DOI: 10.53477/2668-6511-22-18

CYBERGEOPOLITICS AND CYBERGEOSTRATEGY – EMERGING STUDY FIELDS

Marius-Cristian NEACȘU, Ph.D.,
Associate professor, Bucharest University of Economic Studies, Romania.
E-mail: marius.neacsu@ase.ro

Ioana-Andreea CHICIUC,
Master Student, Bucharest University of Economic Studies, Romania.
E-mail: a_chiciuc@yahoo.com.

Abstract: *For some time now, mankind has entered a new phase of evolution, with physical space (land, sea, air, cosmic) being doubled by the virtual one, cyberspace – the global network of interconnected information technologies – and geopolitics and geostrategy could not fail to take into account this new phase in the evolution of history, with the emergence of subfields such as cybergeopolitics and cybergeostrategy, with some authors already anticipating cybernetocracies or cyber powers. It should only be added that cyberspace can be both an environment for the 'new' power (the geopolitical logic being the same) and a weapon – the cyberweapon (the use of cyberattacks as a geostrategic tool). The aim of this study consists in identifying the main components (definition, subject matter, terminology) of the two emerging areas, namely* cybergeopolitics *and* cybergeostrategy. *The results of this qualitative research are based on the critical analysis of the specialized literature, in order to summarize the specific phenomenology and to theorize the concept of cybergeopolitics and its dervates.*

Keywords*: cybergeopolitics; cybergeostrategy; cyber power; cyber security; cyber war.*

Introduction

Context. Starting from the assertions of the German philosopher Herder – "History is geography in dynamics" (Neacșu 2018, 177) – the mastermind Romanian scientist, Simion Mehedinți, founder of modern geography as science and as university subject, and at the same time the one who conducted the first geopolitical analysis in our country, had the great idea ("the great intuition", in his own words), of the "geographical phases of history" (Mehedinți 1940), which he developed in a number of studies and scientific communications throughout his life (Neacșu 2018, 129). Thus, the following phases have been completed so far:

I. *The continental phase*, which from a geopolitical and historical geography perspective corresponds to the continental powers (ancient cities, ancient empires, medieval empires, continental powers in modern history and today: Russia, Germany, etc.) – the so-called *tellurocracies*; it is the longest period of geopolitical evolution of all; the essence of a continental power was theorized within the Anglo-Saxon school of geopolitical-geostrategic thinking (see also Neguț 2015), through the theory of continental power or the theory of the *heartland*, with Halford Mackinder's contribution, since 1904, with the concept of the geographical pivot of history;

II. *The maritime/oceanic phase,* followed the continental phase, overlapping it, highlighting the maritime powers (*the thalassocracies*), the colonial empires and modern maritime powers such as the United Kingdom and the USA; maritime powers were superior to continental powers, given the predominance of water over land, and *sea power theory* was conceptualized by Alfred Mahan in 1890;

III. *The aerial phase* of history has diversified the attributes of power of the two previous dimensions, with the addition of airspace domination, which has led to a conceptual reconfiguration at geopolitical and geostrategic levels; the leading air powers (*aerocracies)* were the two cold War superpowers, USA and USSR, and at theoretical level Carl Schmitt stood out with the theory of the aerocracy.

IV. *The space phase* followed naturally after the aerial phase, with two distinct temporal dimensions: a) traditional space powers (*spatiocracies*) during the Cold War (USA and USSR), to which others have joined (China, Japan, India, etc.) and b) an emerging phase, a new space race, which is very recent and different from the one during the Cold War, by its commercial and private nature and many other aspects, which involves many emerging states (UAE, Turkey, Israel, etc.) and non-state actors (private companies – SpaceX, Blue Origin, Virgin Galactic and others, foundations, various entities, eccentric billionaires, etc.); the conceptualization of new notions, which capture the ongoing phenomenology, was made, among others, within the Master in Geopolitics and Business. (Bucharest University of Economic Studies), with concepts such as *exoeconomics* (Șapera 2015, 2013), *exopolitics, exostrategy* and *exobusiness* (Șapera 2021, Neacșu and Matei 2021) or *exoturism* (Neacsu 2021, in press).

V. *The cyber phase* is the most recent, with cyberspace being global despite its virtual nature, the effects of its manifestation are as territorial as possible, causing conceptual metamorphoses, such as *cybergeopolitics* and *cybergeostrategy* (Neacsu and Chiciuc 2021, 66-71).

The aim of this study is therefore in line with the previously developed phenomenological context, particularly the current phenomenology of the cyber phase of history, and consists in identifying the main components (definition, subject matter, terminology) of two emerging areas, namely *cybergeopolitics* and *cybergeostrategy*.

The novelty of the research is obvious, all these concepts highlight an ongoing phenomenology in a sharp dynamic: from using cyberspace as an environment for power manifestation (whoever is not present in cyberspace is not present in the "big chess" power games, the phrase used by Zbigniew Brzezinski 2000 or the "world scene" in Malița 2007) to turning cyberspace into a geopolitical tool: cyber weapon (and possibilities for use are vast in today's hybrid world).

The study is *innovative* by the concepts analyzed, proposing a new terminology and an attempt to theorize the concept of *cybergeopolics* and everything related to it.

The applicative character of the paper is implicit, in addition to the theoretical contributions, the enrichment and updating of the literature in accordance with the dynamics of the present reality, the study is also a theoretical guide to understanding a phenomenon which is currently in full swing.

1. Cyberspace – the new dimension of geopolitics and geostrategy

As geopolitics refers to the use of the geographical factor in maximizing power, and geostrategy refers to the implementation of geopolitical theory, the new environment of action, the cybernetic one, could not remain exclusively as technological support in the field of "civil" activities, as long as any asset means, from a geopolitical perspective, a step in overcoming the opponent and a better position towards regional or global domination. Especially in the context of the pandemic in the last two years, when almost everything has moved to the online space and digital dependence is growing.

This new reality must be understood in two dimensions: 1. the conflict with a geopolitical nature, despite its substratum which is extremely "territorial", physical, concrete, has now acquired a digital dimension and 2. the digital space is both the environment for the manifestation of power, as well as the instrument itself, as a cyber weapon, with tangible effects, in the physical, geographical space.

The relevant published literature has captured this transition in various words, labelling cyberspace as "the digital face of geopolitics" (Kausch 2017, 2) or "the fifth dimension of geopolitics" (Barrios 2019), "the fifth element of the new world" (Refoyo 2018 quoted by Barrios 2019) or, continuing the great idea from Simion Mehedinti, "the fifth phase of history", i.e. the fifth evolving phase of geopolitics (see also Neacșu and Chiciuc 2021, 67).

As regards cyberspace, its definition has evolved in parallel with its better understanding from "consensual hallucination" and "unthinkable complexity" (Gibson 1984, 37) to "the nervous system – the country control system... composed of hundreds of thousands of interconnected computers, servers, routers, switches and cables made of optic fibre that enable our critical infrastructures to work" (Kuehl 2009). We notice the phrase "critical infrastructures" and the concern for its vulnerability (thus a possible target for the enemy, who might be tempted to consider it as such) are emphasized along with the link between the virtual environment and the reality from the field. The last author further nuances the specificity of virtual space, i.e. "a global domain in the information environment (...) to create, store, modify, exchange and exploit information through interrelated and interconnected networks using information communication technologies" (*Ibidem*).

More recently, the virtual space was defined as "the global network of interconnected IT technologies: hardware, software, information, which hosts some of the most powerful weapons, as well as vulnerabilities of the states" (Segal 2016 cited in Kausch 2017, 2). This applies to all the global actors and parties which are interconnected to this global network which gives cyberspace the quality of being "the vanguard of future geopolitical confrontations" (*Ibidem*). In other words, interdependence (economic and military) – mainly theorized by the liberal school of thought in international relations ("mutual dependence" in Joseph Nye jr. or "interdependence" in Robert Keohane) – has moved into the virtual space and has become a cyber-interdependence (Neacsu and Chiciuc 2021, 68).

In summary, cyberspace has become a *space for the manifestation of power*, maintaining the classical geopolitical and geostrategic logic (maximum destruction with minimal losses, preeminence in front of the opponent), and a new *atribute of power – cyber power*.

These interconnected and interdependent networks and information systems are simultaneously located in both the physical and virtual space and within and across geographical borders. The notions of "space", "time", "distance", "border", "identity" and so on have changed drastically, technical developments and the great advancement of artificial intelligence have created a framework for the emergence of a new type of conflict – *cyber conflict* – which adds to the traditional component of "hybrid", "atypical" or simply "unconventional".

By continuing this hypothesis, cyberspace can become a weapon that gives even small states or smaller geopolitical actors greater power and combat capacity, substantially changing the notion of "asymmetric conflict" (see also Harari 2015, 20-21). Relevant and recent examples of this are the terrorist organization Islamic State (ISIS, which operated in Syria and Iraq, with its recent version of ISS-K, in Afghanistan after the withdrawal of US troops and the international coalition in mid-2021) or the Taliban.

If against a state actor there is a legal framework and an international response mechanisms, against volatile entities that act through cyberspace, it is very difficult to react. In other words, the power monopoly of the nation-state is relative. Since the late ‘90s and especially since the mid-2000s, when cyber attacks against states have increased, governments started to see cyber threats as a national security problem (Desforges 2014, 67-81), while some analysts had already announced early on the possibility of cyberwar (Arquilla and Ronfeldt 1993, 141–165).

Viewed as a 'battlefield' (Ministère des Armées 2013, 38) or 'confrontation field' (*Ibidem*, 45), cyberspace has become the vector of cyber threats. These cyber threats have evolved from cyber crime to cyber geopolitics, namely through the use of cyber attacks as a foreign policy tool (cyber weapon). The most vulnerable to cyber threats are the most developed countries, due to the high degree of interconnectivity between computer networks. Seen as a nation's "nervous system" (Kuehl 2009), networks have become a vital challenge for governments, which have placed *cyber security* or *cyber defense* as a component of national security (Cavelty 2008).

2. Cyber power

In traditional or conventional geopolitics, the following are included among the main attributes of high power (see also Neguț 2015): economic power, military power, nuclear power, cosmic power, membership of various international bodies, such as permanent membership of the UN Security Council.

Considering that more than 75 billion devices were connected to the internet in 2020, interconnecting almost 3 billion people (around 35% of the world's population), a new attribute of great power is emerging: *cyber power* (Neacșu and Chiciuc 2021, 68). The element that makes cyberspace give such power is the interdependency and interconnectivity network that it creates, with our current life being almost inseparable from it.

However, as a particular study (Kuehl 2009) points out, the problem is not controlling electrons or electromagnetic forces, but rather influencing the use of cyberspace, in the same way that airborne or naval superiority does not concern the control of air or water molecules, rather, it controls how they are used in the physical environment. Thus, according to the same study, the definition of cyber power is that *"cyber power is the ability to use cyberspace to benefit us and to influence events in all operational environments and among all other power tools"* (*Ibidem*).

From a military point of view, cyber power has been the most influential instrument in the last two decades. From the Russian concept of *military technical revolution* (Kurtinevich Jr. 2002) in the 1980s, to the transformation of US military defense, cyberspace and cyber power have been at the heart of new concepts and doctrines of the last decades. Cyber power has become an indispensable element of modern technology-based military capability because it occurs across all the levels of conflict.

As it was mentioned before, what is different from the traditional geopolitics is that cyber power is not accessible only for the big powers, small states or non-state actors also being able to access it, thus making the cyber dimension a true geopolitical tool.

3. The cyber weapon. Cyberwar. Players.
Towards conceptualizations of cybergeopolitics and cybergeostrategy

It should be noted that the use of the *cyber attack* is also based on hard power logic, the military invasion of geopolitical and traditional geostrategy being replaced by cyber attacks, either to cause a breach in the opponent's network and to obtain data (digital espionage), or to cause considerable damage (therefore as a digital weapon). The cyber weapon did not replace conventional weapons, but joined them in the battlefield, imprinting the *unconventional (hybrid)* character into conflicts.

Although the recorded cases are already well-known for a long time (the US cyber attacks against Serbia in the ‘90s, the cyber attacks on Estonian public and private institutions in 2007, the Russian cyber attacks in the 2008 war with Georgia, etc.), some authors consider 2012, as the "year 0" of the cyber war (more specifically, the timeframe between June 2012 and June 2013, where information was leaked in the media), when the US, together with Israel, resorted to a cyber attack against Iran's nuclear program (since 2010), using a malware called Stuxnet and compromising the program that was controlling the centrifuges of uranium enrichment facilities. The effect? At least 1 000 engines operating the centrifuges were destroyed (by sudden acceleration and deceleration). The Iranian cyber response came without delay, a group called Izz ad-DIN al-Kassam attacked 50 US financial institutions, which spent around $10 million to get back online (Segal 2016). The era of cyber warfare had begun: the use of the cyber weapon was producing physical damage (in the case of the engines from the Iranian centrifuges and more), with the associated costs...

As a result, cyber defense has become one of the main topics on NATO's public agenda, with the organization stating that "international law applies to cyberspace" (NATO 2020), with Bucharest being chosen to host a European Cybersecurity competency Center as of 2021. A cyberspace that is regulated internationally is thus introduced by a series of "rules" (Ruhl et al 2020), being a "strategic domain" (Popa 2014), with geopolitics and geostrategy now taking a mixed approach, both physical and cyber (Oxford Analytics 2018). And Henry Kissinger, the well-known US diplomat and the "spiritual parent" of a famous "Diplomacy", said "Cyberspace is beyond any historical experience. (...) The threats that come from cyberspace are diffuse and difficult to ascribe" (Kissinger 2014).

Cyber attacks have significant advantages in a conflict compared to conventional instruments. They have high disruptive potential and have a relatively low economic cost for the attacker. The political cost in the form of a risk of retaliation is also low, given the difficulties that arise in tracing the offender. The problem of author identification is perhaps the most acute and presents a real challenge for traditional disincentives (Kausch 2017).

The concept of war is used to describe a diverse set of conditions and behaviors, from a state of violent and armed escalation (such as classical wars) to symbolic disputes or disagreements, which are far from the real meaning of this concept. The concept of cyber war has also been used to describe different situations, ranging from credit card fraud or a campaign of cyber vandalism and cyber-space disruption, to a real state of war conducted by cyber means. (Singer and Friedman 2014, 120).

According to the US Government, in order to turn into cyber war, a cyber attack must cause injuries, significant destruction or even death. While the means of doing this are in cyberspace, they must have physical damage (*Ibidem*) in the real world. *Cyberwar* is thus defined as *the use of cyber attacks to attack a state or disrupt vital information systems, causing damage comparable to real war* (NATO 2013). There is significant debate among experts on the definition of cyber war. One view is that the term "cyber war" is incorrectly used, as no cyber action to date could be described as war (*Ibidem*). An alternative perspective is that cyber war is an appropriate label for cyber attacks that cause physical damage to people and objects in the real world (Lucas 2016).

Hard-power manifestations in cyberwar are generally represented by attacks conducted in the cyber space designed to produce political effects similar to those of conventional wars (Lucas 2017), but elements of hard power such as military intervention, economic sanctions and coercive diplomacy are replaced by elements of cyber war, such as cyber attack, cyber espionage or state-funded *hacktivism*.

McAfee, a cyber security firm published the *Cyber crime report in 2009* under the title *Virtually here: The age of Cyber Warfare*, in which it included a world map of countries that were developing advanced cyber capabilities at the time. The title of the map was: *Cyber war* *is not taking place today, but states are definitely in competition* (Kurtz 2009). This report estimated that there were only about twenty countries, which actually have advanced cyber-war programs and could build something comparable to the Stuxnet virus.

Additionally, some current "major players" inside the cyberspace have been stepped up (Segal 2016), respectively some *cyber powers* – states that use the cyber dimension to increase their competitive advantages as players on the global stage - such as USA, Russia, China, Germany, Brazil, Israel. In addition to those listed, we can add other cyber actors, including Japan, North Korea, Iran, Vietnam, India, Pakistan, etc. (University of Pittsburgh Institute for Cyber Law, Policy and Security 2019).

The complex nature of cyberspace involves several representations, which shape government strategies in this new power environment. In such cases, these representations become geopolitical instruments. For example, Russia has omitted the direct use of the term cyberspace, instead opting for the term "*informational space*". By using this broader concept, Russia is not only limited to the classic idea of cyber attacks, but is choosing strategies that aim at more widespread information control, regardless of their channel of distribution (Desforges 2014, 67–81).

As it is not a physical space, cyberspace is viewed by geopolitical actors as a virtual world generated by the interconnectivity of the Internet network. However, geopolitical conflicts that use cyberspace as a vector of manifestation, and which are, among other things, the focus of cybergeopolitics, are real and reflect the rivalries between states that exist outside the virtual world.

In an article from 1997 entitled *Internet géopolitise le monde*, it was mentioned that "instead of making geopolitical conflicts more difficult to take place, the Internet seems to multiply and complicate them" (Douzet 1997, 222–233), the standard notions from the geopolitics field, such as power, influence and conflict are also "altered" by the new cyber dimension.

As a result, given what has previously been mentioned, the subject of cybergeopolitics studies becomes cyberspace, i.e. the way it works as an amplifying environment for power (in which geopolitical actors are confronted), but also the way it becomes a geopolitical tool (the cyber weapon).

Thereby, *cybergeopolitics* is individualized as the newest geopolitical subbranch, which analyzes *the movements of forces of global actors in the cyberspace, the motivations/interests behind these movements and their impact on relations between actors in the global dynamic*. In addition, *cybergeopolitics* can be used alongside *cybergeostrategy* to study the instruments of *hybrid war*.

Regarding terminology, it has become widely diversified in recent years, with specialized terms coming into existence starting from cyber space such as *cyber threat cyber crime*, *cyber terrorism*, *cyber risk*, *cyber security*, *cyber diplomacy*, *cyber intelligence*, *cyber conflicts*, *cyber war* etc. (Neacșu și Chiciuc 2021, 68).

Furthermore, the related phenomenology is also quite diverse, from simple *disinformation* and the spread of *fake news* to *cyber attacks* against critical infrastructures of other states. If cybergeopolitics sets the goal that needs to be achieved, cybergeostrategy provides the path (tactics, strategies) for achieving that goal.

Conclusions

Analysing the tendency of theoretical conceptualization of the two emerging fields – *cybergeopolitics and cybergeostragy* – the following have been reached:

1. The cybernetic phase is a new stage in the geopolitical evolution of humanity. Continuing the idea of the "geographical phases of history" of the great scientist Simion Mehedinți, we find that humanity has entered a new "era", in which cyberspace has become predominant in all aspects of life. From a geopolitical point of view, the emergence of "cyber powers" (*cyberocracies*) is foreshadowed, just as each major phase of evolution has generated continental (*tellurocratic*), maritime (*thalasocratic*), air (*aerocratic*) or spatial (*spaceocratic*) powers.

2. Cyberspace is the fifth dimension of geopolitics and geostrategy. The role of the geographical factor in maximizing power (control of land, seas and oceans, air, circumplanetary space) has been completed with a new dimension, the cybernetic one, which adds strengths in addition to the previous ones. Being a complex global network, based on interconnectivity and interdependence, cyberspace also presents vulnerabilities, which can be speculated to cause damage, including physical ones. In addition, the inexorable accessibility to the virtual space with minimal costs maximizes the number of potential geopolitical actors, state and non-state, in addition to the already established great powers.

3. Cyber power is a new attribute of great power, in addition to those already known, namely economic, military, nuclear, space power or membership in various international bodies such as permanent membership of the UN Security Council. In essence, cyber power captures the ability of an actor to "navigate" the cyber environment and explore its attributes, turning it into a *cyber weapon*, such as, for example, initiating cyber attacks on critical infrastructures in another state.

4. Cyber conflict originated from the conventional one, attributing to a modern conflict the *hybrid* or *atypical* or *unconventional* label. Thus, theoretically speaking, the translation from the *hard power* to the *hard cyber* can be observed, retaining the geopolitical logic of intervention and force manifestation, but changing the instrument (tanks invasion was replaced by fake-news invasion, as a *softer* version or even actions with results that lead to material damage such as cyber attacks).

5. Cybergeopolitics is an emerging area that seeks to capture the new ongoing phenomenology, with cyberspace as the "study object", in two ways: as *an environment for the manifestation of power* and as *a tool of power* (the cyber weapon). In this context, specialized terminology has enriched itself with new words such as *cyber threat, cyber crime, cyber terrorism, cyber risk, cyber security, cyber diplomacy, cyber intelligence, cyber conflicts, cyber wars*, etc.

6. Cybergeostrategy is a natural extension of cybergeopolitics and consists of applying the theory and achieving its objectives. Therefore, both cybergeopolitics and cybergeostrategy provide the tools for the study of hybrid war.

BIBLIOGRAPHY:

BARRIOS, Miguel Ángel. 2019. “Cyber-geopolitics: a strategic analysis from our America.” Accessed October 2, 2021. URL: https://www.vision-gt.eu/news/cyber-geopolitics-a-new-field-of-study-to-understand-the-attacks-to-critical-infrastructure

BRZEZINSKI, Zbigniew. 2000. *Marea tablă de șah. Geopolitica lumilor secolului XXI,* București: Ed. Univers Enciclopedic.

CAVELTY, Myriam Dunn. 2008. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age,* London: Routledge.

DESFORGES, Alix. 2014. “Les représentations du cyberespace: un outil géopolitique.” *Hérodote* 152-153, no. 1-2: 67–81. URL: https://www.cairn.info/revue-herodote-2014-1-page-67.htm

DOUZET, Frédérick. 1997. “Internet géopolitise le monde.” *Hérodote* 86-87, no. 1-2: 222–233.

GIBSON, William. 1984. "Neuromancer." Accessed October 2, 2021. URL: http://index-of.es/Varios-2/Neuromancer.pdf

HARARI, Yuval Noah. 2015. *Homo deus: scurtă istorie a viitorului*. Iași: Ed. Polirom.

KAUSCH, Kristina. 2017. "Cheap Havoc: How Cyber-Geopolitics Will Destabilize the Middle East." Accessed October 2, 2021. URL: https://www.gmfus.org/news/cheap-havoc-how-cyber-geopolitics-will-destabilize-middle-east

KISSINGER, Henry. 2014. *World Order*. New York: Penguins Books.

KREPINEVICH Jr., ANDREW F. 2002. *The Military-Technical Revolution: A Preliminary Assessment*. Washington: Center for Strategic and Budgetary Assessments. URL: https://csbaonline.org/uploads/documents/2002.10.02-Military-Technical-Revolution.pdf

KUEHL, Daniel T. 2009. "From Cyberspace to Cyberpower: Defining the Problem" In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, ch. 2. Lincoln: University of Nebraska Press. URL: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210

KURTZ, Paul B. 2009. "Virtual Criminology Report 2009: Virtually Here: the Age of Cyber Warfare." Accessed October 2, 2021. URL: https://media.hotnews.ro/media_server1/document-2009-11-17-6518495-0-virtual-criminology-report-2009-virtually-here-the-age-cyber-warfare.pdf

LUCAS, George. 2016. *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*. New York: Oxford University Press.

LUCAS, George. 2017. "State-Sponsored Hacktivism and «Soft War»." *Civil American* 2, art. 2: 1–6. URL: https://goo.gl/R55J4V

MALIȚA, Mircea. 2007. *Jocuri pe scena lumii: conflicte, negocieri, diplomație.* București: Ed. C.H. Beck.

MEHEDINȚI, Simion. 1940. "Fazele geografice ale istoriei. Observări geopolitice" In *Opere Complete. Vol. 1, Partea a II-a*, edited by Simion Mehedinți 1943, 308–319. București: Fundația Regală pentru Literatură și Artă.

Ministère des Armées. 2013. *Le Livre blanc sur la défense et la sécurité nationale*. Paris: Direction de l'information légale et administrative. URL: https://fr.calameo.com/read/000331627d6f04ea4fe0e

NATO. 2013. "Cyberwar – does it exist?" Accessed October 2, 2021. URL: https://www.nato.int/docu/review/articles/2013/06/13/cyberwar-does-it-exist/index.html

NATO. 2020. "Cyber defence." Accessed October 2, 2021. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm

NEACȘU, Marius-Cristian and Chiciuc, Ioana Andreea. 2021. "Conceptul de geopolitică cibernetică (cybergeopolitics)." *Terra* LI (LXXI), no. 2: 66–71.

NEACȘU, Marius-Cristian and Matei, David. 2021. "Concepte emergente: exopolitică, exostrategie, exobusiness" In *30 de ani de la sfârșitul Războiului Rece,* edited by Marius-Cristian Neacșu, 156–175, in press. București: Ed. ASE.

NEACȘU, Marius-Cristian. 2018. *Simion Mehedinți și geopolitica românească*. București: CD Press.

NEGUȚ, Silviu. 2015. *Geopolitica*. București: Meteor Press.

Oxford Analytica. 2018. *Cybersecurity & Geopolitics*. Oxford: Oxford Analytica. URL: https://www.oxan.com/media/2150/oxford-analytica-cybersecurity-and-geopolitics.pdf

POPA, Iulian. 2014. “Cyber geopolitics and sovereignty. An introductory overview” In *Proceedings of The 5th International Scientific Conference National and International Security 2014, 2nd-3rd October*, edited by Armed Forces Academy of General Milan Rastislav Štefánik 2014, 413–417. Demänová: Academy of General Milan Rastislav Štefánik.

RUHL, Christian, Hollis, DUNCAN, Hoffman, WYATT, and Tim MAURER. 2002. *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads*. Washington: Carnegie Endowment for International Peace. URL: https://carnegieendowment.org/files/Cyberspace_and_ Geopolitics.pdf

ȘAPERA, Andrei. 2013. “Towards Exoeconomics – Developing an off-planet economy and its implications.” Accessed October 1, 2021. URL: http://www.fgdb.ro/assets/resurse/Andrei-Sapera-Exoeconomics-2013.pdf

ȘAPERA, Andrei. 2015. “Exoeconomie. Dezvoltarea economiei extraplanetare” In *România noului val*, edited by Marius Stan, Bogdan Gravrilă, 357–363. Bucharest: Civil Society Resource Center.

ȘAPERA, Andrei. 2021. “Exostrategy and Space Industry 4.0.” webinar, March 9 and April 6. Bucharest University of Economic Studies (MA Geopolitics and Business).

SEGAL, Adam. 2016. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. London: Hachette UK. URL: https://books.google.ro/books?id=LDxWDgAAQBAJ&printsec=frontcover&hl=ro&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

SINGER, P.W. and Allan Friedman. 2014. *Cybersecurity and cyber war – what everyone needs to know*. New York: Oxford University Press.

University of Pittsburgh Institute for Cyber Law, Policy and Security, US Government and others. 2019. “Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar.” Accessed October 1, 2021. URL: https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf