial assessment of a third country's legal regime and prepares a draft adequacy decision, (iii) participates in the works of the EDPB, when the Board is drafting an opinion on the draft decision,[71] (iv) is in charge of the comitology procedure that has to approve the draft decision. At the same time, the Commission is not impartial in this process and cannot be seen as an honest broker, as it is defending its own draft decision.

Since the early 90s of the past century, technological progress and globalisation changed the world, and the role of adequacy decisions has

[70] See European Commission, Adequacy decisions How the EU determines if a non-EU country has an adequate level of data protection. Available from: `https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en` [Accessed 1 July 2024].

[71] In line with Article 68(5) GDPR: "The Commission shall have the right to participate in the activities and meetings of the Board without voting rights. The Commission shall designate a representative. The Chair of the Board shall communicate to the Commission the activities of the Board".

significantly increased. More than 30 years later**, it is the right time to rethink the current model**. I argue that adequacy, designed as a technical process, evolved into **a tool in which politics, including economic relations and commercial interests, play an increasingly important role**. This goes against the concept of comitology, the legitimacy of which is built on denying the political nature of what is delegated.[72] In the adequacy context, such a situation may create risks for data subjects' rights. If the adequacy is based on a Commission's assessment, which is incorrect or politically motivated, it might be undermining the protection of the EU's fundamental rights.

In a digitalised and globalised environment, fostering cross-border data flows is of key importance for the European Union. The Commission itself recognises the growing significance of adequacy decisions. In the evaluation of eleven decisions issued under Directive 95/46/EC, the Commission states that "[o]ver the past decades, the importance of adequacy decisions has increased considerably as data flows have become an integral element of the digital transformation of the society and the globalisation of the economy. (...) In that context, adequacy decisions play an increasingly key role, in many ways".[73] Furthermore, the European Union is extending the reach of its data protection standards in parallel with international trade agreement negotiations. Adequacy decisions nowadays serve a purpose, which goes beyond the protection of personal data and Article 16 TFEU. The fact that the adequacy decisions are not purely technical but have a political aspect, could justify the higher level of scrutiny over Commission actions by both Member States and the European Parliament.

Improving the adequacy procedure requires higher transparency, accountability and establishing the EU strategy for data transfers. A departure from the comitology model would be beneficial for the EU and protection of data subjects' rights. It would allow us to have a clearer idea of how decisions are being taken and what are the EU's priorities. We would also be able to hold the Commission accountable for the progress made (or the lack of it) and understand why certain negotiations with third countries did not succeed or are not anymore mentioned in the official Commission's documents. It could also facilitate negotiations with third countries - for example, information about the methodology used by the Commission would make it easier for them to engage in negotiations with the EU, as

[72] Robert, C. (2019) op.cit., p. 16.

[73] European Commission, Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC, COM(2024) 7 final. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A52024DC0007`[Accessed 1 July 2024], p. 2.

they would know what to expect. We also need to discuss whether at all, and if so, to what extent the process of assessing adequacy may take into account politics, including economic relations, and go beyond the objective analysis of a third country or international organisation's legal regime. This discussion is necessary not only in the context of trade agreements but also third countries establishing their own adequacy mechanisms under which they grant adequacy to the EU. The emergence of adequacy mechanisms competing with the EU model and being more efficient than it or initiatives such as APEC CBPR should also trigger discussion about the length of the current EU procedure.

The way forward could be **a separate legal act specifying the procedure for granting adequacy decisions**. The Commission itself already set a precedent for such a solution, as the EU co-legislators are currently negotiating legislation aimed at improving another procedure -the GDPR enforcement in cross-border cases.[74] As the first step, the discussion could focus on what can be achieved without re-opening the GDPR and the LED, for example, on specifying the elements the Commission needs to take into account when conducting its assessments, introducing certain reporting obligations, increasing transparency of the procedure and imposing deadlines. It could also balance the Commission's role and allow for it to be held accountable by Member States or the European Parliament. A temporary solution could be a number of voluntary commitments by the Commission. These could in particular cover transparency of the adequacy procedure, including publication of documents on which the assessments are based, an up-to-date list of third countries, with which the Commission is engaged in negotiations and presenting the Commission's adequacy strategy.

LIST OF REFERENCES

[1] Asia-Pacific Economic Cooperation, APEC Privacy Framework. Available from: https://www.apec.org/publications/2005/12/apec-privacy-framework [Accessed 1 July 2024];

[2] Cohen, N. (2015) The Privacy Follies: A Look Back at the CJEU's Invalidation of the EU/US Safe Harbor Framework. *European Data Protection Law Review*, 240 (3);

[3] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 Apr. 2016 on the protection of natural persons with regard to the

[74] Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, COM/2023/348 final. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A52023PC0348 [Accessed 1 July 2024];

processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119/89. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A32016L068 [Accessed 1 July 2024];

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31. Available form: https://eur-lex.europa.eu/eli/dir/1995/46/oj [Accessed 1 July 2024];

[5] Dordi, C., Forganni, A. (2003) The Comitology Reform in the EU: Potential Effects on Trade Defence Instruments. *Journal of World Trade*, 47 (2);

[6] Drechsler, L. (2020) Comparing LED and GDPR Adequacy: One Standard Two Systems, *Global Privacy Law Review*, 1(2);

[7] Drechsler, L., Kamara, I. (2022) Essential equivalence as a benchmark for international data transfers after Schrems II, Kosta, E. and Leenes, R. (eds), *Research Handbook on EU data protection law*. Cheltenham/Northampton: Edward Elgar Publishing 2022;

[8] Drechsler, L., Matsumi, H. (2024) Caught in the middle: the Japanese approach to international personal data flows. *International Data Privacy Law*, 14(2);

[9] EDRi European Digital Rights, Access Now, Politiscope, Homo Digitalis, IT-Pol Denmark, Bits of Freedom, European Sex Workers' Rights Alliance - ESWA, Statewatch, Vrijschrift.org, Amnesty International, SHARE Foundation, Concerns Regarding European Commission's Reconfirmation of Israel's Adequacy Status in the Recent Review of Adequacy Decisions, a letter sent on 22 April 2024. Available from: https://edri.org/wp-content/uploads/2024/04/Concerns-Regarding-European-Commissions-Reconfirmation-of-Israels-Adequacy-Status-in-the-Recent-Review-of-Adequacy-Decisions-updated-open-letter-April-2024.pdf [Accessed 1 July 2024];

[10] EU Council, Council of the EU, EU-Japan: the Council approves a protocol to facilitate free flow of data, Press release, 29 April 2024. Available from: https://www.consilium.europa.eu/en/press/press-releases/2024/04/29/eu-japan-the-council-approves-a-protocol-to-facilitate-free-flow-of-data/ [Accessed 1 July 2024];

[11] EU Council, Council position and findings on the application of the General Data Protection Regulation (GDPR), adopted on 17 November 2023, document

15507/2. Available from: https://data.consilium.europa.eu/doc/document/ST-15507-2023-INIT/en/pdf [Accessed 1 July 2024];

[12] European Commission, Adequacy decisions How the EU determines if a non-EU country has an adequate level of data protection. Available from: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_ [Accessed 1 July 2024];

[13] European Commission, Comitology Register, Minutes of the fifth meeting of the Committee on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available from: https://ec.europa.eu/transparency/comitology-register/screen/documents/060401/1/consult?lang=en [Accessed 1 July 2024];

[14] European Commission, Comitology Register, Written vote on Draft Implementing Decision on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 and Article 29(7) of Regulation (EU) 2018/1725 and on Draft Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679. Available from: https://ec.europa.eu/transparency/comitology-register/screen/meetings/CMTD\%282021\%29817/consult?lang=en [Accessed 1 July 2024];

[15] European Commission, Comitology Register, Written vote on the draft adequacy decision on the EU-US Data Privacy Framework. Available from: https://ec.europa.eu/transparency/comitology-register/screen/meetings/CMTD\%282023\%291164/consult?lang=en [Accessed 1 July 2024];

[16] European Commission, Comitology Register, Written vote on the draft Commission Implementing Decisions on the adequate protection of personal data by the United Kingdom pursuant to Regulation (EU) 2016/679 and pursuant to Directive (EU) 2016/680. Available from: https://ec.europa.eu/transparency/comitology-register/screen/meetings/CMTD\%282021\%291032/consult?lang=en [Accessed 1 July 2024];

[17] European Commission, Commission Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security /* COM/90/314FINAL */, 13 September 1990. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM\%3A1990\%3A0314\%3AFIN [Accessed 1 July 2024];

[18] European Commission, Commission Staff Working Document accompanying the document: Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decision for Japan' SWD (2023) 75 final, 3 April 2023. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A52023SC0075 [Accessed 1 July 2024];

[19] European Commission, Communication from the Commission to the European Parliament and the Council, Exchanging and Protection Personal Data in a Globalised World, COM(2017) 7 final. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM\%3A2017\%3A7\%3AFIN [Accessed 1 July 2024];

[20] European Commission, Communication from the Commission to the European Parliament and the Council, Second Report on the application of the General Data Protection Regulation, COM(2024) 357 final, Brussels, 25 July 2024. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM\%3A2024\%3A357\%3AFIN [Accessed 1 July 2024];

[21] European Commission, Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC, COM(2024) 7 final. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A52024DC0007[Accessed 1 July 2024];

[22] European Commission, What the European Commission does in law. Available from: https://commission.europa.eu/about-european-commission/role-european-commission/law_en [Accessed 1 July 2024];

[23] European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Available from: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en [Accessed 1 July 2024];

[24] European Data Protection Board, The EDPB data protection guide for small business, Available from: https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en [Accessed 1 July 2024];

[25] European Parliament, Position of the European Parliament adopted at first reading on 12 March 2014 with a view to the adoption of Regulation (EU) No .../2014 of the European Parliament and of the Council on the protection

of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A52014AP0212 [Accessed 1 July 2024];

[26] Greenleaf, G. (2000) Safe Harbor's low benchmark for 'adequacy': EU sells out privacy for US$. *Privacy Law and Policy Reporter*, 32;

[27] Gulczynska, Z. (2021) A certain standard of protection for international transfers of personal data under the GDPR. *International Data Privacy Law*, 11(4);

[28] Judgment of 12 March 2003, Maja Srl v Commission of the European Communities, Case T-254/99, ECLI:EU:T:2003:67;

[29] Judgment of 16 July 2020 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559;

[30] Judgment of 20 September 2017, Tilly-Sabco SAS, C-183/16 P, ECLI:EU:C:2017:704;

[31] Judgment of 6 October 2015 Maximillian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650;

[32] Kuner, C. (2017) Reality and Illusion in EU Data Transfer Regulation Post Schrems. *German Law Journal*, 18(4);

[33] Kuner, C. (2024) International data transfers and the EDPS: current accomplishments and future challenge [in:] Van Alsenoy B. et al. (eds.), *Two decades of personal data protection. What next? EDPS 20th Anniversary*. Luxembourg: Publications Office of the European Union;

[34] Lindsay, D. (2017) The role of proportionality in assessing trans-atlantic flows of personal data, [in:] Svantesson D.J.B. and Kloza D. (eds.), *Trans-Atlantic data privacy relations as a challenge for democracy*. Cambridge: Intersentia;

[35] Opinion of Advocate General Saugmandsgaard Øe delivered on 19 December 2019. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Case C-311/18, ECLI:EU:C:2019:1145;

[36] Padova, Y., (2016) The Safe Harbour is invalid: what tools remain for data transfers and what comes next? *International Data Privacy Law*, 6(2);

[37] Panek, W. (forthcoming) The European Commission's adequacy decisions' content as a guide for applying the adequacy assessment criteria, [in:] Hoepman, J.H., Jensen, M., Porcedda, M.G., Schiffner, S., Ziegler, S. (eds.), *Privacy Symposium 2024 - Data Protection Law International Convergence and Compliance with Innovative Technologies (DPLICIT)*. Cham: Springer Nature Switzerland. Available from: https://kau.app.box.com/s/jn8zb7ntesoafs1rqm6igt9tljfu1k5x [Accessed 1 July 2024];

[38] Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, COM/2023/348 final. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A52023PC0348 [Accessed 1 July 2024];

[39] Regulation (EU) 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers, OJ L 55, 28.2.2011, p. 13–18. Available from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX\%3A32011R0182 [Accessed 1 July 2024];

[40] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88. Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj [Accessed 1 July 2024];

[41] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39–98. Available from: https://eur-lex.europa.eu/eli/reg/2018/1725/oj [Accessed 1 July 2024];

[42] Robert, C. (2019) The political use of expertise in EU decision-making: The case of comitology, *Research Report*. Available from: https://dumas.ccsd.cnrs.fr/SCIENCESPO_LYON/halshs-03021131v1 [Accessed 1 July 2024];

[43] Schrems, M. (2016) The Privacy Shield is a Soft Update of the Safe Harbor. *European Data Protection Law Review,* 2(2);

[44] Schweighofer, E. (2017) Principles for US–EU Data Flow Arrangements. [in:] Svantesson, D.J.B. and Kloza, D (eds.), *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*. Cambridge: Intersentia;

[45] Statewatch, leaked Note from General Secretariat to Working Group. on Information Exchange & Data Protection, Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (18 July 2012). Available

from: http://www.statewatch.org/news/2012/jul/eu-council-dp-reg-ms-positions-9897-rev2-12.pdf [Accessed 1 July 2024];

[46] The White House, Remarks by President Biden and European Commission President Ursula von der Leyen in Joint Press Statement, 25 March 2022. Available from: https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/03/25/remarks-by-president-biden-and-european-commission-president-ursula-von-der-leyen-in-joint-press-statement/ [Accessed 1 July 2024];

[47] Tosoni, L. (2019) Commentary on Article 93 [in:] Kuner, C., Bygrave, L., A., Docksey, C., *The EU General Data Protection Regulation (GDPR). A Commentary*. New York: Oxford Academics;

[48] Treaty on the Functioning of the European Union (consolidated version), O J 115, 09/05/2008 P. 0173 - 0173. Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF [Accessed 1 July 2024];

[49] Voss, W., G. (2020) Cross-border data flows, the GDPR, and data governance. *Washington International Law Journal*, 29(3);

[50] Wagner, J. (2018) The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?, *International Data Privacy Law*, 8(4);

[51] Weber, R. H. (2013) Transborder data transfers: concepts, regulatory approaches and new legislative initiative, *International Data Privacy Law*, 3(2);

[52] Wolf, C. (2014) Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers. *Washington University Journal of Law and Policy*, 227 (43);

MUJLT Official Partner (Czech Republic)

ROWAN LEGAL, advokátní kancelář s.r.o
https://rowan.legal

Cyberspace 2023 Partners

Zákony pro lidi - AION CS
www.zakonyprolidi.cz

ROWAN LEGAL, advokátní kancelář s.r.o
https://rowan.legal

PricewaterhouseCoopers Česká republika
https://www.pwc.com/cz/

Notes for Contributors

Focus and Scope

Masaryk University Journal of Law and Technology (ISSN on-line 1802-5951, ISSN printed 1802-5943) is a peer-reviewed academic journal which publishes original articles in the field of information and communication technology law. All submissions should deal with phenomena related to law in modern technologies (e.g. privacy and data protection, intellectual property, biotechnologies, cyber security and cyber warfare, energy law). We prefer submissions dealing with contemporary issues.

Structure of research articles

Each research article should contain a title, a name of the author, an e-mail, keywords, an abstract (max. 1 500 characters including spaces), a text (max. 45 000 characters including spaces and footnotes) and list of references.

Structure of comments

All comments should contain a title, a name of the author, an e-mail, keywords, a text (max. 18 000 characters) and a list of references.

Structure of book reviews

Each book review should contain a title of the book, a name of the author, an e-mail, a full citation, a text (max. 18 000 characters) and a list of references.

Structure of citations

Citations in accordance with AGPS Style Guide 5th ed. (Harvard standard), examples:

Book, one author: Dahl, R. (2004) *Charlie and the Chocolate Factory*. 6th ed. New York: Knopf.
Book, multiple authors: Daniels, K., Patterson, G. and Dunston, Y. (2014) *The Ultimate Student Teaching Guide.* 2nd ed. Los Angeles: SAGE Publications, pp.145-151.
Article: Battilana, J. and Casciaro, T. (2013) The Network Secrets of Great Change Agents. *Harvard Business Review*, 91(7) pp. 62-68.
Case: *Evans v. Governor of H. M. Prison Brockhill* (1985) [unreported] Court of Appeal (Civil Division), 19 June.
Citation Guide is available from: https://journals.muni.cz/public/journals/36/download/Citationguide.pdf

Formatting recommendations

Use of automatic styles, automatic text and bold characters should be omitted.
Use of any special forms of formatting, pictures, graphs, etc. should be consulted.
Only automatic footnotes should be used for notes, citations, etc.
Blank lines should be used only to divide chapters (not paragraphs).
First words of paragraphs should not be indented.
Chapters should be numbered in ordinary way – example: "5.2 Partial Conclusions".

Submissions

Further information available at
https://journals.muni.cz/mujlt/about

LIST OF ARTICLES