INTERNATIONAL CONFERENCE RCIC'22
Redefining Community in Intercultural Context
Braşov, 5-7 May 2022

ECONOMIC DEVELOPMENT AND DIGITIZATION IN THE CONTEXT OF PANDEMIC CRISIS

Florian COLDEA*

* 'Mihai Viteazul' National Intelligence Academy, Bucharest, Romania

Abstract: *The current paper sets to explore the hypothesis that the COVID-19 pandemic is a strong incentive for accelerated digitalization and a significant shift in economy. The other hypothesis is that developments in those sectors under the novel pressures of a worldwide sanitary crisis also come with significant risks, which require increased attention from the national security establishment. In order to explore those hypotheses, the author has documented the overall highlights of the technological context – including the concept of SMART administration, some security developments during the pandemic – with a stress on the health system, but also on the infodemic that completely altered the course of recent events, while also providing some practical examples pertaining to the Romanian social reality.*

Keywords*: pandemic; infodemic; digitalization; administration; security*

1. METHODOLOGY

The approach of the current topic is not that of an expert in economy or technology, but rather from an intelligence practitioner`s perspective, focused on the general context caused by COVID-19 and its security implications. The paper is, generally, rather descriptive, as it is still too early to identify all the intricate consequences the ongoing pandemic will have, but does come with personal and empirical interpretations, based on practical experience and the author`s intelligence background. The sources are predominantly statistics, but also literature produced by technology experts.

2. TERMINOLOGY

It is important to delineate the overall terminology of the paper as it comprises significant differences among easily confused topics. *Digitization*, for one, is the conversion of data from analogue to digital. The author considers that digitization is one of the first stages for digitalization as it does not entail major developments in the business flows, but rather generates raw data. *Digitalization*, on the other side, means using technology and digitized data to change workflows in order to make them more efficient, from multiple perspectives, starting with increasing profits to reducing operational costs and involved resources in a particular activity. By allowing new workflows and new revenue sources, digitalization further supports *economic development*, therefore all three concepts are interconnected.

In Romania's case, the pandemic led mainly to *digitization* rather than digitalization, in many areas, at least in the first months of utter confusion and shock. For example, in the average citizen`s interactions with the administration, there was the punctual benefit of no longer leaving printed documents at the counter; in many cases, however, digital papers are sent by e-mail for further printing and processing by a clerk. What we actually need is digitalization - in the described case, an electronic form and automatic data processing, interaction with other data basis in order to collect readily-available information without requesting it from the citizen, automated responses wherever possible etc. While costly for private businesses, digitalization is particularly challenging and significant for public bodies and organizations, with even more limited resources and reduced capabilities, lacking experts and the finances that would motivate them, but in turn managing sometimes huge quantities of sensitive data in analogic form. For state bodies, digitalization does not provide immediate economic advantages, as it would with private organizations. However, states need it the most in order to boost their economies.

The challenge of the future for the Romanian public organizations – which is no longer such a novelty as there are many success models in other countries –will be the implementation of the concept of SMART city. This goal would have an extraordinary impact on building efficient and advanced communities, using the human capital and advancing towards sustainable development.

Relevant examples of what SMART cities can do for society as a whole come from most areas of our social life. For instance, in healthcare, they can provide effective communication flows among various medical institutions, helping to develop new services and improve cost-effectiveness. In education, new technologies support proficient pedagogy, leveling up the teaching process and ensuring fair and equal access to quality education; in isolated areas, electronic lessons can compensate for the lack of teachers or for their lack of expertise. Digitalized administration means less bureaucracy, less resources needed for its upkeep, easier interaction of the citizens with authorities, but it also facilitates opening and running legal, tax-paying business. The digitalization of SMART communities provides the proper environment for economic development of the private sector, too.

Romania's experience provides useful lessons for the Western Balkans in general and the Western Balkans candidate countries in particular in their efforts towards the EU integration. The digitalization as part of the Western Balkans transition towards a digital economy and society can bring tangible benefits not only in terms of economic growth and convergence with the EU Single Market, but also in terms of better rule of law, increased transparency and political accountability, strengthened democratic processes, enhanced regional cooperation etc. At the same time, the security implications of the digital transformation have to be carefully assessed, while effective measures should be implemented as early as possible in order to prevent or limit the disruptive impact of cyber incidents.

3. PANDEMIC IN AN ALREADY SHAKY WORLD

The COVID-19 crisis would not have been a full-blown crisis unless factors of various nature had not aggravated the consequences of the virus. Several traits of the world we have lived since December 2019 contributed to the current situation in manners unprecedented by most of the other pandemic situations of the past centuries.

First of all, our modern society`s characteristic trait is *openness* or the lack of virtual and practical barriers in many of its aspects. In analyst Fareed Zakaria's words (2020:14), pre-COVID, "the world was open, fast and unstable". Prior to the start of the pandemic we had free movement, real-time communication at low costs or no costs of all, high-speed connections and heavy interdependencies. We also had free markets while the information revolution allowed for the rapid movement of ideas, services, goods. Our world before the start of the pandemic had both many opportunities and major vulnerabilities.

Digital economy has been assumed all over the world for the past two decades. We are currently used with digitization and digitalization in most areas of our lives: online baking / finances, online shopping and e-commerce, digital administration reducing bureaucracy and intermediating the previously direct interaction between citizens and their state, working online, online entertainment etc. Those were all designed to save time and effort and to allow particulars not to leave their houses, unless they chose to.

This all happened in successive waves of technological advancements, with the regular, material economy giving way gradually to the digital one. Technology is irreversibly shaping our world and has an unprecedented impact on our everyday lives, in all relevant areas. It would be much to say, at this point, that in Romania digital economy prevails over the material one, but is safe to underline its tendency to develop.

We have also witnessed a paradigm shift – the private sector has taken the lead on technological developments and is driving the global innovation. This is an advantage given the large resources they can allocate and the high speed of the innovation processes. But, as we have already seen, this is also a challenge since not always the priorities and interests of private companies are aligned with those of the states.

Against this backdrop, the gap between the technological developments and the state's capacity to keep up with them can become a strategic vulnerability, increasingly difficult to address even by the global actors. This strategic vulnerability is particularly worrisome for countries that do not have the resources needed to keep up with the technological developments.

Moreover, democracies can have a harder time narrowing that gap than illiberal states or authoritarian regimes that do not concern themselves with democratic values or human rights. Some of the authoritarian regimes are even cooperating with or supporting, financially or otherwise, the private firms, to develop digital tools that could be used to strengthen their grip internally, repress or silence their critics, restrict individual liberties, advance their interests etc. In other cases, the authoritarian regimes deny access to technological or digital developments in an effort to preserve their power, prevent the spread of information, exert a strict control or censorship of the information sources etc.

In a highly interconnected world, pandemic meant unprecedented shutting down of economies and societies, thus more instability. Part of this instability is also generated by the overall context of major geopolitical shifts: aggravated competition among the great powers, transition from a unipolar to a multipolar world, tendency towards a new balance of power, but also enough reasons of conflicts and war, including asymmetric and informational war, some conflicts resulting in significant migratory waves.

Besides the virus itself, the author considers that there are two decisive factors in managing, but also, sometimes, in aggravating this unexpected health crisis: the first one, technology, and the second one, individuals themselves.

4. TECHNOLOGY, BOTH SOLUTION AND PROBLEM

As it has already been mentioned, digital transformation was propagating before COVID-19 appeared. It did some good, helping those in digitalized enough societies, to stay isolated and not miss some of the comforts they have previously enjoyed, but also in maintaining some sort of communication and keeping some parts of the economy running. Advanced technologies remain, nonetheless, a constant challenge both for the private sector – since they involve significant costs – as well as for the public one, particularly for intelligence institutions, which tend to have difficulties in keeping up with their opponents. Some managed to use it to their advantage, many – not yet. From the onset of the COVID-19 crisis, enough vulnerabilities that come with technology were stage-center. Probably the most familiar and worrying of all were:

– 5G technology, with many potential applications, ranging from economic to military ones; it means high speed data traffic, but also devices which are more susceptible to DDoS (Distributed Denial of Service) attacks or quicker disruption of servers. The famous Huawei debate had started before the pandemic to question the good faith or intentions of companies under control of strategic opponents; many countries have implemented measures to protect their own infrastructures by paying particular attention to equipment coming from insufficiently trusted producers.

– British telecom providers, for example, were prohibited from buying Huawei 5G equipment after December 31st 2020 and need to replace all Huawei equipment by 2027, with an estimated cost of 2 billion GBP, while Romania has very recently passed a law requiring the approval of the Supreme Council for National Defense in the process of acquiring 5G technology.

– In the Western Balkans, Serbia, "Kosovo" and North Macedonia had signed agreements with the US on 'trustworthy' 5G in 2020, while Albania has signed a similar document in June 2021, in view of Tirana's plans to implement a 5G network in the coming period.

– Cryptocurrency is also a pre-existing risk, with potential to aggravate while everybody is busy with the health crisis. It can generate tax evasion or money laundering, but also be used in financing illicit activities of all sorts.

– Quantum computing, while not yet a reality, can raise even more privacy concerns than we already have, since it will lead to the rapid annihilation or neutralization of most encryptions previously considered secure, such as blockchain.

Cyberspace has, for some time, been a territory for confrontation and conflict, suitable both for offensive and defensive actions. In 2019, the number of cyber-attacks was already high, with 31% of organizations having experienced attacks on their infrastructure. Out of those, 43% attacks were aimed at small businesses (Galov, 2019), and a company needed, on average, six months to discover data breaches. The same source anticipated the costs of cybersecurity by 2020 to be of over 5 trillion USD.

Under those circumstances, it is relevant to take a look at data from Romania and see how the pandemic impacted technological development and viceversa. One of the factors working in our favor has probably been the internet speed, among the highest in the world, but internet access, on the other side, seems lowest in the very areas where it has been needed the most during the pandemic: in rural, isolated and low-income areas:

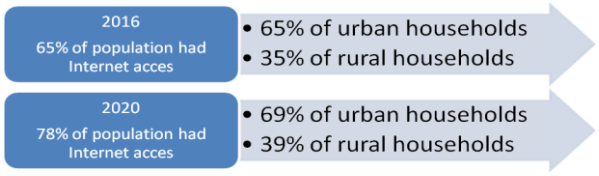

Fig.1 Internet access in Romania

Romania's **digital economy** has already been on a rising trend, but lagging when compared to other European states. Only 12% of Romanian enterprises had e-commerce activities in 2019, compared to the EU average of 17%, but the percentage grew to 18% during the first year of pandemic, similar to that of most EU Member States. The number of Romanian online shoppers was around 35% of internet users in

2017, and forcibly rose to 58%, in 2020 (Eurostat). COVID 19 accelerated digital retail, forced those who preferred the old manners of acting – going to stores or theaters, paying bills at the counter – to adapt. And what is true for individuals is also true for businesses, which acted the same.

But while the Romanian private sector made its best to adapt and survive during crisis, with e-commerce, its time and cost effectiveness, exploitation of increasingly sophisticated mobile devices and potential for increase, as probably the net winner, not the same can be said about using the maximal technological possibilities by the state sector. According to Eurostat, e-government individual activities on websites were only accessed by 9% of the Romanian population in 2019, compared to a EU average of 44%, with a significant increase in 2020, when 18% of the population accessed them, but way under the EU average of 48% (Eurostat). The acute need for actual digitalization of essential services was even more significant during 2020, despite the rapid shift of some activities online. The explanation resides in the lack of the necessary technical and procedural safeguards, as well as adequate staff training.

R&D would have been a key factor in developing the digital economy, but investments made in these areas by the Romanian IT&C sector were also lagging in the years preceding the pandemic, which should have been a reason for concern, too (Eurostat).

A similar digital leap was registered across the Western Balkans since the beginning of the pandemic, a very positive development since the economies in the area were lagging behind the European Union's digital transformation, with the gap narrowing slowly.

Due to economic slowdown in the last years, the region has made some, but not significant, progress in building digital economy and society. The support provided by the EU is gradually increasing the digital convergence between the Western Balkans and the EU member states, with initiatives such as the 2018 Digital Agenda for the Western Balkans and the 2020 Economic and Investment Plan for the Western Balkans (European Commission, 2020) contributing to lowering roaming costs, improving broadband connectivity, increasing cyber security, developing the e-Government, e-Procurement, e-Health, digital skills etc.

Studies conducted in 2020 in the Western Balkans indicate that the use of digital services increased most during the pandemic (between 37.8% and 42.6%) in the areas of entertainment, education, social networks and information, with only 14.3% when it comes to contacts with the administration (Bieber, 2020). The last statistic is not surprising given that, according to the same study, pre-pandemic data showed that one quarter of the population in most Western Balkan economies does not use the Internet at all. Moreover, the use of online administrative services is consistent with the low level of trust the Western Balkans citizens have in their government (no more than 30%) (World Bank, 2021).

Probably the best ally for the digital economy during COVID-19 was the **work from home** system. It replaced regular offices when the type of activity itself allowed for it, and brought surprising collateral benefits: less time wasted in traffic, less pollution, overall less resources used for the same activities. It was a major motor keeping the economy running: a Cisco study on 25 countries and over 4500 public and private organizations revealed 91% of them had at least 25% of all employees working remote at some point during the pandemic (Cisco, 2021). In the Western Balkans, the low level of digital transformation was reflected by the fact that only a quarter of citizens which worked from home used technology more than before the pandemic.

But there were several downsides to it, not considering the fact that some activities could not be transferred in this new system. Most organizations – public and private alike – were unprepared for the online shift; they had no proper security and privacy policies in place. To pinpoint Romania, Bitdefender senior researcher Cătălin Coșoi estimated that 50% of Romanian companies were not prepared to move their activity online when the pandemic started (Cosoi, 2022).

Working from home / online therefore proved to be both risk and opportunity. It boosted both digitization and digitalization, but it also came with an increased number of cyber- attacks of all sorts: based on social engineering techniques – phishing, smishing; attacks on e-learning platforms, ransomware etc. In Romania`s case (not particularized on working from home, but relevant overall), CERT-RO reported a number of 28.745.934 attacks captured by its sensors in infrastructures in 2020[1], with a trend of increased sophistication and frequency.

Various types of problems stemmed from the galloping rise in the digital economy, which, unfortunately, had to happen at a pace which put security and privacy concerns second.

[1] According to a statement by CERT-RO director general Dan Cîmpean at a specialzed conference in April, 2021.

– Careless employees were a significant source of problems, both in the private and in the public sector. 95% of data breaches worldwide during 2020 were attributed to human error by a Cyber Defense Magazine study (Galov, 2021), which shows there was a serious underestimation of the necessity and relevance of training regarding new technologies and also regarding the appropriate channels for sensitive information. Employees make security and privacy compromises either because they are unaware of risks, or in order to avoid further efforts. Thus, using unauthorized channels for confidential information, such as private e-mail addresses instead of the institutional ones, the lack of cyber security culture and enforcement of adequate security policies led to more vulnerabilities for employers worldwide.

– Security issues stemmed from insufficient security policies. In some cases, administrators do not enforce sufficient policies, in others, commercial applications are not concerned enough with devising sufficient layers of security, which leads to vulnerable systems and equipment and, in many cases, lack of integrated security solutions.

– Attackers exploited user and security weaknesses. Their motivations were, obviously, different:

o actors with financial motivations have exploited the context generated by working from home, through exfiltration of data, particularly credentials from personal or official bank accounts. In 2020's Romania, EMOTET was the most frequent type of malware attack of this sort (Buletin Cyberint, 2021) and it tried to exfiltrate financial data, generally starting from a spam e-mail message;

o actors with ideological motivations – hacktivism – normally have a lower technological level than other attackers, but they manage to block resources – particularly, in the state of health crisis, those of public health institutions. In many cases, they use ransomware.

Technology gained new meanings during the pandemic, becoming even more relevant than before for **health care** systems and providers worldwide. Video consultations became a necessity and were used as often of possible, despite former reluctance from both doctors and patients. Electronic prescriptions also became a reality.

Even more important, artificial intelligence, although still in the beginning and having its shortcomings, got more involved in providing health care services. First, its diagnosis capabilities were particularly useful as it compares cases to a much wider data-base than any specialist could do. It processes data for studies and provides them for multiple research teams, in almost real time, which was a crucial part in finding out more about the new virus and how to counter it. It also assists in interpreting imagistic data and has multiple applications in medical research and development. Rudimentary or more sophisticated robots also proved important in hospitals and clinics, when the risk of infection was practically zero if patients were visited by them instead of medical personnel.

Smart devices such as phones or watches help monitor essential functions for patients, such as heart rate or oxygen saturation, and, in some cases, they trigger alarms when the wearer experiences serious trouble, asking for urgent help on users' behalf. But to those opportunities technology brought for the medical systems worldwide, we must also associate significant risks that come with the interconnection our world prided itself on. Attacks on sanitary and medical systems surged. State and private entities became more and more interested in medical data, starting with those concerning research, development and innovation used in the vaccine making and accreditation processes, to top data from patient`s medical records or from big pharma. In December 2020 only, studies show a 51% increase of cyber-attacks against health-care providers, with a monthly average of 178 million attacks on medical organizations during the past year (Buzatu, 2020). Particular for the COVID-19 pandemic, there were data breaches – including at the World Health Organization, regarding vaccines and potential drugs to treat the new disease. Data were leaked online by attackers. Attacks on the vaccine supply chain and on the certification bodies were also frequent phenomena.

Other threats stemming from technological development during the first year of COVID-19 crisis were the Solar Winds attacks. Products of the IT software security solutions producer from the US were attacked by Russian hackers, thus compromising over 100 companies using Solar Winds services.

Illegitimate apps did their share of damage in COVID context. Invoking apparently legitimate and needed user information regarding the number of new cases or daily reports, they generally requested access to personal data, such as those from location or payment history. Malware from such apps infected predominantly mobile devices, and they exploited the fact that the app impersonated official ones. One such example was Covid 19 Tracker, which contains a malware of the ransomware variety. Covid Lock also blocks and encrypts data, requesting a bitcoin reward in order to release them.

Attacks on legitimate apps were frequent, too. Zoom and Skype were among the most accessed apps during the pandemic; while they are encrypted, in theory, there were data leakages as well as attempts to exploit their vulnerabilities by accessing device cameras and microphones for the purpose surveillance and trolling.

From the point of view of intelligence, dilemmas regarding surveillance and human rights were only heightened by the pandemic, when societies were confronted with new technological developments which again brought into discussion the old security – freedom dilemma. Personal health information was now needed in short time, in order to support policy-making and to enforce decision, and it took the odd form of applications of previously national-security-related technology being used for health-related purposes.

The trend was to accelerate the use of Artificial Intelligence for surveillance purposes, the most significant examples being those of Israel and China. Specially developed apps allowed for biometrical surveillance, localization, restrictions on free movement, thus building a new form of social control. Chinese authorities devised helmets that scan body temperature and have included facial recognition functions, cameras were used to monitor entrances into the homes of those under quarantine, and although, in some states, usage of such technology was voluntary, it raised serious and legitimate concerns regarding privacy.

From a strategic perspective, the pandemic made us rethink fundamental concepts we operate with, from globalization, freedom of movement and goods to sovereignty and, subsequently, our approaches in dealing with such global crises.

Closed borders, services and goods no longer available or that could not be delivered across the borders, disrupted transnational supply chains and boosted protectionist measures in regard to technologies, resources or products. All these developments have exposed the vulnerabilities and dependencies at the national and the EU level.

The importance of value chains (microelectronics, batteries, AI) in light of the current level of global digital transformation was particularly emphasized in the case of vital industries. Economic sectors dependent on human contact (automotive or aerospace industry for example) and the manufacturing industries have been the most affected during the first wave of the pandemic (their employees the most exposed to the virus). The ability of different industries and businesses to switch to digital was crucial for mitigating the impact of the pandemic and for their rebound.

At the European level, the COVID-19 crisis accelerated the initiatives towards strengthening the EU strategic sovereignty or autonomy, understood as the ability to act autonomously, to rely on its own resources in key strategic areas and to cooperate with partners whenever needed. Concrete projects were launched or are envisaged in different areas, from economy, energy policy, defense, including defense industry and security, climate action, external action etc.

5. THE INDIVIDUAL AT THE CENTER OF PANDEMIC

The pandemic has affected all areas of life as we knew it. Technology advances has generate both opportunities and risks, the material economy losing ground to the the digital one-businesses were disrupted, authorities were under pressure, while trade, travel, foreign investments and supply chains took serious hits. Vulnerabilities that never occurred to us – or did, but we did not do enough to reduce them - manifested on all levels of our lives, from the globalization phenomenon itself, to the simplest day-to-day activities which have not previously comprised such a threat.

The individual was at the center of opportunities: human knowledge and creativity has and will continue to be crucial in solving problems. At individual level, though, the psychological impact did significant damage. Processes of alienation and isolation or loneliness have already been manifested before 2020 due to the natural developments in our lifestyle. But, during the health crisis, individuals with psychological vulnerabilities, equipped with all facilities of modern communication, became both vectors and targets for threats and manipulation.

The infodemic - difficulty to process enormous quantities of data, not all of them real – became more and more prominent in the context of utter uncertainty. Faced with lack of scientific data, scientists needed to shift and adapt their positions to gradual findings. Political leaders, trying to follow the science, frequently changed policy, which generated further lack of trust and emotional reactions from regular people. The political consequences of those phenomena are obvious and they range from fear to renewed forms of isolationism. Groups of people started neglecting or rejecting evidence in favor of intuitive analysis, and this is, by no means, a new phenomenon, but it altered important decision-making regarding health; conspiracy theories flourished, while successful propaganda stimulated people to make bad decisions

regarding their own health and wellbeing, with impact on those of the others. Classic manipulation instruments were employed by various interested actors, distracting attention from key events with marginal hypothesis, promoting harmful ideas or theories that turn into problematic actions.

Technology and inherent human flaws merged and managed to aggravate the crisis. Social media facilitates organization of users around an idea – the bubbles – but the ideas are, in many cases, debatable, yet not debated. It allows for messages to be disseminated in closed, private groups, which are difficult to follow and to counter and debunk. Instead, closed groups allow for very quick spread of internet propaganda and fake news, which has a negative impact on several levels, from generating a crisis of trust to fake or exaggerated medical advice. Moreover, even outside the privacy of closed groups, the Facebook algorithm, for example, propagates content based on the number of views, not quality, veridicity etc., which promotes viral, but not necessarily scientifically accurate content.

It is true that some social media platforms took measures to counter the spread of COVID-related disinformation and misinformation. Facebook, for example, has dedicated staff, responsible for verifying and eliminating negative or misleading content. It also started informing users if they had contact with disinformation messages, but only if they liked or commented the respective content. There is also a Coronavirus Information Hub on Facebook, as well as a cooperation with WHO to run a COVID-19 chatbot. Whatsapp, on the other side, uses artificial intelligence to eliminate spam accounts and has limited the forwarding options for messages with disinformation potential.

Nevertheless, we are still fighting propaganda, manipulation, fake news with completely inadequate instruments. And some are particularly difficult to debunk: deep fakes, for example, are only an aspect of the fake-news phenomenon, but are credible because they involve manipulation of audio and video content in an almost undetectable manner.

The pandemic was not the beginning, but yet another argument for more solid instruments to counter the impact of disinformation and infodemic.

In a particular note, but of utmost interest for intelligence, is that isolation meant changes in the manifestation of some national security risks and threats, among which terrorism comes to mind. While there was an initial decrease in the number of actual terrorist attacks, online radicalization and self-radicalization have increased, which means complementary measures are necessary, both from the intelligence sector, and at social level (such as de-radicalization programs with significant educational and social assistance contributions).

Disinformation and fake news have found a fertile ground in the Western Balkans during the pandemic, diminishing the already low level of trust in the governments and the national institutions. Promoted by a wide range of actors through conventional channels and social media networks, several conspiracy theories flourished, one of them attributing the spread of the pandemic to the 5G technology.

6. LOOKING TOWARD THE FUTURE

I chose to stress two of the main factors with significant impact upon the digitalization and economy of the COVID world, technology and human reaction. And, while it is difficult to anticipate the best solutions to a crisis while in its midst, from the technological point of view I believe Romania has some advantages and needs to make proper use of them, in order to grow its geostrategic profile.

Cyber security is crucial to make the digitalization process productive and safe. And, in this regard, I need to stress the notable development represented by the establishment of a European Cyber-Security Competence Center (ECCC), on Romanian soil. The new institution will lead a Network of Cybersecurity Competence Centers proposed by the European Commission.

As mentioned before, we do have modern, fast networks, with rapid access to the internet, and, moreover, we also have a valuable talent pool, with worldwide recognized IT&C specialists.

But there are also flaws we need to strive harder to correct. The insufficient and inadequate, old legal and regulatory framework, for one. Despite the significant talent pool, we have insufficient staffing levels and difficulties with recruitment in public and private organizations alike, due to the brain drain phenomenon. We also have low budgetary allocations for cyber security, both in state institutions, and in private ones.

Again, from the intelligence perspective, we have difficulties with legacy infrastructures, which lack coherence, security policies and interoperability. There are also limited research and development enterprises and technological innovations, in spite of our national human potential.

This means that we need to support closer cooperation among CY authorities, the private sector and academia, in order to devise appropriate strategies and enforce proficient security measures. We must enhance information exchange among all involved parties, in order to develop capabilities and

joint response, and this must happen not only among domestic and foreign relevant actors, but also with the private sector.

The Romanian legislative and institutional framework needs to be updated as soon as possible, with at least a new law for cyber security and a new CY security strategy. Those need to be adequate to manage new technological arrivals, such as AI, 6G, machine learning, the internet of things, block chain technology, augmented virtual reality, quantum computing and the hybrid warfare. Cyber-attacks from state-sponsored actors, hacktivists or cyber terrorists/ cyber-crime will continue and become even more sophisticated, and without the proper legal, institutional and human resources, we will be unprepared to counter them.

Special attention must be paid, in my opinion, to education. We all need to educate ourselves regarding technology, learn the basics in order to keep safe. Building a cyber-security culture and awareness among technology users, developers, involved institutions is highly relevant. It would be my pleasure to stress that there are currently a number of post-graduate educational programs at prestigious Romanian Universities, including the West University of Timișoara, focused on cyber security. Public-private partnerships are also crucial to ensure all of the above.

In a more general approach of the future, I think data privacy will continue to gain relevance as the pandemic advances or ends. A CISCO study revealed companies have doubled their privacy budgets in 2020, to an average of 2,4 million USD (Cisco, 2021), and state bodies need to start increasing investments in this regard, too, in order to keep up with change.

The new technologies need to become more and more integrated in functional activities, both as defensive and as offensive instruments. Nevertheless, I think some negative effects will continue, particularly attacks aimed at the health systems, big pharma, on-line education process and online meetings / work from home.

Against this very complicated background, the national decision-makers have a decisive role. Based on the lessons learned during the last two years, they have to assess the vulnerabilities, especially in the vital industries / areas, to identify the resources and the capabilities needed to ensure the economic continuity and prevent the strategic disruptions in a new crisis situation, to put in place efficient, targeted measures adapted to the specificities of each area, and to ensure that these measures are implemented.

The National Recovery and Resilience Plans prepared by the EU Member States provide a huge, but very challenging, opportunity for carrying out during the next years structural reforms and public investments in the six priority areas agreed at the EU level, amongst which the digital transition.

For the Western Balkans, the investment in the digital transformation, with the support of the EU, is vital for the economic recovery, for accelerating the convergence with the EU Member States and the EU integration.

Given the increased importance attached by the EU to the rule of law in the new methodology for enlargement, digitalization will facilitate the efforts of the Western Balkans partners to strengthen their administrative capacity, reduce corruption in the public administration, implement data systems that could increase the cooperation between the national competent authorities, and thus improving the fight against organized crime, cyber-attacks or terrorism. The security implications of the digital transformation in the region have to be carefully assessed, especially when it comes to investments in critical IT&C infrastructures.

Enhancing cybersecurity capabilities and implementing robust cybersecurity measures are particularly important, as highlighted by the highly disruptive consequences of recent cyber-attacks. The EU toolbox regarding cybersecurity risks to 5G networks and other EU standards or recommendations in the area have to be taken into account when drafting the security measures.

Adaptability and preparedness have become key conditions for keeping us with the pace and impact of digital transformation. This particular pandemic managed to **accelerate history,** but faster sequences of events leave loopholes that generate new vulnerabilities and chain reactions, propelling negative effects too. Therefore, we all need to contribute and do our best to avoid cascading failures (if I am allowed to use yet another software term, although I am not an expert).

BIBLIOGRAPHY

1. Bieber, Florian. (2020). *The Digital Leap. How COVID19 Transformed the Digital Future for the Western Balkans.* Berlin: Ostausschuss der Deutschen Wirtschaft e.V. / German Eastern Business Association.
2. Buzatu, Ciprian. (2020). Știrile săptămânii din cybersecurity (14.01.2020). *Directoratul Național de Securitate Cibernetică* [online]. Available: https://dnsc.ro/citeste/stirile-saptamanii-14-01-2020 [Accessed June 11, 2021].
3. Cisco. (2021). *Forged by the Pandemic: The Age of Privacy.* San Jose, CA: Cisco Secure.

4. Cosoi, Alexandru Cătălin. (2022). A private sector perspective on ransomware, its threats and evolution aver time. *Council of Europe* [online]. Available: https://rm.coe.int/bitdefender-perspect ive-on-ransomware/1680a4965f [Accessed April 15, 2022].
5. European Commission. (2020, October 6). *An Economic and Investment Plan for the Western Balkans* {SWD(2020) 223 final}. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions COM(2020) 641 final. Brussels: European Commission.
6. European Union. (2022). E-government activities of individual via websites. *Eurostat* [online]. Available: https://ec.europa.eu/ eurostat/databrowser/view/ISOC_CIEGI_AC__custo m_89001/bookmark/table?lang=en&bookmarkId=311 6213b-5aff-4cd4-8a16-596c80c17f18 [Accessed June 10, 2021].
7. Galov, Nick. (2019, March 21). Cyber Security Statistics for 2019. *Cyber Defense Magazine.* [online]. Available: https://www.cyberdefense magazine.com/cyber-security-statistics-for-2019/. [reading time].
8. World Bank (2021). *Europe and Central Asia Economic Update, Spring 2021: Data, Digitalization, and Governance*. Washington, DC: World Bank
9. Zakaria, Fareed. (2021). *Workbook for Ten Lessons for a Post-Pandemic World.* New York: Penguin.
10. ***. (2021). EMOTET, amenințare cibernetică prevalentă în 2020. *Buletin Cyberint.* No.1. 6.