Przemysław Roguski, PhD

THE GEOPOLITICS OF CLOUD COMPUTING

INTRODUCTION

The preceding chapter argued that data is the "new oil" or the "oxygen" of the digital economy. A similar analogy can be applied to cloud computing. Just as the economic value of oil depends on specialised infrastructure for extraction, refining, storage, and transportation, the economic value of data depends on the internet backbone as well as server infrastructure for storage and processing. With this in mind, this chapter will analyse the geopolitics of cloud computing, focusing on the issue of control over cloud infrastructure as well as control over data stored this way. It will argue that cloud service providers (CSPs) have become not only one of the fundamental building blocks of the digital economy, but also play an important geopolitical role and are factors of strategic competition between states.

CLOUD COMPUTING – A BRIEF OVERVIEW

Cloud computing is best defined as "ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources"[1] such as storage, applications and services. It is composed of three service models: Infrastructure as a Service (IaaS), Platform asa Service (PaaS) and Software as a Service (SaaS), offering various degrees of access to infrastructure and software solutions, depending on the customer's needs. Storing data in the cloud and offering cloud-based services has several benefits for the customer. Most notably, companies do not have to maintain their own servers and large departments tasked with running and protecting those servers from cyberattacks, but can draw on resources, software, and expertise provided by CSPs, which, due to economies of scale, can do

so in a financially competitive way. It is therefore no wonder that cloud computing has drawn clients both from the private and public sectors, including whole governmental departments. Cloud computing also has major benefits for the users, who can access their data and applications on the device of their choice over the Internet.

The cloud computing market has been developed – and is still dominated by – three major American tech companies: Amazon (Amazon Web Services), Microsoft (Microsoft Azure), and Alphabet (Google Cloud Platform),[2] who together hold 59% of worldwide market share (estimated at USD 100 billion in 2019), with smaller American operators like IBM and Oracle adding another 8%.[3] Chinese companies are also dynamically expanding their cloud infrastructure, with Alibaba and Tencent being the biggest players.[4] The market is only set to grow: the European Union estimates that between 2018 and 2025 the global data volume will grow five times, from 33 to 175 zettabytes.[5] At the same time, the estimates show that there will be a shift from cloud to edge computing, i.e. distributed data storage and processing on smart connected objects, resulting in 20% of data processing being done through centralised computing facilities (data centres) and 80% through smart connected objects (as opposed to 80% data centres and 20% smart objects in 2018).[6] Nevertheless, even under this scenario the importance of cloud computing will continue to grow.

The main characteristic of cloud computing is data mobility and portability. Data no longer needs to be stored locally. Instead, it can be stored in large server parks operated by cloud storage providers and telecommunications companies and accessed *ad hoc* from any place on earth (provided it has an internet connection) through the web browser or a dedicated application.[7] This gives cloud data four unique characteristics which will be important for our further analysis:

- high mobility of data and ease of transfer over state borders,
- divisibility and partitionability of data, leading to it being stored on servers in multiple locations,
- independence of location, leading to easy remote access, and
- location of data is a business decision of CSPs, unless states impose data localisation rules.[8]

CLOUD COMPUTING AND GEOPOLITICS

Although data is highly mobile and independent of location, the cloud computing market is not free from significant geopolitical considerations, influences, and effects. Both the nationality of cloud service operators and the choice of location for their data centres have significant geopolitical consequences. The first consequence is in terms of technological innovation and business opportunities. Having access to and being able to develop cloud technology gives states and their businesses better chances for faster growth of their digital economies. The location of data centres, while a business decision of the CSPs, usually depends on several key factors, such as the proximity to the internet backbone (favouring proximity to large Internet Access Points), proximity to customers and skilled workforce, security, energy prices, yearly average temperatures (due to cooling demands for the servers), and the legal environment.[9] It is therefore not surprising that most data centres are located in big, internationally connected cities in economically developed states. A strong economy fuels demand for cloud computing capacities, which in turn fuel the growth of the digital economy and attract businesses not only from the state in which a data centre operates but also from neighbouring states. In this way, this technology helps to develop certain locations into regional technological and economic hubs.

The second consequence is in terms of control which a state can exercise over cloud service providers. This is because under international law states have jurisdiction – i.e. the power to set and enforce laws – over persons and objects located on their territory.[10] **This means that states may apply their laws to CSPs operating within their territory as well as to data located on servers within their borders. This fact gives states on whose territory data centres are located a high degree of control over not only their own citizens' data but also data of citizens and foreign entities stored therein**. This degree of control may be important in pursuit of legitimate purposes, such as for instance law enforcement, but may also raise concerns over the privacy as well as security of data transferred to and stored in foreign jurisdictions. These concerns are greater still when a state not only has control over the operations of CSPs within its territory, but can set and enforce rules which affect CSPs' operations worldwide. This is especially the case when cloud service providers, such as the big three Amazon, Microsoft, and Google, are legally domiciled in one country.

THE *MICROSOFT IRELAND* CASE & THE CLOUD ACT

The degree of state control over cloud service providers is perhaps best demonstrated in the *Microsoft Ireland* case. It began in 2013 when federal prosecutors in the Southern District of New York sought and obtained a warrant for the search and seizure of information, including e-mail, stored in a specified account hosted by Microsoft to disclose the contents of a suspect's messages in an investigation related to drug trafficking.[11] Microsoft provided communications metadata stored on servers in the United States, but refused to hand over content data stored on servers in Ireland noting that the Government sought information by means of a warrant under section 2703(a) of the Stored Communications Act (SCA)[12] and arguing that the court does not have authority to issue a warrant for an extraterritorial search.[13] The Magistrate Judge issued the warrant nonetheless, holding that the warrant under section 2703(a) SCA does not implicate issues of extraterritoriality as the recipient of the subpoena is obliged to produce all information in its possession, regardless of its storage, and the "search" of the e-mail content would occur in the United States.[14]

On appeal, the US Court of Appeals for the Second Circuit (CoA) – overseeing Connecticut, New York, and Vermont – reversed the Magistrate's order.[15] The main issue under discussion by the CoA was whether the SCA warrant provisions permit their extraterritorial application,[16] which would be necessary to rebut the so-called presumption against extraterritoriality, which stipulates that a Statute does not have extraterritorial effect unless specifically provided for by Congress.[a] The CoA, after analysing the language of the Stored Communications Act, came to the conclusion that denying the extraterritorial character of the remote access to e-mail content stored on a server in Ireland would mean that such a search would also be possible if the account holder were an Irish citizen and the disclosure would violate Irish law; this, in turn, would open up the United States to foreign governments' reciprocal searches of data stored in the US.[17]

The case eventually found its way to the Supreme Court,[18] but the Supreme Court did not have the chance to decide the case, as Congress passed the Clarifying Lawful Overseas Use of Data Act or CLOUD Act (H.R. 4943) two weeks after the oral hearings and before the Supreme Court had the chance to render a decision.[19] The Act amends the Stored Communications Act by requiring service providers subject to US jurisdiction to produce data under an SCA warrant regardless of the location of the server where the data is stored.[20] To account for the possibility of conflicting legal

a *Morrison v. National Australia Bank Ltd.*, US Supreme Court, 561 U.S. 247, 130 S.Ct. 2869, [online:] https://www.supremecourt.gov/opinions/09pdf/08-1191.pdf; recently re-stated in *RJR Nabisco, Inc. v. European Community*, US Supreme Court, 579 U.S. ___, 136 S.Ct. 2090, [online:] https://www.supremecourt.gov/opinions/15pdf/15-138_5866.pdf.

obligations under the laws of the State where the data is stored, the CLOUD Act creates a mechanism for the electronic communication service providers to challenge the warrant.[21] However, the conditions under which a warrant may be challenged are quite restrictive; to quash the warrant the provider has to reasonably believe and demonstrate that, *first*, the customer whose data is sought is not a United States person and does not reside in the United States and *second*, the handing over of data would violate the law of a "qualifying foreign government".[22] The Act further provides that only those foreign governments are qualifying, with which the United States has entered into an executive agreement and whose law provides reciprocal substantive and procedural opportunities.[23] Finally, the CLOUD Act removes the prohibition under the SCA to disclose data to qualifying foreign governments of whom the Attorney General certifies that their domestic law offers substantive and procedural protections for privacy and respects universal human rights.[24]

The consequences of the CLOUD Act are therefore twofold. First, American law enforcement can compel American CSPs to produce any data held by them irrespective of the nationality of the data "owner" or the location where this data is stored. Second, US law regulates when American CSPs may disclose data held by them to foreign governments, even if this data belongs to those states' citizens or companies. It has to be noted, however, that these consequences are not unique to the CLOUD Act, but may ensue whenever a state has jurisdiction over CSPs, as for instance China with Tencent and Alibaba.

EUROPEAN "DIGITAL SOVEREIGNTY"

It is not difficult to see that such a system gives a high level of control over data to one or a handful of states where CSPs are domiciled or run data centres (controlling states), while at the same time leaving all other states with the difficult choice of either accepting an asymmetrical power relationship and dependence on the cooperation and goodwill of the controlling states with regard to data access (given that only the controlling state can effectively enforce its rules against a CSP) or rejecting the current cloud computing model and thereby risking to be cut off from key technology. Dependence on American CSPs and the resulting de facto extraterritoriality of American law may be acceptable to many because the United States is a democracy and a rule of law state, thereby reducing the risk of abuse of power. But even between allies, control over data has become an issue not only of business practicalities, but more than that – an issue of sovereignty. This is most impressively evidenced by recent steps of the European Union and certain of its member states to establish an alternative cloud computing model, which would help rebuild European "digital sovereignty".

The notion of "digital sovereignty" was first developed by in France (*souveraineté numérique*).[25] In 2019, the French Senate convened a *Commission d'enquête* on the topic of digital sovereignty with the view of studying the issue and formulating policy recommendations. Its final report, presented by Rapporteur Gérard Longuet, critically examined, among others, the question of cloud storage and extraterritorial jurisdiction.[26] It held that in the modern world data had become an economic strategic issue (*enjeu économique stratégique*), of immense importance for the activities of the major actors in the digital economy.[27] The report discussed the question of data localisation as one of the modes of protecting data, but found it an imperfect solution.[28] It found that data localisation rules might be important with respect to securing digital sovereignty in three instances: to protect the "strategic" or particularly sensible data such as public data of sovereign importance, private financial data or commercial secrets, to guarantee access to essential services, and to support the industrial ecosystem of cloud providers.[29] The report noted, however, that data localisation clauses do not ameliorate the risks posed both by extraterritorial legislation such as the CLOUD Act and by the dependence of certain technology companies on their states (as with certain Chinese companies).[30] It criticised the CLOUD Act as being too broad with respect to the affected entities, the infractions covered, and the type and amount of data collected;[31] it also found the Act to pose a risk of access by American law enforcement to strategic data of legal persons (such as trade secrets) and to be incompatible with the GDPR with regard to the protection of personal data.[32]

To mitigate those risks the report recommends to consider three options: *first*, the legal separation of subsidiary companies for each region and geographical location of services, so that US law enforcement access would not affect European data, *second*, mobilising companies on a case-by-case basis to contest exorbitant law enforcement demands in court, and *third*, the extensive use of robust data encryption technologies.[33] Similar to the report of 26 June 2019, prepared for the French Prime Minister by Raphaël Gauvain,[34] the Longuet Report advises strengthening the 1968 law on blocking measures, extending the protections of the GDPR to non-personal data of legal persons, and encouraging the fast conclusion of a cooperation agreement between the European Union and the US.[35]

While none of these measures have been implemented at the time of writing, what becomes clear from the Gauvain and Longuet Reports is that France is deeply concerned with American (and Chinese) extraterritorial reach, brought about by their dominance of the software and hardware sectors respectively. Therefore, the French view is that it has to take robust action – both legislative and in terms of industrial policy – to protect French data and French strategic interests against the reach of foreign states, even like-minded states such as the US.

Similar considerations underpin the German position with respect to American cloud services. Ever since the Snowden revelations, Germany has been deeply worried about the access of the US National Security Agency (NSA) and US law enforcement to German data. The federal government has repeatedly stressed that while it recognises the importance of facing novel challenges to law enforcement posed by the proliferation of transnational cloud services, any legal solution needs to respect fundamental human rights guarantees and facilitate cooperation between states. To this end, it advocates rapid negotiations between the European Commission and the US government to conclude a cooperation agreement on data sharing, as envisaged by the CLOUD Act.[36] However, besides international cooperation, Germany also seeks to secure its own "digital sovereignty" (*digitale Souveränität*), limiting US law enforcement access to German data. This is done via two routes: *first*, by limiting the type of data which can be stored on US cloud services and *second*, by developing an autonomous cloud storage solution. To address these concerns, on 29 October 2019, the German government has launched the GAIA-X project.[b] The stated motivation for this project is to preserve European "data sovereignty" (*Datensouveränität*) against increasing dependence on foreign digital technologies.[37] To this end, Germany wants to create a data infrastructure which would guarantee European control – and control by Europeans themselves – over the data of European citizens and reduce dependence on foreign cloud service providers.[38] This is to be done by linking centralised and decentralised infrastructures (cloud and edge-services) into one coherent system, based on open technologies and providing interfaces for the facilitation of data exchange and use of applications.[39] Crucially, this is to be done on the basis of existing and yet-to-be-built European services and infrastructure and cutting out US-headquartered CSPs, thereby limiting the exposure to American law enforcement. The Gaia-X project has been recently supported by the European Commission, which in the "European strategy for data" aims at developing common European data spaces and

b The GAIA-X Report is also available in English as: *Project GAIA-X. A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem*, Bundesministerium für Wirtschaft und Energie, 29.10.2019, [online:] https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/project-gaia-x.html.

interconnecting cloud infrastructures and enabling access to "competitive, secure and fair" European cloud services.[40] The urgency of European solutions in the field of cloud computing is highlighted by the Court of Justice of the European Union's decision in the *Schrems II* case, where the Court decided that the domestic law of the United States does not offer protections of Europeans' personal data that are essentially equivalent to those required under EU law and thus invalidated the EU-US Privacy Shield (data protection rules and obligations for US companies from 2016), rendering transfers of European personal data to the US impermissible.[41]

THE CHINESE THREAT AND THE CLEAN NETWORK INITIATIVE

The abovementioned examples show that even allies can have reservations against excessive extraterritorial jurisdiction of a friendly power and may wish to develop their own capacities. The threat is much greater when cloud computing infrastructure and operators are under the jurisdiction of an adversarial power such as China. In this case, security concerns over the amount of Chinese state control over its CSPs such as Tencent and Alibaba, paired with the lack of robust legal protections, as well as examples of past malpractices (such as the theft of intellectual property) have led the US State Department to announce the Clean Network program[42]. The program aims to protect America's critical telecommunications and technology infrastructure and its Clean Cloud component stipulates that sensitive personal information and intellectual property should not be "stored and processed on cloud-based systems accessible to our foreign adversaries through companies such as Alibaba, Baidu, and Tencent".

IS THERE A MIDDLE WAY? THE CASE OF POLAND

The preceding sections argued that cloud computing has significant geopolitical effects due to the control over data that a state can exercise if CSPs are incorporated or data centres located in its territory. States may choose different strategies to cope with the resulting power asymmetries: from acquiescence and various degrees of cooperation to contestation, blocking adversarial cloud computing platforms, and developing their own capabilities.

It has to be noted, however, that not every European State follows the path of achieving digital sovereignty through the exclusion of foreign CSPs from access to key data. In 2018 the Polish government launched the programme Common Information Infrastructure of the State (*Wspólna Infrastruktura Informatyczna Państwa*, WIIP), which aims at creating two public cloud services: Public Computational Clouds (*Publiczne Chmury Obliczeniowe*) and a Governmental Computational Cloud (*Rządowa Chmura Obliczeniowa*).[43] With this, the Polish government does not exclude foreign cloud service providers, but rather applies different security and access standards to different types of data. For instance, the Public Computational Cloud (or simply "National Cloud", *Chmura Krajowa*) will be set up in partnership with Google, which will build a Google Cloud hub in Warsaw. Currently, the largest and strategic client of the National Cloud is the largest bank in Poland, PKO BP and the National Cloud is aimed predominately at the private sector. In contrast, public and local administration will be able to use the Governmental Computational Cloud. For this public cloud, the government will set up security requirements and a Governmental Security Cluster (*Rządowy Klaster Bezpieczeństwa*), presumably for the most sensitive data.[44] It remains to be seen whether Poland will exclude foreign CSPs from this Governmental Security Cluster or try to secure governmental data contractually and through encryption. It has to be noted, however, that Poland cannot rely on big national cloud service providers and therefore is dependent on outside expertise for its national cloud and this thus limited in a potential quest for digital sovereignty.

Looking more broadly on Central and Eastern Europe (CEE), the situation is quite similar. According to two recent studies,[45] CEE states are expected to have more than 365 million internet users and over 2 billion connected devices by 2022. At the same time, only 13.1% of surveyed companies in the region have completed their digital transformation (which includes cloud computing use), while 76.4% of companies take their first steps in this direction. Both factors combined point to a dynamic growth of the cloud computing market in CEE and increased demand for investments in data infrastructure in the region. Similar to Poland, other CEE states do not have large national CSPs which could shoulder this investment either and will need to decide how to develop their cloud computing markets to best serve the needs of both the public and private sectors. Here, again, the choice will be driven as much by geopolitical as by business considerations.

CONCLUSION

This article has argued that cloud computing should not be regarded purely through the business lens. Rather, due to the importance of data for the modern digital economy and national security, the capabilities to store and process data in the cloud have attained special importance for a states' technological or digital sovereignty and thus form an important factor in current geo-economics and geopolitics. Recent examples such as the US CLOUD Act, European efforts to develop own cloud platforms and American efforts to protect sensitive private and business data from the reach of the Chinese state are a case in point. In this adversarial environment, Central Europe must choose which path to follow. Due to its values (such as the rule of law and protection of fundamental rights) and alliances, it seems obvious Three Seas states cannot fall into technological dependence on China. Rather, they should strive to develop its own capabilities, in cooperation with American and European allies. The Polish public and governmental cloud initiatives are a step in this direction and may therefore be a model to follow.

ENDNOTES

1 Mell P., Grance T., *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, Special Publication 800-145, September 2011, p. 2.

2 Dignan L., T*op cloud providers in 2020: AWS, Microsoft Azure, and Google Cloud, hybrid, SaaS players*, ZDNet, 11.05.2020, [online:] https://www.zdnet.com/article/the-top-cloud-providers-of-2020-aws-microsoft-azure-google-cloud-hybrid-saas/.

3 Richter F., *Amazon leads $100 Billion Cloud Market*, Statista, 11.02.2020, [online:] https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/.

4 *Ibidem*.

5 *The European Data Strategy – Factsheet*, European Union, February 2020, p. 2, https://ec.europa.eu/commission/press-corner/api/files/attachment/862109/European_data_strategy_en.pdf.pdf.

6 *Ibidem*.

7 *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, European Commission, 17.04.2018, Doc. COM(2018) 225, Explanatory Memorandum, p. 14, [online:] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN.

8 Daskal J., *The Un-Territoriality of Data*, Yale Law Journal, Vol. 125, No 2, 2015, pp. 365–377.

9 Burrington I., *The Strange Geopolitics of the International Cloud*, The Atlantic, 17.11.2015, [online:] https://www.theatlantic.com/technology/archive/2015/11/the-strange-geopolitics-of-the-international-cloud/416370/.

10 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/70/174 United Nations General Assembly, [online:] https://undocs.org/A/70/174.

11 *In Re Warrant to Search a Certain E-Mail Account*, US District Court (S.D. New York), 15 F.Supp.3d 466 (2014), 468, [online:] https://cite.case.law/f-supp-3d/15/466/.

12 *Stored Communications Act*, United States Congress, 18 U.S.C. §§ 2701-2712, [online:] https://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter121&edition=prelim.

13 *In Re Warrant to Search a Certain E-Mail Account*, US District Court (S.D. New York), 15 F.Supp.3d 466 (2014), 470, [online:] https://cite.case.law/f-supp-3d/15/466/.

14 *Ibidem*, p. 471-472; the Court held further that "an SCA Warrant … does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical presence of service provider employees at the location where data are stored…. [I]t places obligations only on the service provider to act within the United States", *ibidem*, pp. 475-476.

15 *Microsoft Corp. v. USA (In Re Search Warrant)*, US Court of Appeals (2d Circuit), 829 F.3d 197 (2016), [online:] https://law.justia.com/cases/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.html

16 *Ibidem*, p. 210.

17 *Ibidem*, pp. 58-59.

18 *United States v. Microsoft Corp*., US Supreme Court, Docket No. 17-2, [online:] https://www.scotusblog.com/case-files/cases/united-states-v-microsoft-corp/.

19 *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*, as part of the Consolidated Appropriations Act, United States Congress 2018, Pub. L. 115-141, amending the Stored Communications Act, 18 U. S. C. §2701 et seq., [online:] https://www.govinfo.gov/content/pkg/PLAW-115publ141/html/PLAW-115publ141.htm.

20 Galbraith J., *Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Reshaping U.S. Law Governing Cross-Border Access to Data*, American Journal of International Law, 2018, Vol. 112, No 3, pp. 486-487.

21 *Ibidem*, p. 489.

22 *CLOUD Act*, 18 U.S.C. §2703(2)(A).

23 *CLOUD Act*, 18 U.S.C. §2703(1)(A).

24 Galbraith J., *Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Reshaping U.S. Law Governing Cross-Border Access to Data*, American Journal of International Law, 2018, Vol. 112, No 3, p. 491.

25 For an overview of French scholarly literature on this matter see Bellanger P., *La souveraineté numérique*, Stock 2014, Türk P., Vallar Ch. (eds.), *La souveraineté numérique : le concept, les enjeux*, Mare & Martin 2018.

26 Longuet G., *Rapport fait au nom de la commission d'enquête sur la souveraineté numérique*, French Senate - Commission d'enquête sur la souveraineté numérique, 1.10.2019, [online:] http://www.senat.fr/rap/r19-007-1/r19-007-1.html (hereinafter "Longuet Report").

27 Longuet Report, p. 54.

28 *Ibidem*, p. 68.

29 *Ibidem*.

30 *Ibidem*, p. 69.

31 *Ibidem*, p. 71.

32 *Ibidem*, p. 72.

33 *Ibidem*, p. 74.

34 Gauvain M., *Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extrterritoriale*, Rapport à la demande de Monsieur Édouard Philippe, Premier Ministre, French National Assembly, 26.06.2019, [online:] https://www.vie-publique.fr/sites/default/files/rapport/pdf/194000532.pdf.

35 Longuet Report, p. 75.

36 Cf. *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Heike Hänsel, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE*, Deutscher Bundestag, 11.07.2018, BT-Drs. 19/3392, p. 2, [online:] https://dip21.bundestag.de/dip21/btd/19/033/1903392.pdf.

37 *Ibidem*, p. 6.

38 *Ibidem*, p. 9.

39 Ibidem, p. 12.

40 *A European Strategy for Data*, European Commission, 19.02.2020, COM(2020) 66 final, [online:] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

41 *Data Protection Commissioner v. Facebook Ireland Ltd. (Schrems II)*, Court of Justice of the European Union, case C-311/18, Judgment of 16 July 2020, [online:] http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=17518176.

42 *Announcing the Expansion of the Clean Network to Safeguard America's Assets*, U.S. Department of State, 5.08.2020, [online:] https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/.

43 *Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa"*, Rada Ministrów, 24.09.2019, Monitor Polski 2019 r. poz. 862, [online:] https://monitorpolski.gov.pl/MP/2019/862.

44 *Ibidem*.

45 Kroa V., Zajonc P., *Central and Eastern Europe Cloud Services Market: 2019–2023 Forecast and 2018 Vendor Shares*, International Data Corporation 2019, [online:] https://services.idc.com/research/viewtoc.jsp?containerId=EUR244725719; *Central and Eastern European Data Center Markets - Investment Analysis and Growth Opportunities 2020-2025*, ResearchAndMarkets.com 2020, [online:] https://www.researchandmarkets.com/reports/5067353/central-and-eastern-europe-data-center-market.