“PHYGITAL” SECURITY – A FUSION OF EMERGING PHYSICAL AND CYBER-DIGITAL SPACE EFFECTS – A COMPELLING CALL FOR A NOVEL COMPREHENSIVE CYBERSECURITY THEORY FOR DIGITALIZED SOCIETIES –

Paul MÂNDRAȘ, PhD Candidate

Euro-Atlantic Resilience Centre, Bucharest

Colonel Professor Cezar VASILESCU, PhD

Regional Department of Defense Resources Management Studies, Brașov

DOI: 10.55535/RMT.2023.4.6

As technology continues to advance rapidly, it is crucial for society’s key stakeholders – policymakers, governmental organizations, business professionals, researchers, academics, and non-governmental organizations – to provide in-depth specialized awareness regarding security-related issues. To effectively address the impact of digitalization and develop tailored public policies, stakeholders must first fully comprehend novel technological challenges and the “Phygital” space. Nations need to recognize that this digital process involves society as a whole. As the digital evolution and revolution continue to expand, it has become synonymous with economic proficiency and digital disruption. The technological advancements and the emergence of disruptive technologies and digital ecosystems, like social media, artificial intelligence, Internet of Things, Metaverse etc. present opportunities and challenges unlike any we have faced before in human history. Given these circumstances, it is important to reconsider whether cybersecurity fully encompasses digital changes and disruptions or if further research on “Phygital” security is necessary.

Keywords: “Phygital” security; digital space; digitalization of society, cybersecurity; information technology;

RESEARCH AGENDA

Are societies currently being digitalized?

Over 50 years ago, the concept of *“digitalization of society”* was first used by Robert Wachal. In 1971, in an essay published in the *“North American Review”* magazine (Brennen, 2014), Wachal referred to digitalization to describe the debate on the social implications of the use of information technology in the context of objections that were taking shape at the level of American society regarding the development of research activities in human activities assisted by computers.

However, despite opposition, information and communication technology (ICT) systems have continued to develop worldwide from 1971 to the present day. As a result, the debate within societies surrounding digitalization has persisted and even intensified.

Therefore, our article aims to contribute constructively to the ongoing debate regarding the impact of digitalization on societies (see *Figure 1*). After extensive

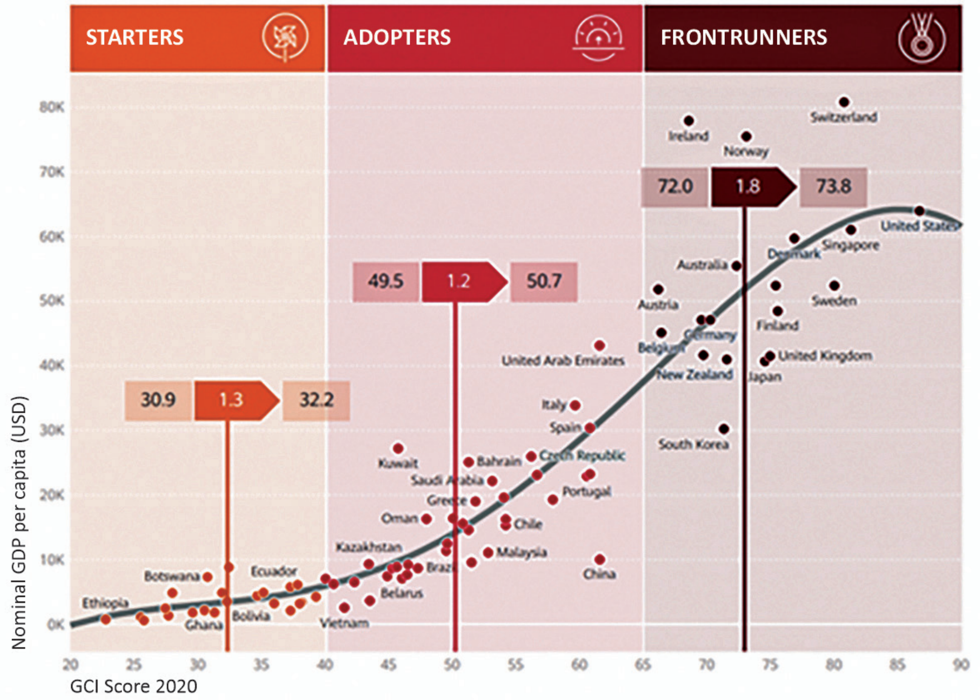

Figure 1: Global Connectivity Index (GCI) versus Gross Domestic Product (GDP)
(Huawei Technologies Co., Ltd., 2020, p. 11)

research, we firmly believe that digital integration is a current global trend that disrupts societies at all levels due to the fusion of physical and cyber-digital spaces that has given rise to a new concept of *"phygital"* space.

Hence, is it required to re-evaluate the cybersecurity concept due to the emergence of novel digitalization of societies?

Throughout this article, we affirmatively answer these two research questions and further provide the necessary arguments, taking into consideration that a novel comprehensive cybersecurity theory that considers the unique challenges posed by this fusion of the physical and digital realms is necessary.

INFORMATION AND COMMUNICATION TECHNOLOGY AS A BRIDGE THAT UNITES THE GAP BETWEEN DIGITIZATION AND DIGITALIZATION OF SOCIETIES

The role of ICT in bridging the gap between digitization and digitalization is crucial. Therefore, it is important to understand the difference between *digitization* and *digitalization* terms and how technology sustains the empowerment of the latter.

Without proper implementation of ICT, the digitization process may fall short of achieving the full potential of digitalization. As a consequence, it is essential to understand how technology enables digitalization and ensures its successful implementation.

From a technical point of view, one of the definitions we consider to be comprehensive regards ICT as the *technology that underlies the development, maintenance, and use of computer systems, software applications, and computer networks for processing and distributing digital data* (Merriam-Webster).

Thus, it is worth noting that ICT encompasses both computer and telecommunications technology (Castagna, Bigelow, 2021), and it has three primary functions that impact the digital infrastructure, applications, and services (like computers, servers, networks, or external storage capacities), as follows:

1. *Implementation* and *maintenance*;
2. *Monitoring*, *optimizing,* and *troubleshooting* the *performance*; as well as
3. *Cyber security* oversight and governance.

Consequently, we consider that *ICT encompasses those physical devices equipped with software programs that can compute, store, and network; as well as the infrastructure and procedures for creating, processing, storing, securing, and exchanging all forms of electronic data* (see *Figure 2*).

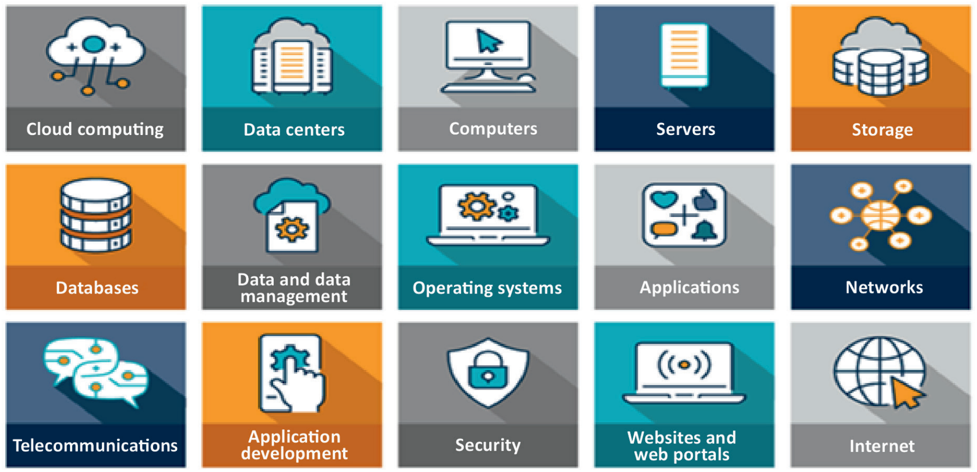

Figure 2: Information Technology Components and Functions (Castagna, Bigelow, 2021)

Furthermore, to avoid confusion, we suggest distinguishing between *digitization* and *digitalization*, which are sometimes used interchangeably in literature. Hence, *digitization* is the process through which data and information represented in physical or analogue format are converted into data and information represented in cybernetic or digital format (Digitization vs. digitalization: Differences, definitions and examples, n.d.), resulting in a transformation from physical to cybernetic objects.

From our perspective, *digitization is a transformational process through which physical space data and information change form into cybernetic data and information*. For instance, digitization can be achieved by photographing a physical document to create an electronic document.

Accordingly, digitization is a crucial process that involves converting hard copies of data into digital form. This approach significantly reduces the physical storage space required for documents and enhances their sharing and accessibility. Furthermore, digitization provides protection against physical damage and natural disasters, as digital copies can be remotely backed up and stored to ensure that crucial information is not lost.

On the other hand, *digitalization* is a much more complex process than *digitization*, and from our perspective, *digitalization includes digitization*, the latter representing the first phase of digitalization, the collection of cyber data and information. From a more comprehensive perspective, we state that *digitalization includes three major dimensions,* respectively *digitization*, the *ICT processes* as previously described, and last but not least, the *human activity within cyberspace*.

Although there is a diverse variety of definitions of *digitalization* (Reis, Amorim, Melão, Cohen, Rodrigues, 2020, pp. 447-448), we agree that *digitalization is a process of using digital technologies to change the economic model of an organization in order to capitalize on opportunities to generate new monetary income and increase added value* (Information Technology, n.d.).

Nevertheless, we emphasize the fact that *digitalization* is currently the most significant trend of change affecting individuals, societies, states, and businesses. This means that organizations of all types – whether they are economic, military, political, social, non-governmental, or governmental operating at national, regional, or international levels – are constantly facing pressure to incorporate digital technologies into their operations and adjust their strategies accordingly in order to remain competitive.

Through *digitalization*, *industrial societies are rapidly transforming at a global scale into informational societies* (Mândraș, 2022, p. 59).

However, even if we agree that *digitalization* has mainly an economic influence, we cannot help but notice that such an approach is limiting, precisely because the impact of *digitalization* is all-encompassing, with repercussions throughout society – individuals, government organizations, non-governmental or economic ones – and its domains – military, political, economic, social and environmental (European Defence Agency, 2023, p. 2). Therefore, limiting our understanding of digitization only to its economic influence is inadequate, precisely because *digitization is socially inclusive, exhaustive, and holistic* (Mândraș, 2020, pp. 78-95).

From a scientific perspective, the debate around the definition of digitalization remains incomplete, in our opinion. The effects of digitalization on societies are increasingly evident and are still not fully known and understood. We have seen that digitalization has been increasingly intense not only economically – as more and more businesses adopt digital processes –, but also among governments around the world. In order to maintain or increase competitiveness, government organizations and the private sector are increasingly incorporating information technologies into their public services and policies. (Reis et al., pp. 443-456).

After careful consideration of the various aspects previously detailed, we believe it is important to critique the focus on economic influence in defining the digitalization of societies.

Consequently, we emphasize that instead, it is crucial to take a holistic approach that takes into consideration the main focus of digitalization: *novel types of cyber technologies generate novel types of human interactions that arise from the newly formed digital ecosystems.*

Digitalization encompasses technology that disrupts all levels of society – macro, micro, and nano.

Hence, we consider that *digitalization is a whole society process through which digital technologies modify, transform, disrupt, or destroy societal processes, models, and strategies in all human domains – economic, military, political, social, and environmental, in order to capitalize on the opportunities, and increase society's efficiency.*

TECHNOLOGICAL EVOLUTION AND SOCIAL REVOLUTION: EXPANSION OF THE PHYSICAL SOCIAL SPACE

The development of digital technologies is closely related to the invention of cyber information, computers, the Internet, artificial intelligence and process automation, bio-materials, and so on. Cumulatively, these technologies have disrupted societies and generated new innovative mechanisms for reconfiguring and streamlining the systems of production of goods and delivery of services, mainly for economic purposes.

Due to the appearance of cyberspace, human activity has expanded the physical realm and a new type of virtual social space has emerged. Hence, according to the latest research, the social space can be either physical or virtual, and it is where people interact with each other for work, leisure, socializing, or other purposes. It has a significant impact on human behaviour, but its nature and complexity, as well as its relationship to context and spatial scale, are not yet fully understood (Balsa-Barreiro, Morales, 2022, p. 1).

Hence, it is reasonable to ask how the expansion of physical social spaces affects security, and to provide an answer to such a question we further explain the Digital and *"Phygital"* space.

Digital space as a new dimension for human activities in the "world" of cyberspace

Is there confusion among specialists and the general public regarding the difference between physical, cyber, and digital space?

We believe so (see Fayard, 2012), and precisely for this reason, we provide a clarifying perspective.

Cyberspace represents a *global domain* composed of the interconnection of all ICTs, networks, and digital data, including independent and isolated ones that process, store, or transmit data. From a military perspective, *cyberspace* is being assimilated in importance to other operational environments in which military actions take place – land, naval, air, and space (NATO, 2020, p. 4).

In terms of cyberspace components, NATO identifies three, respectively: *physical* – which includes the physical components (ICTs devices and networks), located in a delimited geographical space; *logical* – which includes software elements and digital data; and *cyber-persona* – which consists of virtual representations of the identity of physical and real persons or institutions.

It is worth mentioning that the *cyber-persona*, which can exist independently without being connected to a physical or real person or organization, still needs to be closely linked to its physical counterpart in order to function effectively in cyberspace. When we refer to operating in cyberspace, we are emphasizing the actions, behaviours, and activities that individuals or organizations perform in this virtual realm.

Obviously, there is a clear difference between physical and cyberspace, but we argue that cyberspace needs to be further differentiated regarding its components that include human activities and non-human activities.

Precisely for this reason, we consider that *cyberspace must not be confused entirely with digital space*.

Cyberspace and digital space are both virtual. Cyberspace is represented by non-human components (ICT devices, software, procedures, digital data etc.), whilst *digital space is represented by a virtual space within cyberspace where human actions, activities, and behaviours occur, at an individual or organizational level*.

Hence, due to cyber-persona and human activities in virtual space, *digital space links cyberspace to physical space and vice versa*.

Moreover, we argue that there is great interdependency between cyber, digital, and physical spaces, as human or automated operations in cyber, and digital space produce effects in the physical realm concerning four key dimensions, as follows: *physical*, *informational*, *psychological*, and *bio-technological*.

Our perspective completes NATO's one, which argues that cyberspace produces effects at *physical*, *informational,* and *cognitive* levels (NATO, 2020, p. 1).

Regarding the *physical dimension*, it includes all ICT devices located in the physical space that process digital information, whether they work independently or in a network, with or without an Internet connection.

The *informational dimension* is dubbed by some specialists as the *informational environment* (Kuehl, 2009, apud. Schreier, 2015, p. 11). It includes the *virtual information contained in the systems arranged in the physical space, which can be subject to processes of dissemination, processing, storage, exploitation, transformation, manipulation, extraction, destruction* etc.

In terms of both *psychological* and *bio-technological dimensions*, our argument is that physical entities such as individuals or organizations, along with their digital counterparts – cyber-personas, interact with digital information and generate digital human activities. These digital interactions and activities result in societal effects that occur not only at the cognitive level, as NATO suggests, but also at *individual* (*psychological*), *social* (*sociological*), and *biological* levels[1].

As a consequence, we argue that digital relationships between humans occur not just on a simple cognitive level, but on a three-dimensional level. It includes the impact of digitalization on the *psychological level* when *individual behaviours are affected by digital activities*; on the *sociological level* when *social groups are affected by virtual activities*; and last but not least on the *biological level* when *digitalization affects the biological and informational system of living beings.*

All three dimensions – psychological, social, and biological – have physical effects on individuals and society. They influence human behaviour and shape the identity and culture of societies.

Intrinsically, we believe that the *main characteristic of the digital space is its duality*. It is at the same time a physical and cybernetic network that facilitates the exchange of digital information, as well as a global phenomenon that influences people and societies. This influence is constantly growing, due in part to the development of virtual social networks and the ability of virtual space to expand beyond physical boundaries.

Considering human activities in cyberspace, digital space represents a virtual domain where people discover information, educate themselves, work, socialize and, last but not least, play and have fun (Le Merle, Davis, 2017, p. 42).

Moreover, from a societal standpoint, digital relationships between physical entities mirror those in the physical space and fall into three main categories: *cooperation*, *neutral,* or *confrontational* (see *Figure 3*).

[1] Cognitive processes (sensations, perceptions, representations, thinking, memory, imagination, and language), together with affective processes (emotions, feelings, and passions), regulatory (will and motivation), and conditional (attention and skills) form the totality of psychic processes. The latter, combined with mental activities (playing, learning, working, creating, and communication) and mental attributes (temperament, skills, and character), are integrated into the human psychic system.

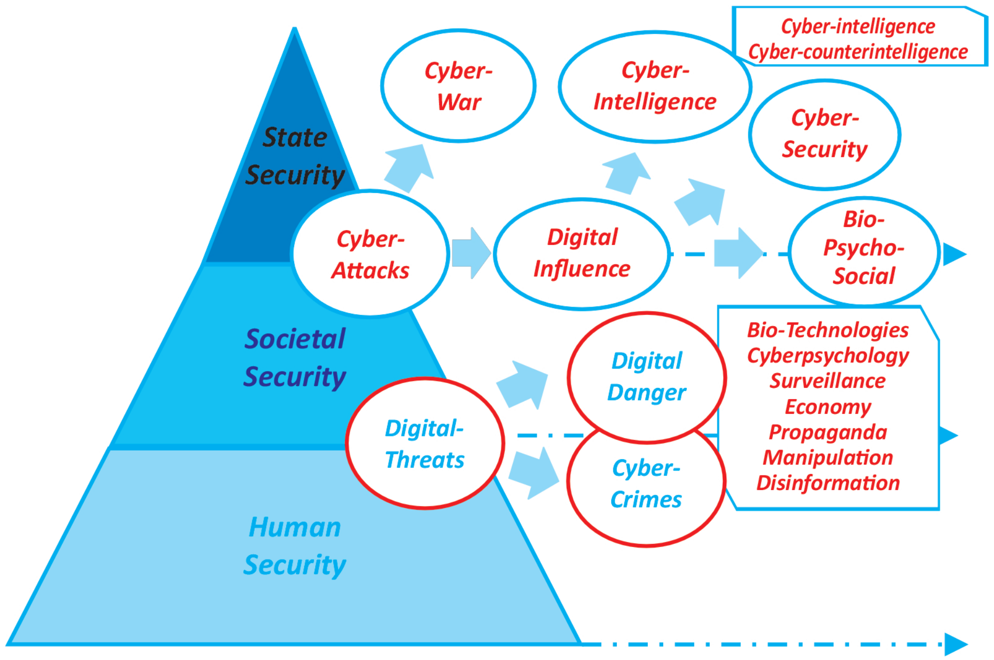

Figure 3: Types of digital conflicts (Mândraș, 2022, p. 63)

"Phygital" space as a conceptual fusion of the physical and cyberspace

Obviously, an expansion of the physical social space where human activities and inter-relationships take place has repercussions on all types of social domains, including security.

But what are these repercussions?

We further provide an answer. Firstly, we note that, when referring to the human experience that transcends these three types of spaces previously mentioned – physical, cyber, and digital, different specialists have observed the emergence of a symbiosis between the physical and cyber-digital space. Secondly, even when disparate, *human experiences in physical and digital space are not independent but interdependent.*

Precisely in order to characterize this mix of human experiences we emphasize that they occur both in a real and palpable world and another virtual *"world"* that cannot be perceived in geographical space. Accordingly, we need to describe and define the complementarity of human experiences in real and virtual environments, and such a physical-digital synergy requires a conceptual redefinition of the social space, which takes into account the transcendence of the physical limits.

Consequently, we believe that such a redefinition finds its form in the *"Phygital"* space concept (see *Figure 4*).

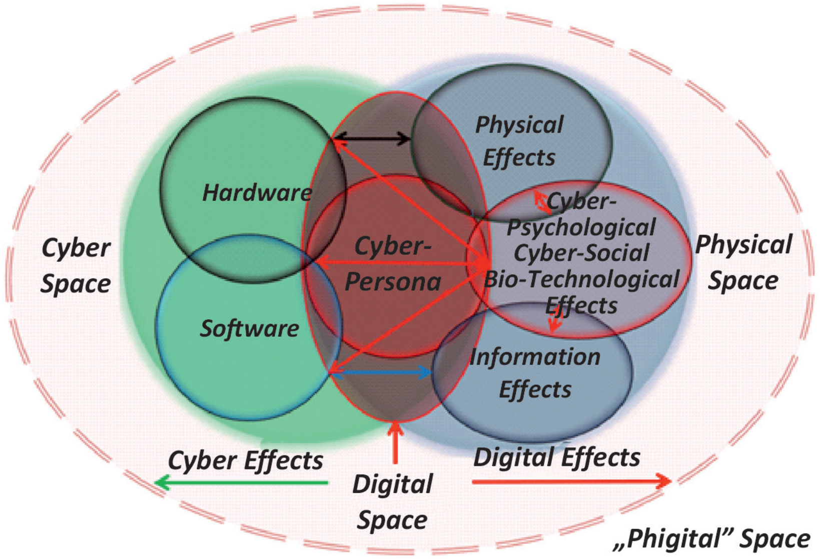

Figure 4: "Phygital" space and digital inter-relationships (Ib.)

The term *"Phygital"* was first used by Chris Weil, CEO of Momentum Worldwide, in 2007, to describe the integration of physical and digital experiences (White-Gomez, 2022). Obviously, Weil used the term because he wanted to set himself apart from competitors in the marketing industry. Since its patent in 2013, the term has gained global popularity, even in academic circles (see LUMSA Universita, 2022).

In our opinion, *"Phygital"* is the most comprehensive concept for human activity in both physical and virtual environments in modern societies (see Welsh, 2023).

As a consequence, we believe that this concept must also be expanded to modern security studies, with reference mainly to those of cyber and digital security (Dow, 2021). Given this context, we aim to act as promoters of the *"Phygital"* security concept and we emphasize that our research within the specialized Romanian security literature has not identified the usage of this term until now.

Therefore, from a security perspective of modern digital societies, we define the *"Phygital" space as representing the space or environment where security behaviours are being manifested, resulting from human and non-human, real and virtual interactions, which occur complementary, simultaneously, or disparately in physical, digital and cyberspace, and generate sources of insecurity or resilience actions.*

Consequently, we believe that the *study of "Phygital" space, security behaviours, sources of insecurity, or securitization actions in physical, digital, and cyberspace represents a domain of security for digitalized societies.*

"PHYGITAL" SECURITY: A COMPELLING CALL FOR A NOVEL COMPREHENSIVE CYBERSECURITY THEORY FOR DIGITALIZED SOCIETIES

As specialized literature does not provide a unitary approach to the concept of security, we join those who believe that it is almost impossible to establish a generally valid definition of security (Miller, 2001, pp. 13-42), arguing that security needs differ for each security actor – individuals, societies, and states.

Nevertheless, the concept of security's complexity must take into account at least four essential elements and provide an answer to the inherent questions, as follows:

Who is the subject of security? Respectively, whose security are we referring to?

What are the sources of insecurity? Respectively, what actions generate them?

Who are the security actors? Respectively, who must ensure the subject's security by countering threats, removing vulnerabilities, and increasing resilience?

Who are the actors that generate insecurity? Respectively, who or what generates the sources of insecurity or actions that manifest in threats and dangers to the subject's security?

As the literature addresses at least 15 types of security, we have previously argued that *security has four main dimensions* (see *Figure 5*), as follows: (1) *security subjects*, classified according to the main security actors – the state, society, and the individual; (2) *domains of insecurity*, classified according to the main sources of insecurity, which simultaneously represent resilience assurance areas – military, political, economy, societal, environment, and digital; (3) *security sources*, which mainly refers to state security, classified according to the behaviour of states in achieving their own security within international relations – joint, collective, and cooperation; and (4) *security environment*, which mainly refers to state security, classified according to the geopolitical and cyberpolitical depth of the security environment at national, regional and international level (see Mândraș, 2021).

Moreover, digitalization represents a new security domain, and a wide variety of digital insecurity sources disrupts the security of all actors (Mândraș, 2020, pp. 86-92).

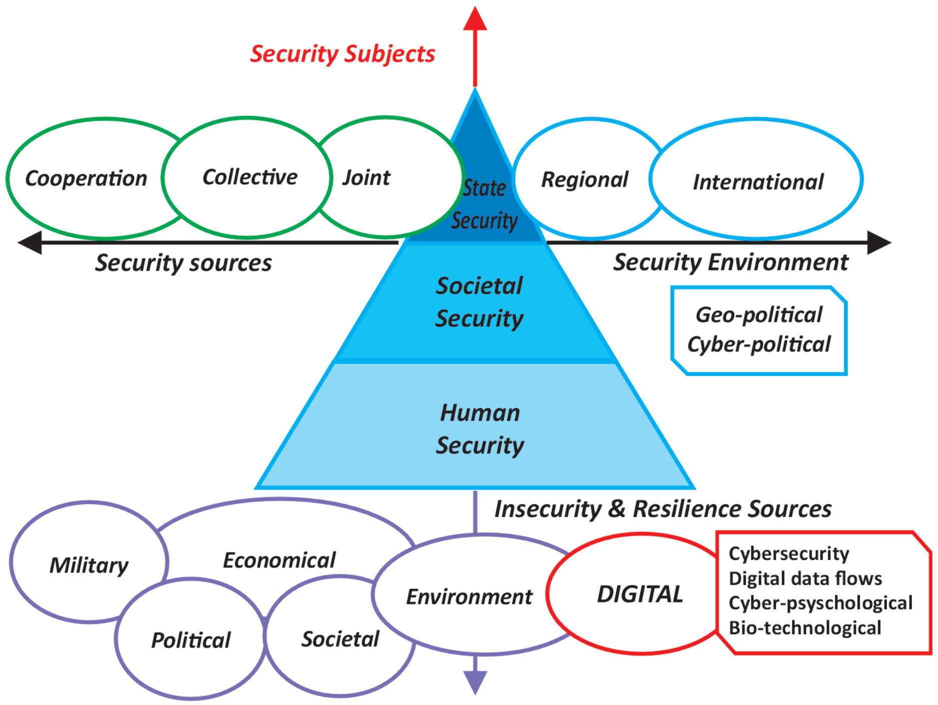

Figure 5: Dimensions of security (Mândraș, 2022, p. 70)

Given these circumstances, is the current theoretical cybersecurity framework inclusive enough?

Prior to providing a comprehensive answer, we note that the security literature provides significance almost exclusively to cybersecurity, which is treated solely from the state security's perspective. Hence, cybersecurity refers to the state's need to ensure security of three main components, respectively: the *hardware* and *software* that contain digital information; the *flows of digital data*, and its *digital informational environment*. More specifically, security literature details two concepts: *cybersecurity* and *security of digital data flows*.

Referring to *cybersecurity*, one cannot identify a universally accepted definition, similar to many other concepts in the field of social and security studies.

For example, NATO regards *cybersecurity* to consist mainly of *defending its own cyber networks, missions, and operations, as well as increasing the organization's resilience, including through the development of capabilities for cyber education, training, and exercises* (NATO, 2023; see also NATO, 2016).

From a US perspective, the White House Cyberspace Policy Review regards *cybersecurity* as an *"activity or process, ability or capability or state by which computer* *and communication systems, as well as the information contained therein, are protected/defended against destruction or access, modification, or unauthorized exploitation”*. Moreover, cyber defence includes a whole range of actions, strategies, policies and standards to reduce threats, vulnerabilities and destruction of cyberspace and its operations, through *“international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure*” (Cybersecurity and Infrastructure Security Agency, 2023).

Even if the *security of digital data flows* can be easily confused with cybersecurity, it has a *distinctive character* given by the existence of a *dual perspective of digital information.* Firstly, it belongs to a specific digital system located within a certain geographical territory. Secondly, the digital information networks digital systems that are located on the territory of several states and are subject to different legal jurisdictions and regulations.

On the other hand, the *security of digital data flows* lays the foundation of digitalization and refers to ensuring the national, regional and international digital security of financial data and ideas exchanges, and not only to ensure the security of digital economic exchanges – energy, products and services (Verhagen, Chavannes, Bekkers, 2020, p. 7).

Considering the above-mentioned arguments, we emphasize that, currently, the security literature regards cybersecurity almost exclusively from the perspective of entailing the security of a single security actor, the state.

Hence, we call for an inclusive cybersecurity perspective that regards individual and societal security issues that arise from cyber and digital space threats. We criticize the approach to cyber security only from the state perspective and consider that the approach must be extended to a new concept of *“phygital”* security in order to include the perspective of the other two security actors – individuals and societies, and all types of sources of digital insecurity.

Consequently, we advocate for a comprehensive cybersecurity approach, which addresses both individual and societal security concerns that result from cyber and digital threats and conflicts. We believe that the traditional state-centric approach to cybersecurity is inadequate and does not entail the full magnitude of digitalization as previously depicted.

More specifically, we call for an expansion of the security of cyberspace to encompass *“phygital”* security, taking into account the perspectives of all three security actors – individuals, societies, and states, as well as all sources of digital insecurity, and types of digital effects in physical space.

Considering that cyber and digital space is an environment of insecurity not only for states, but also for individuals and communities that are part of societies, we believe that such an expansion positively answers Robert Reardon and Nazli Choucri’s call for giving greater importance to individual rights within the objectives of the cyber agenda (Reardon, Choucri, 2012, p. 7).

Consequently, we define *“phygital”* security as an *activity, process, skill, or capability to identify, defend, and build resiliency against any disruptive effect of cyber and digital space in the physical realm, embodied in sources of cyber and digital insecurity* (see *Figure 6*).

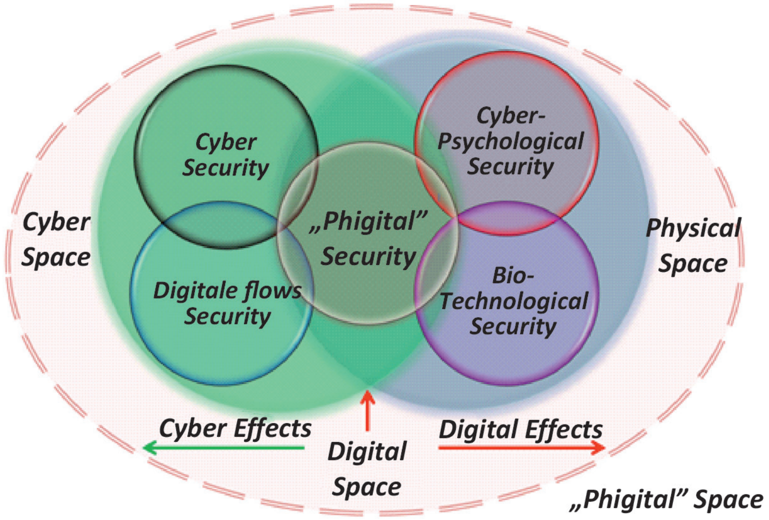

Figure 6: “Phygital” security (Ib.)

As previously detailed, we refer to *physical effects* – cyber protection and defence of ICT; *informational effects* – defence of the informational environment and protection against hostile digital influences; *cyber-psychological effects* – protection against undermining psyche and behaviour (see Harley, Frith, Morgan, 2018, pp. 6-7); and *bio-technological effects* – protection against hostile biological manipulations and hacking (see US National Science Foundation, 2007).

FURTHER RESEARCH AGENDA

We embarked on this research article with two fundamental questions in mind that we believe are critical for the contemporary reality. Firstly, we wanted to determine whether we are currently witnessing a digital transformation of societies and whether this process demands a reassessment of the concept of cybersecurity.

Through literature review and analytical research methods, we discovered that digitalization has a global impact, primarily due to the development of information and communication technologies, as well as the exponential growth of digitization, and human activities within cyberspace. As such, we examined the concept of digitization and distinguished it from digitalization, which we believe is a process that affects all security actors by improving the efficiency of digital technologies in societal activities.

Furthermore, we provided a differentiated perspective of cyberspace from digital space, detailing the effects that automated and human activities have on the physical environment. We also described how security literature approaches cybersecurity and digital data flows almost entirely from a state perspective.

Therefore, our answers to the two questions are affirmative, and this article calls for a re-evaluation of the concept of cybersecurity, considering both the effects of digitization on society and the *"phygital"* effects generated by the fusion of physical space with the cyber-digital environment.

Instead of concluding, we emphasize that we offer a new theoretical approach to cyberspace security, which we call *"phygital"* security, and which addresses four types of digital disruptions with effects in physical space: Cyber, Digital data flow, Cyber-psychological, and Bio-technological security.

As theoretical models correspond to practical needs, our conceptualization aims to serve as a model for the development of appropriate and differentiated public policies that address all sources of cyber and digital insecurity.

We propose continuing research and encourage debates on the opportunities and risks generated by digitization and cyber-digital effects in physical space.

Moreover, we urge the entire society, but especially academia, government decision-makers, businesses, IT and media professionals, as well as non-governmental organizations to identify and promote good practices, procedures and regulations that foster the development of individual, societal and state resilience.

BIBLIOGRAPHY:

1. Akshar. (n.d.). *Top 10 Emerging Technologies in 2022*, WebbyButter: https://webbybutter.com/list-of-emerging-technologies/, retrieved on 16 September 2023.
2. Balsa-Barreiro, J., Menendez, M., Morales, A.J. (2022). *Scale, context, and heterogeneity: the complexity of the social space*. *Scientific Reports,* 12 (9037). DOI: https://doi.org/10.1038/s41598-022-12871-5.
3. Brennen, S., Kreiss, D. (2014). *Digitalization and Digitization*, culturedigitally.org: https://culturedigitally.org/2014/09/digitalization-and-digitization/, retrieved on 20 September 2023.
4. Castagna, R., Bigelow, S.J. (2021). *Information Technology (IT)*, techtarget.com, retrieved on 16 September 2023.
5. Cybersecurity and Infrastructure Security Agency. (2023). *Explore Terms: A Glossary of Common Cybersecurity Words and Phrases*. (N. I. STUDIES, Editor), https://niccs.cisa.gov/:https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary#letter-c, retrieved on 1 October 2023.
6. *Digitization vs. digitalization: Differences, definitions and examples*. (n.d.), truqcapp.com: https://www.truqcapp.com/digitization-vs-digitalization-differences-definitions-and-examples/, retrieved on 16 September 2023.
7. Dow, L. (202). *The Phygital Experience: Security in an Increasingly Digital Future*, IoT For All: https://www.iotforall.com/phygital-experience-security-in-an-increasingly-digital-future, retrieved on 1 March 2023.
8. European Defence Agency. (2023). *Factsheet: Long-term Capability Assessment,* European Defence Agency: https://eda.europa.eu/publications-and-data/latest-publications/enhancing-eu-military-capabilities-beyond-2040, retrieved on 30 September 2023.
9. Fayard, A.-L. (2012). *Space Matters, But How? Physical Space, Virtual Space, and Place Get.* In B.A. Paul M. Leonardi, *Materiality and Organizing: Social Interaction in a Technological World* (pp. 177-195). Oxford: Oxford Academic. DOI: https://doi.org/10.1093/acprof:oso/9780199664054.003.0009
10. Harley, D., Frith, H., Morgan, J. (2018). *Cyberpsychology as Everyday Digital.* London: Palgrave Macmillan.
11. Huawei Technologies Co., Ltd. (2020). *Shaping the New Normal with Intelligent Connectivity. Mapping your transformation into a digital economy with GCI 2020,* https://www.huawei.com/minisite/gci/assets/files/gci_2020_whitepaper_en.pdf?v=20201217v2, retrieved on 10 September 2023.
12. *Information Technology*. (n.d.), Gartner Glossary: https://www.gartner.com/en/information-technology/glossary/digitalization, retrieved on 12 September 2023.
13. Kuehl, D.T. (2009). *From Cyberspace to Cyberpower: Defining the Problem*. In FD. Kramer, S. Starr, L.K. Wentz. *Cyberpower and National Security.* Washington D.C.: National Defense University Press, Potomac Books.
14. Le Merle, MC., Davis, A. (2017). *Corporate Innovation in the Fifth Era. Lessons from Alphabet/Google, Amazon, Apple, Facebook and Microsoft*. Corte Madera, CA: Cartwright Publishing.

15. LUMSA Universita. (2022). *4th Digital Transformation Conference, Phygital Transformation, Constituents, Challenges and Prospects*, lumsa.it: https://www.lumsa.it/4th-digital-transformation-conference, retrieved on 1 March 2023.
16. Manyika, J., Chui, M., Bughin, J., Dobbs, R., Bisson, P. & Marrs, A. (2013). *Disruptive technologies: Advances that will transform life, business, and the global economy.* McKinsey Global Institute, see https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/disruptive%20technologies/mgi_disruptive_technologies_full_report_may2013.pdf, retrieved on 15 September 2023.
17. Mândraș, L.P. (2020). *Security's Multidimensionality. Societal Security in the Age of Information Technology*. In *Romanian Military Thinking International Scientific Conference Proceedings. Military Strategy Coordinates under the Circumstances of a Synergistic Approach to Resilience in the Security Field* (pp. 78-95). București: Centrul Tehnic-Editorial al Armatei.
18. Mândraș, L.P. (2021). *"Desecretizarea"* conceptului de securitate. Noțiuni, componente, dimensiuni, domenii și tipuri de Securitate. *Infosfera* (4), pp. 27-39, https://www.mapn.ro/publicatii_militare/arhiva_infosfera/documente/2021/4_2021.pdf#, retrieved on 15 September 2023.
19. Mândraș, L.P. (2022). *The Digital Century and Its Implications on the International Security Environment. Digital Confrontations in Cyber Space and Real Space.* In *Romanian Military Thinking International Scientific Conference Proceedings. Dynamics of security architecture in the Wider Black Sea area, in the context of the conflict in Ukraine and the new NATO strategic concept (4)*, pp. 58-79. București: Centrul Tehnic-Editorial al Armatei. doi:10.55535/RMT.2022.4.03
20. *Merriam-Webster*. (n.d.), *Definition of information technology*: https://www.merriam-webster.com/dictionary/information%20technology, retrieved on 15 September 2023.
21. Miller, B. (2001). *The Concept of Security: Should it be Redefined?* In *Journal of Strategic Studies, 24*(2), pp. 13-42.
22. Mölling, D.C., Schimmel, F. (2021). *Strategic Compass. Promoting Technological Sovereignty and Innovation: Emerging and Disruptive Technologies.* German Council on Foreign Relations. Berlin: Deutsche Gesellschaft für Auswärtige Politik e.V., https://gateway.ipfs.io/ipfs/iw4bzfbcfqbvhyei7dno4qehw63smn5e4zrb2oyfbviugc?filename=%28DGAP%20eport_%2022_2021%29%20Christian%20M%C3%B6lling%2C%20Florence%20Schimmel%20-%20Promoting%20Technological%20Sovereignty%20and%20Innovation_%20Eme, retrieved on 15 September 2023.
23. NATO. (2016). *NATO Cyber Defence*. (P. D.–P. Section, Editor), www.nato.int: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-en.pdf, retrieved on 20 September 2023.
24. NATO. (2020). *AJP-3.20. Allied Joint Doctrine for Cyberspace Operations.* NATO Standardization Office (NSO), retrieved on 15 September 2023.
25. NATO. (2023). *Cyber defence*, www.nato.int: https://www.nato.int/cps/en/natohq/topics_78170.htm, retrieved on 20 September 2023.
26. Reardon, R., Choucri, N. (2012). *The role of Cyberspace in international relations: A view of the literature.* San Diego: Department of Political Science – MIT.

27. Reis, J., Amorim, M., Melão, N., Cohen, Y. & Rodrigues, M. (2020). *Digitalization: A Literature Review and Research Agenda.* In Z. Anisic, B. Lalic, G. Danijela, *Proceedings on 25th International Joint Conference on Industrial Engineering and Operations Management – IJCIEOM. IJCIEOM 2019. Lecture Notes on Multidisciplinary Industrial Engineering* (pp. 443-456). Cham: Springer.
28. Schreier, F. (2015). *On Cyberwarfare.* 50. Schreier, Fred. *"On Cyberwarfare"*, DCAF HORIZON 2015, The Geneva Centre for the Democratic Control of Armed Forces (DCAF), https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf, retrieved on 15 September 2023.
29. U.S. National Science Foundation. (2007). *Nanotechnology: Societal Implications II. Individual Perspectives* (Vol. 2). (M. C. Roco, & W. S. Bainbridge, Eds.) Dordrecht: Springer.
30. Verhagen, P., Chavannes, E., Bekkers, F. (2020). *Flow Security in the Information Age.* Hague: The Hague Centre for Strategic Studies.
31. Welsh, M. (2023). *The Future is Phygital: Physical and Digital*, mobiquity.com: https://www.mobiquity.com/insights/the-future-is-phygital, retrieved on 1 March 2023.
32. White-Gomez, A. (2022). *What Is 'Phygital'? The Blending of Physical and Digital*, ONE37pm: https://www.one37pm.com/nft/what-is-phygital, retrieved on 1 March 2023.