Chapter 8

Challenges for Digital Transformation in the Manufacturing Industry

Serghei Ohrimenco[1], *Grigori Borta*[2]

1. Introduction

The transitional stage in scientific and technological development, the complex processes of adoption of modern innovations are associated with the implementation of the concept of the fourth industrial revolution, Industry 4.0. At this moment, its analogues and more advanced versions are being implemented all over the world. Having become the universally recognised management term, Industry 4.0 is used in a much broader sense than its original meaning, encompassing many innovations. Among them are smart manufacturing, the Internet of Things, artificial intelligence, a variety of nano-devices, 3D printing (including food, organs and tissues), medical robotic surgeons, and many others. The emergence of new technologies is not accidental, it is an answer to the pressing problems of modern generations who want to save time and money by receiving services in digital format.

Specialists from the World Bank, and the McKinsey Global Institute, and others gave the name to such technologies – 'disruptive' because they create opportunities for radical changes (Manyika, Chui, Bughin, Dobbs, Bisson, Marrs 2013; International Finance Corporation; Petralia, Philippon, Rice, Véron 2019). These changes give rise to global fundamental transformations. The scale of innovation is unprecedentedly huge; it is being implemented at an ultra-high unprecedented pace and is easily spreading around the world, ignoring borders. The previous model of business production and marketing does not meet the requirements of

[1] Academy of Economic Studies of Moldova (Republic of Moldova), ORCID: 0000-0002-6734-4321, e-mail: osa@ase.md

[2] Academy of Economic Studies of Moldova (Republic of Moldova), ORCID: 0000-0003-4120-4731, e-mail: grigori.borta@gmail.com

today and requires a change in the principles of regulation of production, completely new competition arises among producers of goods and services.

All this led to an increase in the need for a variety of information, which characterises almost all aspects of the activities of individuals, society and the state. Simultaneously with these processes, there has been an increase in the volume of illegal activities in relation to the information itself, the processes of its receipt and transmission through communication channels, places of concentration and storage of information resources. In other words, the extraction of information in all its forms, using various products and services, has turned into a highly profitable illegal business (Lusthaus 2018) for a group of entrepreneurs. In addition, the components of Industry 4.0 are used to commit a wide range of unlawful acts against individuals, society and the state. On their basis, illegal markets for products and services are formed, satisfying the needs of both individual users, entire corporations, and government bodies. Thus, a 'shadow' economy is formed, built on the modern achievements of human activity and functioning in parallel with the developed markets of scientific and technological achievements.

The aim of this paper is to analyse the impact of digitalisation processes on the manufacturing sector based on challenges and threats associated with the implementation of the achievements of the Industry 4.0 concept. The analysis of the main threats to digitalisation processes focuses on artificial intelligence, Big Data, 5G networks, and blockchain. Along with innovative achievements, digitalisation processes are accompanied by the development of a digital economy and the growth of illegal activities. This analysis provides a contribution to the development of shadow digitalisation processes and the formation of a shadow digital economy, which is directly related to cybersecurity.

As a methodological approach, the analysis and synthesis of statistical information presented in the reports of leading research companies in the field of information and communications technologies and information security were used. A conceptual diagram of the relationship between the components of Industry 4.0 is proposed, highlighting the concept of cybersecurity. Moreover, a definition of the shadow digital economy (SDE) was proposed where the 'crimeware' is a substantial business and an obstacle to the development of the digitalisation processes in all developed and developing countries.

2. Literature Review

The authors of this paper attempt to achieve three main tasks while working with literature review. First, to analyse the literary sources which characterise the development of the concept of Industry 4.0. In the face of growing inequality for many countries, Industry 4.0 is not a solution to problems, but another huge challenge. There is a constant search for a new managerial paradigm, a large-scale re-

view of organisational processes, approaches to training, hiring and monitoring staff. The main distinctive features of the ongoing processes are the depth, regularity and high speed of change, as well as highlighting social issues.

The second task is to analyse the development of the Industry 4.0 components of the manufacturing sector (including retail, telecommunications, insurance, lending, accounting services, real estate valuation, investments, etc.).

The third, most difficult and important task is to identify and evaluate the spectrum of threats of the Industry 4.0 components in relation to citizens, society and the state.

In accordance with the first objective of the study, the publications of international organisations were analysed: the Okinawan Charter of the Information Society (2000), the report of the Secretary-General of the International Labour Organization, 'Century Initiative for the Future World of Work' (2015), World Bank's reports, OECD (OECD 2019), UNCTAD (United Nations Conference on Trade and Development 2019) documents.

The authors of the famous and popular book *The Age of Cryptocurrencies: How Bitcoin and Blockchain Are Changing the World Economic Order* note that society itself is rapidly and continuously changing. 'Digital technologies and online computing are at the epicenter of these changes, transforming the principles of organization of society, public relations and business relations, because all aspects of our life are increasingly dependent on the power of computers and network communications' (Vigna and Casey 2016).

Of particular relevance is the problem of opposing the illegal processes of extracting, processing and distributing information in a variety of forms and contents in the context of building a digital society and a digital economy. The said digital economy implies total globalisation, creates an extremely highly competitive environment, develops rapidly, is inconceivable without qualified personnel and quality education, kills many traditional areas of activity, provides a new quality of life, business and public services, and is largely virtual, intangible. However, it is impossible without communication with the material world. Therefore, the basis of the digital economy is industrial development.

The World Bank Group's Digital Dividend Report for 2016 states: 'The current expansion of access to digital technology brings many people more choice and more convenience. By enhancing social integration, increasing efficiency and introducing innovations, such access opens up opportunities for the poor and disadvantaged segments of the population that they were previously deprived of' (The World Bank 2016). One cannot disagree with this. However, any coin has another side. In addition to the obvious and understandable achievements, it is necessary to analyse the explicit and hidden threats carried by the digitalisation processes of individuals, society and the state.

The author of the book entitled *Introduction to the Theory of the Digital Economy* indicates: '(…) we consider the digital economy as a necessary stage in the

transition to a more advanced innovative economy, which will open to humanity access to virtually unlimited resources and make creativity a need and priority for every person. The society of creators, based on the network principle, is the present future of humankind. And it is precisely this goal that the innovative economy will serve, which must be built through the digitalisation stage' (Mendeleeva 2018).

We consider it possible to agree and emphasise the importance of theoretical research and the preparation of practical developments in this new area, which is the digital economy itself and its security problems, in particular. The following authors, Keshelava, Budanov, Rumyantsev (2017), note: 'Due to a fateful set of circumstances, the beginning of digitalization coincided with the end of globalization and the Global Economic Crisis. The end of the extensive model of the development of capitalism inevitably requires a review of many of the fundamental tenets of the modern world order. This means that under the auspices of digitalization, a completely new world can be created in which other values of the system of values, managerial paradigms, social norms and economic laws will dominate. Of course, this view already has both supporters and opponents, to whose irreconcilable and violent confrontation we can all become witnesses in the near future.'

On 22 January 2020, the UN Secretary-General, António Guterres, named the main threats to humanity: geostrategic tension, climate change, growing distrust at the global level and the danger of new technologies ('reverse side' of the digital revolution) the 'Four Horsemen of the Apocalypse' (United Nations). According to the Secretary-General, new technologies are developing so fast that we do not have time not only to respond to them, but also sometimes even understand their essence. Despite the fact that they promise enormous advantages, digital technologies and artificial intelligence become an instrument of incitement, spread of false information, interference in privacy, exploitation of people, and committing crimes.

Therefore, he considers the use of combat autonomous systems – 'machines capable of killing without any human involvement and bearing no responsibility' – unacceptable, and calls for banning the use of 'killer robots'. António Guterres strongly recommended that order be put in place in cyberspace, which he called the digital Wild West. 'Terrorists, champions of the purity of the white race and others like them abuse the Internet and social networks', said the head of the UN. 'Bots are spreading misinformation, pushing for polarization and undermining democracy. Next year, cybercrime will cost us $6 trillion.'

Another front in the fight against the costs of new technologies is the labour market, where, as António Guterres predicts, automation will deprive hundreds of millions of workers in the next decade. He sees a way out in the reform of the education system, the task of which is to teach people to learn throughout their lives. According to the Secretary-General, the UN is the most suitable platform for governments, the private sector and civil society to oppose global co-operation to the 'digital split'.

In the report 'The Global Risks Report 2018' (World Economic Forum 2018), which was prepared by the World Economic Forum, information threats were included in the global risk rating. Threats such as cyber attacks and data theft and fraud are among the five highly probable threats to critical infrastructures. There, the main areas of risk are highlighted: economic, geopolitical, environmental, social and technological. It is the technological area that global transformations are focused on: information security, information technology, internet governance, the digital economy and society, labour and employment, the future of economic progress, youth prospects, supply and transport, migration, and the fourth industrial revolution.

The collective monograph on the digital transformation of the economy states: 'The new model is being formed on the technological basis of the next fourth industrial revolution, related to the digitalisation of the economy not only in the field of services, corporate and public administration, but also in the material basis of the economy, in manufacturing and associated logistics infrastructure' (Tolkacheva 2018). The main drivers of digital transformation are the following: the Internet of Things, artificial intelligence, Big Data analytics, neural networks, blockchain, cloud computing, robotics, additive technologies (including 3D printing), virtual and augmented reality. Digitalisation is planned to be introduced in the following areas: state regulation, information infrastructure, research and development, personnel and education, information security, public administration, smart city, digital healthcare. Particular attention is paid to information security, since a change, for instance, of the digital content of such a phenomenon as a 'digital twin' can lead to a catastrophic situation not only in the field of industrial production. Illegal actions in relation to a set of critical technologies pose a potential danger, including the likes of the industrial internet or the Internet of Things, medical equipment, primarily cardiological, computer technologies integrated with biological organisms, etc.

As noted by Keshelava, Budanov and Rumyantsev (2017), the topic of the digital economy is very extensive and is currently extremely popular. 'The excitement around this area, on the one hand, and the lack of a single conceptual field, on the other, leads to the emergence of a huge number of seemingly incompatible opinions and, as a result, to the impossibility of dialogue.' There are three waves of digital technology, each characterised by technological advances and a set of threats. The first wave includes the implementation of information and communications technologies, the computerisation of key areas of activity, the automation of management processes (including the implementation and use of ERP, EDI, CRM, etc.), as well as the introduction of broadband access. The second wave can be characterised by the development and implementation of online platforms, for instance, search engines, marketplaces, distance learning, social networks. The third wave involves the introduction of technologies such as predictive analytics of big data, industrial internet or the Internet of Things, robotics,

additive technologies (including 3D printing), artificial intelligence, including machine learning.

There is reason to believe that interest in illegal activities in the field of the digital economy will rapidly increase this process, and actions need to be investigated in all aspects, primarily in relation to critical technologies to prevent serious consequences.

In addition, as noted by Oltsik (2019), based on Environmental, Social, and Governance (ESG) data and services, the lack of cybersecurity skills is felt. For several years in a row, this company has been conducting a survey, and as a result, the percentage of organisations reporting a problematic lack of cybersecurity skills continues to grow. Below are the results of the last four polls:

- 2018–2019: 53% of organisations report a problematic shortage of cybersecurity skills;
- 2017–2018: 51% of organisations report a problematic shortage of cybersecurity skills;
- 2016–2017: 45% of organisations report a problematic shortage of cybersecurity skills;
- 2015–2016: 42% of organisations report a problematic shortage of cybersecurity skills.

The main goal of this article is to analyse, discuss and develop an approach to determining the reverse (shadow) side of the digital economy, which accompanies the global digitalisation processes.

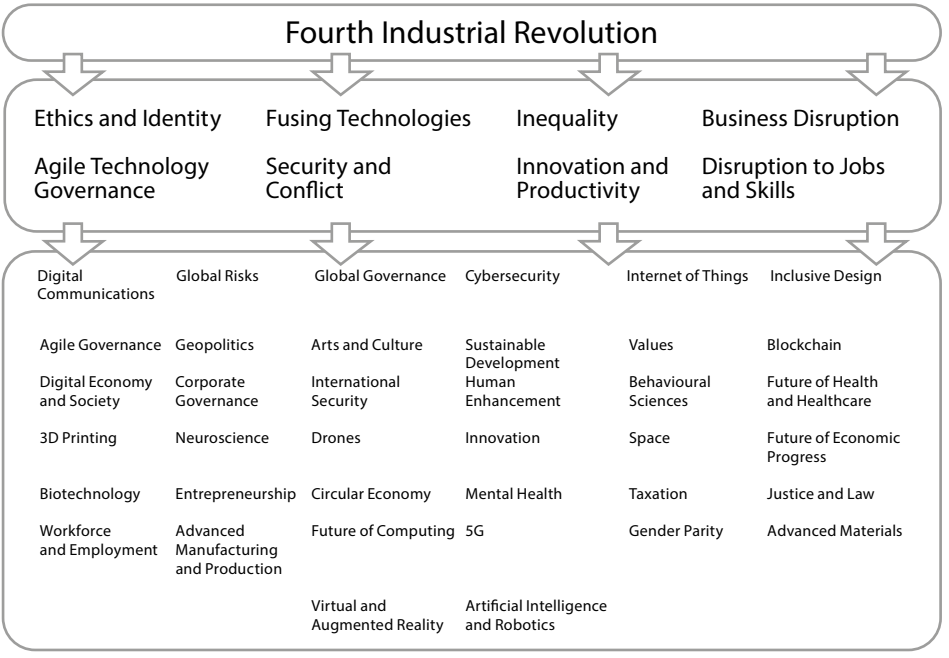
3. Research Methodology

This research is based on the analysis of numerous studies conducted by international organisations and technological companies which associate their activities with the development and implementation of information and communications technologies. For instance, these are materials from the UN, UNESCO, IMF, the World Bank, the World Economic Forum, the Organisation for Economic Co-operation and Development (OECD), etc., as well as reports from research centres, such as McAfee, Kaspersky Lab, Ernst & Young, Kroll, ESET, IBM, EuroPol, Imperva, Panda Security, Ponemon and many others (Reis, Amorim, Melão, Matos 2018).

The methodology of this study is based on the views of a wide range of experts from the World Economic Forum's Expert Network and is curated in partnership with Benjamin Fung, Canada Research Chair in Data Mining for Cybersecurity, Associate Professor, School of Information Studies, McGill University (World Economic Forum 2020b). These materials combine research on the Fourth Industrial Revolution and Cybersecurity. The conceptual diagram of the interconnection of the Industry 4.0 components is shown in Figure 1. This approach should

be expanded and lay the foundation for subsequent research on shadow digitalisation processes.

Figure 1. Conceptual diagram of the relationship of the components of Industry 4.0



Source: own study.

The conceptual content of the cybersecurity direction is represented by a set of the following main modules (World Economic Forum 2020a):

- Technology and the Law – adaptions of the existing laws to the ever-growing list of new hi-tech crime.
- New Norms of Collaboration – better data sharing protocols should be put in place between academic researchers, private sector organisations, non-profits and government agencies.
- Critical Infrastructure Protection – an effective set of measures of protection for the critical infrastructure against digital threats and cyberthreats is required.
- Cyber Privacy – a lot of data that is used is not anonymised or just not anonymised enough, putting privacy at risk.
- Security of Things – with most of the modern devices being interconnected, there is a growing risk of their security being breached, thus requiring thoughtful design of the device software and their communication protocols.
- Cyber War – the lack of international accords in place creates a situation where certain entities can be extremely vulnerable to cyberattacks.

- Systemic Risk and Resilience – regular evaluation of security systems in place can greatly strengthen their resilience.
- Cybercrime – while making our life easier on the one hand, the technologies also make us much more vulnerable to illegal actions, on the other hand.

4. Results

As a result of the research, it was concluded that the shadow digital economy is forming against the backdrop of the development of global digitalisation processes. For this study, the following definition of the shadow digital economy, based on its specificity in terms of the production of products and services, the life cycle of products and services, is proposed: the shadow digital economy (SDE) is a sector of economic relations covering all types of industrial and economic activities, which in their direction, content, nature and form contradict the requirements of the law and are implemented contrary to the state regulation of the economy and bypassing control over it.

We supplement this definition with the following components which were developed by the authors of this paper (Borta 2013; Ohrimenco and Borta 2014; Ohrimenco and Borta 2016):

- All individual and collective activities which are illegal, associated with the design, development, dissemination, support and use of components of information and communications technologies, hidden from society are encompassed by the shadow information economy. That is, the shadow information economy is all the illegal and hidden products and services which use and are based on information technology. The following are the most important economic elements of this sphere: illegal economic relations, illegal activities related to the production, distribution and use of prohibited products and services.
- Shadow information economy – an activity related to the research, design, production, distribution, support and use of components of information and communications technologies, hidden from society and the state, outside state control and accounting, and also, most frequently, illegal. Thus, the reason for the existence of a shadow information economy is the presence of conditions under which it is beneficial to hide own activities, or own individual elements.
- Shadow information economy is all the collective or individual activity that parasitises in all areas of society, on the basis of the use of information and communications technology components. This type of illegal activity should be considered as a special segment, which is characterised by the following systemic properties: universality, integrity, communication with the external environment, structure, ability to organise and continuously develop itself, the presence of a constructive (productive sector) and a destructive (criminal sector) element.

Table 1. The targets, motives and methods of cybersecurity attacks

Specification		Government structures	Financial domain	Online servers	Medical facilities	Education	Services	IT corporations	Industrial companies	Retail	Private persons
Targets	Infrastructure	54	42	20	56	57	42	53	79	22	35
	Web resources	34	32	72	10	17	30	31	4	52	18
	Users	6	10	7	34	26	7	5	17	4	18
	Internet of Things	4	–	1	–	–	2	5	–	–	2
	Mobile devices	2	–	–	–	–	6	3	–	–	27
	ATMs and POS	–	16	–	–	–	13	3	–	22	–
Motives	Financial gain	44	92	–	69	81	70	84	55	74	79
	Data acquisition	34	8	85	28	17	21	16	24	26	19
	Hacktivism	17	–	9	3	2	9	–	7	–	1
	Cyberwar	5	–	5	–	–	–	–	14	–	1
Methods	Use of malware	39	37	–	16	16	17	15	12	8	39
	Software vulnerabilities exploitation	20	8	4	8	9	3	5	2	3	20
	Compromising user accounts	20	2	13	13	14	14	4	4	4	35
	Web vulnerabilities exploitation	19	9	27	7	8	9	3	1	5	12
	DDoS	19	7	10	1	–	2	4	–	2	–
	Social engineering	9	12	2	12	9	2	2	8	2	38
	Other	8	2	3	4	2	6	5	2	3	14

Source: compiled by the authors on the basis of the research in: Positive Technologies (2018).

The main conclusion is that the SDE represents a technical, technological, economic basis for cybercrime and combines a set of actions directed against individuals, society and the state.

The report 'Cybersecurity Threatscape 2017' (Positive Technologies 2018), which was prepared by the well-known company Positive Technologies, examines the results from 2017 in relation to the existing infrastructure and information impact in the context of targets, motives and methods (Table 1).

'The world is just beginning its path to cybersecurity, and although the technologies of the fourth industrial revolution will undoubtedly raise new obstacles, we have many options for innovation and new models of co-operation in combating existing and new threats', says William Dixon, head of operations at the Global Centre for Cybersecurity – Economic Forum (Samartsev and Dixon 2019).

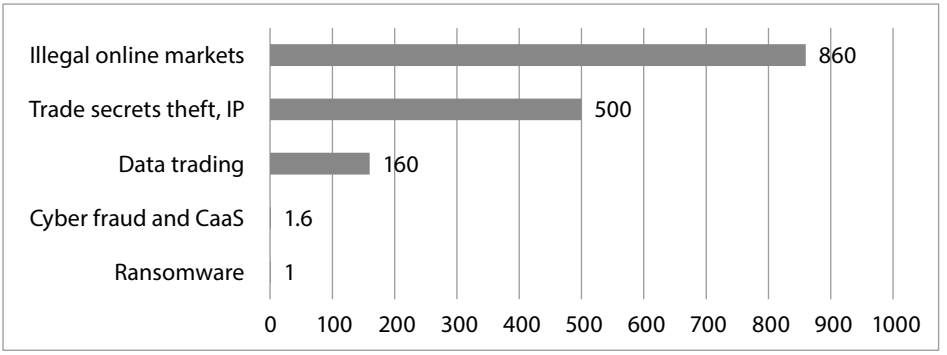
Another very important problem is the study of the economic foundations of cybercrime. In this regard, the data on the economy of cybercrime looks staggering against the background of the collected statistics on the activity of the SDE. Cybercrime was estimated at USD 1.5 trillion in 2018, according to a study by Bromium. This was the first study of its kind to examine the 'dynamics of cybercrime' in the context of revenue stream and profit distribution. The study identified new criminal platforms and a thriving cybercrime economy that is self-sufficient and blurs the boundaries of legality. Gregory Webb, CEO of Bromium, commented on the study's findings as follows: 'It's shocking how widespread and profitable cybercrime has become. The model of crime is to create malware and deliver it to cybercriminals as easily as shopping online. Not only is it very easy to gain access to the tools, services and expertise of cybercriminals, this means that businesses and governments will face more sophisticated, costly, and destructive attacks as the network is profit-driven and gains traction. We cannot solve this problem with old thinking or outdated technology. The time has come for new approaches' (Williams 2019). The report is accompanied by a summary table that provides data on the annual income generated from the implementation of selected cybercrimes.

This paper makes an interesting suggestion that if cybercrime, from an economic point of view, were a sovereign country, it would rank 13th in the world in terms of GDP. The total income, according to approximate data, is equal to USD 1.5 trillion (Figure 2) and includes:

- USD 860 billion – actions in illegal online markets
- USD 500 billion – trade secrets theft, IP
- USD 160 billion – data trading
- USD 1.6 billion – cyberfraud and cybercrime as a service
- USD 1 billion – ransomware.

The report points out that cybercrime operates at multiple levels, with some large 'corporate'-style trading operations bringing in over USD 1 billion and 'small and medium-sized business' orders ranging from USD 30,000 to USD 50,000.

Figure 2. Yearly income from cybercrime in 2018



Source: compiled by the authors based on Williams (2019).

A wide range of economic agents with their deep specialisation (from the development of specific malicious software mechanisms to the rental of ready-made bot systems, etc.), economic relations and other economic factors contribute to the generation, support and confirmation of high incomes on an unprecedented scale.

A preliminary conclusion may be based on the fact that the activities of the SDE are directly related to cybercrime (Walker and Reitano 2019; Lampe 2016; Riek et al. 2016). Consider the main components of digitalisation and threat processes, respectively:

- Artificial intelligence in terms of data security, models and operations. First of all, attacks on AI itself: the intruder steals models and data for training; deception of models through the use of false data; manipulation of training data to modify its behaviour and make decisions; attack on the algorithm by making changes to the algorithm itself; adjustment of actions to the algorithm; adversarial examples; attack on data (entering extraneous data, changing existing data). In addition, AI can be used to search for vulnerabilities in software, modify software abuses, develop and implement phishing attacks, create high-performance bots, set up passwords and change identities.
- 5G communication networks are a breakthrough technology, but can be used as the basis of the MIM (man-in-the-middle) attacks, jamming, mobile edge computing, DOS and DDOS, existing application vulnerabilities may also be exploited.
- Big Data, as the main element of Industry 4.0, are high-performance, high-speed and diverse information assets which require cost-effective, innovative forms of processing information to enhance understanding and decision-making. The main threats can be the following: wiretapping, interception and theft of data, data loss, destruction of records, loss of devices, use of personal and false data. These actions can be implemented using unlicensed software, social engineering, malicious code and targeted attacks.

- Blockchain. It should be noted that threats are shifting to the customer devices (operating system, network protocols, key management). The organisation of attacks, including 'denial of service', on the infrastructure in the closed blockchain, quantum attacks on cryptography, attacks on smart contracts (BatchOverflow, MAIAN, Reentrancy, Bad Randomness, etc.) is not ruled out.
- Biometrics. Threat models are currently being developed for: the data processing (data or device substitution, device reboot, intruder data injection, component replacement, guessing and enumeration, results manipulation, hill climbing, malicious code injection, decision-making manipulation); for the storage process (compromising the database); for inter-processor stages (interception, repetition, selection, manipulation of results, replacement of components, manipulation of the decision made in comparison, etc.).
- All the clear advantages of 'breakthrough' technologies are combined to implement a new widespread threat – misinformation (Bradshaw and Howard 2019; Fallis 2009). This threat is not completely new, but the preparation and implementation have been put on a new technological level – the development and distribution of fake news through social networks, etc.
- Advances in information and communications technology and digitalisation have created new challenges and threats. This applies to the development of encryption programs, the emergence of cryptocurrencies and, as a result, the organisation of attacks on cryptocurrency exchanges and cryptocurrency exchangers.

Crimeware is a serious business. Developers model their activities in accordance with corporate standards to maximise profits. As an example, the emergence of 'crimeware-as-a-service' (criminal software as a service) can be considered as a demonstration of its capabilities. For a short period of time, cybercriminals radically change their toolkits to achieve new results. An additional example is cryptomining as an operation. The cryptocurrency market peaked at the end of 2017 and began to decline by February 2018. The downward trend in the bitcoin index directly affected the activity of cryptomining as an operation, which fell by more than 50% during the year. The statistical correlation between the jumps in the bitcoin index and the popularity of 'cryptomining as an operation' can be considered as a highly profitable tool for influencing the business.

One more important feature of cryptocurrencies should be highlighted – receiving bribes by cryptocurrencies has been very popular among officials and lawyers for several years. Such transactions can be tracked, but neither actually nor legally can they be tied to a person. That is, formal evidence for the investigation and trial cannot be obtained *a priori*. Moreover, cryptocurrency immediately appears outside the state, and it is almost impossible to confiscate it. However, with the internet, it always remains at the disposal of the owner. This is a kind of airbag for detainees.

We consider it possible to refer to the research by the RAND Corporation, entitled *Economic Competition in the 21st Century* (Shatz 2020). This report examines various forms of economic competition, including the concept of national competitiveness, competition for markets and investment, the use of economic instruments in areas of international competition, and competition for the nature of the global economic system. The main idea is the thesis that geopolitical competition using economic instruments can be effective, but the use of such instruments can be very expensive. In any case, the costs of implementing them should be weighed against the benefits obtained. Among other economic instruments for geopolitical competition in the United States, the following stand out:

- Trade policy
- Investment policy
- Sanctions
- Cyber tools
- Financial help
- Financial and monetary policy
- Production and export of energy and goods.

Cyber tools are of particular interest, since they can be used to inflict damage (for instance, a reference is made to the alleged shutdown of the Ukrainian power grid in 2015), as well as to steal intellectual property, technology and trade secrets.

5. Conclusions

The aim of this paper was to analyse the impact of digitalisation processes on the manufacturing industry focused on challenges and threats of the implementation of the Industry 4.0 concept. The analysis revealed that cybercrime and SDE are widespread in the business and society. Effects of a single criminal attack (for instance, DDOS or MIM and other) affect supply chains beyond the realm of cyberspace. Therefore, a qualitative and quantitative review of the content is required, using the following cybersecurity assessment metrics (Daultrey 2017): legal (cybercrime laws, regulations, training); organisational (collection of metrics on cybersecurity, national strategy); technical (industry standards); capacity building (training for cybersecurity professionals, public awareness); co-operation (international, inter-agency and public-private sector).

For instance, 5G communication networks, which are just starting to be launched in several countries, will hardly cope with the growing volume of data transfer by 2028. According to analysts of Bank of America Merrill Lynch, we should expect by this time the next generation networks – 6G. 6G mobile communication technologies may become one of 15 breakthrough technologies which will have a key impact on the global industry in the coming years, among other similar breakthrough technologies (quantum computers, Hyperloop, nanosatellites, geo-

engineering, etc.). Analysts believe that 6th generation networks will be able to increase speed up to 400 times higher than 5G, in addition, the advantages of AI will be used. Based on this, one can assume the expansion of capabilities for implementing various attacks.

A programme to improve the warning system about new software abuse and countermeasures is needed. This work should be implemented in relation to state and private institutions, primarily financial and banking activities. The risk of using malware is clearly underestimated, making protection efforts difficult. This leads to the fact that losses from the impact of criminal software are growing, and countermeasures are taken to reduce the effectiveness of the confrontation. The impact of criminal software is enormous, and if the resistance efforts are not significantly increased, more serious and widespread consequences in terms of coverage and cost may arise.

The growth of criminal software is steady, the frequency of distribution of new species is growing from year to year. Moreover, as a result, criminal software represents a more serious threat to business than targeted attacks on information systems do. The introduction of criminal software is not expensive and does not require much effort on the part of motivated participants. It ensures the optimisation of ongoing attacks to achieve profitable goals. The ability to increase responsiveness and change strategies has led to the emergence of increasingly sophisticated and targeted attacks on business programmes.

References

Borta G. (2013). Analiz etapov razvitiya tenevoy informatsionnoy ekonomiki (Analysis of the Stages of Development of the Shadow Information Economy). Academy of Economic Studies of Moldova.

Bradshaw S., Howard P. (2019). *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*. Available online: https://bit.ly/3ay5YBi (accessed on 30 March 2020).

Daultrey S. (2017). *Cybercrime: Invisible Problems, Imperfect Solution*. Available online: https://bit.ly/2QWks6f (accessed on 30 March 2020).

Fallis D. (2009). *A Conceptual Analysis of Disinformation*. Available online: https://bit.ly/39seC2Q (accessed on 30 March 2020).

International Finance Corporation. Plodotvornyye investitsii (Productive Investment). Available online: https://bit.ly/3dHn41t (accessed on 30 March 2020).

Keshelava A., Budanov V., Rumyantsev V. (2017). Vvedeniye v «Tsifrovuyu» ekonomiku (Introduction to the 'Digital' Economy). Available online: https://bit.ly/2QUOzuC (accessed on 30 March 2020).

Lampe K. (2016). *Organized Crime: Analyzing Illegal Activities, Criminal Structures, and Extra-Legal Governance*. Available online: https://bit.ly/2yjQDWR (accessed on 30 March 2020).

Lusthaus J. (2018). *Industry of Anonymity: Inside the Business of Cybercrime*. Harvard: Harvard University Press.

Manyika J., Chui M., Bughin J., Dobbs R., Bisson P., Marrs A. (2013). Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy. *McKinsey Global Institute*. Available online: https://mck.co/3dABpge (accessed on 30 March 2020).

Mendeleeva D. (2018) Vvedeniye v teoriyu tsifrovoy ekonomiki (Introduction to the Theory of the Digital Economy). Moscow: Grifon.

OECD. (2019). *Economic Outlook May 2019: Digitalisation and Productivity: A Story of Complementarities*. Available online: https://bit.ly/2UrBkDU (accessed on 30 March 2020).

OECD. (2019). *Measuring the Digital Transformation: A Roadmap for the Future*. Available online: https://bit.ly/3bMxHyz (accessed on 30 March 2020).

Ohrimenco S., Borta G. (2014). Zvorotnyy bik informatsiynoho suspil′stva (The Reverse Side of the Information Society). Kiev: Banking University of the National Bank of Ukraine (NBU).

Ohrimenco S., Borta G. (2016). Issledovaniye kharakteristik tenevoy informatsionnoy ekonomiki (Study of the Features of the Shadow Information Economy). D. A. Tsenov Academy of Economics.

Oltsik J. (2019). *The Cybersecurity Skills Shortage Is Getting Worse: More Than Half of Organizations Report a "Problematic Shortage" of Cybersecurity Skills, and There Is No End in Sight*. Available online: https://bit.ly/2Jrp3cm (accessed on 30 March 2020).

Petralia K., Philippon T., Rice T., Véron N. (2019). *Banking Disrupted? Financial Intermediation in an Era of Transformational Technology*. Available online: https://bit.ly/39uRNM1 (accessed on 30 March 2020).

Positive Technologies (2018). Cybersecurity Threatscape 2017. Available online: https://bit.ly/2D2FSe6 (accessed on 27 August 2020).

Reis J., Amorim M., Melão N., Matos P. (2018). *Digital Transformation: A Literature Review and Guidelines for Future Research*. Available online: https://bit.ly/2w3GtsI (accessed on 30 March 2020).

Riek M., Bohme R., Ciere M., Ganan C., van Eeten M. (2016). *Estimating the Costs of Consumer-Facing Cybercrime: A Tailored Instrument and Representative Data for Six EU Countries*. Available online: https://bit.ly/3bBKvYc (accessed on 30 March 2020).

Samartsev D., Dixon W. (2019). *5G, Artificial Intelligence and Biometrics Will Determine the Cybersecurity Strategy for the Next Decade*. Available online: https://bit.ly/2wDfaWv (accessed on 30 March 2020).

Shatz H.J. (2020). *Economic Competition in the 21st Century*. Available online: https://bit.ly/3lmlVQQ (accessed on 27 August 2020).

The World Bank. (2016) *World Development Report 2016: Digital Dividends*. Available online: https://bit.ly/2QVBZvv (accessed on 30 March 2020).

Tolkacheva S. (2018). Promyshlennaya politika v epokhu tsifrovoy transformatsii ekonomiki (Industrial Policy in the Era of Digital Transformation of the Economy). Moscow: Knorus.

United Nations Conference on Trade and Development. (2019). *Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries*. Available online: https://bit.ly/2WU4ddS (accessed on 30 March 2020).

United Nations (2020). Glava OON rasskazal o svoikh prioritetakh na 2020 god (UN Chief Spoke About His Priorities for 2020). Available online: https://bit.ly/3bEt8Gu (accessed on 30 March 2020).

Vigna P., Casey M. (2016). Age of Cryptocurrency. London: Picador

Walker S., Reitano T. (2019). *Fragmented but Far-Reaching: The UN System's Mandate and Response to Organized Crime*. Available online: https://bit.ly/39v5lqI (accessed on 30 March 2020).

Williams J. (2019). *Cybercrime as an Economy*. Available online: https://thefintechtimes.com/cybercrime-economy/ (Accessed on 20 March 2020).

World Economic Forum (2020a). Cybersecurity. Available online: https://bit.ly/3dAOyWC (accessed on 28 August 2020).

World Economic Forum (2020b). *Fourth Industrial Revolution*. Available online: https://bit.ly/2yb9vqP (accessed on 30 March 2020).

World Economic Forum. (2018). *The Global Risks Report 2018*. Available online: https://bit.ly/3dKlRXx (accessed on 30 March 2020).