DOI: https://doi.org/10.12797/Politeja.14.2017.50.09

Robert Siudak
Jagiellonian University in Kraków
robert.siudak@uj.edu.pl

REDEFINING CYBERSECURITY THROUGH PROCESSUAL ONTOLOGY OF THE CYBERSPACE

ABSTRACT The way cyberspace is conceptualized in security discourses shapes strategies, tools and possible solutions developed within the ICT security debate. Putting forward processual ontology of cyberspace helps in apprehending the unique dynamics of this new domain arising from the intersection of ICT with social and political phenomena. Cyberspace is presented as a process of data transmission and information cognition/processing in the digital domain. It contains time as an inherent dimension and includes all subjects and objects of this process: data (codes, packets, files, texts), information (structured or operationalized data), human and computer agents (people, software) and communication environment (hardware, protocols). Processual ontology is based on the fact that ICT is a man-made realm with almost unlimited potential to expand, where physical distance is lapsed and bits are the primary matter. This theoretical stance blurs the line between human and non-human agents, dehumanizing the idea of actorness by categorizing both humans and computers as actors. Finally, processual ontology of cyberspace promotes resilience strategies both in the private sector as well as on national and international level.

Key words: cyberspace, security, ICT, resilience

INTRODUCTION

Through the course of the last two decades cybersecurity has become one of the core terms in security discourses. From political jargon, through military strategies, to media narratives, *cyber* became an indispensable component of individual, national and international security. Due to the wide diversity of perils, referent objects (something we want to secure) and levels of analysis, many raise the question about the functionality and utility of the term *cybersecurity* itself.[1] It has been used to portray varied aspects of risk and perils associated with Information and Communication Technologies (ICT): from internet users' safety and security,[2] through threats concerning industrial control systems vulnerabilities[3] and risk generated by the Internet of Things,[4] to cyber-espionage[5] or even information warfare.[6] Due to this plurality, many experts have argued that cybersecurity is articulated through the interplay of multiple different discourses.[7] Others claim that because of the vague nature of the term, it became almost an empty buzzword with little analytical value.[8] The present multiplicity of referent objects and threats in digital security discourses is accompanied with lack of common conceptualization of the cyberspace itself. The primary and fundamental task of this article is to develop both technologically and socially well-grounded definition of cyberspace, which will help to reframe ICT security debate.

Cybersecurity is not information security, neither computer security, nor network security.[9] The first term is broad, encompassing wide realm of information processing (including non-digital), the following two are sub-disciplines of computer science,

1 J. Brito, T. Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy", *Harvard National Security Journal*, vol. 3, no. 1 (2011), pp. 39-84.

2 E. Kritzinger, S.H. von Solms, "Cyber Security for Home Users: A New Way of Protection through Awareness Enforcement", *Computers & Security*, vol. 29, no. 8 (2010), pp. 840-847, at <http://dx.doi.org/10.1016/j.cose.2010.08.001>.

3 W. Shaw, *Cybersecurity for SCADA Systems*, Tulsa 2006.

4 M. Abomhara, G.M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks", *Journal of Cyber Security and Mobility*, vol. 4 (2015), pp. 65-88, at <http://dx.doi.org/10.13052/jcsm2245-1439.414>.

5 G. Brown, "Spying and Fighting in Cyberspace: What Is Which?", *Journal of National Security Law & Policy*, vol. 8 (2016), pp. 621-643.

6 J. Nye, "Cyber Power", Harvard Kennedy School Belfer Center for Science and International Affairs, May 2010, at <https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf>.

7 R.J. Deibert, "Circuits of Power: Security in the Internet Environment", in J. Rosenau, J.P. Singh (eds.), *Information Technologies and Global Politics. The Changing Scope of Power and Governance*, Albany 2002, pp. 115-142. Deibert itself distinguishing four of them (national security, state security, private security and network security discourse).

8 "Some Perspectives on Cybersecurity: 2012", Internet Society, 2012, at <https://www.internetsociety.org/sites/default/files/bp-deconstructing-cybersecurity-16nov-update.pdf>.

9 M. Bay, "What Is Cybersecurity? In Search of an Encompassing Definition for the Post-Snowden Era", *French Journal For Media Research*, no. 6 (2016), pp. 1-28; R. von Solms, J. van Niekerk, "From Information Security to Cyber Security", *Computers and Security*, vol. 38 (2013), pp. 97-102, at <https://doi.org/10.1016/j.cose.2013.04.004>.

while *cyber* arises from the intersection of ICT with a number of social phenomena from political science, international relations, security studies as well as sociology. Therefore, the multidisciplinary quest for the definition of cyberspace must be driven by more than merely technological factors. Taking into account purpose of this article and the socially mediated nature of cyberspace, it needs to be defined what has to be secured in/through/by the digital domain. The way cyberspace is conceptualized through the list of security referent objects in the digital domain shapes potential tools and solutions which might be adopted to structure and secure this realm. The intersubjective nature of these processes stresses the role of non-technological determinants, such as social, cultural, political or even ideological factors. Furthermore, the linguistic turn in philosophy, applied successfully also in political science,[10] emphasizes the role of language in these processes. The way we think and speak about cyberspace creates boundaries of our cognition and decisively influence our agenda, available procedures and possible policy solutions.[11] This is especially problematic in cybersecurity discourses, where two distinct fields of expertise are mixed: technological – originating from computer science, and social/political – derived from political science and international relations. To sum up the above outlined theoretical background, this article builds on the constructivist paradigm.[12] It stresses that although on the technical level cyber-threats are universal world-wide, intersubjective processes are those which shapes their meaning and perception of them within different communities. In short, technology does not speak for itself – it has to be socially mediated.

The aforementioned theoretical background frames the analysis of two main research questions of this article: Why cyber*space* is conceptualized as a space? What are the main roots and consequences of this spatialization in the context of ICT security? By putting forward hypothesis of triple origins of our spatial tendencies:
1) human species' cognitive predispositions,
2) cultural background,
3) language/discursive practices,
this article redirects the focus of the debate from methodological disputes (how to secure cyberspace) to ontological considerations (what we want to secure in/through/within cyberspace). As a result, pioneering ontology based on the process rather than substance is presented as the alternative to the spatialization of cyberspace.

The first part of the text introduces traditional views concerning cyberspace. The history and initial context of the term *cyber*, as well as present disciplinary debates are discussed. The second part explains why currently disseminated conceptualizations of cyber as a space are misleading and counterproductive. Main sources of these fallacies are examined including our natural cognitive predispositions and the uniqueness of cyberspace in comparison to other spaces. The third part of the text presents proces-

[10] I.B. Neumann, "Returning Practice to the Linguistic Turn: The Case of Diplomacy", *Millennium*, vol. 31, no. 3 (2002), pp. 627-651, at <https://doi.org/10.1177/03058298020310031201>.

[11] G. Lakoff, M. Johnson, *Metaphors We Live by*, Chicago 2003.

[12] A. Kukla, *Social Constructivism and the Philosophy of Science*, London–New York 2000.

sual definition of the cyberspace and its implications on the idea of actorness in the digital domain. It defines the process of cognition and communication of information through computer mediated environment as the primary building block and constitutive function of cyberspace. These specific qualities of the digital realm blurs clear distinction between humans and computer agents, thus changing the notion of actorness in the cyberspace. Finally, the processual nature of the cyberspace is presented as a theoretical background for the resilience strategy and process oriented taxonomy of the cyber domain.

THE CYBERSPACE: TRADITIONAL DEFINITIONS

The following section will present a brief introduction of traditional definitions of cyberspace. The short analysis from selected realms presented below does not aspire to be a comprehensive research on all aspects of cyberspace debate. Due to the limited space and the defined purpose of this article, only chosen domains and theories will be examined with the goal of highlighting ontological assumptions of available cyberspace definitions.

The history of the term 'cyberspace' dates back to 1984 when William Gibson introduced it in his science fiction book *Neuromancer* as *A consensual hallucination* [...] *A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data*.[13] The career of the term in cyber-punk literature and the fact that neither literature not computer nor political science has been the original domain which introduced cyberspace shall not be underestimated. Here could be traced the very first cause of the rather problematic and still undefined status of the cyberspace. A set of strict rules are the founding principles of any scientific domain. A new term introduced in natural or social science has to be clearly defined and described (at least theoretically). Literature, on the other hand is not bound by any scientific rules, and therefore cyberspace from the very beginning did not have a clear and defined status, which then could have been used as a basis for disciplinary debate in political or computer science. Quite the opposite, as we shall see for more than a decade till the late '90s, the term has been coined mainly in literature, press and by the first internet activists, but without wide interest from academia. In this period, the first group of definitions has been introduced, based on the idea of cyberspace as a paraspace or non-space and a virtual environment that excludes physical space.[14] The prime example could be the J.P. Barlow *Declaration of the Independence of Cyberspace* where he states that *Ours*

[13] W. Gibson, *Neuromancer*, New York 1995, p. 51. In fact Gibson once used the term cyberspace two years earlier in his short novel *Burning Chrome*, see L. Strate, "The Varieties of Cyberspace: Problems in Definition and Delimitation", *Western Journal of Communication*, vol. 63, no. 3 (1999), pp. 382-412, at <https://doi.org/10.1080/10570319909374648>.

[14] D.J. Betz, T. Stevens, "Analogical Reasoning and Cyber Security", *Security Dialogue*, vol. 44, no. 2 (2013), pp. 147-164, at <https://doi.org/10.1177/0967010613478323>.

is a world that is both everywhere and nowhere, but it is not where bodies live,[15] or Benedikt's *computer-sustained, computer-accessed, and computer-generated, multidimensional, artificial, or 'virtual' reality*.[16]

The Barlowian cyberspace has been constitutionally political, establishing its own internal independent rules and laws.[17] Following the clash between these libertarian ideas of the first Internet users and the growing IT industry, law practitioners and scholars have been one of the first who stimulated debate over cyberspace qualities. Some scholars argued that there is no qualitative difference between other networks and cyberspace, and in fact it should not be regarded as a space but yet another type of network created by new technologies.[18] Others stressed the need to perceive cyberspace as a useful metaphor that shall be adopted more consciously and in a goal oriented manner in legal systems.[19] Koepsell in his search for the ontological basis of intellectual property laws in cyberspace criticized naïve and incorrect legal categories which laid the ground for the false system based on patents and copyrights.[20] Finally, there have been voices stressing the qualitative difference between legal systems that we have in place, and rules in cyberspace. Lawrence Lessing stated famously that the code is the law in cyberspace and these unique characteristics of that realm must be adopted by the state in order to regulate the cyber-domain.[21]

The career of cyberspace as a controversial term began in the literature and law, but for the purpose of this article, the most important domain of the cyberspace debate has been social sciences. A hugely influential theoretical frame came from Libicki, who distinguished between three layers of the cyberspace: physical (hardware), syntactic (software and protocols) and semantic (information and ideas).[22] Clark in his four-layer categorization not only adds the first additional level the analysis, but also upturns it, putting at the first place people who actively create cyberspace.[23] Strate in his analysis

---

15 J.P. Barlow, "A Declaration of the Independence of Cyberspace", The Electronic Frontier Foundation, 1996, at <http://www.eff.org/pl/cyberspace-independence>, 2 November 2017.

16 M. Benedikt, "Cyberspace: Some Proposals", in idem (ed.), *In Cyberspace. First Steps*, Cambridge, Mass. 1994, p. 123.

17 J.L. Goldsmith, "Regulation of the Internet: Three Persistent Fallacies", *Chicago-Kent Law Review*, vol. 73, no. 4 (1998), pp. 1119-1131.

18 B.M. Frischmann, "The Prospect of Reconciling Internet and Cyberspace", *Loyola University Chicago Law Journal*, vol. 35, no. 1 (2003), pp. 205-234.

19 J.R. Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules through Technology", *Texas Law Review*, vol. 76, no. 3 (1998), pp. 553-593; L. Lessing, *Code and Other Laws of Cyberspace. Version 2.0*, New York 2006.

20 D.R. Koepsell, *The Ontology of Cyberspace: Philosophy, Law, and the Future of Intellectual Property,* Chicago 2003.

21 L. Lessing, *Code 2.0 and Other Laws of Cyberspace*, New York 2006.

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

23 D. Clark, "Characterizing Cyberspace: Past, Present, and Future", ECIR Working Paper, 2010, at <https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf>, 2 November 2017.

defines not layers, but three distinctive orders of cyberspace.[24] His second order called 'cybermedia space' includes among others relational space. This relational nature of the cyberspace is discussed and raised by many scholars, especially Barnard-Wills and Ashenden.[25] At the same time, there is a need to be aware of the distinctive feature of these relations – the inherent role of technology, demonstrated by the fact that in cyber domain *social relations are as much a part of the socio-technical assemblage as hardware and software*.[26] In this view, cyberspace is perceived as a metaphor of an emerging social arena populated by humans, telephones, television and computers, rather than strict designations for physical reality. In contrast the Internet is a clearly defined cluster of hardware, protocols and data exchange through them.

An important conceptual challenge debated among experts is the relationship between cyberspace and media ecology. The crucial challenge for the definition of cyberspace is deciding whether to exclude or include media ecology in cyberspace. The RAND Corporation report published in 1999 excludes media ecology from their definition of cyberspace. It defines three information realms: cyberspace, infosphere and noosphere.[27] Cyberspace is presented as the narrowest one, including hardware and software with all infrastructure connecting them, infosphere consisting of cyberspace plus media ecology and noosphere encompassing all mentioned previously plus the whole information exchange in the society. Because of emerging hybrid threats that are combining and blending attacks on hardware and software layers with the use of new media, it seems highly valuable to build a definition which will be able to grasp the dynamics of both media ecology and ICT within a single term. The campaign of hacking and spreading disinformation during the 2016 US Presidental Elections is the prime example of the intertwined nature of cyberthreats.[28] Interestingly, in Russian political and strategic discourse the technological realm of the cyberspace is marginalized and the main focus is put on information as a prime subject of that domain. Therefore, such terms as *cybernetic* or *network warfare* are used in the sense of informational warfare in

[24] L. Strate, "The Varieties of Cyberspace...", pp. 382-412.

[25] A.R. Stone, *The War of Desire and Technology at the Close of the Mechanical Age*, Cambridge, Mass. 1996; M.D. Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse", *International Studies Review*, vol. 13, no. 1 (2013), pp. 105-122, at <http://dx.doi.org/10.1111/misr.12023>. Cf. D. Barnard-Wills, D. Ashenden, "Securing Virtual Space: Cyber War, Cyber Terror, and Risk", *Space and Culture*, vol. 15, no. 2 (2012), p. 111, at <https://doi.org/10.1177/1206331211430016>.

[26] D.J. Betz, T. Stevens, "Analogical Reasoning...", p. 152.

[27] J. Arquilla, D. Ronfeldt, *The Emergence of Noopolitik. Toward an American Information Strategy*, Santa Monica 1999.

[28] Department of Homeland Security and Federal Bureau of Investigation, *GRIZZLY STEPPE – Russian Malicious Cyber Activity*, 2016, at <https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY STEPPE-2016-1229.pdf>, 2 November 2017; Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections*, 2017, at <http://www.dni.gov/files/documents/ICA_2017_01.pdf>, 2 November 2017.

the digital age.[29] In contrary, most strategic documents in western countries do not include media ecology and the role of mass communication in their cyberspace analysis.

The traditional views on cyberspace presented above in a number of cases have been touching upon its processual character. Especially Barnard-Wills and Ashenden as well as Betz and Stevens, are in some ways including relational or processual nature as an important part of their concepts. The qualitative diffrence beetwen previous conceptualisations and the propostion put forward in this article lays in the level of inclusion of processual charactersitics. In traditional theories process or relation are added as the element linking or animating the role of phisical or logical components (hardware, software, people). In a way they fill in a gap in the 'cyberspace picture'. Therefore ontologically *cyber* is presented there as a domain where different components are in relations to each other and interact in different processes. This means that on the basic level (ontology) cyber is a space where all this might happen. The idea put forward in this article proposes a different conceptualisation based not on domain-focused but process centred ontology. All variables included in the definition of the cyberspace (not only hardware, software or people but now also time) are conceptualized in relation to their role in the process which is presented as the basic unit of analysis.

CYBER AS A SPACE

The inherent spatialization of cyber discourse might be exemplified by this article, which for the sake of introducing non-spatial ontology of the cyber domain has to use the term cyberspace as a central reference. Roots of this situation are to be found on three different levels. The first involves human species' cognitive predispositions, the second our cultural background, and the third our language and discursive practices. In reality, all of these three layers are intertwined and influenced by each other but for the sake of analytical clearance they will be presented separately.

The cognition of homo sapiens is spatialized. Biologically our body is oriented to perceive three-dimensional spaces. Evolutionary anthropology confirms that our cognitive setup evolved through the ages with spatial contextual awareness being one of the most important attribute in the process.[30] Faced with a new technological realm, such as cyber we familiarize it by conforming it to our biological and evolutionary territorial predispositions. Researchers stresses the role of our personal cognitive maps, which we create to aggregate knowledge about certain domains and then to operationalize it

[29] J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, at <https://www.osw.waw.pl/sites/default/files/anatomia_rosyjskiej_wojny_informacyjnej.pdf>, 2 November 2017; eadem, *Diabeł tkwi w szczegółach. Wojna informacyjna w świetle doktryny wojennej Rosji*, at <https://www.osw.waw.pl/sites/default/files/pw_50_pl_diabel_tkwi_net.pdf>, 2 November 2017; eadem, *Rosyjskie siły zbrojne na froncie walki informacyjnej. Dokumenty strategiczne*, at <https://www.osw.waw.pl/sites/default/files/prace_57_pl_sily_zbrojne_net.pdf>, 2 November 2017.

[30] F.L. Dolins, R.W. Mitchell, *Spatial Cognition, Spatial Perception. Mapping the Self and Space*, New York 2010.

in our actions.[31] Adding another layer to this Betz and Stevenson are writing about an *intuitive sense of place*.[32] Apart from brain focused rational analysis, they refer to the embodied experience of space, which is rather egocentric than geocentric.

On the second level, the way we perceive space and spatiality is formed by our cultural background. In western culture, one Enlightenment thinker has to be specifically highlighted for laying down the foundations of nowadays' common sense space concept. Cartesian grid is intrinsically built into our perception and plays a structuring role in our rationalist determinism.[33] Thanks to the French philosopher a three dimensional universal space is the core of modern logic of spatiality.[34] Cyber is presented as a space because of its participation in Cartesian x – y – z coordinates. This universal and substantive stance is in opposition with relational theories such as Einstein's theory of relativity,[35] but Descartes' principles seem still to be the unshakeable foundations of our common sense spatial perception. However, this does not mean that relativist stance could not play a productive role in our understanding of new technological phenomena such as cyberspace. The additional dimension of time which is one of the focal point in relational theories helps also to better grasp the nature of the cyber domain. Einstein in his theory[36] states that space and time should be treated together as two dimensions of the same continuum, which he calls space-time. Being aware of different levels of analysis between Einstein's cosmological theories and our socio-technological disputes, processual ontology of cyberspace has to include a temporal dimension to better understand the nature of the cyber domain.[37] Here, Strate proposes the idea of *Cyberspacetime*[38] and indeed time dependent nature originates from the very make-up of ICT.

The third source of the spatial image of cyber domain is to be found in our language and discursive practices. Linguistic turn taught us that language, perception and our knowledge are inextricably intertwined. Furthermore Sapir-Whorf's hypothesis opened the discussion about language and perception dependency.[39] The way we speak

---

31 A. Kellerman, "Cyberspace Classification and Cognition: Information and Communications Cyberspaces", *Journal of Urban Technology*, vol. 14, no. 3 (2007), pp. 5-32, at <https://doi.org/10.1080/10630730801923110>.

32 D.J. Betz, T. Stevens, "Analogical Reasoning...", p. 151.

33 S. Penny, "Virtual Reality as the Completion of the Enlightenment Project", in G. Bender, T. Druckrey (eds.), *Cultures on the Brink. Ideologies of Technology*, Seattle 1994, pp. 231-248.

34 D.J. Gunkel, A.H. Gunkel, "Virtual Geographies: The New Worlds of Cyberspace", *Critical Studies in Mass Communication*, vol. 14, no. 2 (1997), pp. 123-137, at at <https://doi.org/10.1080/15295039709367003>.

35 R. Bryant, "What Kind of Space Is Cyberspace?", *Minerva*, vol. 5 (2001), pp. 138-155.

36 A. Einstein, *Relativity. The Special and the General Theory*, Oxford 2015.

37 R. Ottis, P. Lorents, "Cyberspace: Definition and Implications", NATO Cooperative Cyber Defence Centre of Excellence, pp. 267-270, at <https://ccdcoe.org/multimedia/cyberspace-definition-and-implications.html>, 2 Novemer 2017.

38 L. Strate, "The Varieties of Cyberspace...", p. 389.

39 E. Sapir, *Language. An Introduction to the Study of Speech*, New York 1921.

about cyberspace, the analogies and metaphors we adopt for that matter – all of this serves not only to present some objective reality, but also to create our intersubjective understanding of cyberspace. The problem of familiarizing ourselves with a new technological realm is especially challenging. To make sense of these unprecedented phenomena, we use concepts already available in our language and culture. The spatial metaphor present in the form of cyberspace and used widely in cybersecurity discourses is a prime example of this mechanism. We need to be aware that metaphors work as cognitive and some even say normative *structuring devices*.[40] They structure our perception of selected phenomena by intertwining different emotional, factual and instrumental sides. Furthermore, in the case of ICT our tendency to perceive and portrait them through well-grounded conceptions goes beyond the spatial metaphor. Biologization of cyber discourse is another example of this mechanism. Worms, viruses, infections and other epidemiological terms are widely adopted in the debate about cyberspace. The source of this is to be found in our tendency to frame technological processes in lifelike schemes.

Finally our spatialized understanding of the cyber domain is embedded in our social and political practices. Cyberspace is positioned as a direct descent from previously 'discovered' and governed spaces, such as seas, air or outer space. Therefore, like those before, it should be mapped and secured. Based on this premise we adopt similar procedures and strategies, coping solutions which gave best results in previously accommodated realms. The fundamental problem is that cyberspace represents completely different concept of spatiality (if any) and because of this, our traditional strategies are not adequate, nor efficient.[41] As it will be presented in this article, in contrast to traditional domains cyberspace is a man-made realm, with almost unlimited potential or multiplication of a new building blocks, with no linear distance applicability and ontological supremacy of bits of information over atoms. As the processual ontology shows *Cyberspace has the potential to interrupt the very structure, substance, and control of modern epistemology*.[42]

PROCESSUAL ONTOLOGY OF CYBERSPACE

The importance of cyberspace in public discourse grew enormously in the 21st century mainly in the context of emerging digital threats. Our growing dependency on ICT created the so called cyber-security dilemma.[43] From media, politicians and secu-

[40] S. Lawson, "Putting The 'War' in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States", *First Monday*, vol. 17, no. 7 (2012), at <http://dx.doi.org/10.5210/fm.v17i7.3848>.

[41] R. Bendrath, "The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection", *Information & Security: An International Journal*, vol. 7 (2001), pp. 80-103, at <http://dx.doi.org/10.11610/isij.0705>.

[42] D.J. Gunkel, A.H. Gunkel, "Virtual Geographies...", p. 126.

[43] B. Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*, Oxford–New York 2017.

rity specialists we have heard about *Cyber Pearl Harbor*, *Cyber 9/11*, and other cyber doomsday scenarios, that are going to happen sooner or later.[44] Scholars from the field of critical security studies described cyberspace as a new arena of successful securitization processes. The processual theory of the cyberspace helps to answer the fundamental question – what shall be secured when it comes to the cyber domain. In other words, what is of most value for certain communities that might be existentially threatened, and if destroyed or distorted will have a lasting and damaging impact. In securitization theory this is called the referent object of security. In traditional security sectors such as military, political or societal, it is usually defined as a place (e.g. national territory), system (e.g. republican and democratic) or a certain set of values (e.g. national or religious identity). The prime error in most analyses of cybersecurity dynamics is the use of these traditional, spatialized and object-oriented categories of referent objects to portrait security problems in the cyber domain.

To counter this spatial and object-oriented cognition of cyberspace, first it has to be emphasized, that in contrast to other spaces (land, air, seas and outer space) ICT created the first totally man-made realm, with practically unlimited possibilities of creating new building blocks. The price and availability of IT infrastructure in the age of cloud computing and on the verge of quantum computing makes it expandable and borderless. This in turn qualitatively changes the character of security dynamics, undermining the value of traditional referent objects in the ICT mediated processes. Unlike in any other space, digital technology enables almost unlimited multiplications of valuable assets. Its decentralized structure enables also enhancing security by distrusted database systems (e.g. blockchain technology). The difference between geographically bounded physical space and the real-time-multi-location nature of the ICT domain is exemplified by the Estonian and Ukrainian security problems with Russia.

Estonia in 2007 had been a victim of the DDOS (distributed denial of service) cyber-attack, which targeted its public sector as well as banks and other crucial service providers. Because of the nature of the cyberspace, the attribution of these offensive actions could not be confirmed with hundred percent certainty, nevertheless most analysts agreed, that they have at least been stimulated by Russian decision makers.[45] After the crisis Estonia adopted a wide range of policies to boost its cybersecurity on a national level. One of the key goals stressed in the Estonian 2014-2017 Cyber Strategy is to *ensure digital continuity of the state* by creating mirrors and backups for all crucial systems and processes.[46] If Estonian servers in Tallinn would be destroyed or corrupted (or even if the whole country would be invaded by foreign forces), thanks

[44] K. Quigley, C. Burns, K. Stallard, "'Cyber Gurus': A Rhetorical Analysis of the Language of Cybersecurity Specialists and the Implications for Security Policy and Critical Infrastructure Protection", *Government Information Quarterly*, vol. 32, no. 2 (2015), pp. 108-117, at <https://doi.org/10.1016/j.giq.2015.02.001>.

[45] S. Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", *Journal of Strategic Security*, vol. 4, no. 2 (2011), pp. 49-60, at <http://dx.doi.org/10.5038/1944-0472.4.2.3>.

[46] Estonian Ministry of Economic Affairs and Communication, *Cyber Security Strategy for 2014-2017*,

to the system of distributed backups abroad, the government would still be able to provide e-services to their citizens and to run administrative processes. It is possible thanks to the real-time-multi-location nature of the digital data enabled by such technologies as blockchain, distributed backup systems and shared cloud infrastructure.[47] This in turn refocuses the dynamics of security dilemma from the object oriented analysis to process similar schemes.

To highlight the qualitative differences we shall consider another example of offensive actions linked to Russia. The military threat that Ukraine faced over its eastern border is an exemplification of rules and limits posed by traditional, object oriented security dilemmas. In 2014, Ukrainian Crimea became an arena of hybrid operations, including physical invasion of (most probably) Russian troops. Not going into details about the political and social divisions within Ukraine and about the turmoil in Kiev at that time, the Ukrainian government lost control over the Crimean territory due to separatist operations. The obvious fact is that there is only one unique Crimean Peninsula and that the annexation has irreversible results for the state of Ukraine. This shows how different ontologies should be applied to physical (object bounded) and cyber (process based) space securities.

An additional intrinsic quality of the ICT domain is the man-made character and the easiness of creation, which causes high and unprecedented mutation of this realm. The permanent change of the IT infrastructure is driven by technological breakthroughs, such as new protocols, new hardware or new systems, but also by social factors such as political decisions, market forces and our daily practices. Taking into account limited physical dependency and the constant mutation of the ICT domain, we can deduct that it is almost impossible to pinpoint selected spatial objects, whose protection will ensure enduring cybersecurity. It is even more problematic if we would take into account the way it abolishes linear distances and clear boundaries. The way in which information circulates in the ICT realm is not constrained by physical distance, vectors nor boundaries. The most known network – Internet – transfers packets between endpoints in a asymmetric, non-linear and almost instant manner.

Finally, spatialized referent objects do not suit cybersecurity because ICT is built on bits and not atoms[48]. Binary digits (bits) are the basic units of digital world.[49] Therefore, not physical atoms, but information made from bits are the primary building blocks of cyberspace. Due to that characteristic the traditional goal in computer security has been to provide information confidentiality, integrity, and availability. Examination of the difference between *data* and *information* in the digital domain will enable to apprehend the processual nature of cyberspace. According to the widely used data – in-

Tallin 2014, at <https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf>.

47 Many R&D project are currently investigating also BlockCloud – introduction of blockchain into the cloud products.

48 N. Negroponte, *Being Digital*, New York 1995.

49 M. Castells, *The Information Age. Economy, Society, and Culture*, vol. 1: *The Rise of the Network Society*, Oxford 2010.

formation – knowledge – wisdom hierarchy (DIKW), data is a symbol, sign or signal, unorganized and raw. Information is an organized, structured or presented in a given context data which allows to make sense of it and to operationalize it. The uniqueness of the cyber domain is to be found in the fact that agents responsible to analyze and organize digital data into information are in most cases not human brains, but computers (software installed on hardware). Nowadays even such 'human' abilities as structuring on the bases of previously processed data or current context are available in the form of machine and deep learning, artificial intelligence and contextual computing.

To understand what has to be secured in cyberspace, it has to be acknowledged that we live in *information societies* which are based on the growing importance of data and information in all forms, but to a growing extent in a digital one.[50] Our *cyber society is a society where computerized information transfer and information processing is (near) ubiquitous and where the normal functioning of this society is severely degraded or altogether impossible if the computerized systems no longer function correctly*.[51] Therefore, the phenomenon we call cyberspace is not created by computers themselves, but by their role in processing and transferring information, in short by their interconnection. It is the introduction of 'Communication' into Information Technologies that opened totally new areas of opportunities and threats. Transformation of IT into ICT is the moment which marked the beginning of cyberspace and cyber threats as we know them today. That is why what has to be secured is not merely data or information. That had been already covered by computer security. Cybersecurity has to protect the whole process of information processing and communication in the digital domain. It has to include all subjects and objects of this process:

- Data (codes, packets, files, texts),
- Information (structured or operationalized data),
- Human and computer agents (people, software),
- Communication environment (hardware, protocols).

Cyberspace is a process of data transmission and information cognition/processing in the digital domain. It is an inseparable mix of human and technological components and their relations where both computers and humans might be able to create and transmit information. This ontology includes time as a dimension and sets process itself as a referent object of security. It also blurs the line between human and non-human agents. This seems indispensable due to the fact that most digitalized services in our societies will in the near future be dependent on machine to machine communication thanks, to the rapid expansion of the Internet of Things and other innovative technologies. Processual ontology also helps to solve the conceptual problem with the dual

[50] In a most basic way there are single data/information of 1 or 0 value.

[51] P. Lorents, R. Ottis, R. Rikk, "Cyber Society and Cooperative Cyber Defence", in N. Aykin (ed.), *Internationalization, Design and Global Development. Third International Conference, IDGD 2009, Held as Part of HCI International 2009, San Diego, CA, USA, July 19-24, 2009*, Berlin 2009, p. 180, at <https://doi.org/10.1007/978-3-642-02767-3_20>.

nature of cyberspace, which is at the same time an infrastructure enabling information processing and communication medium.[52]

REDEFINING CYBERSECURITY PRIORITIES WITH PROCESSUAL ONTOLOG

Finally, an argument has to be offered why processual ontology of the cyberspace should serve a theoretical background for cybersecurity strategies. The prime reason is to be found in the dispersed and manifold characteristics of threats faced in the cyber domain. *Attacks can come at all layers, from destruction of physical components to compromise of logical elements to corruption of information to corruption of the people*.[53] Protection plans have to encompass varied types and levels of possible vulnerability spots including hardware design, source codes, protocols, human factor and procedures, as well as relations between these embedded in a time frame.

Processual ontology introduces a system of categorization of cyber-incidents, based on the characteristics and importance of the process that is at risk. This enables to overcome the entanglement of problematic concepts such as cyberterrorism, cyberwarfare, cyberespionage or cybercrime. Adding cyber to traditional categories does not help to understand better the threats in cyber domain, sometimes it even blurs the picture. These specific terms were created in the physical realm where certain characteristics were the founding principles for them and for the tools and actors ascribed to tackle them. For example, the division between police and army evolved in 12th and 14th century Europe on the bases of borders, power centralization and entrenchment. Police units were designed to fight internal violence and the army was prepared to face external threats. The spaceless cyber domain with almost impossible actor attribution is a problematic environment for a clear distinction between crime and warfare concepts. One of the latest examples of that might be the biggest DDOS attack to date, which took place on 21 October 2016 and affected multiple servers, including Twitter, Spotify, Box, SoundCloud and Reddit. Many experts had speculated that behind this attack has been a national actor, such as China or Russia, who tested how to neutralize part of the Internet. After extensive research, it turned out that most probably the DDOS attack has been prompted by an individual American hacker under nick 'anna-senpai' who was the owner of a large botnet network called Mirami.[54] Picture 1 presents his conversation on one of the hacking forums, where he mocked analysts:

---

[52] J. Eriksson, G. Giacomello, "Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State", *International Studies Review*, vol. 11, no. 1 (2009), pp. 205-230, at <http://dx.doi.org/10.1111/j.1468-2486.2008.01841.x>.

[53] D. Clark, "Characterizing Cyberspace...", p. 4.

[54] B. Krebs, "Who Is Anna-Senpai, the Mirai Worm Author?", Krebs on Security, 18 January 2017, at <https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/>, 2 November 2017.

Picture 1. Conversation of Mirami botnet owner about 21st October 2016 DDOS attack

[10:49:11 AM] *katie.onis:* i love the conspiracy guys thinking this is china or another country hahaw
[10:49:18 AM] *live:anna-senpai:* yea
[10:49:22 AM] *live:anna-senpai:* lol
[10:49:29 AM] *katie.onis:* can't deal with the fact the internet is so insecure
[10:49:31 AM] *katie.onis:* gotta make it sound hard
[10:49:34 AM] *live:anna-senpai:* the scheiner on security blog post
[10:49:40 AM] *live:anna-senpai:* "someone is learning how to take down the internet"
[10:49:47 AM] *live:anna-senpai:* lol

Source: B. Krebs, "Who Is Anna-Senpai, the Mirai Worm Author?", Krebs on Security, 18 January 2017, at <https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/>, 2 November 2017.

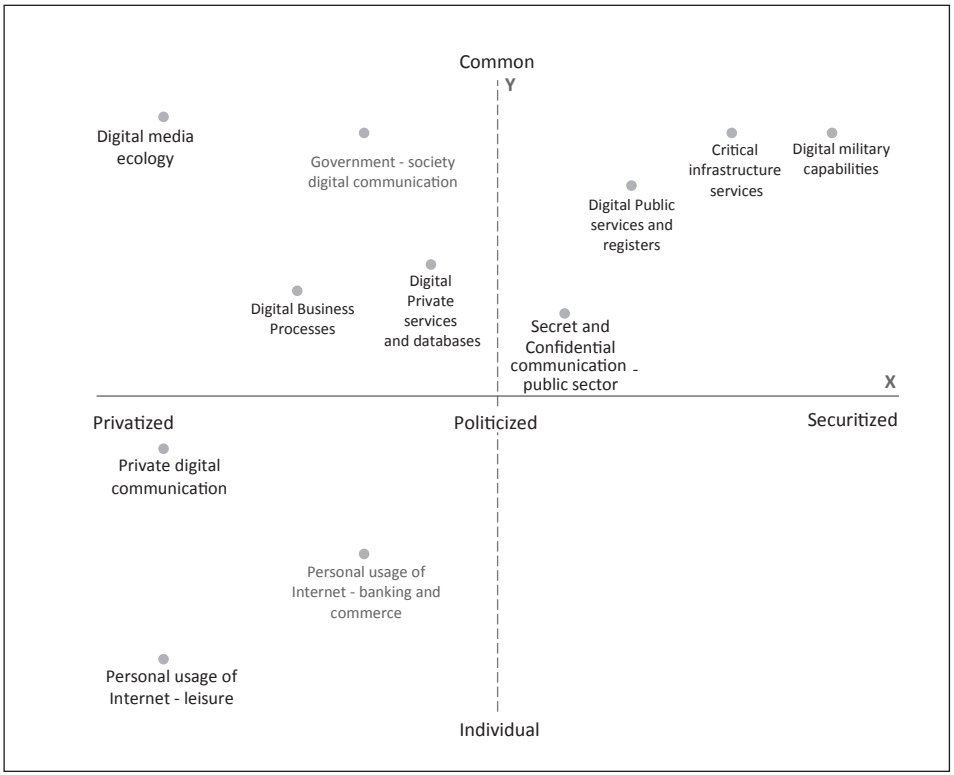
Was it a crime, an act of terror or maybe example of an asymmetric conflict? Processual ontology enables the categorization of cyber-incidents without setting out these false clear cut distinctions. As presented on Graph 1, it creates a taxonomy based on the processes that might be threatened by cyber incidents. Thanks to this it allows to adopt appropriate measures and procedures not on the basis of object, but process-oriented categorization. The attack on the public server of the White House, which hosts its official website will affect government – society communication process, but will not affect national security. But the attack on encrypted communication between White House internal servers might have damaging effects on US foreign policy.

The first continuum which structures the graph (X axis) is based on the social perception of a threatened process. It starts with a privatized perspective, with market-based rules, through politicized stage, introducing public regulations, to the securitized position, where special measures and 'security gramma' are promoted. The second continuum (Y axis) runs from processes influencing individuals to those which affect whole communities. Presented taxonomy is open and changeable over time, due to social processes of privatization, politicization and securitization, and because of technological breakthroughs. The shape of this graph also depends heavily on social context – the same technologically mediated processes might be differently categorized in Western societies, Middle East or Far East countries.

CONCLUSIONS

Cyberspace is a process of data transmission and information cognition/processing in the digital domain. This ontological proposition allows to better apprehend cyberspace phenomena and its role in information society. It promotes multilevel resil-

Graph 1. Processual taxonomy of the cyberspace (Poland)



Source: own elaboration.

ience strategies and technical solutions compatible to it, such as distributed centers of data within peer-to-peer networks. All of this is possible thanks to unique cyberspace characteristics. Cyber is a man-made realm with almost unlimited potential to expand, where physical distance is lapsed and bits are the primary matter. Finally, this theoretical stance blurs the line between human and non-human agents in these processes, dehumanizing the idea of actorness by categorizing both humans and computers as actors.

On the technological level, process-based principles are already dominating the cybersecurity market.[55].Times when products and services for ICT security were focused on passive and object-oriented protection provided by firewalls or air gaps are already long gone. Nowadays innovative solutions are concentrated on the active 24/7 analysis of data transmission and information processing in a secured environment, with tailored actions ready to be taken when anomalies are discovered. On the strategic level process based attitude is also slowly gaining ground. Both in private sector as well as

[55] A.N. Craig, S.J. Shackelford, J.S. Hiller, "Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis", *American Business Law Journal*, vol. 52, no. 4 (2015), pp. 721-787, at <http://dx.doi.org/10.1111/ablj.12055>.

on national and international level the resilience strategy is incorporated in a growing number of laws, regulations, procedures and plans concerning cybersecurity. We already know that our systems are breakable and our information is corruptible. Now we need to prepare appropriate tools on both technological and strategic levels to secure continuity, or at least fast and efficient recovery of key processes in the digital domain. Processual ontology of cyberspace not only allows understanding this paradigm but also helps to create a coherent conceptual framework.

BIBLIOGRAPHY

Abomhara M., Køien G.M., "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks", *Journal of Cyber Security and Mobility*, vol. 4 (2015), at <http://dx.doi.org/10.13052/jcsm2245-1439.414>.

Arquilla J., Ronfeldt D., *The Emergence of Noopolitik. Toward an American Information Strategy*, Santa Monica 1999.

Barlow J.P., "A Declaration of the Independence of Cyberspace", The Electronic Frontier Foundation, 1996, at <http://www.eff.org/pl/cyberspace-independence>.

Barnard-Wills D., Ashenden D., "Securing Virtual Space: Cyber War, Cyber Terror, and Risk", *Space and Culture*, vol. 15, no. 2 (2012), at <https://doi.org/10.1177/1206331211430016>.

Bay M., "What Is Cybersecurity? In Search of an Encompassing Definition for the Post-Snowden Era", *French Journal for Media Research*, vol. 6 (2016).

Bendrath R., "The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection", *Information & Security: An International Journal*, vol. 7 (2001), at <http://dx.doi.org/10.11610/isij.0705>.

Benedikt M., "Cyberspace: Some Proposals", in M. Benedikt (ed.), *In Cyberspace. First Steps*, Cambridge, Mass. 1994.

Betz D.J., Stevens T., "Analogical Reasoning and Cyber Security", *Security Dialogue*, vol. 44, no. 2 (2013), at <https://doi.org/10.1177/0967010613478323>.

Brito J., Watkins T., "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy", *Harvard National Security Journal*, vol. 3, no. 1 (2011).

Brown G., "Spying and Fighting in Cyberspace: What Is Which?", *Journal of National Security Law & Policy*, vol. 8 (2016).

Bryant R., "What Kind of Space Is Cyberspace?", *Minerva*, vol. 5 (2001).

Buchanan B., *The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations*, Oxford–New York 2017.

Castells M., *The Information Age. Economy, Society, and Culture*, vol. 1: *The Rise of the Network Society*, Oxford 2010.

Cavelty M.D., "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse", *International Studies Review*, vol. 13, no. 1 (2013), at <http://dx.doi.org/10.1111/misr.12023>.

Clark D., "Characterizing Cyberspace: Past, Present, and Future", ECIR Working Paper, 2010, at <https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf>.

Craig A.N., Shackelford S.J., Hiller J.S., "Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis", *American Business Law Journal*, vol. 52, no. 4 (2015), at <http://dx.doi.org/10.1111/ablj.12055>.

Darczewska J., *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, at <https://www.osw.waw.pl/sites/default/files/anatomia_rosyjskiej_wojny_informacyjnej.pdf>.

Darczewska J., *Diabeł tkwi w szczegółach. Wojna informacyjna w świetle doktryny wojennej Rosji*, at <https://www.osw.waw.pl/sites/default/files/pw_50_pl_diabel_tkwi_net.pdf>.

Darczewska J., *Rosyjskie siły zbrojne na froncie walki informacyjnej. Dokumenty strategiczne*, at <https://www.osw.waw.pl/sites/default/files/prace_57_pl_sily_zbrojne_net.pdf>.

Deibert R.J., "Circuits of Power: Security in the Internet Environment", in J. Rosenau, J.P. Singh (eds.), *Information Technologies and Global Politics. The Changing Scope of Power and Governance*, Albany 2002.

Department of Homeland Security and Federal Bureau of Investigation, *GRIZZLY STEPPE – Russian Malicious Cyber Activity*, 2016, at <https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY STEPPE-2016-1229.pdf>.

Dolins F.L., Mitchell R.W., *Spatial Cognition, Spatial Perception. Mapping the Self and Space*, New York 2010.

Einstein A., *Relativity. The Special and the General Theory*, Oxford 2015.

Eriksson J., Giacomello G., "Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State", *International Studies Review*, vol. 11, no. 1 (2009), at <http://dx.doi.org/10.1111/j.1468-2486.2008.01841.x>.

Estonian Ministry of Economic Affairs and Communication, *Cyber Security Strategy for 2014-2017*, Tallin 2014, at <https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf>.

Frischmann B.M., "The Prospect of Reconciling Internet and Cyberspace", *Loyola University Chicago Law Journal*, vol. 35, no. 1 (2003).

Gibson W., *Neuromancer*, New York 1995.

Goldsmith J.L., "Regulation of the Internet: Three Persistent Fallacies", *Chicago-Kent Law Review*, vol. 73, no. 4 (1998).

Gunkel D.J., Gunkel A.H., "Virtual Geographies: The New Worlds of Cyberspace", *Critical Studies in Mass Communication*, vol. 14, no. 2 (1997), at <https://doi.org/10.1080/15295039709367003>.

Herzog S., "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", *Journal of Strategic Security*, vol. 4, no. 2 (2011), at <http://dx.doi.org/10.5038/1944-0472.4.2.3>.

Kellerman A., "Cyberspace Classification and Cognition: Information and Communications Cyberspaces", *Journal of Urban Technology*, vol. 14, no. 3 (2007), at <https://doi.org/10.1080/10630730801923110>.

Koepsell D.R., *The Ontology of Cyberspace. Philosophy, Law, and the Future of Intellectual Property*, Chicago 2003.

Krebs B., "Who Is Anna-Senpai, the Mirai Worm Author?", Krebs on Security, 18 January 2017, at <https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/>.

Kritzinger E., Solms S.H. von, "Cyber Security for Home Users: A New Way of Protection through Awareness Enforcement", *Computers & Security*, vol. 29, no. 8 (2010), at <http://dx.doi.org/10.1016/j.cose.2010.08.001>.

Kukla A., *Social Constructivism and the Philosophy of Science*, London–New York 2000.

Lakoff G., Johnson M., *Metaphors We Live by*, Chicago 2003.

Lawson S., "Putting The 'War' in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States", *First Monday*, vol. 17, no. 7 (2012), at <http://dx.doi.org/10.5210/fm.v17i7.3848>.

Lessing L., *Code and Other Laws of Cyberspace. Version 2.0*, New York 2006.

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

Lorents P., Ottis R., Rikk R., "Cyber Society and Cooperative Cyber Defence", in N. Aykin (ed.), *Internationalization, Design and Global Development. Third International Conference, IDGD 2009, Held as Part of HCI International 2009, San Diego, CA, USA, July 19-24, 2009*, Berlin 2009, at <https://doi.org/10.1007/978-3-642-02767-3_20>.

Negroponte N., *Being Digital*, New York 1995.

Neumann I.B., "Returning Practice to the Linguistic Turn: The Case of Diplomacy", *Millennium*, vol. 31, no. 3 (2002), at <https://doi.org/10.1177/03058298020310031201>.

Nye J., "Cyber Power", Harvard Kennedy School Belfer Center for Science and International Affairs, May 2010, at <https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf>.

Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections*, 2017, at <http://www.dni.gov/files/documents/ICA_2017_01.pdf>.

Ottis R., Lorents P., "Cyberspace: Definition and Implications", NATO Cooperative Cyber Defence Centre of Excellence, at <https://ccdcoe.org/multimedia/cyberspace-definition-and-implications.html>.

Penny S., "Virtual Reality as the Completion of the Enlightenment Project", in G. Bender, T. Druckrey (eds.), *Cultures on the Brink. Ideologies of Technology*, Seattle 1994.

Quigley K., Burns C., Stallard K., "'Cyber Gurus': A Rhetorical Analysis of the Language of Cybersecurity Specialists and the Implications for Security Policy and Critical Infrastructure Protection", *Government Information Quarterly*, vol. 32, no. 2 (2015), at <https://doi.org/10.1016/j.giq.2015.02.001>.

Reidenberg J.R., "Lex Informatica: The Formulation of Information Policy Rules through Technology", *Texas Law Review*, vol. 76, no. 3 (1998).

Sapir E., *Language. An Introduction to the Study of Speech*, New York 1921.

Shaw W., *Cybersecurity for SCADA Systems*, Tulsa 2006.

Solms R. von, Niekerk J. van, "From Information Security to Cyber Security", *Computers and Security*, vol. 38 (2013), at <https://doi.org/10.1016/j.cose.2013.04.004>.

"Some Perspectives on Cybersecurity: 2012", Internet Society, 2012, at <https://www.internetsociety.org/sites/default/files/bp-deconstructing-cybersecurity-16nov-update.pdf>.

Stone A.R., *The War of Desire and Technology at the Close of the Mechanical Age*, Cambridge, Mass. 1996.

Strate L., "The Varieties of Cyberspace: Problems in Definition and Delimitation", *Western Journal of Communication*, vol. 63, no. 3 (1999), at <https://doi.org/10.1080/10570319909374648>.

Robert SIUDAK – PhD candidate at the Department of National Security of the Jagiellonian University. Author of two monographies and numerous articles regarding the intersection of new technologies and international security. Research Fellow at the Kosciuszko Institute, Cybersechub.eu Manager and Chief Editor of the European Cybersecurity Market journal. Studied previously at the Jagiellonian University, Tel-Aviv University and Trinity College Dublin.