Digital security- emphasizing the need for a new comprehensive theoretical approach of cybernetic security due to society's digitalization. Glimpses of digitalization in the Black Sea Region

Paul Mândraș[1], Cezar Vasilescu[2]

Keywords: Digital Security, Digitalization of Society, (Social) Internet of Things, Metaverse, Artificial Intelligence, Cybersecurity

Abstract: *As development of information and communications technologies rapidly advances within nations, it is the responsibility of society's key stakeholders – business specialists, non-governmental organizations, researchers, academics and policymakers, to provide specialized in-depth awareness in regards to security related issues. In order to achieve knowledge on technological challenges and build tailor-made public policies, society's key stakeholders ought to tackle the impact of digitalization. Nations need to become aware that the process entails the whole of society. As the digital evolution and revolution emerge and expand become synonymous not only to economic proficiency but to digital disruption as well. We can agree that the evolution of Artificial Intelligence, (Social) Internet of Things, Metaverse, Digital Twins, Human Robots, Virtual Influencers, etc. provides opportunities and challenges to societies that we have*

[1] Phd. Student, „Carol I" National Defense University, Bucharest, Romania.
[2] Professor, PhD, Regional Department of Defense Resources Management Studies (DRESMARA), Brasov, Romania.

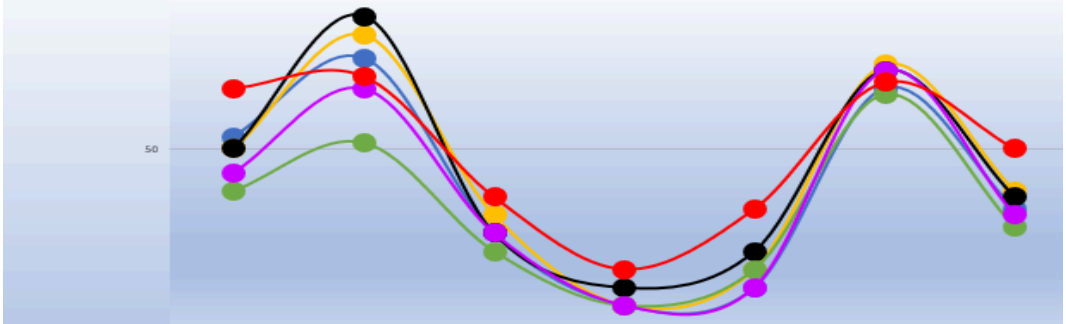
never faced before in human history. Given these circumstances, does cybersecurity fully encompass the digital changes and disruption or do we need to further expand our research on digital security?

1. *Digitalization of societies as a primordial feature of the digital age*

Can societies be digitalized? Not only that our answer is affirmative, but digital integration is a current reality and a global trend (see *Figure no. 1 – Digitalization in the Black Sea Region*).

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 and Kreiss, "*Digitization and Digitalization"*, 2014), 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.

Obviously, despite the opponents, the development of information and communication technology (IT&C) systems has evolved from 1971 to the present day, but together with this evolution, the debate within societies regarding digitalization has persisted and even intensified, a debate to which we do propose to contribute constructively.



	Country Score	Broadband	Cloud	AI	IOT	Experience	Potential
Bulgaria	52	65	36	24	27	60	40
Romania	50	69	39	24	30	64	43
Russia	50	72	36	27	33	63	42
Ukraine	43	51	33	24	30	59	37
Turkiye	46	60	36	24	27	63	39
World Average	60	62	42	30	40	61	50

Figure no. 1 – Digitalization in the Black Sea Region [3]

From a technical point of view, *IT&C designates the technology that underlies the process of development, maintenance and use of computer systems, software applications and computer networks for the processing and distribution of digital data* (Merriam-Webster, "*Definition of information technology*").

Thus, we note that the term IT&C includes both computer and telecommunications technology (Castagna and Bigelow, "Information Technology", 2021), and the main fields are represented by:

1. *Implementation* and *maintenance* of applications, services and digital infrastructure (servers, networks, external storage capacities);

2. *Monitoring*, *optimizing* and *troubleshooting* the performance of applications, services and infrastructure; as well as

3. *Cyber security* oversight and governance of applications, services and infrastructure.

[3] Figure data are based on *2020 Global Connectivity Index* calculated by Huawei Technologies on a sepctrum of 40 indicators. Huawei analized 79 countries (Georgia and Moldova not included) and the potential maximum score for each indicator is 120. GCI Source: https://www.huawei.com/minisite/gci/en/country-profile.html

Consequently, in our consideration, *IT&C represents those physical devices endowed with software programs that have computing, storage and networking capabilities; as well as the infrastructure and processes for creating, processing, storing, securing and exchanging all forms of electronic data* (see *Figure 2 – Information Technology Components and Functions*).

However, precisely to eliminate possible confusion, we propose to clarify the semantic difference between the terms *digitization* and *digitalization*, sometimes treated similarly in the specialized literature.

Thus, *digitization* is the process by which data and information in physical or analog format are transformed into data and information in digital format (TruQC LLC, "*Digitization vs. digitalization: Differences, definitions and examples*").

Practically, *digitization is a transformational process of the form in which the data and information present themselves in the physical space to the cybernetic space*. As a simple example, digitization is the translation of a physical document into an electronic document through the process of photography.

Figure no. 2 – The components and functions of information technology[4]

On the other hand, *digitalization* is a much more complex process than digitization, and from a certain perspective of interpretation, *digitalization includes digitization*, the latter representing a first phase of digitalization, of collecting information.

Digitalization includes, but is not limited to, both *digitization* and the *IT&C processes* described above, precisely because it is a process that involves human activity.

Therefore, although there is a diverse variety of definitions of *digitalization* (Reis, "*Digitalization: A Literature Review and Research Agenda*", 447-448), we note 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* (Gartner Glossary, "*Information Technology*").

Thus, we draw attention to the fact that *digitalization* is the most important current trend of change for both societies and businesses, in the context in which organizations - regardless of their type - are under constant pressure to use digital technologies and adapt models and operating strategies to this new reality.

Through *digitalization*, industrial societies are rapidly transforming into informational societies on a global level.

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 exhaustive and holistic, with reverberations throughout the whole of society and all its domains – military, political,

[4] Source: Castagna and Bigelow, "Information Technology", 2021

economic, social and environmental (Mândraș, "*Security's Multidimensionality. Societal Security in the Age of Information Technology*", 78-95).

From a scientific perspective, the debate on the understanding of the concept of *digitalization* is still far from being completed, but its effects on societies are increasingly visible, noting the intensification of digitalization not only at the level of private entities but also at the government level, which increasingly integrates information technologies in its own mode of operation for the performance of public activities (Reis, "*Digitalization: A Literature Review and Research Agenda*", 443-456).

Considering these aspects, we feel obliged to criticize the approach to the digitalization of societies strictly from the point of view of economic influence, meaning for which we propose a comprehensive approach, taking into account the fact that these *new types of information technologies generate new types of human interactions at all levels of societies* – macro, micro and nano

Therefore, in our opinion, *digitalization of societies is a societal process through which digital technologies modify, transform, disrupt or destroy processes, the models and strategies of individuals and social groups, in all their fields – military, political, social and environmental, in order to capitalize on the opportunities to make all human activities more efficient*.

2. *Digital evolution and societal revolution. Digital space and disruptive technologies*

The development of digital technologies is closely related to the invention of cyber information, the Internet, artificial intelligence and process automation, bio-materials, and so on. Cumulatively, these technologies have generated new

innovative mechanisms for reconfiguring and streamlining the systems of production of goods and delivery of services, mainly for economic purposes.

Information technologies not only make the goods-producing industry more efficient but also generate new types of industries that offer economic services without owning industrial production capabilities.

Thus, the global economic market has come to be dominated by *digital companies* (see Kabra, "Top 20 Biggest Tech Companies in The World in 2022"), among which stand out digital unicorns, which have a cumulative market value of approximately 3.857 billion USD. Individually, digital unicorns have a market value of at least one billion USD, sometimes more than the GDP of entire countries (CBINSIGHTS, "The Complete List of Unicorn Companies", 2022).

Such a value of *digital companies* is not strictly limited to economic power, but sometimes even to the *social influence power* that such companies possess.

Cumulatively, these new economic models stimulated by digitalization, impose not only changes in industrial processes, through the gradual elimination of human labor at the expense of automated and/or robotic labor but also behavioral changes of people and the organizations they belong to, regardless of the type of these organizations.

Consequently, the societal changes produced by digitalization are generated by two distinct elements, which act synergistically at the level of individuals and societies, respectively:

A. The emergence of a new space for human activities – the *digital space*;

B. Development of *disruptive digital technologies*.

2.1. Digital space as a new dimension of human activities in cyberspace

Perhaps one of the current confusions among specialists and the general public is given by the differentiation between physical, cyber (virtual), and digital space.

From a military perspective, *cyberspace* represents a *global domain* composed of the interconnection of all IT&C, networks, and digital data, including independent and isolated ones that process, store, or transmit data, being assimilated in importance to other operational environments in which military actions take place - land, naval, air and space (NATO Standardization Office, "Allied Joint Publication-3.20 (AJP-3.20)", 2020, 4).

In terms of cyberspace components, NATO identifies 3, respectively: *physical* – which includes the physical components (digital devices), 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.

However, we allow ourselves to note that this last component of cyberspace, the *cyber-persona*, even if it can exist independently, without being correlated with the physical and real person or organization with which it is associated, it can only operate in cyberspace in close correlation with its physical and real counterpart. By operating in cyberspace, we mean the actions, activities, or behaviors performed by the individual or organization in this virtual space.

Precisely for these reasons, we consider that *cyberspace is not confused with digital space*. Thus, if *cyberspace (virtual) is represented by IT&C components* (devices, software, and digital data), *digital space is represented by human actions, activities, and behaviors, at an individual or organizational level, within cyberspace, with repercussions both in the space cyber as well as in real space.*

Moreover, the 3 types of spaces are not only interdependent, but human or automated operations in cyberspace produce effects in physical space in 3 interdependent dimensions, and we consider these dimensions to be: physical, informational, and bio-psycho-social (see *Figure no. 3 – Digital inter-relationships*) and not *physical*, *informational* and *cognitive* (*idem*, 1).

Regarding the *physical dimension*, this includes all IT&C devices located in the physical space that process digital information, regardless of whether they work independently or in a network, with or without an Internet connection.

The *informational dimension*, dubbed by some specialists the *informational environment* (Kuehl, "From Cyberspace to Cyberpower: Defining the Problem", *apud.* Schreier, "On Cyberwarfare", 2015, 11), includes the *virtual information contained in the systems arranged in the physical space, which can be subjected to processes of dissemination, processing, storage, exploitation, transformation, manipulation, extraction, destruction*, etc.

Regarding the *bio-psycho-social dimension*, we argue that *physical entities* – persons or organizations, *act on and operate with digital information, and the result of these processes produce societal effects at the biological, psychological, and sociological levels*[5] and not only at the human cognitive level.

As a consequence, human digital inter-relationship does not occur exclusively at a cognitive level, but at a higher, three-dimensional level. Respectively, at the biological level, when *digitalization affects the biological and*

[5] 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, together with mental activities (play, learning, work, creation and communication) and mental attributes (temperament, skills and character), are integrated into what psychology calls the human psychic system.

informational system of living beings; *psychologically*, when *digitalization affects individual virtual relationships and behaviors*, and *sociologically*, when *digitalization affects virtual relationships and behaviors between at least two virtually represented physical entities*.

All these dimensions, bio-psycho-social, have physical effects at the individual and societal level, by affecting human behaviors and, directly or indirectly, by influencing the identity and culture of societies.

Intrinsically, we consider that *the main characteristic of the digital space is its duality*, it is at the same time a physical–cybernetic network of digital information exchange, as well as a global phenomenon of influencing people and societies, which is constantly expanding, specifically due to the development of virtual social networks.

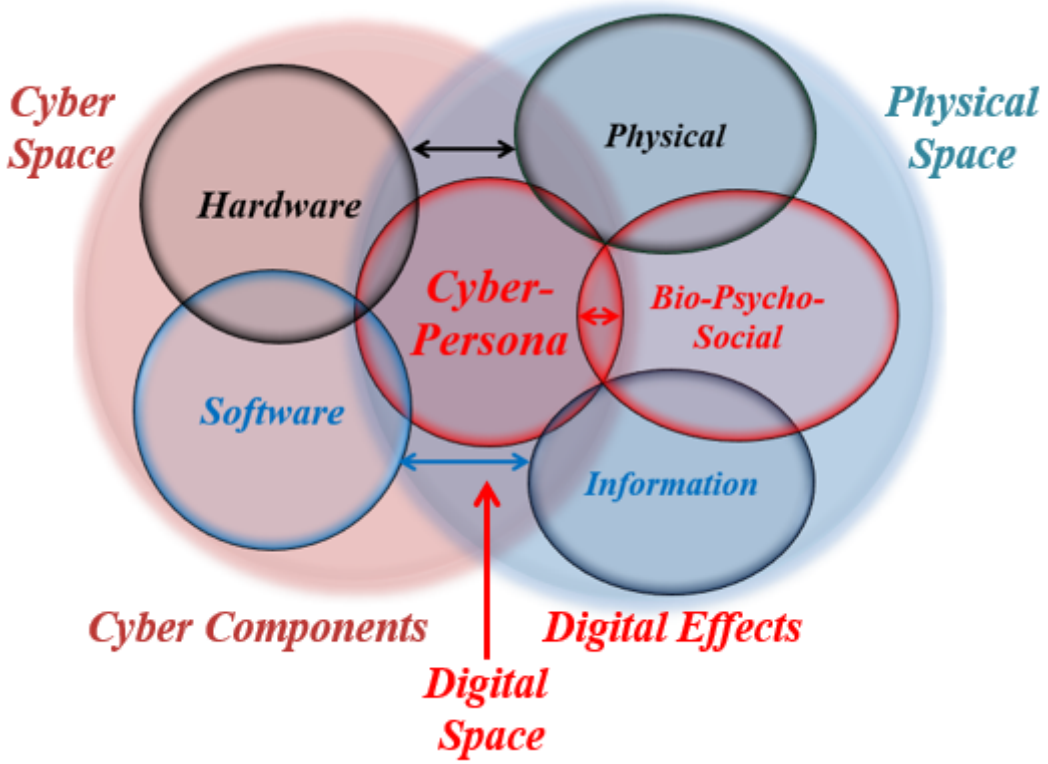


Figure no. 3 – Digital inter-relationships

Through human action 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, and Davis, "Corporate Innovation in the fifth era. Lessons from Alphabet/Google, Amazon, Apple, Facebook and Microsoft", 2017, 42).

Moreover, from a societal perspective, the digital relationships between physical entities are identical to the relationships in the physical space and are of three main types, namely *cooperation*, *neutral*, or *confrontational*.

2.2. Disruptive digital technologies – Internet, Internet of Things, Social Internet of Things, Artificial Intelligence with Machine Learning capability,

Robotics, Metaverse, Digital Twins, Digital and Virtual Influencers, and Humans 2.0

Included in the category of general-purpose technologies (DPTs) (Azhar, "EXPONENTIAL. How Accelerating Technology Is Leaving Us Behind and What to Do About It", 2021, 43 and following), the Internet was developed in the 1960s by the US in the form of small digital communication networks between several government computers, with the main objective of creating a structure that would ensure the integrity and transfer of information, resistant to potential nuclear attacks by the USSR.

Afterward, the Internet developed progressively in two relatively distinct stages. The first stage took place in the 1990s when the Internet was "democratized", being practically made available to the general public and gradually transformed into a global public network in exponential growth due to the popularization of personal computers.

A second stage in the development of the Internet was generated by the rapid development of smartphone-type mobile phones with Internet connection capabilities, which enabled the amazing development of the mobility of digital connectivity.

Currently, the Internet is a global network of human interconnectivity, and at the beginning of 2022 (Kemp, "Digital 2022: Global Overview Report", 2022), out of a total global population of 7.91 billion, 5.31 billion (67.1%) people are mobile phone users, 4.95 billion (62.5%) are internet users, and 4.62 billion (58.4%) are active users of some social networks (see *Figure no. 4 – Digital space in the Black Sea Region*).

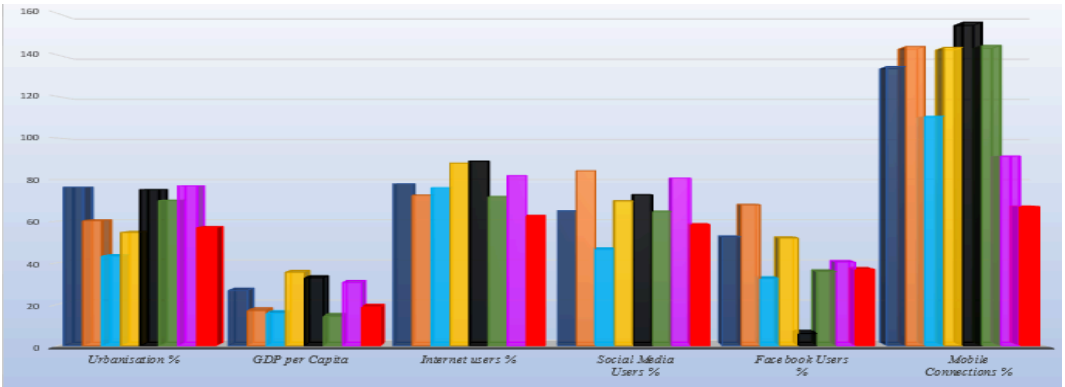
Considered the 3rd wave of Internet development, the *Internet of Things* (IoT) is another type of technology that has the potential to affect all human activities (Tripathy, and Anuradha (ed.), "Internet of Things (IoT): Technologies, Applications, Challenges and Solutions", 2018, p. ix).

Basically, *IoT means the ability of physical devices and people to be permanently interconnected through the Internet*, which causes the emergence of new types of digital ecosystems capable of increased productivity, increased energy efficiency, as well as increased economic profitability, in almost all fields of human activities (see *Figure no 5 - Applications of digital technologies*).

The name "IoT" was proposed for the first time by the British Kevin Ashton in 1999, and the specific difference of IoT from the Internet is given by the fact that digital devices not only have the possibility to collect electronic information from the physical and virtual environment, but essentially, IoT has the ability to analyze this information, make decisions without human intervention and learn from accumulated experience (McAfee, and Brynjolfsson, "Machine, platform. Crowd: Harnessing our Digital Future", 2017 *apud.* Dufva, and Dufva, "Grasping the future of the digital society", 2019, 17).

Complementary to IoT, as its particular form, *Social Internet of Things* (SIoT) describes the symbiosis between human social networks and IoT, in the sense that *digital objects form their own social networks* and, despite constructive particularities, manage to communicate and relate autonomously through the Internet, without direct human intervention (Lee et al., "How and what to study about IoT: Research trends and future directions from the perspective of social science", 2017, pp. 1056-1067 *apud.* Rad et al., "Social Internet of Things: vision, challenges, and trends", 2020). The end result is social networks of digital objects

of different complexities that relate based on common interests in order to provide improved services to end users (Rad et al., "Social Internet of Things: vision, challenges, and trends", 2020).



	Urbanisation %	GDP per Capita	Internet users %	Social Media Users %	Facebook Users %	Mobile Connections %
Bulgaria	76.4	26.705	78	64.8	52.4	134.5
Georgia	60.3	16.997	72.5	84.3	67.9	144.1
Moldova	43.2	15.637	76.1	46.5	32.3	110.5
Romania	54.6	35.414	88	69.7	51.9	143.7
Russia	75.2	32.803	89	72.7	5.9	155.8
Ukraine	70	14.219	71.8	64.6	35.7	144.6
Turkiye	77	30.472	82	80.8	40.3	91.4
World Average	57	18.721	62.5	58.4	36.8	67.1

Figure no. 4 – Digital space in the Black Sea Region[6]

Through SIoT, digital devices imitate the human way of relating in order to communicate and select "friends" to provide increased performances of the services offered. The effects of increased performances occur at different levels, including the level of interactions between people and objects.

Precisely as a consequence of the "socializing" characteristic, digital objects within SIoT become more performing than digital objects that act in a unitary

[6] *GDP per Capita* is expressed in USD. Source of data: The World Bank Group, „GDP per capita, PPP (current international $)". https://data.worldbank.org/indicator/NY.GDP.PCAP.PP.CD?name_desc=false&view=chart. *Urbanisation*, *Internet Users*, *Social Media Users*, *Facebook Users*, and *Mobile Connections* is expressed as a percentage of total population. Source of data: Kemp, „Digital 2022: Global Overview Report". https://datareportal.com/reports/digital-2022-global-overview-report

way, mainly due to the quality and quantity of information that they exchange with the other SIoT member objects.

Human intervention within the SIoT is decisive precisely by owning the function of *owner control* (Rad et al., "Social Internet of Things: vision, challenges, and trends") a function exercised by assigning to the network a set of rules to control the behavior of objects in the network and the way of communication between objects.

From a technical point of view, the functioning of physical devices is based on software codes, without which digital operations cannot be carried out. Thus, *software codes are operating programs* of these devices, which can support changes, updates, repairs, storage and analysis, without direct intervention on the objects that include them.

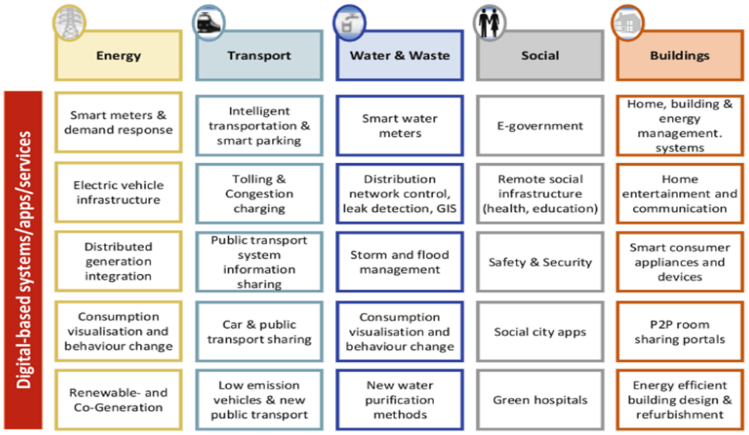


Figure no. 5 – Applications of digital technologies [7]

Obviously, the evolution of software codes has been gradual but galloping in the last decades, and from the first software with the ability to perform simple

[7] Source: Vagadia, „Digital Disruption. Implications and opportunities for Economies, Society, Policy Makers and Business Leaders", 2020, 91.

and repetitive tasks, nowadays they have the ability to perform complex tasks, automatically and with the possibility of self-learning and improving, known as machine learning capabilities, similar to the functioning of the human psychic system.

This last category of software is represented by Artificial Intelligence (AI), a "queen" of software. Even though it is difficult to define it specifically, *AI can be characterized as an artificial decision-making system, similar to the human system, based on unique algorithms and mathematical estimations* (Siroya, and Mandot, "Role of AI in Cyber Security" in Bhargava et al. (Eds.), "Artificial Intelligence and Data Mining Approaches in Security Frameworks", 2021, 2).

According to some authors with whom we agree (Schwab, and Davis, "Shaping the future of the fourth industrial revolution. A guide to building a better world", 2018, 138), AI is already reinventing the digital economy and has the capacity to reconfigure the physical economy in the near future, by empowering autonomous devices to navigate the physical world and by owning the ability to improve and streamline both inter-relationships between people, as well as the inter-relationship between people and information devices.

The main ability of AI lies in its *cognitive capacity*, *learning,* and *reasoning*, including those based on *intuition*, which is based on a rapid pace of self-improvement and which *already clearly exceeds human cognitive capacity*.

Additionally, innovations in physical materials and endowing them with AI capabilities have developed a new industry, *robotics*.

Since 1961, when the first industrial robot was used in a factory (*ibidem*), robots have been subject to amazing developments, and nowadays we can find different types of robots with AI functions within societies, such as *industrial*

robots, *robots with the ability to fly* – drones, auto*nomous vehicles* and, last but not least, *humanoid robots*, capable of providing personal assistant services or even social assistance for people, such an example being *Sophia the Robot* (Lokhande, "Sophia and Other 11 Best Humanoid Robots of 2022").

With the improvement of AI's ability to make decisions, it is expected that the fields of applicability of AI robots will also increase. Implicitly, the influence of AI robots within societies will intensify as well, and maybe one of the most debated topics of this century will regard granting human rights to AI robots (see Marko, "Robot rights - a legal necessity or ethical absurdity?", 2019).

Moreover, AI robot's societal effects can be both beneficial – by identifying solutions to the current problems of humanity beyond the ability to human understanding, as well as harmful – especially through the development of weapon systems based on AI robots, already in the prototype stage and expected to represent 30% of the military forces of some states in the next 10 years (Pro Robots, "Top 5 Most Advanced Army Robots. Tank Robots, Robot Dogs, Unmanned Vehicles. Military Robots", 2020).

Another technology with a fast pace of development is *Metaverse*. First imagined in 1992 by science fiction author Neal Stephenspon in his short story "Snow Crash", the term *Metaverse* denotes a vision of a virtual reality in which people use their own digital avatar to explore the online world via the Internet (Huddleston Jr., "This 29-year-old book predicted the 'metaverse' — and some of Facebook's plans are eerily similar", 2021).

Even if Stephenspon imagined his Metaverse as an alternative virtual form to the dystopian physical reality, the concept was taken over by digital companies such as Meta (Meta, "Inside the Lab: Building for the Metaverse with

AI", 2022), Microsoft (Roach, "Mesh for Microsoft Teams aims to make collaboration in the 'metaverse' personal and fun", 2021), Roblox (McDonald, "Roblox's metaverse is already here, and it's wildly popular", 2021) or Epic Games (Kim, "Metaverse Is a Multitrillion-Dollar Opportunity, Epic CEO Says", 2021). Such companies are trying to develop their own digital universes, sensing both an economic opportunity in people's desire to "escape" from physical reality, but also possibilities to expand lucrative activities in the digital space.

Also called Collaborative Virtual Environments (CVEs) (Eustáquio, and Carneiro de Sousa, "Creative Collaborative Virtual Environments"), or Cyber-Physical Systems (CPS), or Cyber-Physical System Virtual Organization (CPS-VO) (Skilton, and Hovsepian, "The 4th Industrial Revolution. Responding to the Impact of Artificial Intelligence on Business", 11 and following), the *Metaverse is a virtual space where people meet other people, entities or objects, in their virtual replica*, as participants and not spectators, that engage in relational and creative activities. The latter case is specific for CVEs, as it provides its users the ability to create, modify, transform and redistribute media content, such as audio-visual components or even software programming codes.

As digital systems integrating cybernetic components and human users, Metaverses are based on what the literature calls *Digital Twins* (Song et al., "Cyber-Physical Systems: Foundations, Principles and Applications" *apud.* Skilton, and Hovsepian, *idem*), namely a conjunction and coordination of physical and informational resources of virtual representation of physical and human systems. In other words, *Digital Twins are digital avatars of people, places and physical objects*.

Also, according to the most recent developments, correlated primarily with the emergence of digital communications and social networks, but also with Metaverse, the digital environment has allowed the emergence of two new categories of digital entities with the role of influencing people's behavior, attitudes and activities in the online and offline environment, respectively *Digital Influencer* and *Virtual Influencer*.

Thus, a *Digital Influencer is a real person who generates interactions in the online environment, creates content through digital communication channels and who influences the purchasing decision of the public to whom he is addressed, through the authority, knowledge or position or visibility he holds in the digital media environment* (Brandmentions, "What Is a Digital Influencer").

Though, we do not consider it appropriate to use the term Digital Influencer merely to depict it as a marketing tool used by individuals or companies to stimulate their own brands and sales (see Forbes, "Top Creators 2022"). Therefore, we expand our view and agree that a *Digital Influencer is a real person or organization who acts in the digital space as an agent of influencing social relations and behaviors, manifesting itself as a security actor as well.*

With these aspects in mind, what is a Virtual Influencer and what is the specific similarity and difference to a Digital Influencer?

To answer this question, we note both the definition according to which a *Virtual Influencer is a digital character created by means of graphic software, who has a human personality and permanently acts as an influencer on social media platforms*, and the fact that a *Virtual Influencer can have up to 3 times the target community influence rate than a Digital Influencer*, explained by the fact that it can perform all the

activities of the real version, but with *more control and involvement* (Molenaar, "Discover The Top 15 Virtual Influencers for 2022", 2021).

Thus, we consider that, like a Digital Influencer, a *Virtual Influencer is an autonomous digital medium that acts in the digital space as an agent of influencing social relations and behaviors, manifesting itself as a security actor as well.* Unlike a Digital Influencer, who is a physical person, a *Virtual Influencer is a digital "persona" with AI ability to learn and improve its interactions in the digital space with real people*.

Even if at the moment most Digital and Virtual Influencers are assimilated into Social Media Influencers, we consider that it is very likely that digital influencing activities will develop in the near future within the Internet and the Metaverse platforms as well.

In this regard, we note recent research related to creating a *digital workforce for the Metaverse*, such as *Humans OS 2.0* (Soul Machines, "How we bring Digital People to life", 2022), in the form of people's digital twins acting as autonomous animations powered by AI technologies, web services, and other digital means, and we believe that Humans OS 2.0 can also act as a Virtual Influencer.

It is a reality that the COVID-19 pandemic has greatly stimulated both digital economic activities and "work from home" activities carried out "at a distance" from the classic work locations, via the Internet. From this perspective, we can debate Bill Gates' opinion (Gates, "Reasons for optimism after a difficult year", 2021) that this global trend of online "work from home" will continue post-pandemic and that within 2-3 years most online working or social dating will move into the Metaverse, with the help of avatars and digital space.

But if the Metaverse is a form of human imagination becoming a virtual reality through digitalization, it remains to be seen what will really happen in the

medium term regarding the scale of real human activities that will cross the "border" to Metaverse.

At the moment, this new digital environment seems to be treated with humor and sarcasm, especially since Mark Zuckerberg, the CEO of Meta, spent over $10,000,000 to take his first digital selfie in the Metaverse (Parsons, "Mark Zuckerberg responds to everyone that mocked his metaverse selfie", 2022).

However, we consider that the prospects for Metaverse development are obvious and consistent, and from this perspective, we encourage further research of its implications on societies and security.

3. ***The digital disruption of the physical space. Assessing digital insecurity sources***

Considering the evolution of digital space and technologies, it is a logical consequence to inquire ourselves the following question: *are there sources of digital insecurity? If so, which are they?*

As we highlighted previously, *digitalization is a transformational societal process, and new types of information technologies generate new types of interactions at all levels of societies* – macro, micro, and nano, which have effects both in the cyber and real world.

Additionally, these *digital interactions modify, transform, disrupt or destroy the processes, models, and strategies of societies*, in all their fields - military, political, social, and environmental, *producing both opportunities for the development of societies, as well as risks, threats and dangers to security.*

At the same time, the inter-relationships in the cyberspace and the ever-increasing interconnectivity of the physical and virtual environments produce physical, informational, and bio-psycho-social effects in societies. By

default, digital relationships between physical entities are identical to relationships in physical space and are of three major types, namely *cooperation*, *neutral* or *confrontational*.

With these aspects in mind, we believe that *there are sources of digital insecurity that affect all three main security actors – individuals, societies, and states*. These sources of insecurity come both within the framework of confrontations in the cyber and digital space, but also as effects of cyber inter-relationships in the physical environment, in all areas of security.

Thus, as regards the sources of digital insecurity arising from the confrontation in cyberspace, they mainly affect the security of states and are presented as follows:

- At a *physical level*, by affecting the functioning of devices and digital networks or the flow of data between devices in the network – cyberwar and cybersecurity;
- At the *informational level*, through the digital influence of information, ideas and values in order to change the behavior of the population and its leaders – information warfare and digital influence;
- At the bio-*psycho-sociological level*, by affecting the biological information system, at the genetic or psychological level – biohacking and cyberpsychology.

From a technical point of view, the basis of IT&C operation is the software codes, which are programmed to support changes, updates, repairs, storage and analysis, without direct intervention on the objects that contain them.

However, the "Achilles' heel" of software and hardware devices resides precisely in the possibility of intervention on them by external entities, often malicious, who wish to exploit the vulnerabilities of military or non-military

digital systems to extract, corrupt, or destroy data or to obtain prestige, military or political advantages or profit. Such vulnerabilities expose both devices and digital data as well as the entire architecture to cyber security risks, embodied in cyber-attacks and alteration of digital information.

From this perspective, data privacy is equivalent for digital users to the ownership of physical assets, and ensuring the cyber security of digital technologies requires the simultaneous fulfillment of a series of requirements, such as resilience to cyber-attacks; data authenticity; access control; and user data privacy.

Therefore, *the main source of digital insecurity at the physical level derives from the vulnerability of cyber ecosystems*, with negative repercussions in ensuring the integral security of the digital data that the system circulates, but also the confidentiality of this data, in the sense of protecting digital data and ensuring control over digital activities that take place within the digital architecture.

It is indubitable that today's information society benefits from the most developed means of mass communication in human history. Thus, IT&C almost dominates as means of public communication, in times of peace, crisis and war. Virtual communications, through the accessibility of information under the conditions of the existence of mobile phones permanently connected to the Internet, the Internet itself and virtual social networks, have led to an "explosion" in the speed with which information is produced and distributed to target audiences.

Under these conditions, at the regional, national and global level, the digital space is already or is in the process of becoming the main information medium used as a means of mass communication.

Thus, *the main source of digital insecurity at the informational level derives from the manipulation of the informational environment achieved by influencing information, ideas, and values in order to change the behaviors of the population and its leaders*.

From a technical point of view, we agree that we can discuss several *technological developments of digital influencing and conducting "human mind games"* (Chifu, "Aspecte privind războiul informaţional: alterarea realităţii", 2018, 15-16) – disinformation, propaganda, active measures and elements of psychological operations, and from our point of view they can be grouped into seven categories (see *Figure no. 6 – Technological evolution of digital informational influence*), as follows:

(I) *Fake news* – using cyber space to spread fake news;

(II) *Social Media Targeting* – the use of social networks to polarize societies and hijack public debates;

(III) *Big Data Mining* – individual and collective access, based on the analysis of patterns and digital data;

(IV) *Tailor Profiling & Hacking* – "tailor made" digital monitoring and influencing, including through character attack and assassination (see Chifu, "Character assassination" – armă ofensivă în războiul informational", 2017, 11-17);

(V) *Deep Fake* – use of video processing technologies;

(VI) *AI Quantum Virtual Influencers* – automating influence through the use of virtual influencers that combine all previous technological generations through artificial intelligence and quantum computing capacity;

(VII) *Biological Hacking* – the ability to exploit human beings through the ability to combine biological knowledge with quantum computing power and digital data.

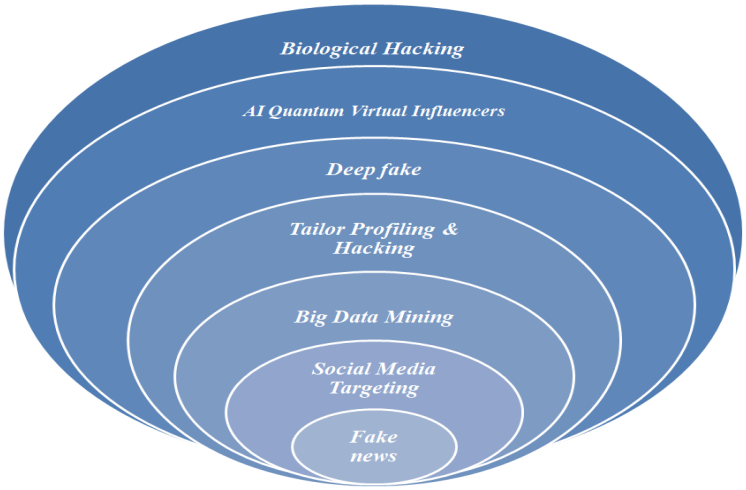


Figure no. 6 – Technological evolution of digital informational influence

For the international community, *information influence* is not defined in an identifiable way, although states officially recognize it. Whilst the Western NATO members acknowledge terms like *information operations* or *influence operations*, the Eastern European states, with reference mainly to the Russian Federation and its predecessors, own terms like *information war* or *psycho-information confrontation* (Fridman, Kabernik, and Granelli, "The Nature of Information Operations", 2022, p. 3) or "*active measures*" or "*information warfare*" (Scîrlet and Ichimescu, "Conflictele/operațiile informaționale ale Federației Ruse în contextul SARS-CoV-2", 2020, 12).

For NATO (NATO, *"AJP-3.10, Allied Joint Doctrine for Information Operations"*, 2009, 1-3, *apud.* Ichimescu, *"Operaţiile informaţionale şi mediul informaţional global"*, 2016, 49), *information* or *influence operations* represent

informational activities carried out during times of peace, crisis, conflict, and post-conflict, in order to create the desired effects on the will, understanding, and capabilities of adversaries, potential adversaries and other types of audiences, in support of the objectives the mission.

For the Russian Federation (Ministry of Defence of the Russian Federation, "Voyennyy Entsiklopedich-eskiy Slovar'" *apud.* Fridman, Kabernik, and Granelli, *op.cit*.), the *psycho-informational confrontation* represents an *informational and psychological system with an impact on the level of informational resources and on the level of consciousness and feelings of the military personnel and civilian population of the adversary, as well as a set of measures to protect one's own informational and psychological resources*.

At least during the Cold War, this Russian psycho-informational system exceeded the manipulation of the informational environment and included what the specialized literature defines as a "*program of active measures*" (Flavius, "Teză de doctorat. Relațiile serviciilor de securitate și informații românești cu structurile similare sovietice în perioada 1964-1989. Impactul programului de măsuri active desfășurat de KGB-GRU asupra securității naționale a României – Lecții învățate", 2018, 41), representing a *set of means, such as disinformation, subversion, intoxication, influence, propaganda, covert actions, deception, rumors, manipulation, forgeries and maskirovka, used to generate strategic events in order to create long-term advantages short, medium and long social, political, military, economic and informational by weakening an adversary informationally*.

In our understanding, *digital information influencing represents any activity or attempt by a state or non-state actor to influence the cyber information environment for its own benefit, at a regional or national level, at the level of the adversary or at the global*

level, both offensively and defensively, for changing the behavior of individuals, societies or their leaders.

With regard to the *bio-psycho-social component*, we note not only the fact that *technological evolution allows changes in the biological-genetic information*, but also the fact that *genetic experiments have begun to be carried out outside specialized laboratories, without complying with specific regulations*. Due to the fact that such biotechnologies are becoming accessible to the public at a relatively low cost, *unregulated biohacking becomes a public health risk* (Zettler, Guerrini and Sherkow, "Regulating genetic biohacking", 2019, 34-36).

At the same time, human activity in the digital space arouses an ever-increasing interest for the scientific community in the field of social sciences, which materializes in a new field, cyber-*psychology*. Current studies and debates on the human use of digital technologies, behavior in the digital space and how it affects the human psyche focus on *digital dementia*, *memory loss* and *cognitive impairment*.

Consequently, *the main source of digital insecurity at the bio-psycho-social level derives from the faulty handling of genetic information and the damage to the human psychic system as a result of uncontrolled activity in the digital space*.

Moreover, the sources of digital insecurity arise as effects of cyber-digital-physical inter-relationships, affect all security actors, and occur in all domains of security. Under these circumstances, the digital domain becomes itself a security domain, along with the military, political, economic, social and environmental.

Briefly (see Mândraș, "Security's Multidimensionality. Societal Security in the Age of Information Technology", 2020, 78-95), the *sources of digital insecurity*

affect all areas of security, and they consist at least of: *the automation of weapon systems* – affecting the military domain (see *Table no. 1 – Military power and autonomous systems in the Black Sea region*); *the paternalism, control, influence and manipulation of individual and societal behavior* – affecting the political and social domain; *the authoritarian behavior of states that use the collection of digital data of their own citizens for social and individual control* – affecting the political and social domain; *the digital addiction and digital dementia* – affecting the social field; *the unjust social justice* – affecting the political and social field; *the creation of a digital surveillance economy* (Clarke, " Risks inherent in the digital surveillance economy: A research agenda", 2019) – affecting the economic field; *the economic exploitation, discrimination and even social exclusion* – affecting the economic, political and social field; and, not least, *the security of digital devices and data* – affecting the military and economic domain.

Table no. 1 – Military power and autonomous systems in the Black Sea region[8]

Black Sea Region	Military Strength Power Index	Defense Budget (USD)	Military Personnel (Active, Reserve and Paramilitary)	Local companies that develop autonomous military systems
Bulgaria	1.1071	1,105,760,000	33,000	***No***
Georgia	2.0014	286,020,000	30,400	***No***
Moldova	2.2515	47,640,000	19,000	***No***
Romania	0.5938	5,148,090,000	132,000	***No***
Russia	0.0501	154,000,000,000	1,350,000	1. ***Almaz-Antey:***

[8] Source of data for *military strength power index* – lower index provides stronger power, *defense budget*, and *military personnel*: GlobalFirePower, „ 2022 Military Strength Ranking"; Source of data for *local companies that develop autonomous military systems*: Slijper, „Slippery Slope. The arms industry and increasingly autonomous weapons", 2019, pp. 6-8.

				a. ***Unmanned modular electric platform*** (BMPD, "Almaz-Antey presented an unmanned modular electric platform", 2021)**;** b. ***Sarma autonomous underwater drone*** (TASS, "Russian tech firm to feature versatile underwater drone at Urals industrial show", 2021) 2. ***Rostec*** (***Kalashnikov – ZALA Aero***; ***Ural vagonzavod):*** a. ***Lantset loitering munitions:*** Lantset (Lance) loitering munition comes in two configurations: the heavier Lantset-3 carries a 3-kilogram warhead and has a 40-minute mission endurance, while the lighter Lantset-1 has a 1-kilogram warhead and 30-minute mission endurance. 143 b. ***KYB drone:*** KYB was presented at the IDEX arms fair in Abu Dhabi in 2019. its producer also developed *artificial intelligence visual identification* (AIVI). c. ***Uran-9 UGV:*** The Uran UGVs includes the Uran-6 mine clearing vehicle and the Uran-9 combat tank, which was used by Russia in the war in Syria. d. ***Unmanned T-72 tank.*** 3. ***United Aircraft (Sukhoi):*** a. ***Sukhoi Okhotnik unmanned combat aerial vehicle (UCAV)*** (Vranic, "Russian Okhotnik UCAV conducts first PGM launches", 2022)

				4. ***National Center for the Development of Technology and Basic Elements of Robotics and the Android Technics company*** a. ***Marker UGV robot*** (TASS/Army Recognition Group, "Russian Marker UGV robot to operate in friend-or-foe identification mode", 2021)
Ukraine	0.3266	11,870,000,000	500,000	***No***
Turkiye	0.1961	9,690,000,000	775,000	1. ***Savunma Teknolojileri Mühendislik ve Ticaret (STM):*** ***a. KARGU (autonomous tactical multi-rotor attack)*** KARGU system was improved through the use of AI, including facial recognition, as well as increasing the diversity of the explosives the system can use, currently thought to include fragmentation and thermobaric options. Weighing less than 7 kilograms each, KARGU has a range of 15 kilometers and can stay in the air for 30 minutes. It is possible to operate up to 30 KARGUs together in a swarm that could destroy a military unit or warship. ***b. ALPAGU (fixed-wing autonomous tactical attack);*** ***c. TOGAN (autonomous multi-rotor reconnaissance) loitering systems.***

4. ***DIGITAL SECURITY. The need for a new theoretical approach. Expanding cybersecurity to bio-technological and cyber-psychological security threats***

Is it needed a new theoretical approach to digital security in cyberspace considering the actual "inflation" of cyber-security studies?

The specialized literature from various fields, such as international relations, security studies and military sciences, psychology or sociology, does not offer 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, "The Concept of Security: Should it be Redefined?", 2001, 13-42), and our argumentation rests on the fact that security has differentiated characteristics that cannot be treated comprehensively and unitarily for all possible situations in real life.

Therefore, when dealing with the issue of security, it is necessary to take into account at least 3 essential elements and provide an answer to the inherent questions.

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

What is the reference object of security? Respectively, what are the sources of insecurity and what are the actions that generate them?

What are the security actors? That is, who must ensure security by countering threats, removing vulnerabilities, and increasing resilience? Who are the insecure actors? Respectively, who or what generates the sources of insecurity that manifest in threats and dangers?

An answer to all of these questions that is valid in every human situation is challenging and has yet to be identified. However, in our attempt to conceptually clarify the term *security*, we found that the literature addresses at least 15 types of security.

For a better understanding of these types and their integration into a unitary concept, we consider that *security has 4 main dimensions* (see Mândraș, "Desecretizarea" conceptului de securitate. Noțiuni, componente, dimensiuni, domenii și tipuri de Securitate", 2021, 27-39), grouped by specific fields, as follows: (1) *the dimension of security subjects*, classified according to the main security actors – the state, society and the individual; (2) *the dimension of domains of insecurity*, classified according to the main sources of insecurity, which simultaneously represent security assurance areas – military, political, economy, societal, environment; (3) *the dimension of security sources*, which mainly refers to state security, classified according to the behavior of states in achieving their own security within international relations – joint, collective, cooperation; and (4) *the dimension of the security environment*, which mainly refers to state security, classified according to the geopolitical depth of the security environment – regional and international.

Given this wide variety of digital insecurity sources, as we have previously detailed, is the current theoretical framework inclusive enough?

Prior to providing an answer, we note that the specialized literature gives almost exclusive importance to cyber security which it treats from the perspective of state security. In this situation, the sources of digital insecurity derive from the need to protect the hardware and software components that contain digital information, the flows of this digital information, but also the digital informational environment that is of interest to state actors, the types of security studied being *cyber security* and *security of digital data flows*.

Regarding *cyber security*, we note that it does not have a universally accepted definition, similar to many other concepts in the field of security studies.

For NATO ("Cyberdefence", 2020), cyberspace has been recognized since July 2016 as a field of military operations, along with land, air, naval, and space, following the cyber-attacks on some public and private institutions in Estonia in 2007. Therefore, such a recognition implied that the alliance must entail measures for the defense of the member states in cyberspace, for which it also adopted a *Policy on cyber defense* on the occasion of the September 2014 Summit (See "NATO Cyber Defence", 2016).

Within this policy, *NATO considers cyber security to consist mainly of defending its own cyber networks, its missions and operations, as well as increasing the organization's resilience, including through the development of capabilities for cyber education – training and exercises*.

From the US perspective, *cyber security* represents 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*" (Cybersecurity and Infrastructure Security Agency, "Cybersecurity Glossary", 2021).

According to the US Cybersecurity and Infrastructure Security Agency, the defense of cyber security and activities includes a whole range of actions, strategies, policies and standards to reduce threats, vulnerabilities and destruction, through international engagement, incident response, resilience, ensuring information availability, law enforcement, diplomacy, development of military capabilities, or carrying out missions within the intelligence activity,

ensuring the security and stability of the global infrastructure of information and communication systems.

At first glance, the *security of digital data flows* can be easily confused with cyber security, but its distinctive character is given by the existence of digital information both from the perspective of its belonging to an IT system located in a certain geographical territory, and from the perspective of the flow that digital information travels within several digital systems, especially if they are located on the territory of several states and are subject to several jurisdictions and legal regulations.

Thus, *the security of digital data flows* does not only refer to ensuring the security of digital economic exchanges – energy, products and services, but also to ensuring the digital security of financial exchanges, data and ideas (Verhagen, Chavannes, and Bekkers, "Flow Security in the Information Age", 2020, 7).

As depicted above, we can only note that security studies treat cyber security almost exclusively from the perspective of ensuring the security of a single security actor – the states, almost ignoring the perspective of individual and societal security.

Given these circumstances, we agree with the need claimed by Robert Reardon and Nazli Choucri for giving greater importance to individual rights within the objectives of the cyber agenda and creating a stronger link between the rulers and the ruled (Reardon, and Choucri, "The role of Cyberspace in international relations: A view of the literature", 2012, 7), and we argue that cyberspace is an environment of insecurity both to states, but also to individuals and communities that are part of societies.

Consequently, we criticize the approach to cyber security only from the state perspective and consider that the approach must be extended to digital security in order to include the perspective of the other two security actors – individuals and societies, and all types of sources of digital insecurity.

Security is three-dimensional, as it is (1) *a reality formed by sources of insecurity*, (2) a *perception formed by the interpretation of the dangers generated by these sources of insecurity*, but also (3) an *action or non-action taken diminish and counter the sources of insecurity.*

Under these conditions, the reality of security is also formed through the cyber inter-relationships between different security actors, which have independent or congruent effects in the cyber and digital space, and generate digital insecurity sources.

Considering the above-mentioned arguments, we conclude that the *digitalization of societies generates a new type of security, which affects all security subjects* – individuals, societies, and states, and *we argue the need to* ***expand the concept of cyber security to the concept of digital security*** (see *Figure no. 7 – Dimensions of security*).

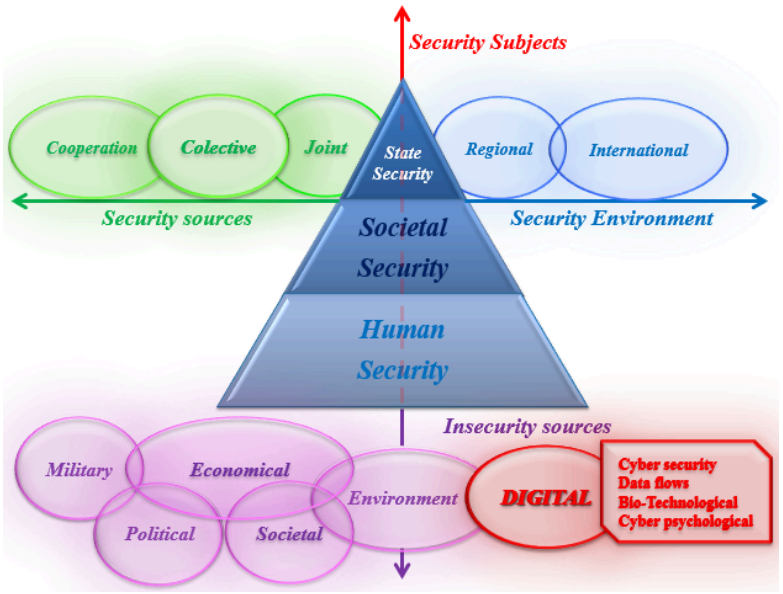


Figure no. 7 – Dimensions of security

Consequently, ***digital security consists of all the activities, processes, skills, or capabilities to identify and defend against the disruptive effects of cyberspace, and digital space in physical space, embodied in sources of digital insecurity, respectively physical effects – cyber protection and defense; informational effects - defense of the informational environment and protection against hostile digital influences and bio-psycho-social effects – protection against bio-technological and cyber-psychological dangers***

Within our interpretation of the security concept, digital security (see *Figure no. 8 – Digital security*) is part of the dimension of insecurity sources domain, it refers to all digital insecurity sources, it affects all security subjects, and includes four components:

- Cyber security;
- Security of data flows;
- Bio-technological security; and

- Cyber-psychological security.

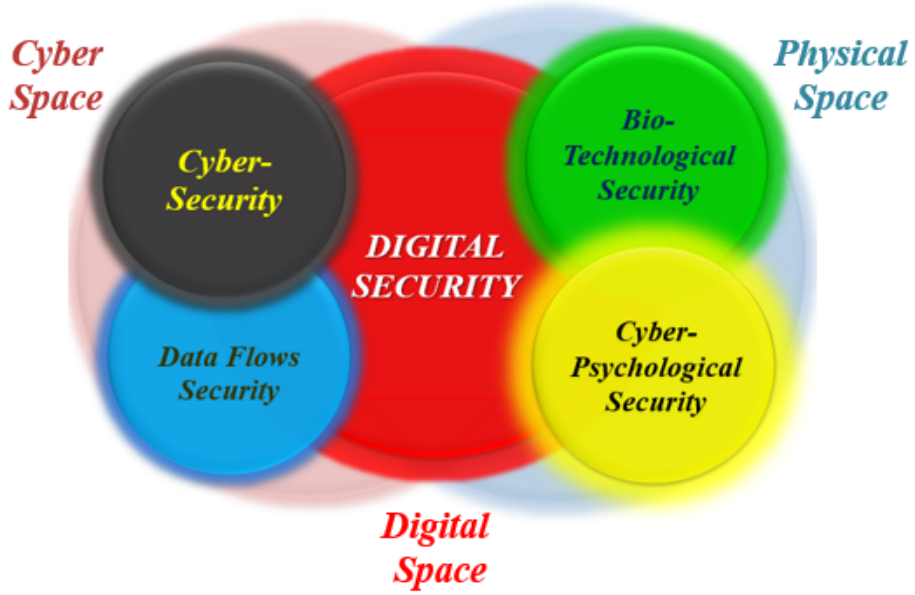


Figure no. 8 – Digital security

Instead of conclusions, we emphasize that a new theoretical approach to digital security in cyberspace is needed due to the wide variety of digital insecurity sources.

Given the facts and circumstances detailed above, we consider that cybersecurity does not provide a theoretical frame that fully encompasses the digital changes and disruption societies face due to the technological evolution and societal revolution of human activities conducted in digital space.

Therefore, we provide a new theoretical approach of digital security that encompasses 4 types of mainstream digital disruptions and stands out as a model for building more appropriate tailor-made public policies that should tackle all types of digital insecurity sources.

Nevertheless, we encourage the whole of society, but especially its key stakeholders – business specialists, non-governmental organizations, researchers, academics, and governmental policymakers to further assess the impact of digitalization, expand research on all types of digital disruptions and provide guidelines for further regulations.

5. ***Bibliography***

1. Army Recognition, "Russian Marker UGV robot to operate in friend-or-foe identification mode", October 27, 2021. https://www.armyrecognition.com/defense_news_october_2021_global_security_army_industry/russian_marker_ugv_robot_to_operate_in_friend-or-foe_identification_mode.html.

2. Azhar, Azeem. "EXPONENTIAL. How Accelerating Technology Is Leaving Us Behind and What to Do About It", UK: Pinguin Random House Business, 2021;

3. BK Tripathy, and J Anuradha, ed., *Internet of Things (IoT): Technologies, Applications, Challenges and Solutions*, Boca Raton: Taylor & Francis Group, LLC, 2018;

4. BMPD, " Almaz-Antey presented an unmanned modular electric platform", August 26, 2021. https://vpk.name/en/536042_almaz-antey-presented-an-unmanned-modular-electric-platform.html.

5. Brandmentions, "What Is a Digital Influencer". Accessed at 01.03.2022. https://brandmentions.com/wiki/What_Is_a_Digital_Influencer.

6. Brennen, Scott, and Kreiss, Daniel. "Digitalization and Digitization", September 8, 2014, https://culturedigitally.org/2014/09/digitalization-and-digitization/.

7. Carke, Roger, " Risks inherent in the digital surveillance economy: A research agenda" in *Journal of Information Technology* volume 34, issue 1, 2019. https://doi.org/10.1177/0268396218815559.

8. Castagna, Rich, and Bigelow, Stephen J. "Information Technology (IT)", August 2021. https://www.techtarget.com/searchdatacenter/definition/IT.

9. CBINSIGHTS. "The Complete List Of Unicorn Companies". Accesed at 15.04.2022. https://www.cbinsights.com/research-unicorn-companies.

10. Chifu, Iulian. "Aspecte privind războiul informaţional: alterarea realităţii", in *Infosfera* no. 4, 15-16, 2018;

11. Chifu, Iulian. "Character assassination" – armă ofensivă în războiul informational" in *Infosfera* no. 4, 11-17, 2017;

12. Cybersecurity and Infrastructure Security Agency. "Cybersecurity Glossary", March 4, 2021. https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#C.

13. "Digitization vs. digitalization: Differences, definitions and examples", Accessed at 20.01.2022. https://www.truqcapp.com/digitization-vs-digitalization-differences-definitions-and-examples/.

14. Dufva, Tomi, and Dufva, Mikko. "Grasping the future of the digital society" in *Futures* no 107, 17-28, 2019;

15. Eustáquio, Luís, and Carneiro de Sousa, Catarina. "Creative Collaborative Virtual Environments" in *Encyclopedia of Information Science and*

Technology, Fourth Edition, edited by Mehdi Khosrow-Pour, Hershey PA: IGI Global, 2018;

16. Forbes. "Top Creators 2022". Accessed at 15.09.2022. https://www.forbes.com/sites/alexandrasternlicht/2022/09/06/top-creators-2022/.

17. Fridman, Ofer, and Kabernik, Vitaly, and Granelli, Francesca, eds., "Info ops: from World War I to the Twitter era", Londra: Lynne Rienner Publishers, Inc., 2022;

18. Gartner Glossary. "Information Technology", accessed at 20.01.2022. https://www.gartner.com/en/information-technology/glossary/digitalization.

19. Gates, Bill. "Reasons for optimism after a difficult year", December 7, 2021. https://www.gatesnotes.com/About-Bill-Gates/Year-in-Review-2021.

20. GlobalFirePower, "2022 Military Strength Ranking". Accessed at 30.09.2022. https://www.globalfirepower.com/countries-listing.php.

21. Huawei Technologies. "2020 Global Connectivity Index". 2021. Accessed at 30.09.2022. https://www.huawei.com/minisite/gci/en/country-profile.html

22. Huddleston Jr., Tom. "This 29-year-old book predicted the 'metaverse' — and some of Facebook's plans are eerily similar", November 3, 2021. https://www.cnbc.com/2021/11/03/how-the-1992-sci-fi-novel-snow-crash-predicted-facebooks-metaverse.html.

23. Ichimescu, Cristian. "Operaţiile informaţionale şi mediul informaţional global" in *Buletinul Universităţii Naţionale de Apărare "Carol I"*, 2016;

24. Kabra, Archana. "Top 20 Biggest Tech Companies in The World in 2022", The Teal Mango, February 11th, 2022. https://www.thetealmango.com/featured/biggest-tech-companies-in-the-world/.

25. Kemp, Simon. "Digital 2022: Global Overview Report". January 26, 2022. https://datareportal.com/reports/digital-2022-global-overview-report

26. Kim, Sohee. "Metaverse Is a Multitrillion-Dollar Opportunity, Epic CEO Says", November 17, 2021. https://www.bloomberg.com/news/articles/2021-11-17/metaverse-is-a-multitrillion-dollar-opportunity-epic-ceo-says.

27. Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem" in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart Starr, and Larry K. Wentz Washington D.C.: National Defense University Press, Potomac Books, 2009;

28. Le Merle, Matthew C., and Davis, Alison. "Corporate Innovation in the fifth era. Lessons from Alphabet/Google, Amazon, Apple, Facebook and Microsoft", Corte Madera, CA: Cartwright Publishing, 2017.

29. Lee, So-Eun, and Choi, Mideum, and Kim, Seongcheol. "How and what to study about IoT: Research trends and future directions from the perspective of social science" in *Telecommunications Policy* no. 10, vol. 41, 1056-1067, 2017;

30. Lokhande, Nishant, "Sophia and Other 11 Best Humanoid Robots of 2022", August 1, 2022. https://techresearchonline.com/blog/sophia-and-11-humanoid-robots-2022/.

31. Marko, Kurt. " Robot rights - a legal necessity or ethical absurdity?", Diginomica, January 3, 2019. https://diginomica.com/robot-rights-a-legal-necessity-or-ethical-absurdity.

32. Mândraș, Laurențiu Paul. (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, 2020. https://www.ceeol.com/search/chapter-detail?id=919259.

33. Mândraș, Lauențiu Paul. "Desecretizarea" conceptului de securitate. Noțiuni, componente, dimensiuni, domenii și tipuri de Securitate" in *Infosfera* no. 4, 27-39, 2021. https://www.mapn.ro/publicatii_militare/arhiva_infosfera/documente/2021/4_2021.pdf#page=27.

34. McAfee, Andrew, and Brynjolfsson, Erik. "Machine, platform. Crowd: Harnessing our Digital Future", New York: WW Norton & Company, 2017;

35. McDonald, Jordan. "Roblox's metaverse is already here, and it's wildly popular", December 10, 2021. https://www.morningbrew.com/emerging-tech/stories/2021/12/10/roblox-s-metaverse-is-already-here-and-it-s-wildly-popular.

36. Merriam-Webster, "Definition of information technology". Accessed at 31.09.2022. https://www.merriam-webster.com/dictionary/information%20technology.

37. Meta, "Inside the Lab: Building for the Metaverse with AI", February 23 2022.

https://about.fb.com/news/2022/02/inside-the-lab-building-for-the-metaverse-with-ai/.

38. Miller, Benjamin. "The Concept of Security: Should it be Redefined?" in *Journal of Strategic Studies*, vol. 24, Issue 2: *Israel's National Security Towards the 21st Century*, 13-42, 2001;

39. Molenaar, Koba. "Discover The Top 15 Virtual Influencers for 2022", December 14, 2021. https://influencermarketinghub.com/virtual-influencers/.

40. NATO. "Allied Joint Publication-3.20 (AJP-3.20), Allied Joint Doctrine for Cyberspace Operations", Edition A, Version 1, January 2020, NATO Standardization Office. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

41. NATO. "Cyberdefence", September 25, 2020. https://www.nato.int/cps/en/natohq/topics_78170.htm.

42. NATO. "NATO Cyber Defence", July 2016. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-en.pdf.

43. Parsons, Jeff. "Mark Zuckerberg responds to everyone that mocked his metaverse selfie". Accessed at 16.09.2022. https://metro.co.uk/2022/08/22/mark-zuckerberg-responds-to-everyone-that-mocked-his-metaverse-selfie-17221119/.

44. Rad, Mozhgan Malekshahi, and Rahmani, Amir Masoud, and Sahafi, Amir, and Qader, Nooruldeen Nasih. "Social Internet of Things: vision,

challenges, and trends" in *Human-centric Computing and Information Sciences* no. 10, 2020. https://doi.org/10.1186/s13673-020-00254-6.

45. Reardon, Robet, and Choucri, Nazli. "The role of Cyberspace in international relations: A view of the literature", San Diego: Department of Political Science – MIT, 2012;

46. Reis, João, Amorim, Marlene, Melão, Nuno, Cohen, Yuval, and Rodrigues, Mário. "Digitalization: A Literature Review and Research Agenda" in *Proceedings on 25th International Joint Conference on Industrial Engineering and Operations Management – IJCIEOM. IJCIEOM 2019. Lecture Notes on Multidisciplinary Industrial Engineering*, edited by Zoran Anisic, Bojan Lalic, and Danijela Gracanin, 443-456, Cham: Springer, 2020;

47. Roach, John. "Mesh for Microsoft Teams aims to make collaboration in the 'metaverse' personal and fun", November 2, 2021, https://news.microsoft.com/innovation-stories/mesh-for-microsoft-teams/.

48. Russian News Agency, " Russian tech firm to feature versatile underwater drone at Urals industrial show", June 22, 2021. https://tass.com/defense/1305581.

49. Schwab, Klaus, and Davis, Nicholas. "Shaping the future of the fourth industrial revolution. A guide to building a better world", New York: Currency, Penguin Random House LLC, 2018;

50. Schreier, Fred. "On Cyberwarfare", DCAF HORIZON 2015 WORKING PAPER no. 7, The Geneva Centre for the Democratic Control of Armed Forces (DCAF), 2015. https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf.

51. Scîrlet, Petre, and Ichimescu, Cristian. "Conflictele/operațiile informaționale ale Federației Ruse în contextul SARS-CoV-2" in *Gândirea militară Românească* no. 3, 2020;

52. Siroya, Navani, and Mandot, Manju. "Role of AI in Cyber Security" in în (ed.), *Artificial Intelligence and Data Mining Approaches in Security Frameworks*, edited by Neeraj Bhargava, Ritu Bhargava, Pramod Singh Rathore, and Rashmi Agrawal, Hoboken, NJ: John Wiley & Sons, Inc., 2021;

53. Skilton, Mark, and Hovsepian, Felix. "The 4th Industrial Revolution. Responding to the Impact of Artificial Intelligence on Business", Cham: Palgrave Macmillan, 2018;

54. Slijper, Frank. "Slippery Slope. The arms industry and increasingly autonomous weapons", November 2019, PAX for Peace. https://paxforpeace.nl/media/download/pax-report-slippery-slope.pdf.

55. Song, Houbing, and Rawat, Danda B., and Jeschke, Sabina, and Brecher, Christian, ed *Cyber-Physical Systems: Foundations, Principles and Applications*, included in series *Intelligent Data-Centric Systems: Sensor-Collected Intelligence*, edited by Fatos Xhafa, Elsevier AP, 2017;

56. Soul Machines, "How we bring Digital People to life", Accessed at 01.03.2022. https://www.soulmachines.com/technology/.

57. Stan, Mircea Flavius. "Relațiile serviciilor de securitate și informații românești cu structurile similare sovietice în perioada 1964-1989. Impactul programului de măsuri active desfășurat de KGB-GRU asupra securității naționale a României – Lecții învățate". PhD diss., Academia Națională de Informații "Mihai Viteazul", 2018;

58. The World Bank Group. "GDP per capita, PPP (current international $)". Accessed at 30.09.2022. https://data.worldbank.org/indicator/NY.GDP.PCAP.PP.CD?name_desc=false&view=chart.

59. Vagadia, Bharat. "Digital Disruption. Implications and opportunities for Economies, Society, Policy Makers and Business Leaders", Cham: Springer Nature Switzerland AG., 2020

60. Verhagen, Paul, and Chavannes, Esther, and Bekkers, Frank. "Flow Security in the Information Age", Haga: The Hague Centre for Strategic Studies, 2020;

61. Vranic, Miko. "Russian Okhotnik UCAV conducts first PGM launches", Janes, May 31, 2022. https://www.janes.com/defence-news/news-detail/russian-okhotnik-ucav-conducts-first-pgm-launches.

62. Zettler, Patricia J., and Guerrini, Christi J., and Jacob S. Sherkow, "Regulating genetic biohacking" in *Science* no. 365 (6448), 34-36, DOI: 10.1126/science.aax3248.