THE DIGITAL CENTURY AND ITS IMPLICATIONS ON THE INTERNATIONAL SECURITY ENVIRONMENT. DIGITAL CONFRONTATIONS IN CYBER SPACE AND REAL SPACE

Paul MÂNDRAȘ
Expert, Ministry of National Defence
DOI: 10.55535/RMT.2022.4.03

Starting with the end of the 20th century and the beginning of the 21st century, humanity is experiencing a new societal type, the information society. The emergence of computers, the Internet, digital information, artificial intelligence and digital devices with the ability to automatically process information, work autonomously, or even form networks with other devices, cyber and virtual space and so on have led to a technological explosion and the digitalization of societies.

Under these circumstances, the digitalization and virtualization of many human activities and relationships in all societal domains constitutes a postmodern "game changer" of societies. Consequently, digitalization has major repercussions at the level of security and the international security environment. We are witnessing a transition from the nuclear century to the digital century, through the emergence of a new type of human confrontation, the digital confrontation. This new type of confrontation manifests itself both in virtual space, through what we so often hear as cyber war, and in real space, through digitalization of defence and the battlefield. Thus, if the security environment of the 20th century was characterized by globalization under the auspices of the nuclear threat, is it appropriate to consider that the 21st century will be characterized by de-globalization under the auspices of the digital threat?

Keywords: security; digitalization; digital society; cyber attacks; digital threats;

SOCIETAL EVOLUTION AT THE BEGINNING OF THE 21ST CENTURY. THE LEAP FROM THE INDUSTRIAL SOCIETY TO THE INFORMATION SOCIETY

Considering the development of information technology, humanity is at a crossroads of societal evolution, the type of human society being in a process of qualitative transformation, from the industrial society specific to the 18th - 20th centuries to the informational and digital society specific to this new beginning of century and millennium.

Specifically, the industrial economy, based on the production of goods by people, is losing capacity, being gradually replaced by a *knowledge-based economy, where the production of goods and services becomes primarily based on digital information and devices with capabilities to collect, process, storage, analysis and distribution of products to the consumer market*.

In a special and avant-garde vision of the information society, the Government of Japan launched in 2016 a new societal concept, *"Society 5.0"* (Deguchi, Hirai, Matsuoka, Nakano, Oshima, Tai and Tani, 2020, pp. 1-23) , defined as a *super intelligent society in which the technologies that can achieve physical-cybernetic fusion are developed at a scientific level for the benefit of humanity, especially from the perspective of developing the wealth of the population (figure no. 1)*.

Thus, with reference to the *information society*, we allow ourselves to define this latest form of societal evolution as *a social, physical, biological and digital process through which large volumes of data are collected, analysed and processed by means of digital technologies in information with applicability in the physical world, which acts simultaneously at all levels of societies, while modifying individual and collective actions and behaviours to identify the best solutions to increase efficiency and effectiveness in all societal fields – military, political, economic, social, environmental and digital*.

Given these conditions, are there repercussions of the evolution of informational society on security and, implicitly, on the international security environment? If so, which are they?

	Society 1.0	Society 2.0	Society 3.0	Society 4.0	Society 5.0
Society	Hunter-gatherer	Agrarian	Industrial	Information	Super smart
Productive approach	Capture/Gather	Manufacture	Mechanization	ICT	Merging of cyberspace and physical space
Material	Stone • Soil	Metal	Plastic	Semiconductor	Material 5.0*
Transport	Foot	Ox, horse	Motor car, boat, plane	Multimobility	Autonomous driving
Form of settlement	Nomadic, small settlement 	Fortified city 	Linear (industrial) city 	Network city 	Autonomous decentralized city 
City ideals	Viability	Defensiveness	Functionality	Profitability	Humanity

Figure no. 1: Conceptualization of Society 5.0 (Hitachi-UTokyo Laboratory, 2020, p. xii)

DIGITAL CONFRONTATION IN CYBERSPACE. CYBER ATTACKS AND DIGITAL DANGERS

Information societies entail inter-relationships in cyberspace and an ever-increasing interconnectivity of physical and cyber environments that produce physical, informational and bio-psycho-social effects. From a societal perspective, *digital relationships* between physical entities are identical with the relationships formed in the physical space and are of three major types, namely *cooperation*, *neutral* or *confrontational*.

In the case of the latter type, *digital confrontations*, the functioning of devices and digital networks or the flow of data between devices in the network or behavioural influencing thus becomes critical at the level of societies – regardless of whether we are referring to the individual, societal or state level.

Thus, *digital confrontations* take place in conditions where state and non-state actors intentionally or unintentionally exploit the vulnerabilities of military and/or non-military digital systems to extract, corrupt or destroy cyber and/or physical space or to obtain prestige, military or political advantages or profit (NATO Standardization Office, 2009, p. 1).

Correlated with *digital confrontations*, there arises the need to discuss the offensive and defensive power of security actors in cyberspace. From this point of view, the specialists are debating a new notion, namely the *digital* or *cyber power* of these security actors, regardless of their type.

Therefore, we agree to those specialists who refer to this new type of power in state terms, placing it alongside military, economic, diplomatic and informational power, considering that *digital power or cybernetic power represents the ability to use cyberspace to create advantages and influence events in other operational environments and at the level of other instruments of power* [Kuehl in Kramer, Starr & Wentz, (eds.), 2009 apud. Schreier, 2015, p. 11].

However, although we do not dispute such a definition, we believe that it is limiting, and from our perspective, *digital/cyber power must also be defined in societal terms, not only in state terms*, with reference to the ability and power of other non-state security actors to use cyberspace, arguing that informational digital influence is not carried out by states only and affects the whole of society – the individuals, societal and state levels *(figure no. 2)*.

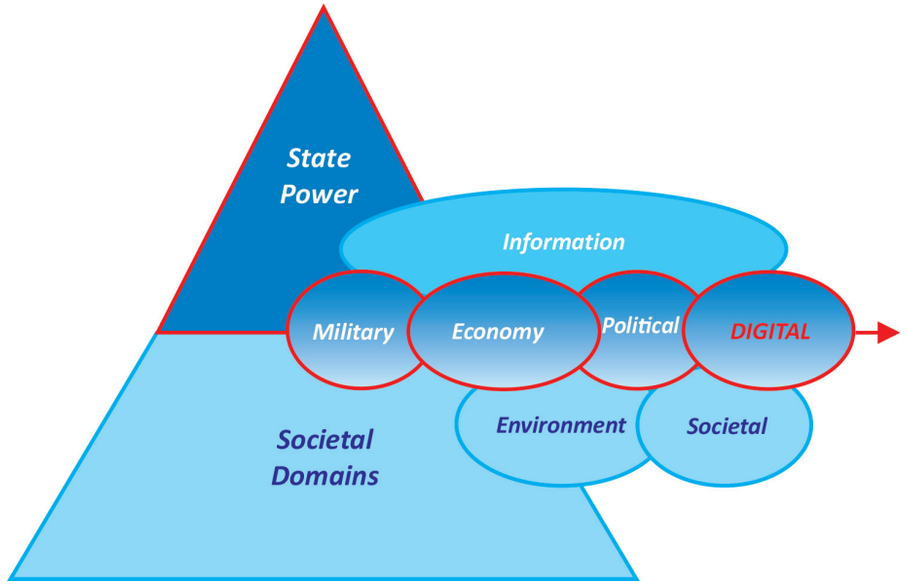


Figure no. 2: Digital power as state power and societal domain of threat

As a consequence, we argue that the *digital power* or *cyber power of informational societies represents both the ability to use cyberspace to create advantages and influence events in all societal fields – military, political, economic, social, digital and environmental as well as the ability to defend against hostile digital actions that produce negative effects at a physical, informational and bio-psycho-social level, regardless of their type*.

This new type of power is directly correlated with the *digital index* of societies *(figure no. 3)*.

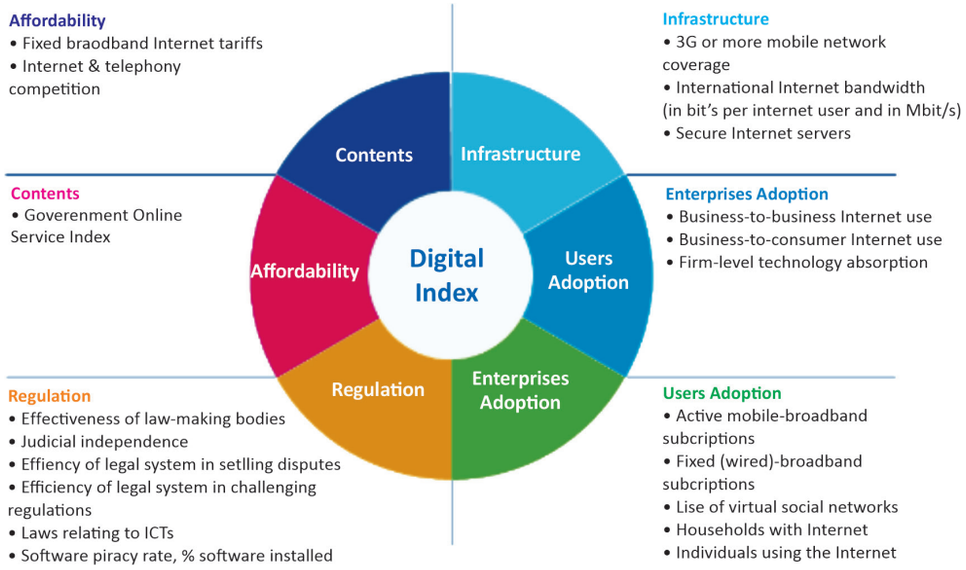


Figure no. 3: Digital Index (DiGiX: The Digitization Index)

Considering these aspects, from our point of view, the *confrontation in the digital space (figure no. 4)* acquires at least two dimensions, often synergistic and overlapping, namely:

❖ *At the state-societal level*: *cyber-attacks*, which take place in two forms:

- *cyber war*, and
- *digital information influence* or *digital influence*, respectively *war* or *cyber information operations*, *"information warfare"/"information operations"/ "influence operations"*;

❖ *At the societal-individual level*: *digital threats*, which occur in two other forms:

- *cybercrime* and
- *digital danger*.

Included by some authors in the category of *"non-classic"* (Hlihor, Băncilă, 2020, p. 229) or *"hybrid"* (Chifu, 2020, pp. 12-13) conflicts, the *cyber attack is carried out by a state actor directly or indirectly, through a non-state actor, singular or correlated with other means of power, mainly for the purpose of fulfilling some economic and financial, but also military and political interests*.

It takes place either by *attacking cyber devices and networks*, in the case of *cyber warfare*, or by *digitally influencing political-military decision-makers*

and the public opinion of the adversary, especially by changing political ideologies, in the case of *digital informational influencing*.

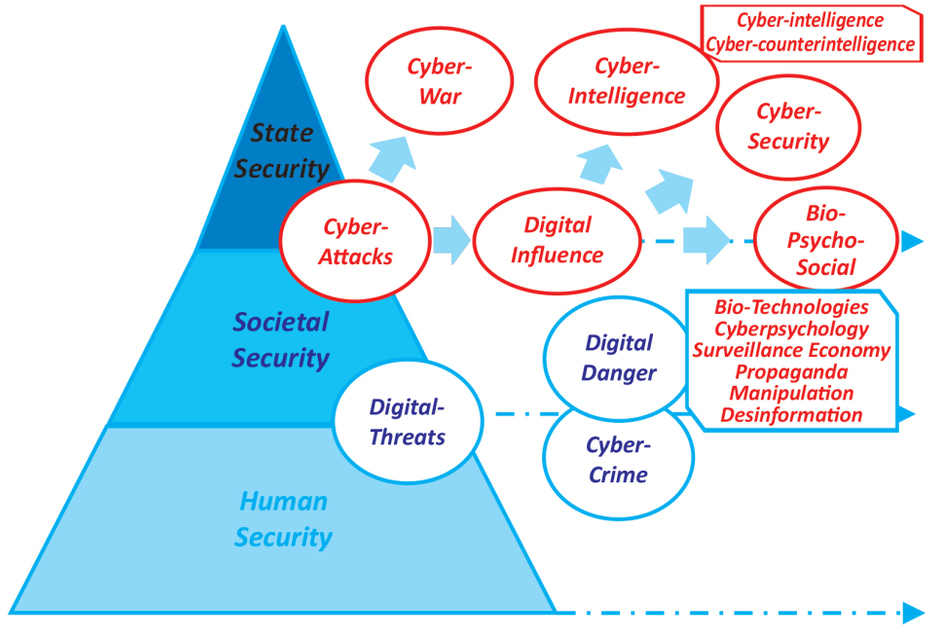


Figure no. 4: Types of digital conflicts

Regarding the notion of *cyber war*, we agree that it represents *any action of penetrating computers and digital networks carried out by a state actor against an adversary, with the aim of causing damage and destruction* (Clarke and Knake, 2010, p. 14).

In addition, we allow ourselves to supplement this definition with the fact that *the adversary can be another state actor or a non-state actor of strategic importance to the attacked state actor, and the damage and destruction can be of any kind, by affecting the physical or cyber integrity, both to IT&C and physical entities – citizens or institutions*.

Another component of the *digital conflict* is represented by *digital information influencing*, which in our understanding represents *any activity or attempt by a state or non-state actor to influence the cyber information environment for its own benefit, at the national level, at the level of the adversary or at the global level, both offensively and defensively*.

From the perspective of the goals pursued and the effects provoked by the digital information, we consider that there are *several types of digital informational*

influences, as follows: *digital bio-psycho-social influences* – that include the actions of propaganda, manipulation and disinformation, individualized or mass spread, which seek to change behaviours at the level of the opponent; *cyber-intelligence* – that include actions specific to the information activity carried out in the digital environment (Intelligence and National Security Alliance, 2015), of an offensive type – *cyber-espionage*; and defensive type – *cyber-counterintelligence* – include the activities of penetrating cyber systems and networks to identify and assess the capabilities, intentions and digital activities carried out by the adversary; and *cyber-security* defensive activities – that include the activities of securing systems and networks and digital information.

The second category of *digital conflicts* is represented by those who mainly affect society and its individual members and which we name as *digital threats*, which take place in two other forms: *cybercrime* and *digital danger*. Regarding *cyber crime* [Klimburg (ed.), 2012, pp. 13-15], we refer to *those types of legal or illegal activities carried out by non-state actors that constitute social dangers, have mainly an economic purpose and are penalized by states and/or at the level of regional and international organizations*.

Regarding the *digital danger*, we consider that it consists of the *activities carried out through digitalization in the political* (Farrow, 2022), *economic, social* (Milanovic, Schmitt, 2020, pp. 261-269) *and environmental domains by state or non-state actors*. *Such dangers can be carried out by states against their own citizens or by non-state actors against the societies where they operate and they affect societal identity and human rights.*

DIGITAL CONFRONTATION IN REAL SPACE. DEFENCE DIGITALIZATION AND BATTLEFIELD AUTOMATION

Considered to be part of the third wave of military technology development, following the invention of firearms and nuclear weapons, *autonomous lethal weapons with artificial intelligence* are already a reality of humanity (Lee, Qiufan, 2021, pp. 337 et seq.). Furthermore, they were already used on the battlefield. Essentially, such autonomous weapons have the ability to search for a target, make the decision to fire on the target, and ultimately kill the target, *all without human involvement in the process*.

Also called *"slaughterbots"* or *"killer robots"*, autonomous lethal weapons with artificial intelligence are pre-programmed to kill a certain profile of a human target, and in the process use a wide range of digital data collected from different sensors and have facial recognition capabilities.

Already in the possession of the Turkish Armed Forces, which used them in Syria in 2021 (United Nations, 2021, p. 148), or the Israeli Armed Forces, which used them in the separatist regions of Gaza (Gross, 2021), *lethal autonomous weapons exist, have been used and are currently allowed at the international level*, even if the UN had initiated expert-level discussions for their international regulation starting 2013 (United Nations, 2022).

The only notable success of the international community took place in 2019, when the signatory countries of the *Convention on the prohibition or limitation of the use of certain categories of classic weapons that could be considered as producing excessive traumatic effects or that would strike indiscriminately* (The Convention on Certain Conventional Weapons – CCW A.N.) have adopted a number of *11 guiding principles regarding the use of lethal autonomous weapons* (CCW, 2019, p. 10), which, however, are not binding for the CCW signatory states, but only have the status of *recommendations*.

Unfortunately, despite calls for a total ban on *slaughterbots* mot only from several CCW member states, such as Austria or New Zealand, but also from several non-governmental organizations, such as the International Committee of the Red Cross (ICRC), the regulation of lethal autonomous weapons failed at the Sixth CCW Review Conference held on 17 December 2021 in Geneva (Klare, 2022), following the blocking of consensus by the USA and the Russian Federation, both states having ambitions to integrate *slaughterbots* into their own military arsenals.

In this context, we consider it important to mention that the *International Committee of the Red Cross has issued recommendations* (ICRC, 2021) *for the regulation of lethal autonomous weapons*, through the adoption by states of some legally binding rules, which ensure the fulfilment of the following three primary requirements:

a. *Unpredictable autonomous weapon systems should be expressly excluded, particularly because of their indiscriminate effects*. This would be best achieved by banning autonomous weapons systems that are designed or used in such a way that their effects cannot be sufficiently understood, predicted and explained;
b. *The use of autonomous weapons systems to target human beings should be precluded,* in light of ethical considerations to protect humanity and uphold the norms of international humanitarian law for the protection of civilians and non-combatants. This would be best achieved through a ban

on autonomous weapon systems that are designed or used to apply force against individuals;

c. *The design and use of autonomous weapons systems that would not be prohibited should be regulated* in order to protect civilians and civilian property, to comply with the rules of international humanitarian law and to protect humanity; through a combination of:
   - a) Limits on the types of targets, such as restricting them to objects that are military objectives by nature;
   - b) Limits on the duration, geographic scope and scale of use, including to allow for human judgment and control in relation to a particular attack;
   - c) Limits of the situations of use, such as their constraint to situations where civilians or civilian goods are not present;
   - d) Requirements for human-machine interaction, in particular to ensure effective human supervision and timely intervention and deactivation.

Precisely in order to further highlight the need for the international adoption of the above-mentioned recommendations, we also propose a brief analysis of the *risks generated by autonomous lethal weapons*, before and during a military conflict.

In this regard, we agree with certain non-governmental specialists who have identified a number of seven (LethalAWS) as follows:

- *Actionable unpredictability* – such weapons are unpredictable by the very way they were built, with behaviour to annihilate the adversary while being difficult to detect and destroy. Such unpredictability is all the easier to achieve not only in a real complex operational environment, but also in the operational conditions of human-machine interactions; as well as car – car (Ekelhof, Paoli, 2020, p. 1);
- *Non-state proliferation* – slaughterbots are cheap and easy to mass-produce weapons, quick to transport and difficult to detect and destroy, which makes them accessible to non-conventional groups;
- *Degeneration of interstate disputes into military conflicts* – the low cost of construction and operation, both in financial and human terms, intensifies the risks of escalation of interstate conflicts into military conflicts, to the detriment of diplomatic, economic or informational de-escalation measures;
- *Escalation of military conflicts* – under the conditions of an increased speed and area of operation, autonomous systems induce risks of accidental and rapid escalation of conflicts, perpetuation of instability and military crisis,

simultaneously reducing the period of time and space necessary for taking measures to de-escalation by belligerents;

- *Ease of transformation into weapons of mass destruction* – in general, software is characterized by *"scalability"*, i.e. the ability to be modified, both quantitatively and qualitatively, and digital devices inherently include this capacity, including in terms of networks of devices they form swarms to which they attach. Slaughterbots, in their *"quality"* as digital devices, are no exception to this *"scalability"* capability and, although they act autonomously, they can also act in a network, thus forming groups of autonomous lethal weapons that act in unison and coordinated to fulfil the assigned mission. Such groups of slaughterbots, also called swarms of robotic systems (Ib.), or armed fully autonomous drone swarm – AFADS (Kallenborn, 2020), can generate victims in large numbers and we agree that they must be included in the category of weapons of mass destruction;
- *Selectivity in choosing targets* – with the ability to select targets based on biometric data and facial recognition software, slaughterbots can be used to commit crimes against groups of people based on age, gender, race, ethnicity, or religious dress;
- *Promoting the arms race* – in the absence of regulation or a total international ban on slaughterbots, states are practically encouraged to invest in the research and development of these types of weapons, thus generating a new arms race, this time with autonomous weapons.

However, we consider that the risks presented above represent *military risks to state-societal security generated by lethal autonomous weapons* and we allow ourselves to complete this list with two more risks *(figure no. 5)*, namely:

- *Crime escalation* – at an estimated unit cost of less than $1000 (Lee, Qiufan, 2021, pp. 337 and f.), all component parts can be purchased online, and operationalization can be achieved through downloadable open-source technologies from the Internet for free, thus being easy to procure, assemble and use, both by individuals acting independently and by organized crime groups;
- *Traceability difficulties* – given the ease of procurement and assembly, traceability (United Nations) is almost impossible, especially in conditions of illicit use, but also in conditions of use by state actors who do not want to take responsibility in production or application in different situations of disputes or military conflicts.

In this context, we also draw attention to the fact that the use of artificial intelligence in the field of weapons and military technologies is not limited only to slaughterbots. The applicability of AI is currently being studied at the level of other types of classic weapons, in order to assign them the ability to act autonomously without the presence of a human operator, individually or in a network. Such weapons being developed include firearms, missiles, military ships, military vehicles, fighter planes, or drone ships, as well as military robots to replace human soldiers (Özdemir, 2019, pp. 16-22).

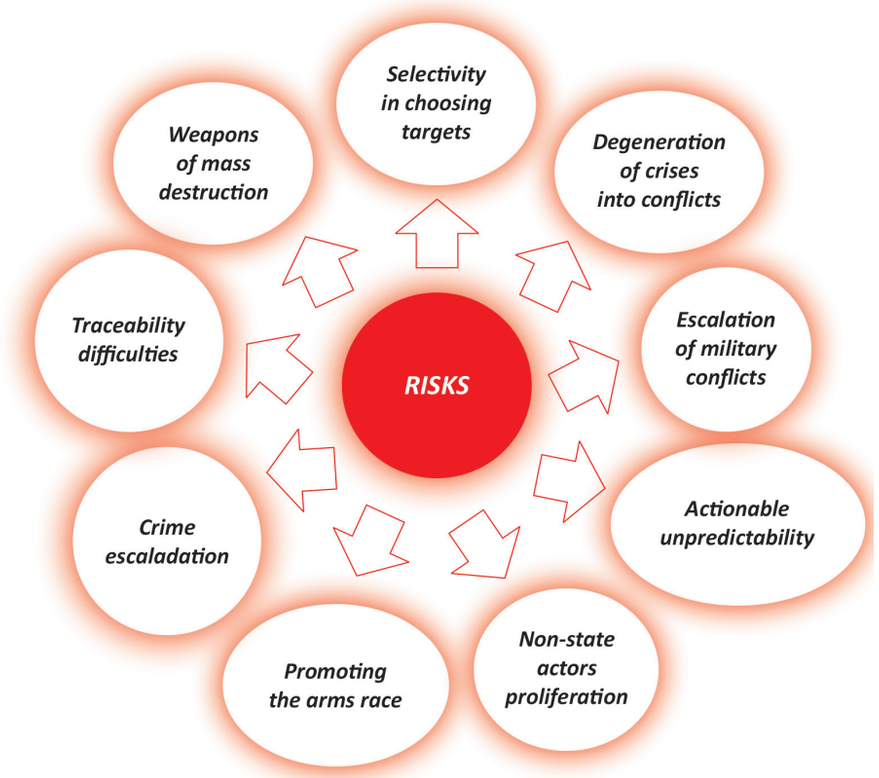


Figure no. 5: Security risks generated by lethal autonomous weapons

Considering the new informational-digital military technologies, the popular television series Star Trek has a good chance of becoming a reality. Though, the specificity of these new technologies is that they are neutral by themselves, and their effect, positive or negative, depends to the greatest extent on people, the societies and states that build and use them.

SECURITY AND SECURITY ENVIRONMENT AT THE BEGINNING OF THE DIGITAL AGE. DIGITALIZATION, GLOBALIZATION, DE-GLOBALIZATION AND THE MULTIPLICATION OF SECURITY CRISES

Security is a complex psycho-social phenomenon, almost impossible to define in a unitary and universally accepted way, precisely because of its multidimensionality (Mândraș, 2020, pp. 78-95).

However, before highlighting the main aspects of security and the current security environment, we consider it useful to further clarify the theoretical notions.

Therefore, we reiterate the fact that security includes at least 4 main dimensions (Mândraș, 2021, pp. 27-39), grouped by types of security and specific domains *(figure no. 6)*, as follows:

❖ The dimension of *security subjects*, classified according to the historical evolution of the concept of security and the main security subjects: the state, society and the individual;

❖ The dimension of the *domains/sources of insecurity*, classified according to the main sources, risks, threats and dangers of insecurity, grouped by the main societal domains;

❖ The dimension of the *sources of security*, classified according to the state's behaviour and degree of introversion or extroversion in achieving its own security within international relations;

❖ The dimension of the *security environment*, classified according to the geopolitical depth of the security environment and the relationships established by the security actors and their involvement in combating the sources of insecurity, at national, regional or international level.

❖ Thus, with regard to the *security environment*, we can consider that it has a multivalent character, in the sense that it represents an essential dimension of state security, which manifests itself at the national, regional or international level, but is also correlated with the other subjects of security – individuals and the societies they form.

Composing the *three essential components of the security concept*, alongside the *reality constructed through discourse* and *security policies and strategies* (Hlihor, 2008, p. 13. *apud* Mândraș, 2021, pp. 28-29), the security environment is represented by the objective reality in which security relations take place, at the societal or state level.

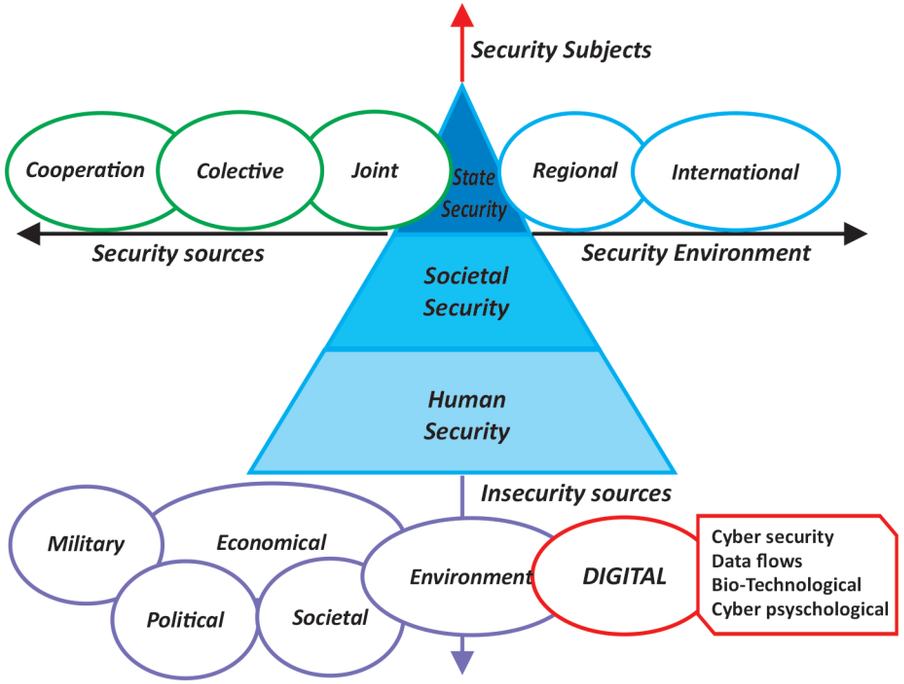


Figure no. 6: Dimensions of security

At the same time, the *security environment* is defined both by the specific threats and dangers that exist in the national, regional or international social reality, and by the preventive or defensive behaviours adopted by security actors to counter these threats and dangers, whether they are state or non-state actors.

Under these conditions, which are the main general characteristics of the current security environment and what is the impact of the digitalization of societies on the social reality?

First of all, starting with the period of the 90s, characterized by the end of the Cold War, it was manifested an *"openness"* to studying other types of security rather than the national-state one, as well as to other types of sources of insecurity and non-state security actors. Therefore, it was agreed that there exists a new reality of international relations resulting from the dissolution of the Soviet Union and the promotion of human freedom and the free market.

Obviously, we are referring to this new reality as *globalization*, which along with the *"dynamism, flexibility (...) the emergence, complexity, radicalism and perpetual crisis that take place in the international security environment and that influence all areas of social life"* (Mocanu, 2013, p. 11) leads us to anticipate and conclude

that *change is the constant nature of postmodernism – the current stage of development of international society in the 21st century*.

In a holistic perspective, *globalization resides in the generalized global interconnectedness that exists within and between individuals, social groups, societies, nation-states, organizations, and regions, achieved through the international expansion of trade and access to markets for the production and distribution of goods and economic-financial services, but also the transport and freedom of movement of people, goods and financial or non-financial capital, on the background of the development of digitalization, which has amplified global interconnectivity (figure no. 4)*.

In practical terms, this expansion has eliminated or diminished geographic and geopolitical barriers and profoundly transformed global politics and its study [Little, Smith (ed.), 2005, p. 135], a field that is increasingly concerned with the negative impact of these transnational and international transformational processes on individuals, societies, nation states, or even the Earth.

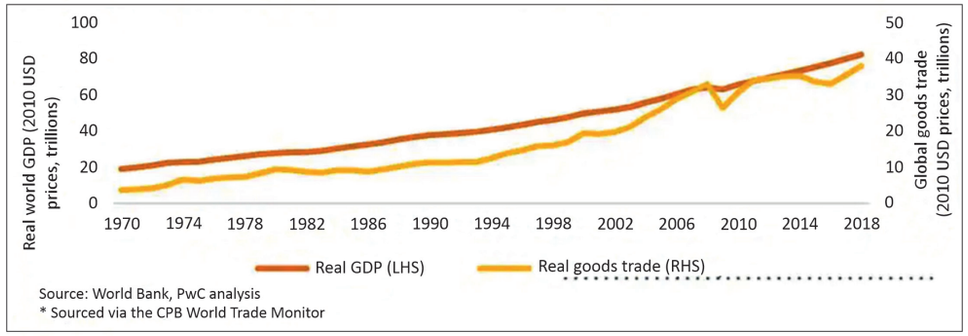


Figure no. 7: The tandem between the growth of world Gross Domestic Product (GDP) and the growth of trade in goods (RHS) (Kupelian, 2020)

Regarding the impact of globalization on the current political system still dominated by nation states, some authors (Drezner, 2008; Dreher, Gaston, Martens, 2008) debate the *risk of dissolution*, especially of small states. Arguments include the burden of social and economic transformations, cultural and political aspects of the global system. The issues regarding the autonomy and sovereignty of these nation states are being debated within the contemporary international system (Najam, Runnalls, Halle, 2007), under the effect of the interdependencies generated by the global economy and financial system, technological and communications developments, consumerism, the permeability of national borders and cross-border threats, such as international terrorism, illegal migration or ecological disasters.

As for the concept of the sovereignty of the states, traditionally, it was defined by the absolute political authority of the states exercised within the framework of international relations (Hinsley, 1986, pp. 1-27). However, considering the modern evolutions, the concept of sovereignty has suffered modifications, which resides in its expression as an absolute authority of states to exercise their exclusive right to apply special measures to protect the rights of their own citizens, as well as their own security (Edkins, Shapiro, Pin-Fat, 2004, p. 79).

Moreover, given the dynamics of the international environment in the context of cross-border risks that threaten the states themselves and, implicitly, their sovereignty, security specialists have focused on this issue, trying to identify whether the risk of dissolution mentioned above is real or not and whether the states are willing to give up their own sovereignty in favour of a supranational, even global body [Waltz, 1979; Hobbes, Shapiro (ed.), 2009].

This risk almost certainly exists, but our response to these dilemmas must be differentiated, depending on the types of power that the states in question have at their disposal to counter the threats and dangers to which they are subject, including the new type of digital power to which we have previously referred.

At least in terms of relinquishing one's own sovereignty and the risk of dissolution, an eloquent example is Great Britain itself, faced in the last decade with two referendums – one regarding the acquisition of independence by Scotland, and the other regarding separation from the EU, which is a reality of the present.

Theoretically, we agree that the dissolution of states into a supra-state organization with collective sovereignty and capitulation of national sovereignty would fail. At least at the present time, such a supra-state organization would not be able to offer viable security solutions in the face of global threats to human security, justice, or environmental changes (Tännsjö, 2008, pp. 122-125), especially in the absence of a monopoly on decision-making authority, the imposition of law and the use of force to ensure the security of societies, recognized, accepted and implemented at the regional or global level, with the support of the population.

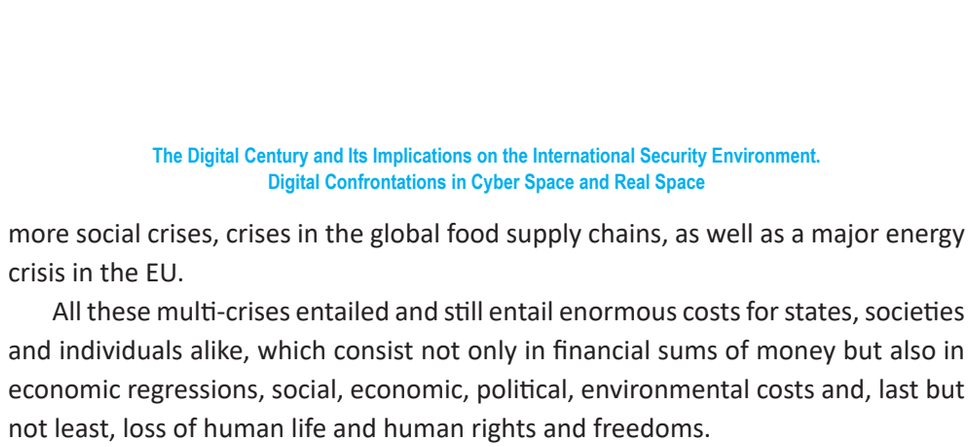
At the same time, in the last two decades, the global system has been subjected almost simultaneously to several serious crises, such as: the financial crisis of 2008; the migration crisis that marked Europe and the USA in 2016; BREXIT; the public health crisis generated by the SARS COV virus 2 initiated in China at the end of 2019 and spread across the globe in 2020; the crisis of the political rise of extremist and populist parties; and, last but not least, the current crisis generated by the illegal military invasion of Ukraine by the Russian Federation, which in turn generates

more social crises, crises in the global food supply chains, as well as a major energy crisis in the EU.

All these multi-crises entailed and still entail enormous costs for states, societies and individuals alike, which consist not only in financial sums of money but also in economic regressions, social, economic, political, environmental costs and, last but not least, loss of human life and human rights and freedoms.

In addition, these multi-crises also accentuate the change in the global order specific to the end of the 20th century, and American unipolarism is already a matter of the past, being gradually replaced by a USA-China bipolar global competition that captures more and more states.

Additionally, we believe that the basis of these multiple crises is not only the competition between state actors, larger or smaller, but also another characteristic of the current security environment manifested at the individual and societal level, namely the global economic inequalities *(figure no. 8)*, which manifest at the level of states, regions, but also of individuals, who are increasingly influenced by digitalization.



Interpretation: In Latin America, the top 10% captures 55% of national income, compared with 36% in Europe. Income is measured after pension and unemployment benefits are received by individuals, but before income taxes and other transfers.
Sources and series: wir2022.wid.world/methodology

Figure no. 8: Income inequality differentiated by region (WIR, 2022)

These inequalities not only affect the security of states, but also erode the global social foundation, being assumed that these differences in economic well-being have amplified the increasingly violent and daily social movements in Western states and beyond. We briefly recall the movements of the *"yellow wests"* in France, the anti-immigration protests in Germany, the *"Black Lives Matter"* protests

in the USA and the invasion of the Capitol by American Protestants in January 2021, or even the current protests in the Russian Federation against the background of the illegal invasion of Ukraine. They all affect all areas of security.

Under these conditions, what stands at the basis of these movements and social crises? The economic poverty and the supposed crisis of societal identity generated by the cultural interference of immigrants in the American and European majority culture (Xinchun, 2020, p. 39)?

We believe that an affirmative answer to such a question would be too simplistic, as it is quite far removed from reality, and would obviously be almost exclusively in accord with the Chinese Communist Party's foreign policy doctrine.

However, this does not mean that identifying the genesis factors of the current global crises should be ignored, especially by the states that define themselves as democratic-liberal. Moreover, at least in the case of crises in the Euro-Atlantic space there are accusations and evidence regarding the involvement of the Russian Federation (Cunningham, 2020) and the People's Republic of China (Solon, Dilanian, 2020) in informational manipulation and fake news campaigns through social networks. Consequently, we can investigate the premise of digital social media platforms being employed as new means of digital power utilized by some states against others as part of a more comprehensive information operations campaigns.

However, we agree that currently the world scene is being affected by *uncertainty due to globalization and digitalization* and we are witnessing a process of de-globalization in the sense of slowing down and reconfiguring global economic exchanges and resizing regional and global security, generated especially by initiating a new global strategic confrontation.

However, if the global competition specific to the second half of the 20th century was based predominantly on the confrontation of two economic models – capitalism versus communism, the current global competition has a higher level of importance, being based on the confrontation between two diametrically opposed ideological systems, democratic-liberal and authoritarian-illiberal, obviously represented by the two big current global state actors, the USA and China.

Like a centrifugal effect, this new geopolitical confrontation and mutation of the international security environment has already contaminated and will inevitably keep on globally contaminating more and more state and non-state actors of varying sizes and importance.

Even though some Asian authors are already preaching the globally decline and failure of Western politics and are clamouring for China's centralized leadership

and its policy of *"putting the people first"* (Peng, 2020, p. 11), we believe it is far too early to reach such conclusions. At least for citizens of the former communist states of Eastern Europe who were born after 1991, such a claim could be viewed with great scepticism.

For how can you put people first and what kind of global leader can you be considering the accusations of using digitalization to increase authoritarian social control over your own population through a social credit system (Canales, 2021), or affecting the human rights of a *"vociferous"* minority, such as the one of the Muslim Uyghur minority in China's Xinjiang region (Minority Rights Group International, 2007)?

QUO VADIS?

At the beginning of the digital century, humanity is witnessing a confrontational diversification with repercussions at both state and non-state levels, manifested both in the physical-real space and in the digital/cybernetic-virtual space.

The current background consists of the worldwide amplification of digitalization and the development of multiple security crises manifested almost simultaneously at the regional or global level. De-globalization through the slowdown of international trade; SARSCOV-2 medical crisis; the financial and economic crisis; the food and energy crisis; social protests generated by financial inequality; the political rise of the populist and extremist movement; increasing global economic inequality; and, last but not least, the illegal military invasion of Ukraine by the Russian Federation are just some examples.

Therefore, *the international security environment at the beginning of the 21st century is in the process of rearranging the world order, which promises to be unpredictable and fluctuating, full of dangers and threats to the security of all security subjects – individuals, communities, states*.

Among these dangers and threats, the competition between the US and China for world supremacy, especially in the field of digitalization and control of the cyber and digital space, particularly draws our attention.

Thus, *digital confrontations take on new historical dimensions and show a global increase in scale*, especially through new *types of digital conflicts – cyber attacks and threats*; and, last but not least, *the global risks posed by the digitalization of the field of defence and automation of combat weapons*.

We agree that the security environment of the present century will be characterized by at least three essential features, such as *opacity in government*

transparency, confused and competitive global interventionism, and inadequate responses to security crises (Gowan, 2018). However, we believe that these features must be supplemented by the fourth, namely the *digital bipolarism and competition*, manifested by the *exponential development of digitalization and its expected disruptive impact on all types of security subjects – state, societal and individual*.

Despite the complexity and diversification of regional and international security structures that have developed since 1950 to the present days, it is becoming increasingly clear that they have not been prepared to diminish and neutralize current dangers.

Therefore, humanity and international security is currently evolving from a global *"cold war"* specific to the 20th century, which consolidated peace in Europe, to a *"hot peace"* that includes a war at the eastern end of Europe and reshapes the world order.

In conclusion, given the experience of the 20th century, we are confident that a major nuclear conflict will be avoided in the 21st century, but the nuclear threat is joined by a new type of *digital threat* that must be diminished.

Are societies and the current national, regional and international security structures capable of countering this new type of threat, or is it time to reconfigure the security systems?

We take this opportunity to invite specialists and the general public to answer such a question, and within this context, we note the establishment in Bucharest of the Euro-Atlantic Centre for Resilience, which aims to promote and pursue resilience objectives within seven communities of interests, including societal resilience, emerging and disruptive technologies, or the resilience of communication systems and new technological ecosystems (Euro-Atlantic Resilience Centre, 2022).

BIBLIOGRAPHY:

1. Cámara, C., Tuesta, D. (2017). *DiGiX: The Digitalization Index*. BBVA Research, https://www.bbvaresearch.com/en/publicaciones/digix-the-digitalization-index/, retrieved on 15 September 2022.
2. Canales, K. (2021). *China's 'social credit' system ranks citizens and punishes them with throttled internet speeds and flight bans if the Communist Party deems them untrustworthy*. Insider Inc, https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4, retrieved on 15 September 2022.
3. Chifu, I. (2020). *Ameninţări neconvenţionale* şi *noile tipuri de conflicte de natură hibridă* în *secolul 21.* In *Gândirea militară românească*, no. 1/2020.
4. Clarke, R.A., Knake, R.K. (2010). *Cyber War. The Next Threat to National Security and What to Do About It*. HarperCollins e-books.

5. Cunningham, C. (2020). *A Russian Federation Information Warfare Primer*. The Henry M. Jackson School of International Studies. University of Washington, https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/, retrieved on 15 September 2020.
6. Deguchi, A., Hirai, C., Matsuoka, H., Nakano, T., Oshima, K., Tai, M.&Tani, S. (2020). What is Society 5.0? In Hitachi-UTokyo Laboratory (H-UTokyo Lab.). *Society 5.0. A People-centric Super-smart Society* (pp. 1-23). Singapore: Springer.
7. Dreher, A., Gaston, N., Martens, P. (2008). *Measuring Globalisation: Gauging Its Consequences*. New York: Springer.
8. Drezner, D.W. (2008). *All Politics Is Global: Explaining International Regulatory Regimes*. Princeton: Princeton University Press.
9. Edkins, J., Shapiro, M.J., Pin-Fat, V. (2004). *Sovereign Lives: Power in Global Politics*. New York: Routledge.
10. Ekelhof, M., Paoli, G.P. (2020). *Swarm robotics. Technical and operational overview of the next generation of autonomous systems*. UNIDIR.
11. Farrow, R. (2022). *How Democracies Spy on Their Citizens*. The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens?utm_campaign=likeshopme&client_service_id=31202&utm_social_type=owned&utm_brand=tny&service_user_id=1.78e+16&utm_content=instagram-bio-link&utm_source=instagram&utm_medium=social&client_service_name=the%20new%20yorker&supported_service_name=instagram_publishing#main-content, retrieved on 20 April 2022.
12. Gross, J.A. (2021). *In apparent world first, IDF deployed drone swarms in Gaza fighting*. The Times of Israel, https://www.timesofisrael.com/in-apparent-world-first-idf-deployed-drone-swarms-in-gaza-fighting/, retrieved on 15 March 2022.
13. Gowan, R. (2018). *Muddling Through to 2030: The Long Decline of International Security Cooperation.* New York: United Nations University, https://cpr.unu.edu/publications/articles/muddling-through-to-2030-the-long-decline-of-international-security-cooperation.html#info, retrieved on 20 March 2021.
14. Hinsley, F.H. (1986). *Sovereignty,* 2nd Edition. Cambridge: Cambridge University Press.
15. Hlihor, C. (2008). *Politica de securitate* în *mediul internațional contemporan. Domeniul energetic*. Iași: Editura Institutului European.
16. Hlihor, C., Băncilă, A. (2020). *„Vechiul" sau un nou tip de război* în *confruntările viitoare din politica internaţională? O perspectivă istorică* şi *geopolitică*. In *Gândirea militară românească*, no. 2/2020.
17. Hobbes, T., Shapiro, I. (ed.) (2009). *Leviathan: Or the Matter, Form & Power of a Common-Wealth Ecclesiastical and Civil (Rethinking the Western Tradition)*. Auckland: The Floating Press.
18. Lee, K.F., Qiufan, C. (2021). *AI 2041. Ten visions for our future*. New York: Penguin Random House LLC.
19. Little, R., Smith, M. (ed.). (2005). *Perspectives on World Politics*, 3rd Edition, London: Routledge.
20. Kallenborn, Z. (2020). *Swarms of mass destruction: the case for declaring armed and fully autonomous drone swarms as WMD*. Modern War Institute at West Point, https://mwi.usma.edu/swarms-mass-destruction-case-declaring-armed-fully-autonomous-drone-swarms-wmd/, retrieved on 1 April 2022.

21. Klare, M.T. (2022). *Conference Makes No Progress on Robotic Weapons*. Arms Control Association, https://www.armscontrol.org/act/2022-01/news/conference-makes-progress-robotic-weapons, retrieved on 15 March 2022.
22. Klimburg, A. (ed.). (2012). *National Cyber Security Framework Manual*. NATO Tallinn: CCD COE Publication.
23. Kuehl, D.T. (2009). *From Cyberspace to Cyberpower: Defining the Problem*. In Kramer, F.D., Starr, S., Wentz, L.K. (eds.). *Cyberpower and National Security.* Washington D.C.: National Defense University Press, Potomac Books.
24. Kupelian, B. (2020). *Predictions for 2020: "Slowbalisation" is the new globalisation.* Pricewaterhouse Coopers LLP, https://www.pwc.com/gx/en/issues/economy/global-economy-watch/assets/pdfs/predictions-2020.pdf, retrieved on 20 March 2021.
25. Mândraș, L.P. (2020). *Security's Multidimensionality. Societal Security in the Age of Information Technology*. In *Romanian Military Conference Proceedings* (pp. 78-95), https://www.ceeol.com/search/chapter-detail?id=919259, retrieved on 21 April 2022.
26. Mândraș, L.P. (2021). *„Desecretizarea" conceptului de securitate. Noțiuni, componente, dimensiuni, domenii și tipuri de securitate.* In *Infosfera*, year XIII, no. 4 (pp. 27-39), https://www.mapn.ro/publicatii_militare/arhiva_infosfera/documente/2021/4_2021.pdf#page=27, retrieved on 21 April 2022.
27. Milanovic, M., Schmitt, M.N. (2020). *Cyber Attacks and Cyber (Mis)information Operations During a Pandemic.* In *Journal of National Security Law and Policy*, no. 11 (1), GT-JSLP200044 247.284 (reading.ac.uk), retrieved on 1 April 2022.
28. Mocanu, M. (2013). *Intelligence* în *operațiile militare ale secolului XXI*. București: Editura Universității Naționale de Apărare *"Carol I".*
29. Najam, A., Runnalls, D., Halle, M. (2007). *Environment and Globalization: Five Propositions*. Winnipeg: International Institute for Sustainable Development.
30. Özdemir, G.S. (2019). *Artificial Intelligence application in the military: the case of United States and China*. In *SETA*, nr. 51 (pp. 16-22). Istanbul.
31. Peng, Y. (2020). *The COVID-19 Pandemic and Changes Unseen in a Century*. In *China Institutes of Contemporary International Relations*, vol. 30, no. 4, http://www.cicir.ac.cn/UpFiles/file/20200813/637329122703768052108857 2.pdf, retrieved on 15 March 2021.
32. Schreier, F. (2015). *On Cyberwarfare.* In DCAF HORIZON 2015 WORKING PAPER, nr. 7. The Geneva Centre for the Democratic Control of Armed Forces (DCAF). OnCyberwarfare-Schreier.pdf (dcaf.ch), retrieved on 1 April 2022.
33. Solon, O., Dilanian, K. (2020). *China's influence operations offer a glimpse into the future of information warfare*. NBC UNIVERSAL, https://www.nbcnews.com/business/business-news/china-s-influence-operations-offer-glimpse-future-information-warfare-n1244065, retrieved on 15 September 2022.
34. Tännsjö, T. (2008). *Global Democracy: The Case for a World Government*. Edinburgh: Edinburgh University Press.
35. Xinchun, N. (2020). *International Politics in Transition: The Pandemic and Beyond*. In *China Institutes of Contemporary International Relations*, vol. 30, nr. 4, http://www.cicir.ac.cn/UpFiles/file/20200813/637329122979120085481 2324.pdf, retrieved on 15 March 2021.
36. Waltz, K.N. (1979). *Theory of international politics*. Reading: Addison-Wesley Publishing Company.

37. CCW (2019). *Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be Deemed to be Excessively Injurious or to Have Indiscriminate Effects*. Geneva, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/343/64/PDF/G1934364.pdf?OpenElement, retrieved on 15 March 2022.
38. DiGiX: The Digitization Index, https://www.bbvaresearch.com/en/publicaciones/digix-the-digitization-index/, retrieved on 12 April 2022.
39. Euro-Atlantic Resilience Center (2022). *Mission Statement*, https://e-arc.ro/en/about-e-arc/mission-statement/, retrieved on 15 September 2022.
40. Hitachi-UTokyo Laboratory (2020). *Society 5.0. A People-centric Super-smart Society*. Singapore: Springer, p. xii.
41. Human Rights in China (2007). *China: Minority Exclusion, Marginalization and Rising Tensions*. Minority Rights Group International, https://minorityrights.org/wp-content/uploads/old-site-downloads/download-165-China-Minority-Exclusion-Marginalization-and-Rising-Tensions.pdf, retrieved on 15 September 2022.
42. Intelligence and National Security Alliance (2015). *CYBER INTELLIGENCE: Preparing Today's Talent for Tomorrow's Threats*, INSA_Cyber_Intel_PrepTalent.pdf (insaonline.org), retrieved on 1 April 2022.
43. International Committee of The Red Cross (2021). *ICRC position on autonomous weapon systems*. ICRC, https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems, retrieved on 15 March 2022.
44. LethalAWS (2022). *The risks of Lethal Autonomous Weapons*. LethalAWS, https://autonomousweapons.org/the-risks/, retrieved on 1 April 2022.
45. NATO (2009). *Allied Joint Publication-3.10 (AJP-3.10). Allied Joint Doctrine for Information Operations*. NATO Standardization Office.
46. NATO (2020). *Allied Joint Publication-3.20 (AJP-3.20). Allied Joint Doctrine for Cyberspace Operations*, ed. A, version 1. 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, retrieved on 1 April 2022.
47. United Nations. *Background on LAWS in the CCW***,** https://www.un.org/disarmament/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/, retrieved on 15 March 2022.
48. United Nations. *Small arms: Tracing***.** https://www.un.org/disarmament/convarms/small-arms-tracing/#:~:text=Tracing%20is%20the%20systematic%20tracking,at%20which%20they%20became%20illicit., retrieved on 1 April 2022.
49. United Nations (2021). *Letter dated 8 March 2021 from the Panel of Experts on Libya established pursuant to resolution 1973 (2011) addressed to the President of the Security Council*. Security Council, Annex 30, p. 148, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/037/72/PDF/N2103772.pdf?OpenElement, retrieved on 15 March 2022.
50. WIR/World Inequality Report (2022), https://wir2022.wid.world/insights/, retrieved on 23 April 2022.