THE KOSCIUSZKO INSTITUTE | POLICY BRIEF | APRIL 2020
ISSN 1689-9873

危机 [wēijī]

Izabela Albrycht – President of the Kościuszko Institute
Michał Kanownik – President of ZIPSEE
Robert Siudak – Non-Executive Director, Kościuszko Institute

INTRODUCTION

The word "crisis" in Chinese (危机) consists of two characters. One stands for "threat" and the other stands for "chance". The world is currently facing a threat caused by the global pandemic of SARS-CoV-2 coronavirus and COVID-19 disease, which originates from the People's Republic of China, and, according to all economic analyzes, will lead to global recession or even depression, and as a consequence, to the remodeling of global economy. There are many indications that the epidemic caused by the coronavirus will be less absorbent than its great predecessors, such as the Spanish Influenza or the plague, but it will certainly be an epidemic that destroys the existing economic and social order, with potential repercussions also in terms of international security. According to the calculations of the British organization, Henry Jackson Society, the G7 countries have already allocated $ 4 trillion to support their economies. These estimates are based not on declared but formally announced expenses as of April 5, 2020. The United Kingdom has allocated spending of $ 449 billion, the United States of America – $ 1,200 billion, Canada – $ 59 billion, Australia – $ 37 billion.[1] As part of the anti-crisis shield program, Poland plans to allocate $ 51.3 billion to support the economy.

1 Matthew Henderson, Dr Alan Mendoza, Dr Andrew Foxall, James Rogers, Sam Armstrong, *Coronavirus Compensation? Assessing China's Potential Culpability and Avenues of Legal Response*, https://henryjacksonsociety.org/publications/coronaviruscompensation/, [online: 5.04.2020].

Facing the challenge of the SARS-CoV-2 pandemic, in addition to specific public health, national security and social policy activities, Poland must already think of the economic strategy for the future and identify economic opportunities that will arise with the birth of a new digital world, which is being formed right before our eyes.

MANAGING THE STATE IN TIMES OF CRISIS IS NOT JUST CRISIS MANAGEMENT

As far as the Polish state's activities are concerned, unquestionable number one priority is ensuring the well-functioning healthcare system and limiting the spread of SARS-CoV-2 virus (as a part of a suppression strategy aimed at eliminating the transmission of disease between people) in order to secure the production, purchase and distribution of sufficient medical and logistics resources. The second key challenge is to support the entrepreneurs and employees in order to minimize the negative social and economic effects of a slowdown, if not economic collapse, in the individual industries, as well as the entire economy. The slowdown that is a result of the adopted suppression policy, which has an impact on both the demand and the supply components of the economic equation. In both contexts, politicians and government administration take a number of initiatives that are widely analyzed by experts, by the media and by citizens. In Poland, the preventive measures (non-pharmaceutical interventions – NPI) aimed at limiting the spread of disease

in society through self-isolation and limiting the mobility of citizens were introduced at an early stage. As the research based on the data from the previous great epidemic – the Spanish Influenza of 1918 – shows, such actions, contrary to appearances, may also have a long-term economic meaning. The regions that introduced NPIs faster in 1918 were able to end the disease eradication phase faster and move on to the next phase, i.e. the fight against the effects of the pandemic. Experts' findings therefore indicate that NPIs not only reduce mortality, but also indirectly reduce the negative economic effects of a pandemic.[2]

> **The aim of this brief is to draw attention to the third, necessary dimension of current reflection and actions, which is absolutely essential at a later phase of the fight against the pandemic. It can be called strategic and economic reflection, and can be summarized in the question "what next?". How the Polish state, its economy and society should develop in a new geopolitical and economic reality that will crystallize after the current period of crisis and transformation? The conclusions drawn from such questions should already, at the stage of tackling ad hoc challenges during the epidemic and economic crisis, shape the policy of support and redistribution of funds by the Polish state.**

Polish society has not so distant experience of transformation and the economic crisis, which was one of the effects of the transformation model adopted in 1989. Thirty years later, while the Polish state has a developed free market economy, analyst resources in both public administration and expert centers, as well as the political class, facing the challenge of transformation and crisis, it has to be able to think, adopt the strategy and implement it. In the first step, we should select key sectors, which in the short period of the worst economic crisis will be specially supported in order to "keep them alive", so that in the medium and long term, after the collapse, they will become the driving force for the development and competitiveness of the Polish economy in subsequent decades of the 21st century. Our goal should be to draw conclusions from the difficult time of post-communist transformation, and to avoid mistakes related to the lack of intentional state action to protect and support key sectors from a perspective of further development of our country.

The trend currently observed in other countries is redefining the importance of such sectors as healthcare, industrial production (including production of personal protective equipment and medical equipment), technological and agricultural sector.

There is also reflection on radical actions that do not fit into the current canons of the common EU market. The example of such action is that of the Italian government, which is already planning to extend its control powers to the entire banking and insurance sector, as well as to health and food industry, so that during the crisis foreign investors, also from other European Union countries, could not buy assets of industries considered strategic for the country. The share prices of many companies have collapsed due to the epidemic crisis. So far, this type of protection has been implemented (but not in European Union countries) in such industries as the defense, energy and telecommunications, as well as in the area of key financial infrastructure and payment systems.[3]

Behind such a task for Poland lies an important assumption concerning the role and scope of support and protection of the state during the crisis. All workplaces are equally important from the social policy perspective, but not all branches of the economy are equally important from the perspective of the economic policy of the state. While in the first context, the task of the government is to spread the protective umbrella over all citizens, in the second context the Polish state can and should say it straightforward – we have to **protect** all strategic sectors of the Polish economy, but we cannot afford to **support** all branches of the economy at the same time.

> **Wise economic policy (not social, because this is not the case here) in times of crisis, must be able to strategically select and allocate funds and support industries and sectors that, after a period of market collapse, will be able to create competitive advantages of the recovering economy, provide innovation, increase in productivity and security.**

Looking at global economic and political changes, which were also catalyzed by the crisis associated with the SARS-CoV-2 pandemic, the thesis put forward by the authors of this brief is as follows: **the Polish state, as one of the key sectors, should select the broadly understood market of information and communications technology (ICT) solutions**. It should include segments such as gaming and the Internet of Things (IoT), but also cyber security, artificial intelligence, production automation, Big Data analysis and others. The key sector for the first industrial revolution was textiles, for the second – metallurgy, for the third – manufacturing industry. The broadly defined fourth industrial revolution, which in the 21st century will drive the global economy, is based on the ICT sector.

2 Sergio Correia, Stephan Luck, Emil Verner, *Pandemics Depress the Economy, Public Health, Interventions Do Not: Evidence from the 1918 Flu*, https://ssrn.com/abstract=3561560, [online: 1.04.2020].

3 *Italy plans to widen special powers over strategic sectors*, Reuters, https://www.reuters.com/article/health-coronavirus-italy-golden-powers/italy-plans-to-widen-special-powers-over-strategic-sectors-idUSL8N2B-S0IU, [online: 5.04.2020].

It is important, that Poland is not again a periphery of economic changes and that it can participate in this race, occupying a sufficiently high position in the production value chain. That is why at the stage of combating the current economic crisis, it is necessary to support the Polish ICT sector so that it can be the driving force of Polish GDP in the subsequent decades.

DIGITIZATION IN THE TIME OF CRISIS

It is necessary to map those sectors for which the condition for maintaining further competitiveness will be a rapid digital transformation of management or production processes. In this respect, either the state cannot remain passive. The sectors selected for deep and rapid digital transformation in connection with the pandemic are first of all manufacturing, banking, health and transport sectors.[4] This is a chance to connect, where possible, domestic demand for digital and cybersecurity solutions with domestic supply. In his speech presenting the assumptions of the anti-crisis shield in the Senate, Prime Minister Mateusz Morawiecki rightly pointed out that it is necessary to create a model of driving domestic supply by demand. In the case of support for the broadly understood technology sector, including cyber security, this solution seems to be of particular use.

Despite the crisis, it will also accelerate the process of building modern telecommunications infrastructure, the issue of building a new generation Internet network – 5G, which, although due to the pandemic is no longer on the headlines, is still one of the most important challenges of modern countries and will further affect their competitiveness after the epidemic.

In the USA, AT&T and Verizon companies have already stated that they will spend most of their investment funds on expanding the internet network, pointing out not only to the increased demand for data transmission as a result of changes in work culture and spending free time, but also to the need to ensure companies have a good position when the pandemic passes and the economy begins to bounce back[5]. In this context, work on the development of 5G networks in Poland, with state support, will be significantly accelerated. Especially since 5G will drive the digital economy, generating new workplaces and stimulating economic growth. According to the latest GSMA data, 5G technology is expected to contribute $ 2.2 trillion to the global economy by 2034.[6]

At the same time, due to the increasing number of digital attacks, we should take into account the need to build network that is not only effective, but also resistant to threats. For this reason, as we have pointed out many times in our analyzes, trusted technology providers should be used.[7] Currently, it will be more important than ever to understand that our own digital technology resources, also in the cybersecurity and 5G sectors, as well as locating scientific and research activities and factories of ICT companies in Poland, are the basis for building a technological base and resources of competences in the economy, enabling to secure the functioning of the state in the 21st century.

Therefore, efforts and actions should be made to support, in particular, those 5G technology suppliers, that are rooted in Europe. Emphasis should be put on them in the next financial perspective of the European Union to participate in the construction of the 5G network in Europe. Another reason for that is because this year we are observing a strong trend in which the Chinese market clearly prefers Chinese suppliers, probably as a response to the economic effects of the pandemic, but first of all because it finds the security of its network so important, that it entrusts it to the trusted companies. Recently, Huawei and ZTE won the tender of the telecommunications giant China Mobile for the construction of a 5G network covering 90% of the demand for technology.[8] Europeans should do the same, recognizing both the opportunities and threats associated with building a new generation networks.

Certainly, the pandemic will leave the world more digital than it has found, and trends such as data-driven economy or automation will not be for the most part just a concept, but will become our reality. The faster we accumulate this knowledge at all levels of state and economy management, the better. At the same time, it will also be necessary to address the effects on those economic models that, as a result of a pandemic, may be endangered, such as the sharing economy model, popular since the previous financial crisis.

THE END OF GLOBALIZATION AS WE KNOW IT

The starting point for this analysis should be the fact that in spite of the fight against COVID-19, deglobalizing changes are progressing more rapidly. These processes began in connection with the growing strategic rivalry of the United States

4 The Kościuszko Institute wrote about the application of artificial intelligence technology to some of them in a report entitled *Sztuczna Inteligencja – AI made in Asia*, see more: https://ik.org.pl/publikacje/sztuczna-inteligencja-made-in-asia/, [online: 5.04.2020].

5 John Hendel, *After the virus: A 5G gold rush?*, https://www.politico.com/news/2020/04/02/coronavirus-5g-network-160296, [online: 5.04.2020].

6 *The Mobile Economy 2020*, GSMA, https://www.gsma.com/mobileeconomy/?utm_source=Organic_Social&utm_medium=Twitter&utm_campaign=Mobile_Economy_Report_2020, [online: 5.04.2020].

7 Izabela Albrycht, dr Joanna Świątkowska, *Przyszłość 5G czyli Quo Vadis, Europo?* https://ik.org.pl/publikacje/przyszlosc-5g-czyli-quo-vadis-europo-2/, [online: 4.04.2020].

8 Izabela Albrycht, *Koronawirus pozwala się mnożyć wirusowi cyberzagrożeń. Jak chronić się przed atakami?*, https://biznesalert.pl/izabela-albrycht-koronawirus-cyberbezpieczenstwo-praca-zdalna-5g-cyberprzestrzen/, [online: 4.04.2020].

and the People's Republic of China, and are manifested primarily in dynamic decoupling of global supply chains. In the course of these changes, we observe the nervous movements of Chinese entities to gain the largest space possible for further business presence in Europe. Europe is a particularly important area in this competition.

In order to discount the crisis, when creating strategies to fight the pandemic, individual countries and the whole European Union must assume that it is necessary to allocate resources in those areas of the economy that will ensure the best rate of economic and social return, while supporting the construction of strategic autonomy in every key dimension, which will also be affected by the effects of decoupling. This process is particularly evident in the digital supply chain.

> **In the new world, the digital dimension is already critically significant in terms of business continuity and the functioning of the state. If anyone doubted it, they certainly already recognize that technology has a nationality and having stable and uninterrupted telecommunications and IT services, as well as a secure supply chain in the ICT sector is a must.**

This issue in the context of the digital dimension was highlighted by the European Commission in the publication "Rethinking Strategic Autonomy in the Digital Age",[9] which wrote that "In the 21st century, those who control digital technologies are increasingly able to influence economic, societal and political outcomes. Policymakers around the world are waking up to the critical imprint that digital technologies have on their countries' strategic autonomy and a global race for technological leadership has ensued. Despite its many assets, the EU is in danger of falling behind in this race. This not only places its long-term economic prosperity at risk, but opens it up to a whole range of strategic vulnerabilities – all the more so against a backdrop of escalating geopolitical tensions." The so-called geopolitical European Commission, whose term of office began in November 2019, placed great emphasis on a digital strategy for Europe. In the face of the rapid digital transformation taking place during the pandemic, it can be expected that efforts to build digital sovereignty will be intensified. Poland should cooperate closely with other EU countries in this respect.

Global technology companies that in fact have become public utilities and are already permanently attached to the socio-economic system of countries and international institutions, have recently passed the test of reliability and responsibility. They will probably also be the entities for whom the crisis will be the least painful. The demand for their services not only will not decrease, but it will even increase and the companies themselves will be equal partners for countries in addressing global challenges. In the global technology race, however, agility and innovation will be the most important advantages, which is why it will become crucial for individual countries but also for technology giants to support the development of this sector of ICT and cybersecurity companies. The companies that invest significant resources in the development of their own products, as well as in research and development (national champions and SMEs) and that propose ground-breaking solutions, which, however, may be associated with some initial investment risk for the market (start-ups).

As far as Central and Eastern Europe is concerned, it is essential to continue the proposals outlined in the Digital Three Seas concept.[10] The region, after analyzing its competitive advantages, must also jointly take steps to seize the opportunity that decoupling brings, together with the increasing likelihood of transferring foreign investment in the modern technology sector from China to other places in the world,[11] as well as transferring production, more and more automated over time, from China, to other regions of the world.

In Europe, we must understand the crisis we are in, as it is understood by the Chinese – as a danger from which, however, new opportunities are emerging, in this case digital opportunities.

CYBER VIRUS

Another issue that needs to be raised in the context of the growing importance of technology companies, is the currently observed epidemic of cyber threats. Its range increases with the spread of the SARS-CoV-2 virus around the world. Although it should be seen as an indirect consequence of the pandemic, its costs will directly affect the condition of the global economy, and to a greater extent than before. We can already see an increase in the number of attacks in cyberspace targeted both at individual users (mainly working in home office mode), as well as at organizations facing the pandemic on the first battle front (medical centers). In other words, at the time when our attention is focused on the fight on the biological front, the digital battle between good and evil is increasingly fierce. While private internet users use a global network, devices, software and applications to continue their business activities, communicate with friends and family, buy products and services, cyber criminals are looking for vulnerabilities in the systems and devices we use in an attempt to steal our data, identity or money. Our online activity is increasing, as well as their activity.

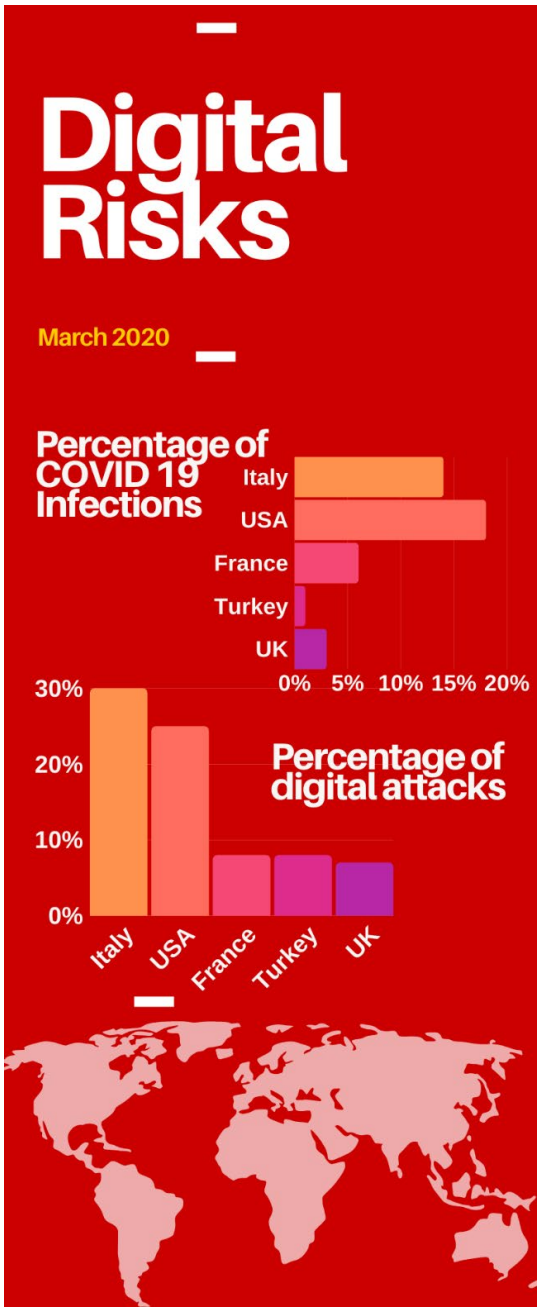
9 European Commission, *Rethinking Strategic Autonomy in the Digital Age*, https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategic_note_issue30_strategic_autonomy.pdf, [online: 28.03.2020].

10 Description of the initiative available on: https://digital3seas.eu/.

11 Izabela Albrycht, *Cyfrowa Zimna Wojna*, https://www.forbes.pl/opinie/cyfrowa-rywalizacja-miedzy-usa-a-chinami-komentarz-instytutu-kosciuszki/7kh4nhv, [online 28.03.2020].

At the same time, according to the SecDev Group, a direct correlation is visible between the number of infections in a given country and the increase in threats in cyberspace and digital attacks. The increase in incidence in Italy, the USA and France is accompanied by an increase in attacks in cyberspace, significantly increasing the digital risk profile in these countries (see Graphics 1). We also see that there has been a significant increase in the number of malicious attacks on medical facilities containing ransomware. Cybercriminals are flooding hospitals, medical laboratories, vaccine testing facilities and critical service providers by phishing and forcing some of them to shut down. Such attacks have already occurred in the United States, Spain, UK and France.

Graphics 1.



source: SecDev Group

Other forms of attacks invoked by SecDev include phishing attacks on companies and governmental administration forced to quickly move office work to homes where employees do not use adequate network security architecture and end devices. Also malicious applications and fake virus tracking websites, offering COVID-19 spread maps and analysis, that can steal user credentials are a threat. Data provided by SecDev indicate, that domains concerning the COVID-19 pandemic are 50% more susceptible to malware than other domains registered in the same period. However, particular sectors of the economy and institutions on the first front of the fight against the epidemic are particularly vulnerable to attacks. It is so because their employees are actively looking for information on COVID-19 and are more likely to click on malicious links or attachments, which makes them attractive targets for hackers. Such entities include hospitals and other health and epidemiological institutions, as well as central and local government administration, educational centers and research centers.

> **Cyber security companies have identified several entities actively involved in cyber-operations associated with the SARS-CoV-2 pandemic. Some of these entities, in their opinion, may be sponsored by states. They are, among others, Hades Group, operating outside of Russia with connections with APT28 (Fancy Bear), Chinese Mustang Panda and Pakistani APT36.**

In this situation, it is necessary to mobilize on both sides. Companies and institutions exposed to cyber-attacks have to implement secure solutions and procedures, while companies offering security solutions for ICT networks and systems have to mobilize to cooperate with public institutions and critical sectors of the economy, and within the sector cooperation, they should exchange information and know how.

At the same time, despite the fact that global technology companies show a great responsibility for the security of digital transformation during the pandemic, it is also a time of increased vigilance and strenuous actions for the companies that should aim at implementing security in the DNA of devices, systems, software, applications, platforms for communication and collective work, and many other digital facilities. Issues with security and privacy when using the ZOOM platform are a clear example of this.

As far as threats to network security are concerned, one should also perceive the issue of increased traffic and potential problems with the bandwidth of the Internet on these days. In this situation, telecommunication network operators and Internet providers have become a critical resource of the state on which the liquidity of business operations and the work of public administration depend. That is why steps should be taken today to develop the Internet network in Poland, which we have already emphasized in the previous part of the publication.

THE CRISIS AND THE DYNAMICS OF THE ICT MARKET

The epidemic crisis has forced many industries to rapid digital transformation related to the need for remote work and digitization of key processes. We are witnessing an express education in practice process of the entire market and society in the field of digital needs. We also observe an increase in threats to the security of network and information systems.

In the medium and long-term scenario, this will translate into an increased demand for both ICT and cybersecurity services and products in the world, as well as in Poland. At the same time, in the short term, probably at least until Q1 of 2021, the market will limit the purchase of solutions in response to demand and supply shock – which may even lead to the elimination from the market and bankruptcy of the entire segment of Polish SMEs/startups from the ICT sector, which in the vast majority do not have assets reserves to survive such a slowdown.

This negative scenario will mean that entities from markets with large assets, that have sufficient reserves, will survive the crisis and then in the medium and long term (Q4 of 2021, 2022/2023) will discount and monetize the demand of global and Polish economy for ICT and cybersecurity solutions, also due to the lack of significant competition from regional markets, largely depleted by the crisis. To remedy this, deliberate state action is necessary, also in cooperation with larger ICT companies.

At the same time, during the epidemic crisis, following the example of other countries, the government and security services should support the construction of cyber-coalitions of private companies and cooperate with them. Such coalitions have emerged voluntarily, e.g. in Canada – COVID-19 Cyber Defense Force, which provides hospitals, municipalities and critical infrastructure with a full package of cyber security services.[12] Similarly, in the United States there is Covid-19 CTI League and in the UK there is CV19, which focuses on prevention and response to threats in the healthcare sector – the sector that is particularly vulnerable and critically threatened by attacks.[13]

12 Further information on COVID-19 Cyber Defense Force: https://www.cisomag.com/canadas-cyber-defense-and-world-cti-league-fight-against-covid-19-cyberattacks/?utm_source=Rafal+AUDIENCE&utm_campaign=d5b59784b1-Covid19-John-Contacts-March-1_COPY_01&utm_medium=email&utm_term=0_6e92156d31-d5b59784b1-395352172, [online: 6.04.2020]

13 Further information on Covid-19 CTI League and British CV19: https://www.sdxcentral.com/articles/news/security-experts-battle-hackers-covid-19-cyberattacks/2020/03/?utm_source=Rafal+AUDIENCE&utm_campaign=d5b59784b1-Covid19-John-Contacts-March-1_COPY_01&utm_medium=email&utm_term=0_6e92156d31-d5b59784b1-395352172, https://cyberv19.org.uk/?utm_source=Rafal%20AUDIENCE&utm_campaign=d5b59784b1-Covid19-John-Contacts-March-1_COPY_01&utm_medium=email&utm_term=0_6e92156d31-d5b59784b1-395352172, [online: 6.04.2020]

NATIONAL ACTION NEEDED

In practice, at least 5 proposals of targeted support for the ICT and cybersecurity sector in Poland in the following months can be identified, which arose after consultation with companies associated in the initiative of the Kościuszko Institute supported by ZIPSEE named #CyberMadeInPoland:[14]

1. "Technology loans" or direct investments carried out by the Polish Development Fund or Bank Gospodarstwa Krajowego.

Low-interest or non-repayable express loans for SMEs and startups, depending on the assessment of the business value of a service or product from a key sector. A low-interest loan would be returned when the company earns revenues above a given ceiling over a certain time horizon (e.g. Q4 of 2021), if this not happens, the loan becomes non-repayable (the rule used in many countries for college loans). As far as Polish companies in the cybersecurity industry are concerned, if they enter foreign markets, a dedicated insurance and investment support offer should also be developed under KUKE.

Development fund operators should also consider, as part of anti-crisis measures, the possibility of direct capital entry, purchase of shares in case of interested companies from the domestic ICT and cyber security sector.

2. Support of the demand-supply model:

    a. System promotion of SME/startups as part of the digitization of public administration.

The support action may take many forms, including, e.g. establishing special non-price criteria in public proceedings promoting solutions offered by companies of Polish origin (compliance with the criteria gives the bidder additional points in the proceedings, but does not introduce preference for specific entities, in order to avoid the charge of limiting competitiveness), or introduction of certain system requirements, such as the need to obtain a bid from a Polish SME in every public procurement process. Another activity may be obliging specific entities responsible for the digitization of the public sector, e.g. COI, NASK, to cooperate with the SME/startups segment. Another idea developed by the Ministry of Digitization are the so-called public digital robots, which would enable companies to participate in processes related to the computerization of public administration. It is a solution that has more added value than the transfer of support funds for the functioning of these companies.

    b. In the medium term, support of traditional branches of the economy by stimulating the demand in the field of digitization.

14 Similar proposals have been put forward to the Council for Digital Affairs at the Ministry of Digital Affairs; the Council began working on the *Position on supporting the Polish ICT sector with regard to anti-crisis measures*, which is included in its resolution No. 4: https://www.gov.pl/web/cyfryzacja/dokumenty-rady-kadencji-2019-2021, [online: 16 April 2020].

In order to stimulate the demand, the state has a number of tools, including tax breaks or programs dedicated to purchases connected with the demand for specific solutions. An example of action ensuring the security of digital transformation in the country on the one hand, and supporting the domestic cybersecurity market on the other, may be the classification of expenditure on cybersecurity as expenditure on innovation (a dedicated investment relief for expenditure on cybersecurity could be created), which would enable CIT deduction, extension of the "Innovation BOX" use by reducing the level of taxation of income obtained from intellectual property rights to 10% and extending the scope to include costs of producing cybersecurity products.

A desirable action would also be the launch of the "cyber security vouchers" program, i.e. public funds available to local government units for the purchase of ICT security services or solutions prepared for them by Polish companies or research units.

3. Support for research and development activities by increasing immediately the levels of funding under existing and planned projects.

The National Center for Research and Development, the Polish Agency for Enterprise Development and the Industrial Development Agency as well as other agencies and institutions should reformulate the rules of both de minimis aid and public aid for key sectors, in particular cybersecurity and ICT. Levels of funding should be increased depending on the size of the company, up to 90-100% for SMEs and startups. It is true that if the allocated funds for specific R&D programs are not increased, fewer projects will receive support, but thanks to this another key goal will be achieved, i.e. maintaining the smoothness of project implementation. If such actions are not taken, the implementation of projects already functioning will be threatened (which will mean wasting millions of zlotys spent so far) and the interest in subsequent calls for proposals will decrease (which consequently, will cause a decrease in the innovation of the Polish sector). Project companies, due to the collapse on the market, are already facing problems in finding funds to complete R&D projects, although not even a month has passed since the beginning of the COVID-19 crisis. In the coming months, they will probably not be able to generate funds from the market to contribute at the level of 80% or 40% to ongoing R&D projects. To address this problem, state intervention is indispensable to change the funding rules.

4. Support in the form of introducing alternative ways of evaluating companies applying for EU funds.

The assessment of the advisability of supporting an enterprise based on its financial statements from the last year (or 3 years) will become a fiction in the scenario of a deep economic crisis. Due to the broader macroeconomic conditions, such a report in many cases will not reflect the value of a company or a technological idea. Therefore, in the next EU financial perspective, the implementation of which will begin during a period of significant economic slowdown, alternative forms of assessment of enterprises applying for support from EU programs, including regional operational programs, should be allowed. They can be based on the methodology used by incubation or acceleration programs – e.g. assessment by an expert panel regarding the business value of a solution or technology.

ACTIVITIES IN THE THREE SEAS REGION

> **The ongoing pandemic is also the highest time for the region of Central and Eastern Europe (CEE) to recognize the changes and adapt to them in the global economy brought by the extremely rapid digital transformation combined with geopolitical and geo-economic changes. This process should start with the ambitious development of digital infrastructure, including the construction of a fiberoptic connection with the USA as part of the implementation of the concept of the transatlantic cable "3Seas1Ocean" proposed by Exatel, followed by the concept of the Kościuszko Institute, i.e. the 3 Seas Digital Highway (3SDH) – one of the strategic projects under this Digital Three Seas initiative.[15]**

The development of digital infrastructure is not only necessary in the light of a further increase in demand for data transmission, but also because it can support the development of the digital economy and encourage companies to make investment decisions concerning the construction of data centers or relocation of science and research centers. The implementation of joint infrastructure projects should take place in parallel with the development of initiatives concerning modern technologies, especially in those sectors, where data is the most important currency, such as services based on cloud computing, the Internet of Things, artificial intelligence or e-commerce centers. A special VC Fund could also be created as part of the existing Three Seas Fund, which would be aimed at supporting entities from the ICT sector in the region and investment support for projects from key sectors.

Furthermore, the proposals already described in 2019 can be used to direct the technological potential of the CEE region so that it attracts foreign investments in the modern technologies sector. "This would help the countries of the region to make a civilizational leap. Threat in the form of economic

15 3SDH, which is inscribed on the list of priority projects at the Summit of the Three Seas countries in Bucharest in 2018, fills in the gaps in fiberoptic telecommunications infrastructure from the north to the south of the region. This international digital infrastructure, which could also be supplemented with 5G technology, should be implemented along with the Tri-Sea transport projects already planned (e.g. Via Carpatia).

stagnation, the so-called middle income trap, which could prevent CEE countries from catching up on economic backlogs, can be ultimately overcome thanks to the innovation and agility of economies. The development of modern digital technologies can be an important driving force of economic growth. Therefore, one of the strategic goals of the region should be climbing up the ladder of the global supply chain in the IT and cybersecurity sectors, as well as providing products and services with high added value. Therefore, the current challenge for the Three Seas countries is to prepare and implement development strategies directed not only at convergence, but also at high innovation, as well as at creating a balance between the development of traditional industry and investments in the modern technology industry.

> **The CEE region has enormous potential for digital competences necessary to support the development of new technologies such as artificial intelligence, the Internet of Things, robotization and automation. In order to implement them, it is necessary to support the development of qualified specialists and vocational retraining programs, data-based education and the development of broadly understood digital competences of the society. Recognizing the potential competitive advantages and dynamically developing product niches can help CEE to become one of the leaders of the technology race and thus gain a better position in the global value chain."[16]**

CONCLUSIONS

Even before the COVID19 pandemic, we observed changes in the power projection potential – soft and hard power, which are increasingly influenced by modern technologies. Digital technologies have become a very important factor determining the geopolitical and economic position of individual countries. The technologies increasingly condition potential of the countries, both in the defense and economic areas. Individual countries are beginning to understand the critical impact that digital technologies have on the strategic autonomy of their countries and stakes in the global race for a technological leadership. This is reflected in the strategies, regulations, incentives and investment decisions of the companies. For the reasons described in this publication, the Polish state, as one of the key sectors, should choose the broadly understood market of ICT solutions, including cybersecurity, as one of the main pillars of economic growth. The strategic challenge will therefore be the skillful and wise support of the domestic ICT and cybersecurity sector during the SARS-CoV-2 pandemic, the so-called "cyber virus" and the expected economic crisis, as well as putting these activities into EU modes. Those countries that understand and redirect the outlined opportunities and threats to the economic and financial crisis strategy, will overcome the crisis faster and have more opportunities to build their position in the region, and in case of powerful countries, in the world.

> **Remembering the ambitious economic projects of the Second Polish Republic, which, responding to the great crisis of the 1930s, was able to initiate a program to build factories, steel mills, metallurgical and processing industries as part of the Central Industrial District, let's not be afraid of bold visions in hard times. In response to challenges related to the economic crisis after the SARS-CoV-2 pandemic, the Polish state must create an appropriate program for the development of key sectors in the economy of the 21st century, in particular the digital technologies sector.**

We do not mean, however, attempts to build state-owned juggles, but an effective cooperation with the private sector, in which there is both knowledge capital, experience, and often knowledge of international good practices concerning such cooperation.

16 Izabela Albrycht, *Cyfrowa Zimna Wojna*, https://www.forbes.pl/opinie/cyfrowa-rywalizacja-miedzy-usa-a-chinami-komentarz-instytutu-kosciuszki/7kh4nhv, [online 28.03.2020].

The Kosciuszko Institute is a non-profit, independent, non-governmental research and development institute (think tank), founded in 2000.
The Kosciuszko Institute's aim is to influence the socio-economic development and the security of Poland as a new member of the EU and a partner in the Euro-Atlantic alliance. Studies conducted by the Institutes have been the foundation for both important legislative reforms as well as a content-related support for those responsible for making strategic decisions.
The Kosciuszko Institute organizes the European Cybersecurity Forum – CYBERSEC – the first conference of its kind in Poland and one of just a few regular public policy conferences devoted to the strategic issues of cyberspace and cybersecurity in Europe, and also publishes the European Cybersecurity Journal – a new specialised quarterly publication devoted to cybersecurity.
More on the European Cybersecurity Forum: http://cybersecforum.eu/
More on the European Cybersecurity Journal: https://cybersecforum.eu/en/about-ecj/.
Office: Wilhelma Feldmana 4/9-10, 31-130 Kraków, Polska, tel.: +48 12 632 97 24,
www.ik.org.pl, e-mail: instytut@ik.org.pl

Digital Poland Association is a non-profit industry-wide organisation of companies that represents the Polish digital and new technology sector. Under its banner are the largest RTV and IT companies operating in Poland. They are both producers, importers and distributors of electric and electronic equipment. The association actively works to, e.g., digitise the Polish economy and society by engaging in the adoption of law that helps develop the sector and in educational efforts to spread knowledge about the latest technologies.

#CyberMadeInPoland

Initiated by the Kosciuszko Institute, a special work group *#CyberMadeInPoland* affiliated with the Digital Poland Association was set up. Its goal is to bolster the cybersecurity sector development in Poland, and it consists of both firms that create digital security products and services and business environment institutions that focus on the subject matter. The team's main task is to spark interest in cybersecurity topics among both Poland-based companies and local governments or public administration bodies. *The initiative subscribes to the wider EU philosophy of striving to build Europe's "digital sovereignty".*
The *#CyberMadeInPoland* group is also going to work on launching a special-purpose fund for foreign expansion by Polish cybersecurity companies and on revamping the R&D grant offer so that it tangibly supports the development of globally competitive cybersecurity solutions in our country.
As part of the *#CyberMadeInPoland* group activity, the Polish government receives briefs of problems and challenges which the cybersecurity sector in Poland is facing.