GIS Odyssey Journal

2022 • Volume 2 • Number 1

https://doi.org/10.57599/gisoj.2022.2.1.141

Grażyna Szpor[1], Agnieszka Gryszczyńska[2]

HACKING IN THE (CYBER)SPACE

Abstract: The article analyzes the concept of hacking, taking into account its evolution from a neutral term that means going beyond specific schemes of action to a negative context in which the concept is often equated with a cyber-security breach or cyber-crime. A study of the understanding of the concept of space and cyberspace, as well as selected cyber threats, shows the impact of the development of modern technologies on the blurring of the boundaries between real and virtual space. Based on selected cases in the field of cybercrime, the specific features of actions in cyberspace and their effects in the real world are indicated. New methods of cybercriminals open up new areas of criminological research on the geography of crime. The paper points out the involvement of State-Actors in cyber attacks, which makes it challenging to eliminate safe harbors for cyber criminals and reduces the effectiveness of instruments of international cooperation in criminal cases.

Keywords: hacking, cybersecurity, cybercrime, spatial data, cyberspace, incident

Received: 25 August 2022; accepted: 2 September 2022

[1] Cardinal Stefan Wyszyński University in Warsaw, Faculty of Law and Administration, Department of Informatics Law, ORCID: 0000-0002-3264-9360, g.szpor@uksw.edu.pl.
[2]Cardinal Stefan Wyszyński University in Warsaw, Faculty of Law and Administration, Department of Informatics Law, ORCID: 0000-0003-3004-5253, a.gryszczynska@uksw.edu.pl.

Introduction

The term "hacking" is interpreted in different ways. Most broadly, it is understood as breaking security measures. It is mainly related to cyberspace and is subject to regulations in this context. Technological progress, especially the expansion of the Internet of Things, is resulting in increasingly strong and complex interconnections between virtual and real space. Spatial data, which may constitute personal data or legally protected secrets, are also targets of attacks, affecting the principles of their protection, causing the negative consequences of their breach, and leading to potential criminal liability. An analysis of these issues is needed to answer whether the legal regulation of hacking should change due to the fusion of cyber and real space.

The evolution of the concept of hacking

The term "hacking", which has been in use since the mid-20th century, was initially associated mainly with specific "intellectual experiments". Its negative connotation began to emerge in the 1980s (Britannica). However, it did not become exclusive, not least because of public authorities' legitimate use of hacking techniques (Legal Frameworks for Hacking by Law Enforcement, 2017).

In a broader perspective, the verb 'to hack' has numerous meanings and is considered the moment's word. Its technological connotations have been evaluated in both scope and presence. It derives from a verb meaning "to cut or chop with repeated and irregular blows" (The American Heritage Dictionary of the English Language, 2022). In 1955 at the Massachusetts Institute of Technology, the word "hack" first came to mean fussing with machines. According to Jessie Sheidlower, president of the American Dialect Society, the terms early references to machines "share a relatively benign sense of 'working on' a tech problem in a different, presumably more creative way than what's outlined in an instruction manual" (Yagoda, 2014). In the 1960s, the terms' hack' and 'hacker' were incorporated into the vocabulary of computer enthusiasts, but they had positive connotations. Predominant definitions were that a hacker is a person who enjoys exploring the details of programmable systems and stretching their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. Hacking was characterized as 'an appropriate application of ingenuity' (more: The Jargon File; RFC 1392). The word "hack" is also defined as "to manage to deal successfully with something" or "a good solution or piece of advice" (Cambridge Dictionary). Also increasingly popular as a method of finding creative solutions to specific problems are hackathons, defined not only as an event in which a large number of people meet to engage in collaborative computer programming but also as a form of civic innovation in which participants represent citizens can point out existing problems or social needs and propose a solution (Nikiforova, 2022).

Despite those benign definitions, over time, most individuals have come to understand the term "hack" to mean malicious meddling (Eckart, 2019), and the word quickly became synonymous with "digital trespasser".

In the legal literature, the term "hacking" appears in a broad or narrow sense. There is a distinction between "hacking sensu stricto", i.e. behavior of gaining unauthorized access to an information system or computer data, and "hacking sensu largo", i.e. any attack on the security of information systems and data, including, for example, the disruption of the operation of an information system, the modification or destruction of computer data (Radoniewicz, 2016).

The Convention on Cybercrime (2001) imposes an obligation on state parties in Article 2 to adopt such legislative and other measures that may be necessary to establish intentional access to the whole or any part of a computer system without right. as criminal offences under its domestic law. A state party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system. Ratification of the Convention required individual states to ensure that their domestic law complied with its norms.

Defining cybercrime and, more narrowly, hacking may also be influenced by the ongoing work of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, established by Resolution 74/247 (2019) of the General Assembly. In the course of work on the new UN Convention, the most contentious issue is determining the material scope of the new instrument. It is undisputed that the Convention should cover cyber-dependent crimes, i.e. crimes against the confidentiality, integrity and availability of computer systems, networks and data as well as the misuse of such systems, networks and data. Some states parties indicate that the Convention should also cover narrowly defined cyber-enabled crimes (as defined in the Convention on Cybercrime (2001), including offences related to child pornography). Several states parties, however, have a much broader approach, seeking to extend the new Convention to cover all crimes committed using information and communications technologies. Regardless of the final decision on the exact material scope of the Convention, the regulation will indisputably cover the conduct defined in Article 2 of the Convention on Cybercrime (2001) and Article 267 of the Polish Criminal Code.

The Polish Criminal Code (CC) criminalizes illegal access to information in Article 267. This article introduces punishment of a fine, community sentence or imprisonment for a maximum term of 2 years to anyone who:

- without being authorized to do so, acquires information not intended for him or her, by opening a sealed letter, or connecting to a telecommunications network or by breaching or bypassing electronic, magnetic, informatic or other special protection for such information (§ 1);
- gains access to an entire computer system or any part thereof without authorization (§ 2);
- installs or uses any wire-tapping, visual or other special equipment for the purpose of obtaining unauthorized access to information (§ 3);
- divulges to another person the information obtained in the manner specified in §§ 1 to 3 (§ 4).

The prosecution of the above offence, referred to in legal doctrine as the crime of hacking (The Great Encyclopedia of Law, 2021), is carried out at the aggrieved party's motion (§ 5.).

The word hacking is used to describe a crime and in the broader context of Internet security threats (Madej & Terlikowski, 2009). Frequently distinguished forms of ICT threats are "hacking, hacktivism, cybercrime, cyberterrorism, cyberespionage, the use of cyberspace as a fifth theatre of military operations, or the effects of uncontrolled use of the Internet in the social and psychological sphere" (Banasiński, 2018). Illegal hacking is considered a cyber security incident.

The legal doctrine also distinguishes the 'political hacking' category, outlining its evolution from hacktivism to cyber-terrorism and "info wars" (Corcoran, 2020; Szpor,

2016; Filipkowski, 2015). An example may serve Russian investments in IT systems related to social media.

According to a press release from 2012, Russia's foreign intelligence service announced three tenders, worth more than $1 million, to build a system for controlling mass consciousness through social networks. The first stage covered by the tenders was to create the Dysput system for monitoring the blogosphere and determining factors influencing the popularity and spread of information. The next one was to make the "Monitor-3" system based on developing methods for organizing and directing a virtual community of experts on the Internet and receiving answers from them on assigned topics. The third stage was the "Storm-12" system uploading messages approved by Russian intelligence to the network (Szpor, 2016).

In 2022, Scott has characterized four elements of Ukraine's digital tactics: 1. Controlling the narrative 2. Splitting the internet 3. Data processing in cooperation with companies advanced in big data and artificial intelligence applications. 4. IT Army of hackers. About this last element, Scott pointed out that Mykhailo Fedorov, Ukraine's digital minister, called for volunteers, both in and outside the country, to create an "IT Army" of hackers to target Russia with predominantly unsophisticated cyber attacks in response to the invasion. "During six months, hundreds of thousands of would-be hacktivists took down scores of Russian websites, attacked the country's state media and leaked mass of sensitive data onto the Internet – much to the embarrassment of the Kremlin. In this cyber battle, Russia's own digital troops still far outgun Ukraine's volunteer squad" by Kremlin-linked groups have repeatedly attacked its Western neighbor with malware and hacking campaigns, and, most recently, tried to bring down the country's electricity network in April (CERT-UA registered 1123 attacks in the period six months of the war). According to Ukrainian officials, hackers with ties to Belarus, a close Moscow ally, also successfully targeted Ukrainian government websites earlier in the year. By crowdsourcing its hacking efforts, Kyiv is borrowing from Russia's years-long strategy to unleash rogue cybersecurity specialists if it plays to its geopolitical favor" (Scott, 2022).

The broadest meaning of the term "hacking" is used by Yuval Harari, who points out that the growth of biological knowledge, computing power and data resources adds up to the ability to 'hack people', their body, brain and life. This means an AI-based system that understands humans better than they understand, can predict and manipulate their feelings and decisions, and ultimately can make human decisions. The use of AI could lead to job losses and the creation of a class of 'expendable people', relegating many countries to the category of 'data colonies' and, at the same time, the creation of 'digital dictatorships' that will control everyone at all times (Harari, 2020).

Space and cyberspace

Hacking is classified as a negative phenomenon in cyberspace (Morańska, 2015). An element of this compound term is the word space [space], which was known in ancient times.

Space (Latin: spatium; English: space; French: espace; nm: Raum) as a philosophical category has been the subject of many definitions. "Absolute space" (imaginary space) is an extensible, unbounded receptacle that contains all bodies (the Universe) to the exclusion of themselves. As the Encyclopedia Britannica defines space as a boundless, three-dimensional extent to which objects and events occur and have relative position and direction. In classical physics, physical space is often conceived in three linear dimensions. However, with time, modern physicists usually consider it to be part of a

boundless four-dimensional continuum known as spacetime. The concept of space is considered to be of fundamental importance to an understanding of the physical Universe. However, philosophers disagree over whether it is an entity, a relationship between entities, or part of a conceptual framework (Podsiad, 2001; Britannica, 2022; Wikipedia, 2022).

In the economy context, geographic space (land, water, and air) is defined as a scarce good, i.e., one that cannot be significantly expanded in the production process. The way to expand space relatively is to substitute it with inputs of labor and capital, allowing higher outputs from the same "pieces of space," leading to a reduction in the space necessary for humans to live. Information technology is considered to consume fewer material resources, and its products can save energy and materials to meet human needs. At the same time, the space over which man has control (allowing for the self-satisfaction of life's needs) is shrinking, and the space available is expanding, thanks to the development of communications. An essential measure of the distance between objects – beyond the meter or mile – is becoming the time or cost of covering it. There is talk of political, economic, cultural, sociological, psychological, and organizational spaces (and relative distances). Virtual space or cyberspace is emerging as a new category of relative spaces (Szpor, 2016).

The origin and evolution of the term "cyberspace" have already been extensively analyzed in scientific papers (Wasilewski, 2013; Worona, 2021). The computer science literature points out that in the computer science the term "cyberspace" is explained as "a network of interconnected computer systems through which electromagnetic impulses flow with coded signals controlling the operation of digital multimedia devices", "an IT-generated virtual reality with network access", and in other approaches cyberspace is called "a field of consciousness, a sphere of activity, a living environment, a decision environment, a plane of unification, a control architecture, a method of influence, a horizon of expansion, a means of virtualization, a place of movement, a network of connections, an information resource, and an activator of the senses." It is "a world of interconnected computer networks creating an information space with the possibility of exploring it, and feeling it with the help of senses stimulated by computer-assisted devices" (Janowski, 2012) or an immaterial emanation of the Internet, a new space in which social life takes place in a specific way – a combination of two components: technical and social (Dobrzeniecki 2004). Following the current view, the technical infrastructure of cyberspace is mainly owned by global IT companies. Therefore, the law should effectively protect the infrastructure from attacks so that it doesn't come to the point where multinational corporations are the ones starting wars. A Comparative Study of Domestic Laws Constraining Private Sector Active Defense Measures in Cyberspace shows that current regulations are inadequate (Corkoran, 2020).

According to the Polish legal definition, cyberspace is the space for processing and exchanging information created by information and communication systems, along with the links between them and relationships with users. Such a definition is contained in the Act of 29.08.2002 on martial law and the competencies of the Supreme Commander of the Armed Forces, and the principles of his subordination to the constitutional bodies of the Republic of Poland in Article 2(1b) (unified text: Dz. U. of 2017, item 1932), the Law of 21.06.2002 on the state of emergency in Article 2, paragraph 1a (unified text: Dz. U. of 2017, item 1928), and the Law of 18.04.2002 on the state of natural disaster in Article 3, paragraph 4 (unified text: Dz. U. of 2017, item 1897). To these three acts of law, the definition of cyberspace was introduced by a single act: the Act of 30.08.2011 on

amending the Act on martial law and on the competencies of the Commander-in-Chief of the Armed Forces and the principles of his subordination to the constitutional bodies of the Republic of Poland, and some other acts (Dz.U. item 1323). The laws on states of emergency allow for the introduction of: 1) in the event of an external threat to the state caused by actions in cyberspace; 2) in the event of a specific threat to the constitutional system of the state, the security of citizens or public order caused by actions in cyberspace; 3) to prevent the consequences of natural disasters or technical failures bearing the hallmarks of a natural disaster caused by events in cyberspace, and to remove them.

In the "Cybersecurity Strategy of the European Union: an open, secure and protected cyberspace" of 2013, cybersecurity refers to safeguards and actions that can be used to protect the "cyber domain," both civilian and military, from those threats that affect its interdependent networks and information infrastructure and that can damage those networks and that infrastructure. The 2015 cybersecurity doctrine of the Republic of Poland, referring to this EU strategy, defines cyberspace as "the space of information processing and exchange created by information and communication systems (ensembles of cooperating IT devices and software that provide for the processing, storage, as well as the sending and receiving of data over telecommunications networks by means of a telecommunications terminal device appropriate for the type of network intended to connect directly or indirectly to network terminations), together with the links between them and the relationships with users". The term cyberspace appears 34 times in the current Republic of Poland's Cyber Security Strategy for 2019–2024. The term cyberspace also appears, without definition, in the preamble to the 2016 NIS Directive (Szpor, 2016; Great Encyclopedia of Law, 2021).

The evolution of threats in (cyber)space

At present, electronic communication is used by several billion users. Global growth is being observed in the number of Internet users – in January 2022, they accounted for about 62.5% of the population, cell phone users, accounting for 67.1% of the population, or social media users, 58.4%. The amount of time spent online is also growing, which among Internet users aged 16 to 64 was already 6 h 58 m per day at the beginning of 2022 (DataReportal, Digital, 2022). Global trends show a significant increase in the popularity of e-commerce, which, boosted by the COVID-19 pandemic, shows no signs of slowing down once some restrictions are lifted. Therefore, it should not be surprising that criminals are also becoming more active online.

Depending on the definition of hacking adopted, most of the crimes committed in cyberspace can be classified as hacking. Since representatives of the doctrine of criminal law in Poland understand hacking as a criminal act involving unauthorized access to information by breaking or bypassing security measures, the broader concept of cybercrime will be used for the general characterization of cyber threats caused by humans.

The hacking problem in the (cyber)space can be analyzed in several dimensions.

New opportunities for the exploration and use of space data make such data an object of interest on the part of criminal groups – both as a primary target for perpetrators and as a necessary means to prepare for other cyber attacks, including geographically targeted disinformation operations. Thus, focusing on the object of protection, it is possible to analyze attacks on spatial data and examine the perpetrators' criminal liability, taking into account the nature of the acquired data. At this point, however, it should be noted that spatial data are not subject to specific protection under

Polish law. They are subject to protection on general principles as information, while if they are processed in electronic form – they will be protected as computer data. If they constitute personal data or are a component of a legally protected secret, they will also be subject to specific regulations (Gryszczyńska, 2019).

Hacking can also be analyzed considering the problem of crime mapping and geographic profiling. The idea of crime mapping has its roots in the theoretical assumptions of environmental criminology, which seeks relations between crime and its environmental and geographic determinants. Crime maps enable us to seek the reasons for the concentration of criminal activity in the area. Geographic profiling allows for establishing the most likely estimated place of residence of serial offenders (based on information concerning crime location and places of significance to the incident). The problem of uneven distribution of crime in time and space is one of the most essential and inspiring phenomena of modern criminology. When studying the movement of crime to cyberspace, it is also important to see the impact of this phenomenon on criminological studies on the spatial distribution of crime (Goldschneider, 2010). The typical and most common methods identified in criminology studies must be revisited. For example, studies on crime scene locations are related mainly to hot spots, places where more criminal incidents than the average are reported. However, it should be taken into account that hacking, or more broadly, cybercrime, has transitioned previously geographically located crimes (e.g., fraud, theft) to a space without borders (Chang & Whitehead, 2022). By its very nature, cybercrime is characterized by global reach (the perpetrators' actions are not limited to a specific place or geographic area), anonymity (it is difficult to locate the source of the attack, where the perpetrator acted, make attribution or establish the perpetrator's identity) or, finally, ease of asymmetric effect (thanks to simple and cheap access to information resources and data processing systems, it is possible to cause significant damage with relatively small forces and resources). This makes it possible for a criminal with a single action to simultaneously bring about the effects observed in many places (e.g., infecting many victims with malware). Victims of such an act will file crime reports with many different law enforcement units (e.g., police stations). What's more, actions in cybersecurity usually have a cross-border nature – their adverse effects are observed in many countries, and the perpetrators also use infrastructure from many providers around the world. An example is a case involving Korean military hacking units, known by multiple names in the cybersecurity community, including Lazarus Group and Advanced Persistent Threat 38 (APT38). According to the indictment, the perpetrators launched attacks on numerous financial institutions worldwide. Around October 2016, the hackers gained unauthorized access to the Polish Financial Supervision Authority's computer network and turned its website into a watering hole (Indictment, 2020 a). The same group is responsible for the WannaCry ransomware attack (Criminal Complaint, 2018), which was estimated to have affected more than 200,000 computers across 150 countries, with total damages ranging from hundreds of millions to billions of dollars. Examining the locations of concentrated crime notifications in space will therefore not always be a good indicator. Using anonymizing network traffic tools (VPN, PROXY, TOR) by perpetrators also makes it unreliable to determine the perpetrator's physical location based on IP addresses.

However, a caveat should be made that some attacks are geographically targeted (at a specific facility, a business entity, or a specific country), and attack attribution can also be carried out on this basis. For example, in 2020, a federal grand jury in Pittsburgh returned an indictment charging six computer hackers, all residents and nationals of the

Russian Federation and GRU officers. These hackers and their co-conspirators engaged in computer intrusions and attacks intended to support Russian government efforts to undermine, retaliate against, or otherwise destabilize Ukraine; Georgia; elections in France and the 2018 PyeongChang Winter Olympic Games after Russian athletes were banned from participating under their nation's flag, as a consequence of Russian government-sponsored doping effort (Indictment, 2020 b).

However, attacks that target a particular geographic location sometimes have global implications. The NotPetya malware, for example, spread worldwide, damaged computers used in critical infrastructure, and caused enormous financial losses. The target of the attack was Ukraine (about 80% of affected companies were from Ukraine). Still, the malware also spread to several companies in other geolocations due to those businesses having offices in Ukraine and networking around the globe (for example, Mondelez International, APM Terminals, FedEx, Saint Gobain, Heritage Valley Health System of Pittsburgh, law firm DLA Piper, pharmaceutical company Merck & Co). The NotPetya malware, among others, impaired Heritage Valley's provision of critical medical services to citizens of the Western District of Pennsylvania through its two hospitals, 60 offices, and 18 community satellite facilities. The attack caused the unavailability of patient lists, patient history, physical examination files, and laboratory records, thereby causing a threat to public health and safety (Indictment, 2020 b).

The example mentioned above shows that when investigating the hacking phenomenon, it is also necessary to assess the impact of the perpetrators' actions on real and virtual space – in particular, taking into account the intertwining of these two dimensions and the kinetic effect of attacks initiated in cyberspace. Given the pandemic's status and significant risks to patients' lives and well-being, the cyberattack on Brno University Hospital was considered an attack on critical infrastructure (Europol, 2020). In contrast, due to a patient's death in connection with a ransomware attack, German authorities are investigating the perpetrators on suspicion of negligent manslaughter (Wired, 2020). Analysis of incident reports, popular studies and press reports indicate the use of information operations. Gathering information on the location of selected individuals or objects in space results not only in the ability to identify the location of military bases (e.g. based on data from the Strava app) but also in classic kinetic attacks using conventional weapons – for example, in 2015, US troops bombed one of ISIS's command centres after one of the militants posted on social media a selfie taken a right in front of it (Castillo, 2015).

With the development of smart cars, autonomous drones, smart medical devices and the Internet of Things, our physical world is becoming even more intertwined with the virtual one. A disruption of Internet services and other information infrastructure can paralyze a whole country. Increasingly, attacks initiated in cyberspace have a kinetic effect. This creates additional incentives for hacking activities. As a direct consequence, we observe the emergence of new categories of hackers: state-sponsored hackers, spy hackers or even cyber-terrorists. In parallel, new concepts such as cyber-war, cyber-defence and cyber-peace have emerged as a response to cyber perpetrators' actions (Jaquet-Chiffelle & Loi, 2020). Cyberspace can also be used as a fifth theatre of war. Alongside land, water, air and outer space, the progressive militarization of the Internet, manifested by the emergence of specialized military units, is prompting a redefinition of terms such as security or national sovereignty. Military operations in cyberspace aim to facilitate or replace conventional military operations in other locations. One of the most advanced and, at the same time, most dangerous forms of threats are cyber-attacks that

will affect the course of events in outer space, leading to the descent of satellites from designated orbits around the earth (Lakomy, 2015).

Conclusions

With the development of advanced technologies, the physical world is increasingly intertwined with the virtual one, and it is ever more challenging to draw a line between space and cyberspace.

Today's bank robbers use keyboards rather than guns and steal digital wallets of cryptocurrency instead of sacks of cash. By operating in cyberspace, they do not have to devise a plan for a spectacular bank escape from law enforcement. Thanks to the abuse of the anonymity provided by the services available online, they remain unpunished. Cyber attacks attributable to state actors show that cyberspace is also an area for cyber-operation or cyber-warfare.

The development of cybercrime, including hacking, leads to the revision of current legal regulations, the development of instruments of international cooperation in cybercrime cases or the identification of new areas of criminological research. The examples given show that attacks carried out in cyberspace cause kinetic effects in real space, and thanks to the asymmetry effect, the damage caused by cybercriminals exceeds that caused by conventional perpetrators. Changes in substantive and procedural law must follow changes in the threat landscape. Unfortunately, the involvement of some countries in cyber operations and their support of cybercrime groups brings into question the effectiveness of international cooperation instruments in cybercrime cases, which are necessary due to their cross-border nature.

References

Banasiński C. (ed.). (2018). Cyberbezpieczeństwo (*Cybersecurity*). Warszawa 2018, p. 23.

Britannica. https://www.britannica.com/topic/cybercrime/Hacking [access: 14.08.2022].

Cambridge Dictionary. https://dictionary.cambridge.org/pl/dictionary/english/hack [access: 14.08.2022].

Castillo W. (2015). Air Force intel uses ISIS 'moron' post to track fighters, CNN, 5.06.2015. https://edition.cnn.com/2015/06/05/politics/air-force-isis-moron-twitter/index.html [access: 14.08.2022].

Chang L.YC., Whitehead J. (2022). What the Hack: Reconsidering Responses to Hacking. Asian J Criminol, 17, pp. 113–126. https://doi.org/10.1007/s11417-021-09356-1.

Corcoran B. (2020). A Comparative Study of Domestic Laws Constraining Private Sector Active Defense Measures in Cyberspace. Harvard National Security Journal, 11, no. 1, 1-ix.

Criminal Code of June 6, 1997 (Journal of Laws of 2020, item 1444, as amended).

Criminal Complaint. 2018. United States District Court for the Central District of California, Case No. MJ 18 – 1479. https://www.justice.gov/opa/press-release/file/1092091/download [access: 15.08.2022].

DataReportal, Digital 2022. Global Overview Report, https://datareportal.com/reports/digital-2022-global-overview-report [access: 14.08.2022].

Dobrzeniecki K. (2004). Prawo a etos cyberprzestrzeni (*Law and the ethos of cyberspace*). Toruń, p. 10.

Eckart J.P. (2019). The Department of Justice Versus Apple Inc. – The Great Encryption Debate Between Privacy and National Security, 27 Cath. U. J. L. & Tech 1. https://scholarship.law.edu/jlt/vol27/iss2/3 [access: 14.08.2022].

Europol, 2020. Pandemic profiteering: how criminals exploit the COVID-19 crisis. Europol. https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis [access: 14.08.2022].

Glossary of key cybersecurity terms (*Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*) NSC 7298 1.0 01/09/2021 https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber [access: 26.08.2022].

Goldschneider M. (2010). Geography of crime. Remarks on spatial analyses of crime with the use of digital technologies (*Geografia przestępczości. Uwagi na temat przestrzennych analiz przestępczości przy wykorzystaniu technik cyfrowych*), Archiwum Kryminologii, XXXII (2010), p. 23–43, DOI 10.7420/AK2010B.

Great Encyclopedia of Law, T. XXII, Information Technology Law (*Wielka Encyklopedia Prawa, T. XXII, Prawo informatyczne*), Warsaw 2021, pp. 149–150.

Gryszczyńska A. (2019). Handling incidents involving spatial data breaches. In: I. Basista, P. Cichociński, E. Dębińska, M. Gajos-Grzetić (ed.), 26th Geographic Information Systems Conference and Exhibition "GIS Odyssey 2019". Zagreb, Croatian Information Technology Society – GIS Forum, pp. 81–90, http://www.gis.us.edu.pl/index.php/past-gis-conferences/26-gis-odyssey-2019/1081-10-handling-incidents-involving-spatial-data-breaches [access: 14.08.2022].

Harari Y. Rich elites and exploited "data colonies", https://businessdialog.pl/artykuly/bogate-elity-i-wyzyskiwane?xg_source=linkedin [access: 26.08.2022].

Indictment. 2020 a. United States District Court for the Central District of California, CR 2:20-cr-00614-DMG 2020. https://www.justice.gov/opa/press-release/file/1367701/download [access: 15.08.2022].

Indictment. 2020 b. United States District Court Western District of Pennsylvania, Criminal No. 20 316. 2020. https://www.justice.gov/opa/press-release/file/1328521/download [access: 15.08.2022].

Janowski J., 2012. Cyberkultura prawa. Współczesne problemy filozofii i informatyki prawa (*Cyberculture of Law. Contemporary problems of the philosophy and computer science of law*). Warsaw, p. 38.

Jaquet-Chiffelle D.O., Loi M. 2020. Ethical and Unethical Hacking. In: M. Christen, B. Gordijn, M. Loi (ed.), The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, vol 21. Springer, Cham. https://doi.org/10.1007/978-3-030-29053-5_9.

Lakomy M. (2015). Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw (*Cyberspace as a new dimension of competition and cooperation among states*). Katowice, pp. 168–172.

Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices (2017). Directorate General For Internal Policies Policy Department C: Citizens' Rights And Constitutional Affairs. https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf [access: 14.08.2022].

Madej M., Terlikowski M. (ed.) (2009). Bezpieczeństwo teleinformatyczne państwa (*State ICT security*). Warszawa, pp. 96–97.

Morańska D. (2015). Patologie w cyberprzestrzeni. Profilaktyka zagrożeń medialnych (Pathologies in cyberspace. Prevention of media threats). Dąbrowa Górnicza.

Nikiforova A. (2022). Open data hackathon as a tool for increased engagement of Generation Z: to hack or not to hack? Electronic Governance with Emerging Technologies Conference, Springer. Forthcoming, Available from: https://www.researchgate.net/publication/362229959_Open_data_hackathon_as_a_tool_for_increased_engagement_of_Generation_Z_to_hack_or_not_to_hack [access: 14.08.2022].

Radoniewicz F. (2016). Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym (*Criminal liability for hacking and other crimes against computer data and information systems*). Warsaw.

Resolution 74/247. 2019. Resolution adopted by the General Assembly on 27 December 2019, A/RES/74/247; https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/28/PDF/N1944028.pdf?OpenElement [access: 14.08.2022].

RFC1392. 1993. Malkin G., LaQuey Parker T., Internet Users' Glossary, RFC 1392, Interop, Inc., January 1993, https://www.rfc-editor.org/rfc/rfc1392 [access: 14.08.2022].

Scott M. (2022). How Ukraine used Russia's digital playbook against the Kremlin. From hacktivists to info wars, Kyiv is mastering digital warfare in ways previously associated with the Kremlin. 24.08.2022. https://www.politico.eu/article/ukraine-russia-digital-playbook-war [access: 25.08.2022].

Szpor G. (2016). Jawność i jej ograniczenia. Idee i pojęcia (*Openness and its limitation. Ideas and concepts*). Warsaw 2016.

The American Heritage Dictionary of the English Language (2022). Fifth Edition, https://www.ahdictionary.com/word/search.html?q=hacking [access: 14.08.2022].

The Convention on Cybercrime of the Council of Europe (CETS No.185) (2001). https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 [access: 14.08.2022].

The Jargon File, version 4.4.7, http://catb.org/jargon/html/H/hack.html [access: 14.08.2022].

Wasilewski J. (2013). Zarys definicyjny cyberprzestrzeni (*A definitional outline of cyberspace*). Przegląd Bezpieczeństwa Wewnętrznego, no. 9, p. 226.

Wired (2020). A Patient Dies After a Ransomware Attack Hits a Hospital. 19.09.2020. https://www.wired.com/story/a-patient-dies-after-a-ransomware-attack-hits-a-hospital/ [access: 14.08.2022].

Worona J. (2020). Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy (*Cyberspace and International Law. Status quo and perspectives*). Warsaw, p. 56.

Yagoda B. (2014). A Short History of Hack. The New Yorker. https://www.newyorker.com/tech/annals-of-technology/a-short-history-of-hack [access: 14.08.2022].