NBP JOURNAL OF CRIMINALISTICS AND LAW ŽURNAL ZA KRIMINALISTIKU I PRAVO
NBP 2020, 25(1): 81–97

Original scientific paper
Submitted: 2020-04-27
Published: 2020-07-17

doi:10.5937/nabepo25-26316

CHALLENGES, RISKS AND THREATS TO HUMAN SECURITY IN THE 4TH INDUSTRIAL REVOLUTION

Ljubomir M. Mitrović[1]
University of Belgrade, Faculty of Security Studies, Belgrade, Serbia

Abstract: The world has been gradually entering the fourth industrial revolution, where a new wave of technological advancement will bring humanity into a new era of globalization. Global supply chains will become more efficient while reducing transport costs, which will contribute to opening new markets and drive economic growth. According to an analysis by the World Economic Forum, the fourth industrial revolution will increase the level of global income and quality of life for people around the world. However, increasing intersectionality and emerging technological trends will expose humanity to new forms of security challenges, risks and threats such as Internet fraud and data theft, cyberattacks, large-scale spontaneous migration, climate change, etc., as stated in the 2020 Global Economic Forum's Global Risk Report.

Keywords: human security, fourth industrial revolution, globalization, challenges, risks and threats.

INTRODUCTION

"What are the challenges, risks and threats to human security brought by the fourth industrial revolution?" represents the key research question of this paper. In addition to trying to discover the link between the fourth industrial revolution and the new era of globalization, the paper focuses on analysing the possible negative implications that a new era of interconnectedness and technological advancement for the security of the individual and society. The example of the position of the Republic of Serbia within the Belt and Road Initiative will be used to present possible security challenges, risks and threats to which a society and individuals may be exposed in the new era of the industrial revolution.

1 Corresponding author: ljubomir.mitrovic@hotmail.com

THE 4th INDUSTRIAL REVOLUTION AND GLOBALIZATION

The fourth industrial revolution (Industry 4.0 or 4IR) is characterized by a fusion of technology that is blurring the lines between the physical, biological, and digital worlds. In fact, it is the development and combination of new and emerging technologies in the field of nanotechnology, biotechnology, information and communication technologies, cognitive sciences, and their convergence in the form of artificial intelligence that will facilitate the building of wholly automated "factories of the future" (Gillieron, 2019). In this way, technological development shifts the world of labour in the fourth industrial revolution that will radically change the way we live, work and communicate (WEF, 2016; Davis & O'Halloran, 2018). In terms of scale and complexity, the 4IR will be completely different from anything that the humanity has experienced before. A new wave of technological advancement encouraged by Industry 4.0 will bring humankind to a new era of globalization, the so-called "Globalization 4.0" (Gillieron, 2019).

In the process of globalization, technology plays a key role in shaping opportunities and risks, so it can be concluded that globalization and technology are closely linked. Namely, one of the key scientific and technological breakthroughs that are important prerequisites for globalization are the global availability and exchange of information through new information and communication technologies that allow jobs the relocation of job opportunities across globe to the countries where workers have necessary qualifications, because we live in a time when it becomes clear that the business needs not be tied to a fixed location (Ljajić et al., 2016). However, unlike the previous eras of globalization that were driven by economic-political liberalization and information and communication technology, the only driving force behind the new era of globalization will be technology (Williamson, 1998; Fukuda-Parr, 2003). Today, it can truly be confirmed that Globalization 4.0 is shaped solely by the development of new technologies brought to us by Industry 4.0 (WEF, 2019).

Globalization is a phenomenon driven by technology and the movement of ideas, people, and goods. Essentially, with the emergence of new technologies, the flow of people, goods, capital, and ideas has been accelerated, enabling each of us, no matter where we live, to reach around the world further, faster, deeper, and cheaper than ever before, and enabling the world to reach into each of us further, faster, deeper, and cheaper than ever before (Friedman, 1999). On the other hand, each new era of globalization has a different and stronger impact on employment, income and human health, creating new security risks and threats primarily in the economic and social spheres (Robertson & Khondker, 1998; Fukuda-Parr, 2003; Kamei, 2012). Given the assumption that a new era of globalization will have the strongest impact on society so far, it can be concluded that Globalization 4.0 will produce the most serious challenges, risks and threats to the security of people and communities by reaching further, faster, deeper, and cheaper.

IMPACT OF GLOBALIZATION 4.0 AND INDUSTRY 4.0 ON THE SECURITY OF THE INDIVIDUALS AND SOCIETY

Globalisation is a wild process involving interconnectedness and exclusion, integration and fragmentation, homogenisation and diversity (Kaldor, 2000: 4). Nevertheless, unlike the previous stages of globalization, Globalization 4.0 is the latest stage of globalization which involves cutting-edge new technologies like artificial intelligence that powers forward with the explosion of information technology. These technologies shrink distances, open up borders and minds, and bring people all across the globe closer together. However, introducing the world into the global age, disruptive technologies foster more intense interconnectedness, creating the so-called "network society" (Castlls, 1996). Considering that, the most basic human needs, such as water and energy supply, or service sectors such as health, economy and education, are becoming more and more digitized and dependent on 4.0 technologies. Due to a high degree of technological interconnectedness in the era of Globalization 4.0, network society is multiplying increasing the vulnerability of every human being, as well as the importance of human security. In fact, Globalization 4.0 encouraged by Industry 4.0 has an impact on transforming the systems of communications, transportation, production, energy and distribution, health, producing new threats to human security or enhancing the intensity of traditional threats to human security.

Human security and Globalization 4.0

The concept of human security was first defined in the UNDP Human Development Report (1994) as "freedom from fear" and "freedom from want". In the light of such comprehension, human security concept envisions protecting human beings from various threats through an independent and subjective lens. The basic human needs of food security, healthcare, education and a safe habitat, are enshrined in the notion of human security along with socio-economic notions such as providing for one's family, the stability of livelihood, trust in surrounding community and associated social relationships (Chugh, 2018). Essentially, the concept of human security involves protection against chronic threats such as hunger, disease and repression, i.e. protection against sudden and harmful disorders in patterns of daily life (UNDP, 1994). These threats to the security of an individual come from seven different dimensions of human security, i.e. economic security (e.g. unemployment, inflation, homelessness), food security (e.g. problems related to the physical and economic access to healthy food), health security (e.g. infectious and parasitic diseases, HIV and other viruses), environmental security (e.g. degradation of ecosystems, natural disasters), personal security (e.g. physical, domestic and workplace violence), community security (e.g. ethnic tensions and violent conflicts) and political security (e.g. state repression and human rights violations). Since there are four basic dimensions of the globalization process (economic, political, socio-cultural, and environmental) and given that the security of human collectivises, according to

Buzan (2007), is influenced by factors from five sectors (economic, political, social, military, and environment), we can conclude that globalization affects all of these dimensions of human security. In summary, the threats to human security caused by globalization in the economic sphere are: social inequality, the dominance of economically powerful states, the generation of a global economic crisis, etc.; in the socio-political: illegal migration to developed countries, domination of certain languages and cultural patterns, interventionism on behalf of certain ideas or ideals, etc.; in the environmental sphere: global warming, the spread of viruses and diseases, the depletion of non-renewable natural resources, etc.; in the military sphere: the spread of knowledge and technology for the production of weapons of mass destruction, more intensive proliferation of weapons, new forms and greater destructiveness of wars, terrorism, etc. (WEF, 2017; WEF, 2018; WEF, 2019).

Therefore, globalization is a complex multidimensional phenomenon that connects all aspects of society, and as such is a total threat to security of the individual and society. However, to what extent it will be > total < for a society directly depends on the degree of globalization, but also on other factors such as the degree of economic and technological development, openness of society, etc.

Economic dimension of human security in Globalization 4.0

Consideration of the impact of globalization on society and individuals is most commonly approached from an economic point of view, since other dimensions of globalization are a side effect of economic globalization, or in its service (Ljajić et al, 2016).

If we observe economic security in the narrowest sense, according to Bjelajac (2016), we can differentiate five distinct meanings of economic security: the first meaning refers to production and trade, which directly affect a country's defence capability (e.g. production and trade in military technology, weapons, and key supplies important for the defence system); the second meaning refers to economic policy instruments used as an offensive or defensive tool of security policy, such as boycotts, restrictions on energy supplies, sanctions and various forms of economic assistance; the third meaning refers to the ability to achieve and/or maintain a certain level of economic development in order to ensure internal security stability, that is, to improve a country's international military political position; the fourth meaning refers to the economic security of the individual, which in the narrow sense means access to food, drinking water and other foodstuffs, or conditions necessary for his physical survival, and more broadly includes issues of employment, poverty, education, etc.; the fifth meaning refers to global economic, social and environmental stability (e.g. stability of the global financial and economic system, depletion of non-renewable resources, environmental pollution, and climate change).

Considering that, since economic globalization directly affects economic security, in case it is at risk, all other aspects of human security are at risk.

The impact of globalization on the economy is closely linked to advances in information technology that facilitate the operations of multinational corporation (Mehdi, 2013). In that way, globalization is connecting and transforming world into a single market, while national industries lose the race with multinationals, leading to fall in employment and rising in inequality. The combination of globalisation and privatisation of economy can give rise to a process, which is almost the reverse of the process through which modern states were constructed resulting in the loss of authority and legitimacy of the state (Kaldor, 2000).

In the era of Globalization 4.0, humanity will face the most serious challenge so far due to the tendency to replace humans with (semi-)automated systems. In these circumstances, low-skilled jobs are exposed to the greatest danger since the percentage of their automation will be significantly higher than high-skilled jobs of automated high-skilled jobs (Bonekamp & Sure, 2015; Heinrich, 2018). As automation replaces low-skilled workforce, society faces new challenges in the form of job losses, higher unemployment rates, and a greater gap between rich and poor, resulting in social change often accompanied by social tensions (Kamei, 2013; Wolf, 2015). A growing economy associated with increased inequalities, unemployment, and rural-urban migration in search of better employment opportunities, combined with the loss of state authority and legitimacy, weakens the rule of law and may lead to the re-emergence of privatised forms of violence such as organised crime and the substitution of "protection" for taxation, vigilantes, private security guards protecting economic facilities, especially international companies, para-military groups associated with particular political factions, etc. (Kaldor, 2000). As unemployment has the negative impact on the fundamental psychic functioning of people, and above all the transformation of identity (Arnett, 2002; Ljajić et al, 2016), under the influence of globalization, a global culture emerges cancelling the boundaries between national and international, and identifies itself as a threat to national identity and values. This creates "cultural nationalism", that is, a relationship in which national culture struggles to preserve its cultural authenticity, protecting itself from foreign influences (Mehdi, 2013). Considering that, the economic deprivation and frustration of domicile population, while creating a sense of victimization in certain groups due to foreign influences, can become the basis for the emergence of organised violence and terrorism. Essentially, globalization is a conductive environment for extremists to promote their ideas, win new sympathizers and expand the space of conflict (Nacionalna strategija za sprečavanje i borbu protiv terorizma, 2017). Because of the lack of authority of the state, the loss of confidence of the society that the state is able/willing to respond to public concerns, or the inability and/or unwillingness to regulates the privatisation and informalisation of violence, may result in violent conflicts. Conflicts raised in circumstances like this are called "new wars" by Mary Kaldor (2000).

However, the consequences of 4IR in the form of job losses, migration, or terrorism, do not pose the only threats to society. According to Kamei (2013), much more serious security threats for most people come from disease, hunger, environmental pollution, street crime, or domestic violence whose intensity will also be multiplied in the era of Globalization 4.0.

Traditional threats to individual security in Globalization 4.0

The range of traditional human security threats that accompany every era of globalization is rather wide. Namely, globalization, *per se*, increases the level of prosperity and poverty, while the gap between rich and poor grows and, as such, is one of the main catalysts for criminal behaviour (Morgan, 2002; Nye, 2003). In fact, economic depression and rising unemployment constitute an important factor conducive to the development of organized crime in sense of a conducive ground to destructive and illegal activities, and in particular to the creation of criminal organizations. Specifically, criminological research has found a causal link between economic crises and organized crime, proving that in times of economic crises the number of certain forms of organized crime can almost double (Veljović & Rakočević, 2018).

Therefore, the globalization of the world economy opens the possibility for an increase in the number of crimes committed in the global economy directly threatening human security, such as frauds in the world market, export of unsafe products, offering prohibited products and Internet services, money laundering, trafficking in human beings and white slaves, prostitution, industrial espionage, arms trafficking, weapons proliferation, environmental pollution and degradation, disease spreading, etc. (Williamson, 1998; Fukuda-Parr, 2003; Mehdi, 2013; Eldridge, Koser, Levin, & Rai, 2017; Ignjatović, 2018; Elamiryan, 2019). In this way, the increase in the scope and diversity of organized crime threatens national, but above all, human security.

However, besides the increase in the scope and diversity of crime, the control and oversight of committed crimes such as trafficking in human beings and white slaves, drugs and/or weapons, smuggling, white collar crime, etc., are much more difficult in Globalization 4.0 because of the new methods and techniques for committing these offences that are made possible by 4IR. In fact, there has been a change in the nature of crime, which has become digital, organized and globally connected thanks to the influence of 4.0 technologies (Tomašević et al., 2020). For example, information technologies have strengthened the black economy and eased the flow of a huge amount of money encouraging transnational organized crime and the relocation of one part of controls over security from state to non-state actors, such as drug cartels, terrorist groups, private security services, paramilitary units, military companies, etc. (Defort, 2015). Moreover, high-tech crime is on the highest increase and millions of people, including children, become victims of attacks every day (Cybersecurity Strategy of the European Union, 2013). Like criminality, disease has become global, since the cancelation of borders (e.g. within the EU) makes it difficult to monitor and control infectious diseases (e.g. COVID-19 pandemic). The intensity of all these threats is compounded by uncontrolled migration flows triggered by Industry 4.0 which directly affect the increase in crime rates and other crime offences related to migration, such as forgery of documents, illegal crossing and mediation in illegal crossing of the state border, prostitution, kidnapping, coercion, terrorism, etc., while increasing the risk of internal and interstate conflicts (Vulević, 2018). With the increased intensity of traditional threats

and the fact that globalization as a process, in a certain sense, internationalises criminal offences, the fear of traditional threats to human security in Globalization 4.0 is more than justified.

New threats to individual security in Globalization 4.0

The security implications of 4IR are too complex to fully grasp. However, it should be noted that the most dangerous threats to security of the individuals and society come from the fields of "4.0 technology" or in other words: nanotechnology, biotechnology, information and communication technologies (ICT), cognitive sciences, and their convergence in the form of artificial intelligence (Vu, 2018).

The development of nanotechnology has created the potential for the production of "nano-weapons", whose proliferation has been significantly facilitated compared to conventional and nuclear weapons (Kaspersen, 2015). Besides nanotechnology, 3D printing technologies also contribute to the production of a wide range of weapons, allowing avoiding the control of sales, imports, and/or exports. Developments in the fields of cognitive sciences, neurobiology, synthetic biology and pharmaceuticals, have contributed to the creation of (synthetic) drugs that can influence a person's behaviour, in terms of its change and/or control (e.g. the so-called "Jihadist drug", amphetamine and phenethylamine, are known to be used by terrorists in suicide missions to overcome fear of (fatal) outcome), while technological advances in the field of biotechnology and DNA profiling have opened the possibility of creating new, deadly viruses that can be used to harm the target group or population (Kaspersen, 2015; Vu, 2018).

The Internet of Things (IoT) is a new ICT technology that enables unlimited networking of devices to improve the way we live, work and communicate, but makes us unsafe. Namely, IoT allows collecting information about a person's movements and life habits, which increases the vulnerability of a person because the attackers can use the information collected to steal personal information (e.g. identity). Since digital addiction makes us more vulnerable, the misuse of ICT in the form of cyberattacks or information warfare has enormous consequences in the network society and can cause great material and human losses (WEF, 2019). Namely, the vulnerability of modern societies has been increased by the realization that the targets of cyberattacks can be the structures and systems of particular, vital importance to the functioning of the community, causing devastating consequences for life and health of people, for the economy and the environment (e.g. cyberattacks on Estonia in 2007). However, the ICT sector can generate other, already wide-spread dangers, such as the "social engineering" technique or new forms of environmental threats, like the popular cryptocurrency Bitcoin (WEF, 2019). In a nutshell, all aspects of the state and society are exposed to attacks from the ICT sector.

Nevertheless, the greatest threat posed by Industry 4.0 to human security is the convergence of the mentioned 4.0 technologies embodied in artificial in-

telligence (AI), that is, an "intelligent machine" that could replace humans in production (Schwab, 2016). The analysis of the impact of artificial intelligence at the societal level shows the possibility of increased marginalization of poor, indigenous and vulnerable groups, as well as the level of inequality in society (Obar & McPhail, 2018; WEF, 2019). In addition to endangering the economic security of the individual, the security implications of AI technology could be significantly more dangerous. Namely, the combination of all these technologies, e.g. broad-ranging networks and artificial intelligence tools, has the potential to transform future conflicts at both conventional and strategic levels (Kaspersen, 2015; Schwab, 2016; Hersman & Stadler, 2019; WEF, 2019). In fact, current conflicts already got hybrid in nature with a combination of conventional battlefield methods accompanied by the elements of informational and cyber warfare, while the globe represents the battlefield. The turning point in the changing nature of the conflict was the Gulf War, which indicated the introduction of new technologies (artificial intelligence and (semi-)autonomous weapons systems) into the battlefield.

Lastly, we should bear in mind that the set of mentioned Industry 4.0 threats and challenges is not final, and that as such it is a unique feature of the fourth industrial revolution.

Summary of the main risks to individual security in Industry 4.0

In order to gain a final observation of primary and unavoidable security challenges, risk and threats to security of the individuals and society that can be brought to us by 4IR, see Figure 1. As it can be seen, these are economic risks, that are associated, e.g. with high or false investments, or social risks such as the job losses. Investing in 4.0 technologies brings a high financial risk of incorrect investment in poor or often immature technologies, or economically unprofitable processes. Also, economic opportunities will be uncertain because many people may not have the skills needed for the jobs of the future. If states and communities are not fully prepared for the new wave of globalization, Globalization 4.0 may increase income inequality even if it can create more wealth. Besides the economics and social spheres, risks can be associated with technical risks, e.g. technical integration, information and communication technology related risks such as data security, and legal and political risks, such as for instance unsolved legal clarity in terms of data possession. From a legal point of view, open questions need to be clarified with regard to e.g. data protection, handling and protection; jurisdiction; labour law; intellectual property; etc. Certain risks can be seen in the ecological sphere in sense of environmental degradation and pollution caused by increased waste generation and emissions due to the need for larger amounts of energy and raw materials in 4.0 technological processes. In a nutshell, Globalization 4.0 in conjunction with Industry 4.0 will produce many consequences which may not be foreseeable for now and for which the world is vastly unprepared.

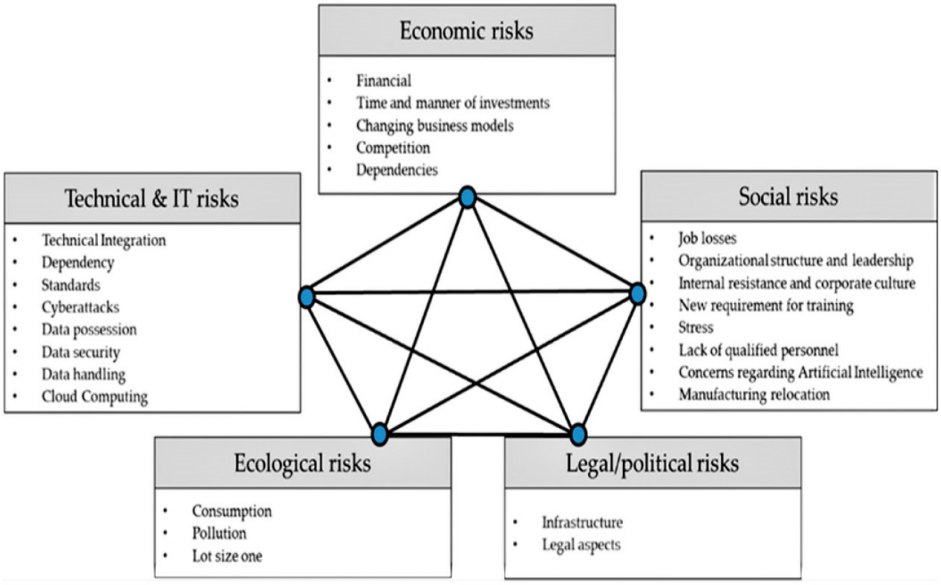

Figure 1. *Main risks of 4IR to individual security*
(Source: Kodym et al., 2020: 76)

Considering all mentioned, the question arises as to how to adequately face the security challenges and risks to human security in Globalization 4.0? As the new era of interconnectedness and technological advancement is creating the network society while humankind becoming more and more digitized and dependent on 4.0 technologies, the key answer lies in the "information security culture" of the individual and society.

Information security culture, as an imperative of modern society, consists of two elements: information security and security culture. Information security implies not only to eliminate all risk nor to determine the way of doing business, but to enable information technology users to use the benefits and advantages offered by modern technologies: on the Internet, local network, or completely isolated computer systems. Information security, in addition to protecting privacy and unhindered use of information technology, should also provide protection of intellectual and material information assets of users and corporations. On the other hand, security culture is a set of adopted attitudes, knowledge, skills and rules in the field of security, expressed as behaviour and process, on the need, ways, and means of protection of personal, social, and international values from all sources, forms and bearers of threats, regardless of place or time of their manifestation (Stajić et al., 2006). In fact, security culture is closely related to our upbringing, values, and value systems that we support.

In sense of that, information security culture, according to Milanović & Radovanović (2015), is a product of individual and group values, expertise, and patterns of behaviour that characterize the commitment, style, and knowledge aimed at a "healthy atmosphere" in the society and management of security. Information security culture within the society manifests itself through various aspects of security related to values, behaviours, attitudes, actions, management activities, as well as the physical

environment. Summing up, the security culture of information technology users reflects, directly or indirectly, on their overall security and protection from the risks to which they are exposed in the era of Globalization 4.0.

POSITION OF THE REPUBLIC OF SERBIA UNDER THE BELT AND ROAD INITIATIVE IN THE LIGHT OF INDUSTRY 4.0

The Belt and Road Initiative connects more than 60 countries in the Asian, European and African continents, which together account for over 30% of global GDP, 62% of the population and 75% of known energy reserves (WEF, 2019). Due to the possibility of developing an intercontinental infrastructure network, increasing trade, and reducing temporal and spatial barriers between partner countries, all thanks to the development of technology, the Belt and Road Initiative is a unique example of Globalization 4.0. However, in addition to the potential to increase the national income and the quality of life of partner country residents, the Initiative simultaneously creates new security challenges and risks, and threatens the internal and external security of partner countries (Pop, 2016; World Bank, 2018).

Namely, security threats do not always appear in isolation and do not affect the reference facility in only one sector. Spill overs most often occur, which means that uncertainties arising in the social sector can easily spill over into the political sector, and thus cause instability of the political order in a country, which can result in spill over into the military sector and may lead to the acquisition of new weapon systems and the so-called "security dilemma". In the context of transnational cohesion and blurring of national borders, as in the case of the Belt and Road Initiative, the possibility of threat spill overs exists also beyond the borders of one partner country. This would mean that threats against one partner country of the Initiative could easily become a threat to other partners of the Initiative.

The Belt and Road Initiative is made up of countries with different degrees of technological development, most of which can be categorized as developing countries, including the Republic of Serbia. Since the process of globalization is accompanied by a disproportion in the development of regions and countries, differences in the speed of technological development are becoming more pronounced. In addition to creating inequalities in terms of the degree of modernization and increased impact of other cultures, partner countries are at risk of uncontrolled refugee migration, religious terrorism, transnational organized crime, environmental threats, etc. (Haiquan, 2017; Cvetković, 2018). Due to differences in the states regarding the effective and efficient response to human security threats caused by differences in the level and speed of technological development and the countries' globalization index, it is not possible for all partner countries of the Initiative to be equally protected. This state of affairs is particularly pronounced in the field of information and communication technologies and critical infrastructure (Lam, 2015; Maráczi, 2017). In relation to some Initiative partner countries, Serbia is, in this area, especially threat-

ened because of an insufficiently doctrinal and strategically regulated security system, which is a consequence of the ongoing security sector reform process (Mitrović, 2019).

As part of the Belt and Road Initiative, a major threat to Serbia's security comes from the ICT field, especially cyberspace. Due to its specific geopolitical and geostrategic position, the Republic of Serbia represents a potential target of contemporary terrorism, including its manifestation in cyberspace (Dragišić & Milošević, 2016). The significance of modern technologies as a threat is confirmed in the Serbian National Strategy for the Prevention and Combating Terrorism for the period 2017-2021. In fact, the Strategy states that the development and availability of state-of-the-art information and communication technologies have increased the risk of their misuse and extended beyond the system of communications, propaganda, recruitment and terrorist training (Nacionalna strategija za sprečavanje i borbu protiv terorizma, 2017). Due to the wide-spread use of ICT in all aspects of society, a large number of partner countries of the Belt and Road Initiative have already put in place mechanisms to respond to cyber incidents. Specifically, there are documents such as the Cybersecurity Framework for Critical Infrastructure Protection in the US; the European Critical Infrastructure Protection Programme with the Network and Information Security Directive in the EU; the Five-Year Plan for National Computerization (2016-2020) and the Law on Cyber Security with the Regulation on Critical Infrastructure Protection in China. However, Serbia is lagging behind in this area. There are security measures in place to protect ICT resources, but they are not sufficient for complete protection of critical infrastructure against cyberattacks (Rizmal, 2018; Todorović, 2018, Vujović, 2019).

Historically speaking, criminal law framework for opposing the cyber-crime in Serbia began to be built in 2003, with the adoption of the Law on Amendments to the Criminal Code, when the criminal legislation was amended by the introduction of criminal offenses against computer data security. However, it is worth emphasizing that the notion of high-tech crime in Serbian legislation is broader than the scope of criminal offenses against computer data security (Milošević & Putnik, 2019). According to the Law on Organization and Competence of Public Authorities for Combating High-Tech Crime (2005), high-tech crime includes the commission of criminal offenses in which computers, computer systems, computer networks, computer data, as well as their products in material or electronic form, appear as an object or means of committing criminal offenses.

However, in the light of the latest emerging technological trends and recognizing the easy availability and possibility of misuse of modern information technologies, the Republic of Serbia adopted the Strategy for the Fight against High-Tech Crime for the period 2019-2023, thus widening the range of areas in which ICT could be misused, which were not covered by the National Strategy for Prevention and Combating Terrorism. A significant step towards more adequate ICT protection of critical infrastructure was the adoption of the Strategy for the Development of Information Security in the Republic of Serbia for the period 2017-2020. Other important documents that make up the regulatory framework for information security of the Repub-

lic of Serbia, including the protection against threats originating from cyberspace, are: the Law on Information Security; the laws on protection of personal data, data confidentiality, electronic signature, electronic document, electronic communications; the Law on Military Security Agency and Military Intelligence Agency; the National Security Strategy; etc. There are also the bodies established on the basis of these and similar documents, such as the National Centre for the Prevention of Security Risk in ICT systems, the Serbian National Internet Domain Registry, the Commissioner for Information of Public Importance and Personal Data Protection, etc. Essentially, it can be concluded that Serbia is on its way to raising and enhancing its level of information protection. However, if it does not accelerate the development of critical infrastructure, in this case the ICT sector, the advantages of its favourable geopolitical position can turn into weaknesses and endanger infrastructure security, and slow down economic development (Mišev et al., 2018).

Management of globalization is very often beneficial for the developed countries, which will not be an exception even in the case of Globalization 4.0. Serbia, as developing country, needs to be aware of the fact that the Belt and Road Initiative includes economically dominant countries that seek to strengthen their influence in other regions and countries, and dictate the pace of technological development. In these circumstances, the question arises whether the economically weaker Initiative partner countries, such as Serbia, will be able to respond to the given challenge, i.e. whether they will be able to follow the speed of technological progress. Due to the existing differences in the degree of modernization and the globalization index, it is almost certain that the 4IR will not have the same impact on all Initiative partner countries, which will manifest in all aspects of society, including the ability to respond appropriately to threats. In a word, those countries that currently have (technological) potential will be able to respond to the most recent security threats at a given moment. Therefore, Serbia must pay particular attention to the promotion of the level of (information-)security culture in society, as well as to development of the technology sector and to safeguarding security against threats that may arise from it.

CONCLUSION

Due to its complexity and multidimensionality, it is impossible to predict all the security implications of Industry 4.0. What is certain is that the fourth industrial revolution has consequences in all segments of society. 4IR has the potential to inflame the economic crisis and increase the level of unemployment and inequality in society; limit human rights and freedoms (e.g. in terms of restricting the right to freedom of expression through the monopoly of the media); threaten national and cultural identities; cause environmental degradation, change the way the service sectors function, as well as the nature and extent of modern conflicts. Because of its ability to integrate all of these elements into a single globalization process and transform the world into a "global village", as well as to produce threats to human security at local (e.g. insufficient level of

democratic development), regional (e.g. environmental degradation) and global (e.g. threatening national identity, internationalization of crime, terrorism) level, it can be concluded that Industry 4.0 has the potential to become a total threat to human security.

Given these facts, the question arises as to how to face and adequately address the potential challenges, risks, and threats to the security of the individual in the fourth industrial revolution?

The answer lies in the synergy of (information-)security culture, economic security and sustainable development, and technological advancement. Specifically, the fear of automation due to new technologies, job loss and livelihoods are the first challenges faced by individuals and society in Industry 4.0. In order to reduce the fears of the new industrial revolution, it is necessary to work on continuous education of the workforce in different 4.0 disciplines, such as digitalization, data analytics, biotechnology, artificial intelligence, etc.; to mitigate the risks of job loss; to improve the resilience of society; and prepare individuals and society to adequately respond to the new challenges of the future market and labour. In addition, it is necessary to develop new skills in individuals, such as the ability to effectively and efficiently solve problems, critical thinking, emotional intelligence, cognitive flexibility. Moreover, building mutual trust, integrity, and tolerance in the network society is another step towards more adequate protection of the individual and society from the negative implications of Industry 4.0. Raising public awareness about security risks on the Internet, or the importance of critical infrastructure for the functioning of community, is a necessary step towards maintaining the stability of social order in crisis situations. Also, 4.0 technologies can be used to ensure greater transparency in the work of state and public institutions, thus creating the basis for building mutual trust. In this way, corruption, misuse of personal and medical data of citizens, and other similar problems, which are often linked to the work of these institutions, can be more easily addressed. Essentially, improving the level of (information-) security culture in the individuals and in society is the first and the most important response to the potential security challenges, risks, and threats that the fourth industrial revolution brings to us.

REFERENCES

Arnett, J. J. (2002). The psychology of globalization. *American Psychologist*, *57*, 774-783.

Bjelajac, Ž. (2016). Sektorski pristup bezbednosti: Analitički okvir kompleksne bezbednosne dinamike. *Kultura polisa, 13*(31), 303-315.

Bonekamp, L., & Sure, M. (2015). Consequences of Industry 4.0 on Human Labour and Work Organisation. *Journal of Business and Media Psychology*. Retrieved February 27, 2020, from https://journal-bmp.de/2015/12/auswirkungen-von-industrie-4-0-auf-menschliche-arbeit-und-arbeitsorganisation/?lang=en.

Buzan, B. (2007). *People, states and fear: an agenda for international security studies in the post-Cold War era*. Colchester: ECPR Press.

Castlls, M. (1996). *The network society*. Oxford: Blackwell.

Chugh, A. (2018, September 19). *How to build a model for human security in the Fourth Industrial Revolution*. Retrieved March 30, 2020, from https://www.weforum.org/agenda/2018/09/how-to-build-a-model-for-human-security-in-the-fourth-industrial-revolution/.

Clifford, C. (2017, November 8). *Hundreds of A.I. experts echo Elon Musk, Stephen Hawking in call for a ban on killer robots*. Retrieved April 02, 2020, from https://www.cnbc.com/2017/11/08/ai-experts-join-elon-musk-stephen-hawking-call-for-killer-robot-ban.html.

Cvetković, V. N. (2018). Neizvesna bubućnost i neograničeno vreme (O dugoročnoj ne/održivosti Novog puta svile). In V. N. Cvetković (Ed.), *Novi put svile: evropska perspektiva* (pp. 21-46). Beograd: Univerzitet u Beogradu - Fakultet bezbednosti.

Cybersecurity Strategy of the European Union. (2013). Retrieved March 17, 2020, from https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.

Davis, N., & O'Halloran, D. (2018, November 8). *The Fourth Industrial Revolution is driving Globalization 4.0*. Retrieved March 10, 2020, from https://www.weforum.org/agenda/2018/11/the-fourth-industrial-revolution-is-driving-a-new-phase-of-Globalization/.

Defort, M. (2015). *Human security in the digital age: a relocation of power and control over security from state to non-state actors*. Retrieved March 16, 2020, from https://smallwarsjournal.com/jrnl/art/human-security-in-the-digital-age-a-relocation-of-power-and-control-over-security-from-stat.

Dragišić, Z., & Milošević, M. (2016). Ugrožavanje nacionalne bezbednosti Republike Srbije terorizmom u sajber prostoru. *Politika nacionalne bezbednosti, 2*, 157-176;

Elamiryan, R. G. (2019). *Human security in context of globalization: information security aspect*. Retrieved March 11, 2020, from https://www.academia.edu/21857072/human_security_in_context_of_globalization_information_security_aspect.

Eldridge, R., Koser, K., Levin, M., & Rai, S. (2017). *What does the Fourth Industrial Revolution mean for migration?* Retrieved March 17, 2020, from https://www.weforum.org/agenda/2017/06/what-does-the-fourth-industrial-revolution-mean-for-migration/.

Friedman, L. T. (1999). *The Lexus and the Olive Tree: Understanding Globalization*. New York: Farrar, Straus and Giroux.

Fukuda-Parr, S. (2003). New threats to human security in the era of globalization. *Journal of Human Development, 4*(2), 167-179.

Gillieron, L. (2019). *Davos: leaders talk about globalization as though it's inevitable – when it isn't*. Retrieved February 30, 2020, from https://theconversation.com/davos-leaders-talk-about-Globalization-as-though-its-inevitable-when-it-isnt-110216.

Haiquan, L. (2017). The Security Challenges of the "One Belt, One Road" Initiative and China's Choices. *Croatian International Relations Review, 23*(78), 129-147.

Heinrich, M. (2019). *Industry 4.0: How it will affect employment and what skills will be required to match the requirements of the market*. Retrieved March 20, 2020, from https://www.researchgate.net/publication/330995136_INDUSTRY_40_How_it_will_affect_employment_and_what_skills_will_be_required_to_match_the_requirements_of_the_market.

Hersman, R., & Stadler, B. (2019). *When is more actually less? Situational awareness and nuclear risks.* Retrieved March 12, 2020, from https://css.ethz.ch/en/services/digital-library/articles/article.html/13e901d2-c1dd-400e-bc04-c4eacd5bd853.

Ignjatović, Đ. (2018). *Kriminologija*. Beograd: Univerzitet u Beogradu, Pravni fakultet.

Kaldor, M. (2000). *Cosmopolitanism and organised violence*. Paper prepared for Conference on 'Conceiving Cosmopolitanism', Warwick, 27-29 April 2000.

Kamei, K. (2013). Human Security and Globalization. *Journal of Poole Gakuin University, 53*, 63-76.

Kamei, K. (2012). Globalization and security: an evolution of economic security. *Journal of Poole Gakuin University, 52*, 39-50.

Kaspersen, A. (2015). *How can international security keep up with technology?* Retrieved April 05, 2020, from https://www.weforum.org/agenda/2015/10/how-can-international-security-keep-up-with-technology.

Kodym, O., Kubáč, L., & Kavka, L. (2020). Risks associated with Logistics 4.0 and their minimization using Blockchain. *Open Engineering, 10*, 74-85.

Lam, R. (2015). *Risks and Challenges for Global ITS Product Companies For China's One Belt One Road.* Retrieved April 15, 2020, from http://itsproducts.com/risks-and-challenges-for-global-its-product-companies-for-chinas-one-belt-one-road/.

Law on Organization and Competence of Public Authorities for Combating High-Tech Crime, Art. 2, Para, 3, *Službeni glasnik Republike Srbije*, 61/2005.

Ljajić, S., Meta, M., & Mladenović, Ž. (2016). Globalizacija: ekonomski i psihološki aspekti. *Ekonomski signali: poslovni magazin, 11*(1), 39-62.

Maráczi, F. (2017). *Security Challenges of One Belt One Road Initiative*. Retrieved April 15, 2020, from http://beltandroadcenter.org/2017/11/07/security-challenges-of-one-belt-one-road-initiative/.

Mehdi, A. (2013). *Dimension of Globalization*. Retrieved March 29, 2020, from https://shodhganga.inflibnet.ac.in/bitstream/10603/24318/9/09_chapter_3.pdf.

Milanović Z., & Radovanović R. (2015). Informaciono-bezbednosna kultura: imperativ savremenog društva. *NBP - Nauka, bezbednost, policija, 20*(3), 45-65.

Milošević, M., & Putnik, N. (2019). Specifičnosti izvršenja krivičnog dela prevare uz korišćenje informaciono-komunikacionih tehnologija. *Bezbednost, 61*(2), 68-88;

Mitrović, Lj. (2019). Reforma sektora bezbednosti Republike Srbije u kontekstu EU integracija. In B. Stojanović, M. Pejić & N. Jović (Eds.), *Evropska unija i evropske integracija Republike Srbije* (pp. 59-76). Beograd: Krovna organizacija mladih Srbije – KOMS.

Mišev, G., Stanojević, P., & Jeftić, Z. Neki aspekti bezbednosti srpske infrastrukture na „Novom putu svile". In V. N. Cvetković (Ed.), *Novi put svile: evropska perspektiva*. (pp. 193-208). Beograd: Univerzitet u Beogradu, Fakultet bezbednosti.

Morgan, E. C. (2002). Globalization and human security: a neo-gramscian perspective. *International Journal of Peace Studies, 7*(2), 57-73.

Nacionalna strategija za sprečavanje i borbu protiv terorizma. (2017). Retrieved April 21, 2020, from http://www.mup.gov.rs/wps/wcm/connect/4e85c9e8-6b07-42ed-9224-01573a1f0d61/strategija-terorizam+1_LAT.pdf?MOD=AJPERES&CVID=mfqgT.n.

Nye, S. N. (2003). *Understanding international conflicts: an introduction to theory and haistory.* London: Longman.

Obar, J., & McPhail, B. (2018). Preventing Big Data Discrimination in Canada: Addressing Design, Consent and Sovereignty Challenges. *Data Governance in the Digital Age: Special Report*, 56–64.

Pop, I.I. (2016). *Strengths and Challenges of China's "One Belt, One Road" Initiative*. Retrieved March 16, 2020, from https://beltandroad.hktdc.com/en/insights/strengths-and-challenges-chinas-one-belt-one-road-initiative.

Rizmal, I. (2018). *Vodič kroz informacionu bezbednost u Republici Srbiji 2.0*. Beograd: OEBS.

Robertson. R, & Khondker. H. H. (1998). Discourses of Globalization: preliminary considerations. *International sociology, 13*(1), 25-40.

Schwab, K. (2016). *How will the Fourth Industrial Revolution affect international security?* Retrieved April 10, 2020, from https://www.weforum.org/agenda/2016/02/how-will-the-fourth-industrial-revolution-affect-international-security/.

Stajić, Lj., Mijalković, S., & Stanarević. S. (2006). *Bezbednosna kultura mladih: kako živeti bezbedno*. Beograd: Draganić.

Strategija razvoja informacione bezbednosti u Republici Srbiji za period od 2017. do 2020. godine. (2017). Retrieved March 25, 2020, from http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2017/53/1/reg.

Todorović, B. (2018). Inicijativa „Pojas i put" i zaštita kritične infrastrukture na balkanskom raskršću. In V. N. Cvetković (Ed.), *Novi put svile: evropska perspektiva* (pp. 209-224). Beograd: Univerzitet u Beogradu, Fakultet bezbednosti.

Tomašević, K., Virijević Jovanović, S., & Zdravković, J. (2020). Uticaj digitalnih tehnologija na unapređenje rada policije. *Bezbednost, 62*(1), 48-64.

UNDP (1994). *Human Development Report 1994*. Oxford: Oxford University Press.
Veljović, V., & Rakočević, V. (2018). Crna Gora na ekonomskom i pomorskom putu svile u XXI vijeku i činioci ugrožavanja bezbjednosti. In V. N. Cvetković (Ed.),

Novi put svile: evropska perspektiva (pp. 21-46). Beograd: Univerzitet u Beogradu, Fakultet bezbednosti.

Vu, C. (2018). *The Fourth Industrial Revolution: its security implications*. Retrieved March 30, 2020, from https://www.rsis.edu.sg/rsis-publication/rsis/co18086-the-fourth-industrial-revolution-its-security-implications/#.XXdxt25uLDe.

Vujović, D. (2019). The challenges of income convergence at times of the Fourth Industrial Revolution. *Ekonomika preduzeća, 67*(1-2), 73-82.

Vulević, M. S. (2018). Migrantska kriza kao izazov socijetalnoj bezbednosti u Evropskoj uniji. *Vojno delo, 3*, 55-74.

World Economic Forum (WEF). (2020). *The Global Risks Report 2020*. Retrieved March 17, 2020, from http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.

World Economic Forum (WEF). (2019). *Globalization 4.0: Shaping a New Global Architecture in the Age of the Fourth Industrial Revolution*. Retrieved March 17, 2020, from http://www3.weforum.org/docs/WEF_Globalization_4.0_Call_for_Engagement.pdf.

World Economic Forum (WEF). (2017). *Harnessing the Fourth Industrial Revolution for the Earth*. Retrieved March 17, 2020, from https://www.weforum.org/projects/fourth-industrial-revolution-and-environment-the-stanford-dialogues.

World Economic Forum (WEF). (2016). *The Future of Jobs Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution*. Retrieved March 17, 2020, from http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf.

Williamson, J. (1998). *Globalization: The Concept, Causes, and Consequences*. Retrieved February 27, 2020, from https://www.piie.com/commentary/speeches-papers/Globalization-concept-causes-and-consequences.

Wolf, M. (2015). Same as It Ever Was: why the techno-optimists are wrong. *Foreign Affairs, 94*(4), 1-9.

World Bank. (2018). *Belt and Road Initiative*. Retrieved March 15, 2020, from https://www.worldbank.org/en/topic/regional-integration/brief/belt-and-road-initiative.