WIEDZA OBRONNA

2023, Vol. 285 No. 4

ISSN: 2658-0829 (Online) 0209-0031 (Print)

Journal homepage: http://wiedzaobronna.edu.pl

DOI: https://doi.org/10.34752/2023-l285

BARTŁOMIEJ ADRIAN TEREBIŃSKI[*]

Akademia Sztuki Wojennej, Warszawa Polska

THE TECHNICAL BORDERS OF CYBERSPACE

ABSTRACT: Cyberspace is a domain of information collecting, storing and processing in a digital form. It operates based on digital signal transmission but sometimes, which is often forgotten, based on electromagnetic radiation. The literature analyses indicate that cyberspace is intangible in its essence but functions owing to ICT infrastructure that generates and sends the signals. A cyberspace user, i.e., a human, takes action based on measurable and geographically located infrastructure which exists in the material world but penetrates the "aterritorial" cyberspace. This paper aims to present various perspectives on the attempted answer to the question of whether technical borders of cyberspace exist.

KEYWORDS: cyberspace, ICT infrastructure, incidents, world wide web.

[*] **dr Bartłomiej Adrian Terebiński,** War Studies University, Warsaw, Poland
https://orcid.org/0000-0002-6124-9905 b.terebinski@pracownik.akademia.mil.pl

> ”The Internet revolution has come. Some say it has gone. What was responsible for its birth? Who is responsible for its demise?”
>
> Lawrence Lessig[1]

INTRODUCTION

Before introducing the issues related to cyberspace and its technical aspects in order to try to answer the question being the key research issue of the presented deliberations, i.e. *Does cyberspace have technical borders?*, some facts related to digital information generated globally should be emphasised. According to research results developed between 2016 and 2020 for the European Commission in twenty-eight member states, the volume of the data market increased by nearly 37% in the referenced period. According to other estimates, the data were worth up to five billion USD. Only seven sectors of the economy were taken into consideration. In 2022, the annual expenditure on IT reached nearly 4.5 trillion USD worldwide, which is 5.1% more than in 2021 (see Fig. 1).

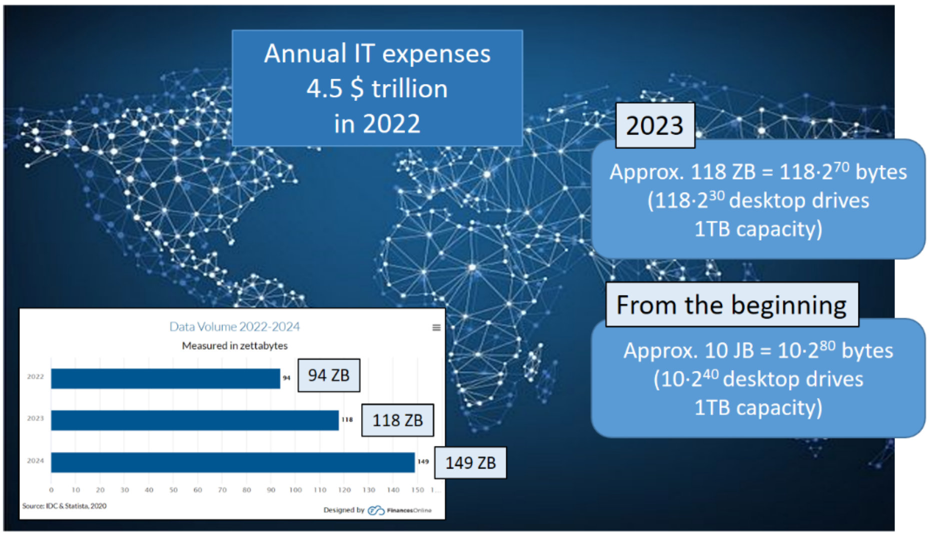


Figure 1. Digital data worldwide

Source: own study based on[2]

[1] https://typeset.io/papers/the-future-of-ideas-the-fate-of-the-commons-in-a-connected-7vfrzhownd [Accessed: 23 February 2023].

[2] financesonline.com/how-much-data-is-created-every-day/ [Accessed: 20 February 2023].

Experts expect the most significant increases in such areas as corporate software, IT services and data centre solutions. The highest rise is anticipated in the computational cloud market[3]. For contemporary companies, data storing offers the opportunity to implement innovation, reduce costs and improve performance. Data are fuel for the digital transformation engine. Still, in addition to companies, institutions, services, offices etc., namely entities that generate and store data in a formalised way, data are primarily generated for private use.

According to literature[4], this leads to generating data quantities previously hard to imagine; according to the digital data unit of measure, the data quantity was estimated as ca. ten yottabytes (10 YB). Only by the end of 2022, a total of 94 zettabytes of data (94 ZB) were generated. One can ask a question if it is a lot, and the conclusions from literature analyses suggest that the answer is not unequivocal[5]. On the one hand, referring to expert research through the prism of the mass of electrons being data carriers, the total mass of all data accumulated in the virtual world ranges "only" from 40 to 80 kg. The estimated data are often contrasted with the number of data carriers. If the entire Internet's content was copied to Blu-ray discs, once stacked one onto another, the discs would cover the way from the Earth to the Moon and back. On the other hand, taking a time perspective, copying the data above would take hundreds of millions of years. Finally, if one tried to close all the data on standard capacity discs in the commonly used personal computers, it would take millions of sextillions of equipment pieces. According to research, the vast data volume will be increasing annually, reaching ca. 20% data gain on a year-to-year basis.

MANY DEFINITIONS - OVERVIEW

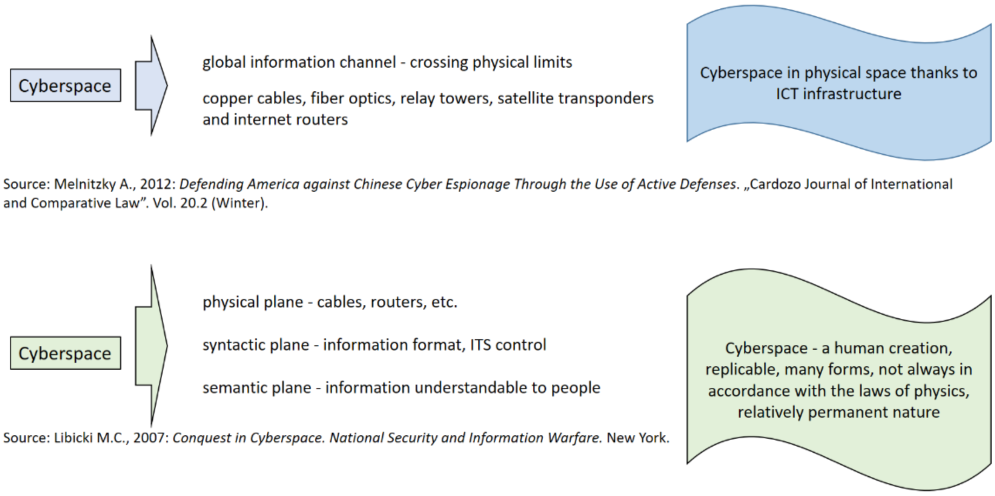
A synthesis of literature review results promotes a general conclusion that many definitions of cyberspace have been developed in the last twenty years. The definitions seem highly diversified in their nature. Some definitions focus on the general rules of cyberspace functioning, often presented in an abstract way, while other ones attempt to include social and technical issues, trying to handle the topic more comprehensively. One should note that researchers did not even reach a consensus on such fundamental aspects as cyberspace's technical characteristics (see Fig. 2). Some researchers

[3] itwiz.pl/w-2022-roku-swiatowe-wydatki-na-it-osiagna-wartosc-45-biliona-dolarow/ [Accessed: 20 February 2023].

[4] financesonline.com, ed. cit.

[5] Review of the Armed Forces No. 5/2022, Warsaw (Poland), https://zbrojni.blob.core.windows.net/pzdata2/TinyMceFiles/psz5_2022.pdf [Accessed: 21 February 2023].

indicated that cyberspace is purely intangible or does not include network-connected computers (Alexander Melnitzky's definition). According to Melnitzky, on the one hand, cyberspace has become a "global information channel" that crosses physical constraints, but on the other hand, cyberspace also covers material objects such as satellite transponders, BTS, copper cables, fibre optic cables and Internet routers. In this sense, although cyberspace goes beyond the physical space, it is directly embedded in it owing to the ICT infrastructure.


Cyberspace
global information channel - crossing physical limits
copper cables, fiber optics, relay towers, satellite transponders and internet routers
Cyberspace in physical space thanks to ICT infrastructure
Cyberspace
physical plane - cables, routers, etc.
syntactic plane - information format, ITS control
semantic plane - information understandable to people
Cyberspace - a human creation, replicable, many forms, not always in accordance with the laws of physics, relatively permanent nature

Source: Melnitzky A., 2012: *Defending America against Chinese Cyber Espionage Through the Use of Active Defenses*. „Cardozo Journal of International and Comparative Law". Vol. 20.2 (Winter).

Source: Libicki M.C., 2007: *Conquest in Cyberspace. National Security and Information Warfare*. New York.

Figure 2. Cyberspace – many definitions

Source: own study based on[6].

Martin C. Libicki divided cyberspace into three planes (layers). The first one is the physical plane, including cables, routers, etc. The second, syntactic one, is the information format in cyberspace and the methods of ICT systems designing and control. The third, semantic plane, is the information understood by humans. Getting access to one of the planes does not mean controlling the other. Capturing the ICT infrastructure does not necessarily entail accessing the syntactic layer. Controlling the syntactic layer does not mean open access to the semantic one. The final conclusions of the deliberations are included in the statement that cyberspace was developed by humans and is a replicable construct, meaning it exists simultaneously in several places and can be repaired. Moreover, cyberspace can take many forms and manifestations, as the laws governing cyberspace do not have to comply with the laws of physics or those established by humans. Generally, some

[6] Melnitzky, A. (2012) Defending America against Chinese Cyber Espionage Through the Use of Active Defenses. "Cardozo Journal of International and Comparative Law". Vol. 20.2 (Winter), and Libicki, M. C. (2007) Conquest in Cyberspace. National Security and Information Warfare, New York (USA).

cyberspace aspects are durable. The rules of cyberspace, including those based on mathematics (cryptography laws) or rules determined by software developers, make good examples.

THE ESSENCE OF CYBERSPACE – TECHNICAL DIMENSION

Cyberspace is a domain of information collecting, storing and processing in a digital form. It operates based on the transmission of digital signals and electromagnetic radiation. Cyberspace is intangible in its essence. Nonetheless, it functions owing to the ICT infrastructure that generates and sends the signals. A cyberspace user's role is well described in the following quotation derived from the reference literature (see Fig. 3): "Taking actions in the material world, based on measurable and geographically located infrastructure, a human [...] enters the "aterritorial" cyberspace world"[7]. Cyberspace is then a being that functions inside the ICT infrastructure. Owing to cyberspace, all data stored, processed and exchanged in computer networks and all other components, including single workstations (hosts), form the ICT infrastructure. Computers are the essential components of cyberspace. Still, opinions vary on whether this concept covers all computer stations or only those connected to the Internet. An ICT space analysis cannot neglect offline computers. It applies to actions taken to protect the referenced space.

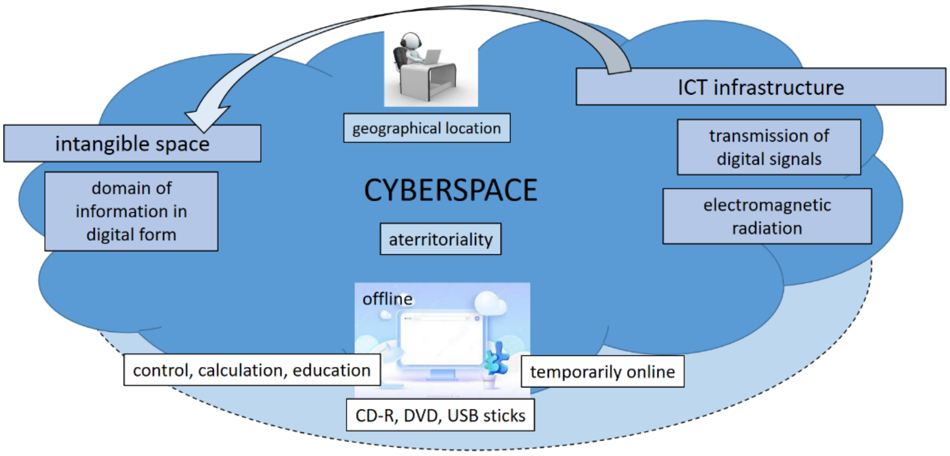


Figure 3. Essence of cyberspace

Source: own study.

[7] Lakomy, M. (2015) Cyberspace as a new dimension of competition and cooperation between states, University of Silesia, Katowice (Poland), pp. 83.

Despite a lack of Internet connection, computers can still perform vital functions from the point of view of units, companies, societies and states. What does it mean? It should be emphasised that computers control machines, help in calculations, and support education and development. It means they significantly contribute to various domains of human life. Autonomous computers (working offline) can communicate with other devices or their networks. Potentially every device, despite being isolated, can contact cyberspace owing to various data carriers (CD-R, DVD, USB flash disks). Furthermore, the development of mobile devices and wireless networks facilitates situations where the user only uses the world wide web for some time. Therefore, ignoring the processes and events which occur in this area contradicts a holistic approach to the analysed research issue.

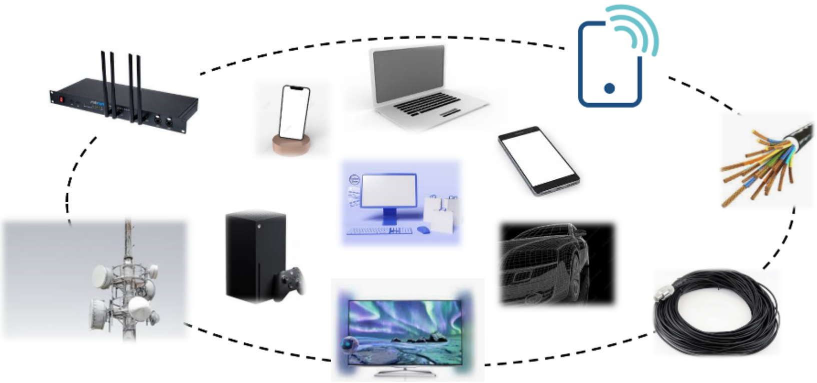


Figure 4. Technical foundation of cyberspace

Source: Own study.

Cyberspace includes many other "controllable" (programmable) electronic devices such as smartphones, tablets or even game consoles, smart television sets or modern cars. Their architecture includes programmable components functioning on the Internet, namely in a shared communication platform. This category also covers individual computers and isolated networks. Finally, it shall be stated that cyberspace works owing to a huge number of other components building the ICT infrastructure. It enables data archiving, processing and transferring in a digital form. The ICT infrastructure includes routers and base transceiver stations sending electromagnetic signals in wireless networks, as well as standard copper cables and fibre optics (Fig. 4). Assuming the approach to cyberspace as presented above, its primary technical properties should be characterised. A computer is an essential device forming an ICT space. Autonomous computers linked together and capable of exchanging information with one another create a system. Such systems form another fundamental element of cyberspace, i.e., local, urban and vast computer networks.

Sometimes public networks controlled by Internet providers are also mentioned as part of the system[8]. For individuals or companies, they become a basis for taking any action in the contemporary digital world. In a broad sense, all computer networks are covered by the notion of telecommunication networks.

It is also worth referring to the perception of cyberspace layers in the military area (see Fig. 5). According to NATO doctrine[9], there are three cyberspace layers depending on one another, i.e. the physical, logical and digital identity layers. The physical layer, consisting of servers, portable and stationary workstations, network devices, digital sensors and armament and command systems, is the first of the layers above. The logical layer includes data or software and interfaces for the physical and digital identity layers. Finally, the abstract digital identity layer forms an information area and relations between the system components. It applies to virtual identities constructed by actual entities (people, organisations). It should be emphasised that "one entity can have many virtual counterparts, and many entities can form a single virtual personality, e.g. a shared account, discussion group, community centred around a specific idea, a hackers' group", *etc.*[10]. Consequently, the physical layer's components are characterised by an exact geographic location, while the digital identity and logical layers are of cross-border nature.

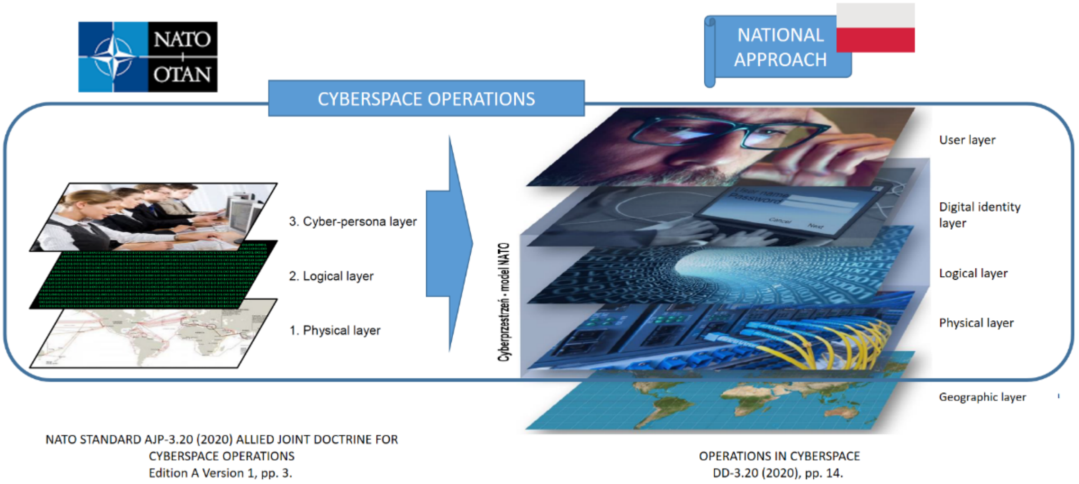

NATO
OTAN
NATIONAL APPROACH
CYBERSPACE OPERATIONS
3. Cyber-persona layer
2. Logical layer
1. Physical layer
Cyberprzestrzeń - model NATO
User layer
Digital identity layer
Logical layer
Physical layer
Geographic layer
NATO STANDARD AJP-3.20 (2020) ALLIED JOINT DOCTRINE FOR CYBERSPACE OPERATIONS Edition A Version 1, pp. 3.
OPERATIONS IN CYBERSPACE DD-3.20 (2020), pp. 14.

Figure 5. Operations in cyberspace as an operational domain

Source: Own study based on[11].

[8] Terebiński, B. (2022) Military ICT, War Studies University, Warsaw (Poland), pp. 22.

[9] NATO Standard AJP-3.20, (2020) Allied Joint Doctrine For Cyberspace Operations, Edition A Version 1, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf [Accessed: 22 February 2023].

[10] NATO Standard AJP-3.20, (2020), ed. cit., pp. 4.

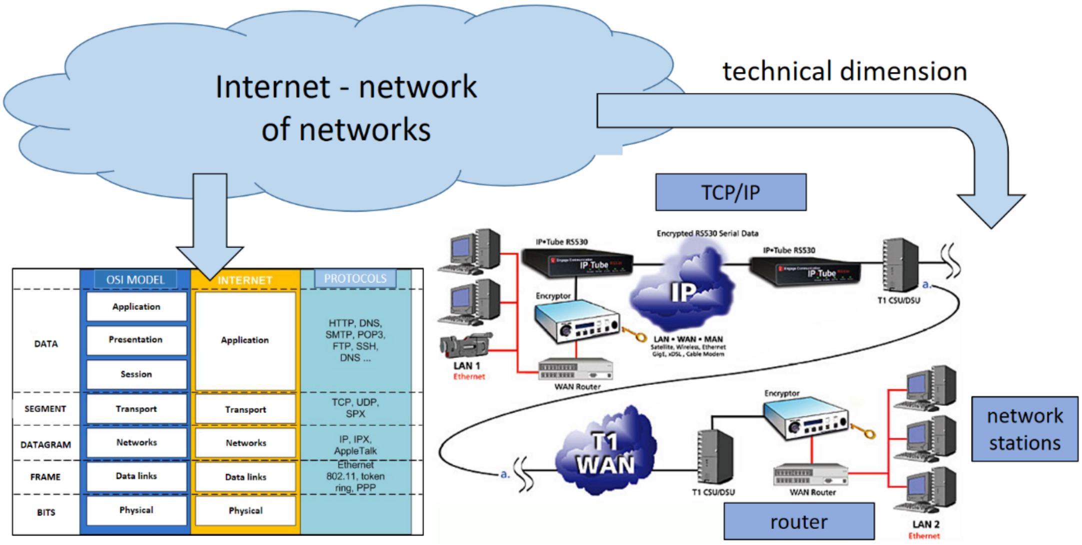
[11] NATO Standard AJP-3.20 (2020), ed. cit., pp. 3, and Operations in cyberspace DD-3.20 (2020), Poland, pp. 14.

In a national approach, an additional layer is included, allowing for identifying the geographical location of the cyberspace items. It is related to assigning responsibility for the actions performed in cyberspace, which is called attribution in the literature and is associated with the user's layer functions. Moreover, it is pointed out that any action related to the items in the geographical layers is not treated as cyberspace operations.

From the point of view of this study's research objective, the technical properties of cyberspace are most important; hence the rules of cyberspace's foundation operation are discussed, i.e., of the world wide web called the "Internet" in 1969[12]. It is common knowledge that, technically, the Internet's operation is essentially based on routers. Routers are indirect gates for exchanging information between networks using various addressing patterns, broadcasting media or technologies. Owing to routers, a web user gains access to another network's resources, regardless of its different technical properties. The network stations (hosts) are the end devices. The infrastructure diversity at the physical level does not affect communication homogeneity owing to TCP/IP communication protocols. Hence, from the technical point of view, the Internet has a layered structure being a collection of various network stations and computer networks linked with routers and other devices and components forming the global ICT infrastructure (see Fig. 6). The essence of cyberspace is another aspect worth mentioning. Although founded in and dependent on the tangible ICT infrastructure, its nature is intangible. The tangible and non-tangible nature of the actions taken through a device using computer technologies implies the status quo. The tangible (material) aspect means the user's interaction with the computer interface, but the intangible (non-material) aspect pertains to the device's arithmetic and logical unit executing specific instructions (procedures). Cyberspace's open and dispersed architecture is another property. This applies primarily to the Internet as a global network but also to other items, such as autonomous networks separated with galvanic isolation from the Internet and autonomous workstations (offline computers). Consequently, such solutions ensure that damage to many network components will not lead to cyberspace failure as a whole owing to the equipment's

[12] The first nodes of the ARPANET network were established in 1969, and this date is considered to be the beginning of the Internet (author's comment).

redundancy[13]. Diversified entries to cyberspace (open architecture) are definitely a hazard and hamper preventing incidents, e.g., due to the perpetrator's (adversary's) anonymity.



	OSI MODEL	INTERNET	PROTOCOLS
DATA	Application Presentation Session	Application	HTTP, DNS, SMTP, POP3, FTP, SSH, DNS ...
SEGMENT	Transport	Transport	TCP, UDP, SPX
DATAGRAM	Networks	Networks	IP, IPX, AppleTalk
FRAME	Data links	Data links	Ethernet 802.11, token ring, PPP
BITS	Physical	Physical	

Figure 6. Technical properties of cyberspace – layered structure

Source: Own study based on[14].

Cyberspace's total dependence on the infrastructure's performance is another characteristic feature. The reliability of equipment (routers, transmitters) and transmission media (cables, fibre optics) is pivotal. In this regard, one should remember bottlenecks, i.e. places in the world characterised by the highest network traffic. This is where the redundancy of links results in capacity constraints, i.e. slower network operation. Taking into account the number of fibre optic cables laid at the ocean bottoms to create the world wide web's backbone, one can reach a valid conclusion that the fibre optic cables, rather than satellite stations, provide for most network traffic in cyberspace (see Fig. 7).

[13] Redundancy - excess in relation to what is necessary. Ct Terebiński, B. (2022) Military ICT, ed. cit., pp. 88.
[14] Lipiński, Z. Computer Networks. DoD model TCP/IP. A family of TCP/IP protocols. https://www.math.uni.opole.pl/~zlipinski/ skW/SieciKomp¬ 07¬ TCP¬ IP.pdf [Accessed: 22 February 2023].

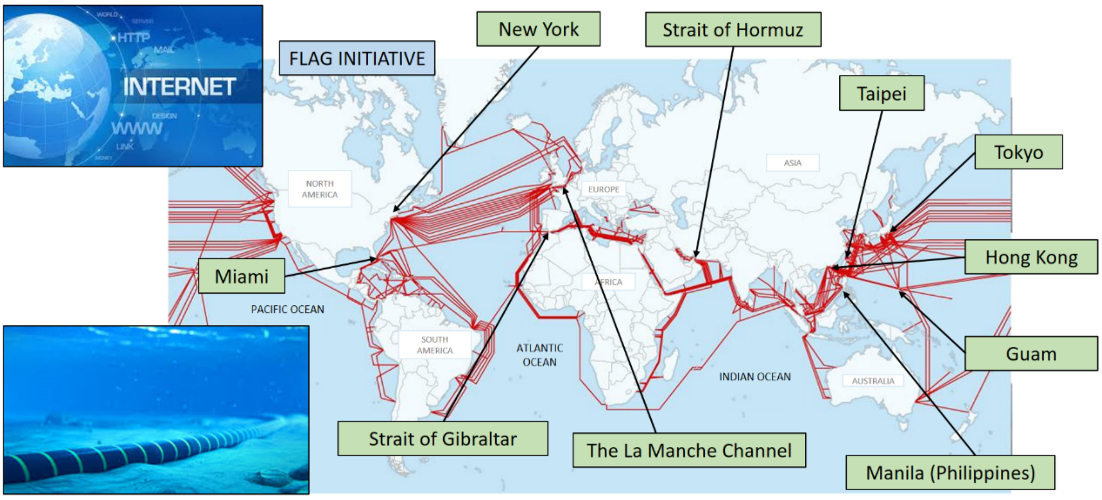


Figure 7. Cyberspace bottlenecks

Source: Own study based on[15].

Two considerable failures in the places marked as bottlenecks can be quoted to confirm the close dependence of cyberspace functioning on the ICT infrastructure performance. This applies to the vicinity of the most significant bottleneck, i.e., the Suez Canal and the Red Sea. At the beginning of 2008[16], the FALCON cable linking India to the countries of the Persian Gulf was damaged there; the failure of SEA-ME-WE 4 and FLAG Telecom near Alexandria (Egypt) followed. The failure was among the most severe Internet failures in a dozen or so years of the world wide web's history. It covered Egypt, India, Bahrain, Afghanistan, Bangladesh, Kuwait, the Maldives, Pakistan, Saudi Arabia and the United Arab Emirates. In Egypt, ca. 70% of the Internet traffic was blocked, while in India, it was ca. 50%. The failure struck over 86 million internet users. Generally, 2008 was disastrous for this part of the world (see Fig. 8), as successive failures occurred between Oman and the United Arab Emirates and Qatar and near Malaysia. Towards the end of the reference year, the cable systems linking Egypt, Sicily and Malta were cut.

[15] https://www.wykop.pl/wpis/38530149/tak-wyglada-rozklad-swiatlowodow-na-naszej-kuli-lu/ [Accessed: 22 February 2023].

[16] https://www.tygodnikprzeglad.pl/ktos-przecial-kable/ [Accessed: 22 February 2023].

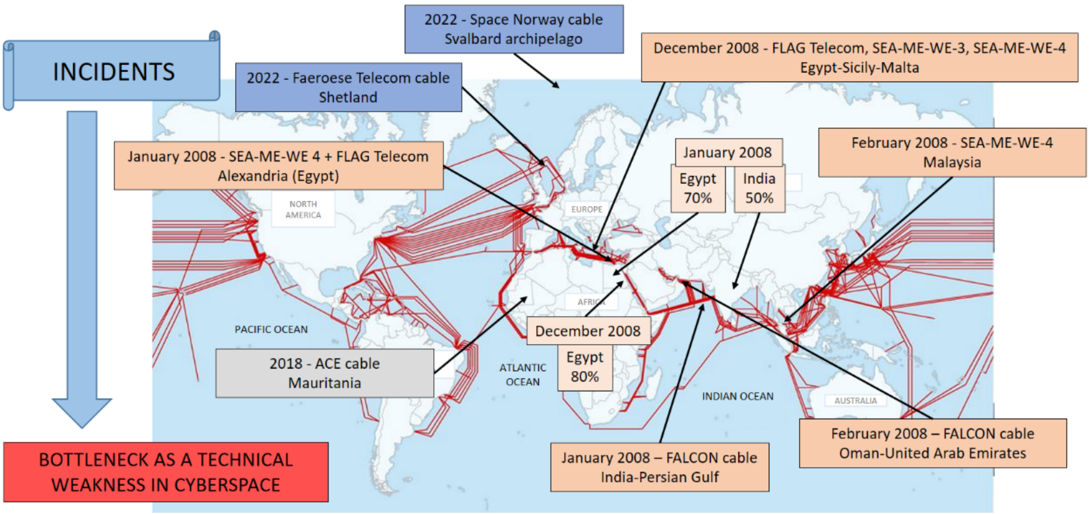

INCIDENTS
2022 - Space Norway cable
Svalbard archipelago
2022 - Faeroese Telecom cable
Shetland
December 2008 - FLAG Telecom, SEA-ME-WE-3, SEA-ME-WE-4
Egypt-Sicily-Malta
January 2008 - SEA-ME-WE 4 + FLAG Telecom
Alexandria (Egypt)
January 2008
Egypt
70%
India
50%
February 2008 - SEA-ME-WE-4
Malaysia
NORTH AMERICA
EUROPE
AFRICA
PACIFIC OCEAN
December 2008
Egypt
80%
2018 - ACE cable
Mauritania
ATLANTIC OCEAN
INDIAN OCEAN
AUSTRALIA
February 2008 – FALCON cable
Oman-United Arab Emirates
January 2008 – FALCON cable
India-Persian Gulf
BOTTLENECK AS A TECHNICAL
WEAKNESS IN CYBERSPACE

Figure 8. Incidents in the global ICT infrastructure

Source: Own study based on[17].

This resulted in reducing the network capacity by 80% in Egypt, while telephone communication was significantly reduced between Europe, the Middle East and Asia. Recently, gradually more cases have been observed of infrastructure damage due to human error and negative environmental impact[18]. It is testimony that underestimating the need to keep the network components in good working order, including but not limited to the bottlenecks mentioned above, is a major technical weakness. Ensuring the objects' safety is a challenge but also a starting point to ensure international safety. The operation of the DNS, which is responsible for the whole Internet traffic but is based only on thirteen servers, can be a constraint[19]. The DNS paralysis is likely despite geographic scattering – they are located in 1,557 places[20].

The electromagnetic field being a combination of the electric and magnetic fields, occurring in active network devices (computers, mobile phones, Wi-Fi routers, Bluetooth devices), is an essential technical feature of cyberspace. Despite the ongoing discussion on the degree of such objects' harmfulness to health, the most significant aspect is that the armed forces of different countries have used the electromagnetic field for many years. It applies to various kinds of

[17] https://www.wykop.pl/wpis/38530149/tak-wyglada-rozklad-swiatlowodow-na-naszej-kuli-lu/ [Accessed: 24 February 2023].
[18] Terebiński, B. (2022) Military ICT, War Studies University, Warsaw (Poland), pp. 22.
[19] As of the end of 2022, https://root-servers.org/?rel=nofollow,noopener,noreferrer&target=_blank [Accessed: 24 February 2023].
[20] As of the end of 2022, https://root-servers.org/, ed. cit [Accessed: 24 February 2023].

weapons based on electromagnetic pulses, inducing high voltage that generates heat amounts sufficient to damage or destroy equipment.

SUMMARY

A synthesis of conclusions from the analyses promotes a statement that the technical nature of cyberspace is highly complicated. This results from the referenced domain's multidimensional, intangible and aterritorial nature and open architecture. Nonetheless, technical borders of cyberspace exist, although they become gradually more difficult to determine due to the number of new devices increasing annually in geometric progression. The virtual world, which is cyberspace's interior, seems to have no size, and only human imagination can limit its functioning.

There is one more aspect worthy of attention in the Summary, as owing to the Internet, anybody able to use Google or another browser can find information on any topic of interest. A fundamental question emerges, what if digital data carriers fail suddenly? Rephrasing Albert Einstein's statement, in the case of successive world wars, humankind would take a step back in its development, and none of its achievements would be left on Earth[21].

The Arctic World Archive (AWA) is a physical location which is supposed to ensure our civilisation's survival. The most essential information and digitalised books are stored in the AWA. Hence, it is about preserving knowledge. The knowledge owing to which Einstein's famous quote will never come true[22]. ”Crypt 2” was built on Spitsbergen to regularly save and keep data for up to 1,000 years. Interestingly, the data are saved in a highly ”analogue” way. A decision was made to use archaic photosensitive films instead of the omnipresent clouds, CD-ROMs, disks and similar solutions. The choice was determined by the much higher resistance of such films to the passage of time - information stored this way is expected to survive intact even for a millennium. A dedicated capsule protects the films against mechanical damage. No Internet connection is another vital element – the Internet's operation does not affect the data in the AWA in any way. Although the database of the archive items is available online, the records are kept separately.

[21] I don't know what weapons will be used in World War III, but World War IV will be fought with sticks and stones. Eintein, A. (1949) Monthly Review, https://i.pl/slowa-ktore-zmienily-swiat-te-wypowiedzi-zapamietamy-na-dlugo-oto-najslynniejsze-cytaty-ostatniego-stulecia/gh/c15-15540118 [Accessed: 24 February 2023].

[22] https://arcticworldarchive.org/ [Accessed: 20 February 2023].

BIBLIOGRAFIA

REFERENCES LIST

PIŚMIENNICTWO

LITERATURE

Lakomy M., Cyberspace as a new dimension of competition and cooperation between states, University of Silesia, Katowice (Poland) 2015.

Libicki M. C., Conquest in Cyberspace. National Security and Information Warfare, New York (USA) 2007.

Melnitzky A., Defending America against Chinese Cyber Espionage Through the Use of Active Defenses, "Cardozo Journal of International and Comparative Law", 2012, Vol. 20.2 (Winter).

NATO Standard AJP-3.20, Allied Joint Doctrine For Cyberspace Operations, Edition A Version 1, 2020.

Operations in cyberspace, DD-3.20, Bydgoszcz (Poland) 2020.

Terebiński B., Military ICT, War Studies University, Warsaw (Poland) 2022.