DOI: https://doi.org/10.46793/6461-101.488L
Scientific Review Article

"CYBERWORLD" AND THE GREEN ECONOMY - HELP AND DANGER, SUPPORT AND FRAUD

Dragana Lazić
Faculty of Business and Law, MB University, Belgrade

e-mail: dragana1908@yahoo.com
https://orcid.org/0000-0001-6227-139X

Živanka Miladinović Bogavac
Faculty of Business and Law, MB University, Belgrade

e-mail: zivankamiladinovic@gmail.com
https://orcid.org/0000-0003-0477-8277

Jelena Vuković
Faculty of Business and Law, MB University, Belgrade

e-mail: vukovic.jelena2@gmail.com
https://orcid.org/0000-0002-6993-6267

Abstract: In the world as we know it, at the time of writing this paper, it is unimaginable for us to live, do business, communicate, socialize, or rest, without using some resource of the "cyber world". Which resource we use the most, out of all the resources on offer, (digitally literate people, academically educated people in the field of digitalization, a home „flooded" with digital devices, a business environment based on digitalization...) - it is difficult to decide. And is such an environment safe, ethically, morally and legally acceptable, is this environment exactly the environment that encourages us to develop and research or is it an environment that creates "digital slaves" of us, is this the environment that we want for our descendants? And this is a question that provokes many contradictory views. That is why the authors decided to provide answers to the questions posed above and contribute to resolving the aforementioned dilemmas. Namely, managing micro or macro communities with the help of digitalization can be considered a great relief. However, the issue of the security of such management and the community managed in this way remains questionable. Therefore, the main goal of this paper is to provide answers, with the help of scientific

methods, to the questions of who prevails: sustainable development or cyberspace - is digitalization our chance for success or the fear that paralyzes us? Our society is capable of noticing all the benefits and positive effects of digitalization, but is it aware and capable of recognizing and analyzing the dangers that come with it? With the help of scientific methods, the paper provides answers and clarifies the previously mentioned dilemmas, with an explanation of the most common risks and dangers that occur in our country and in neighboring countries, but also, in the last part of the paper, recommendations and advice for improving the functioning of the researched area are provided.

Keywords: *computer fraud, computer sabotage, cybersecurity, digitalization, green economy, human resources.*

INTRODUCTION

The terms "sustainable development", "green economy" has become part of everyday communication, and you can hear and read information about this phenomenon. Nature has forced man to think deeply about the consequences of his decades of careless behavior, and to realize the hard way, through the ruthlessness of nature (floods, fires, etc.) or human reckless, stubborn decisions (wars, conflicts, etc.), that he cannot have a greater friend or enemy than nature. Using advanced technology, man intended to turn nature into a subject, a servant, but he failed, and humanity finally realized that it must live in harmony with nature and listen to its needs.

Information technologies, artificial intelligence, the entire "cyber world" have harnessed their joint forces to outwit natural forces, to predict them, to control them, and we are witnesses that even to this day they have not succeeded in doing so. And the cause and reason for this is always man. Namely, man is the one who exploits nature, man is the one who wants to master nature and use the best that nature has to offer through technology and technique, but in the end, it is always man who suffers when that same nature "rebells". Therefore, the aspiration of all humanity is to find a compromise way of functioning with nature, a way in which nature will provide a safe and pleasant environment for people, and people will respond to it by preserving it. Finally, we have the feeling that awareness of the obligation to preserve nature has been raised to a higher level.

However, despite this, man finds a way to use technology and techniques ideally, but also to misuse it. So today, we come to fraud, sabotage, diversion and everything that can be done in a conventional way, but also using digital technology. Man as the main resource, as the initiator of all these processes, noticed the problem, tried and found a solution and chose the right path in solving global environmental challenges, but at the same time developed systems that threaten the stability and security of the sustainability of the green economy. It is man who is both the cause and reason for

the existence of environmental crises, and it is man who devises and improves measures for the implementation of the green economy or sustainable development, but it is also man who commits the most abuses in this area. Therefore, we detect human resources as the biggest problem, but it must be established which aspect of human resources represents the greatest danger in this area (De Busser, 2025) – is it ethics, morality, education, upbringing or something else? (Ran et.al, 2022)?

RESEARCH RESULTS - DETECTED PROBLEMS

Energy efficiency, smart cities or any other segment of sustainable development (Alevizos & Stavrou, 2023; Antczak 2024), sustainable future (Burke, et.al 2024) or green economy increasingly relies on and uses digital technology and digital resources in its functioning. Along with the development of digitalization, cybercrime is also developing. Based on this, we detect the weaknesses of digitalization. Smart cities, smart buildings, smart apartments, etc., can function perfectly and make people's lives easier. And not only make it easier, but also improve it. However, failure to control these "digital omnipotent resources" can lead to paralysis of all the "smart" things that we have previously listed (but also many more that we have not). Cyberattacks can lead to a complete collapse of the entire infrastructure of the green economy, they can endanger numerous projects or lead to intrusions into systems that are entrusted with all the data necessary for the smooth functioning, smooth implementation of the sustainable development strategy. Therefore, digital security becomes a full-fledged competitor to the green economy.

We have witnessed that failures in the implementation of green economy projects have already occurred, and since the process of digitalization of countries and cities has advanced considerably and is unstoppable, it is to be expected that such incidents will occur more and more, which is why it is necessary to point out the importance of cybersecurity, digital security, and digital literacy.

Modern green technologies and their application through solar systems or eco-structure is completely based on digital systems. This indicates that just one cyber attack, a successful attack, can disrupt the production and distribution of renewable energy. Cybercriminals can falsify various certificates or data, reports, and thus lead to a misconception, or a wrong idea about the real state of affairs and influence the making of (wrong) decisions at multiple levels (state, local, company, etc. and in multiple different areas (Wan, Cui, 2025). Also, financial fraud is not uncommon (Zhang, 2025). Through cybercrime, it is possible to create fake projects dealing with renewable energy sources and the green economy, while in fact the money allocated for such projects is redirected to other (most often criminal) activities.

Cybercrime does not choose areas and spheres of human life and work, so the target of an attack can be anyone or any area. Waste management systems represent a very risky area in which the activities of cybercriminals can be disastrous for the

entire society. This behavior can lead to natural disasters and large-scale environmental contamination (Chakraborty, et.al, 2024). The right to a healthy environment is a right guaranteed to us by the highest legal act, the Constitution of the Republic of Serbia. Therefore, such cyber activities can lead to the violation of constitutionally guaranteed rights. This problem can be even more serious. Damage to smart systems for monitoring climate change or changing data, introducing viruses into monitoring systems can lead to situations that are dangerous for all of humanity. If such abuses are not discovered in time, scientists who are engaged in research on this topic can be led to completely different conclusions, incorrect conclusions, and then this leads to the ruined reputation of science, to a decrease in the level of trust in science and scientists.

In support of our appeals, we will cite examples and potential vulnerabilities that have been or could cause by weak digital protection. For example, 10 years ago, in 2015, Ukraine suffered a cyber-attack on its energy infrastructure. As a result of this attack, 230,000 people left without electricity at one point. Organized cyber-attacks disabled several Ukrainian energy companies, thus disrupting the functionality of this system. There have been similar attacks in other countries, some with less success, some with more.

Even developed countries, rich countries, which distribute a large part of their funds specifically for improving the environment and living environment, are not immune to cyber-attacks. Germany also faced an attempted attack on energy systems, but due to large investments in digital security, this action stopped short of an attempt. It is common for websites and platforms to create that offer to function as intermediaries or consultants for "green investments" in completely natural and ecological projects, and after citizens pay the money, they disappear and lose all trace of them. Factories or companies often falsify reports on CO2 emissions through digital systems and adjust data to obtain right certificates that later enable them to conduct their business (illegally) without hindrance, while endangering the green economy. We can list such examples endlessly, but we believe that this is enough for readers of any educational level and orientation to understand the importance and seriousness of the subject of research.

DISCUSSION

Analyzing the problems in other countries, we considered it necessary to dedicate a part of the work to the Republic of Serbia and to establishing the factual situation regarding this issue on our territory. Namely, cyber terms are not present in our legislation, because our country has opted for the term high-tech crime. In order to combat this phenomenon, it has also formed special departments in the prosecutor's office and in other bodies whose job description includes combating crimes committed through "high" technology.

The regulation that appears in this area, and which is primary and most important for detecting such abuses and punishing perpetrators of criminal acts, is the Criminal Code of the Republic of Serbia. It prescribes criminal acts and their forms, determines sanctions, but also clarifies what is considered under the terms "computer data", "computer", "computer system", "computer program", "computer virus", etc.

Following the Council of Europe Convention on Cybercrime (Budapest Convention), the Republic of Serbia has taken steps to include criminal offences closely related to this topic in its legislation. Such criminal offences exist in several areas, such as criminal offences against computer data security, criminal offences against sexual freedom, criminal offences against intellectual property and others. Of course, it should note that other conventional criminal offences can also be committed via the Internet, i.e., a computer or similar data transfer device can used as a means of committing a criminal offence.

In accordance with the obligations assumed under the aforementioned Convention (Bjelajac, Matijašević & Dimitrijević, 2012), The Republic of Serbia has included eight criminal offenses in the field of computer data security in its legislation, namely: Damage to computer data and programs (Art. 298), Computer sabotage (Art. 299), Creation and introduction of computer viruses (Art. 300), Computer fraud (Art. 301), Unauthorized access to a protected computer, computer network and electronic data processing (Art. 302), Prevention and restriction of access to a public computer network (Art. 303), Unauthorized use of a computer or computer network (Art. 304), Creation, acquisition and provision to another of means for committing criminal offenses against the security of computer data (Art. 304a). For the aforementioned criminal offenses that have the security of computer data as the object of protection, the legislator has most often provided for a fine or imprisonment of three or five years, depending on the nature of the offense, the severity of the consequences, the characteristics of the passive subject and other privileging or qualifying circumstances.

In relation to crimes against sexual freedom, two criminal offenses have been added: Displaying, obtaining and possessing pornographic material and exploiting a minor for pornography (Art. 185) and exploiting a computer network or communication by other technical means to commit crimes against sexual freedom against a minor (Art. 185b). The legislator has decided that the adequate criminal sanction for such crimes is a fine and imprisonment for five or eight years, depending on the characteristics of the passive subject and other circumstances of the case.

In addition to the above, the Criminal Code of the Republic of Serbia also holds five criminal offenses that attack intellectual property as a protected object and are closely related to high-tech crime. These are: Violation of the moral rights of authors and performers (Art. 198), Unauthorized exploitation of a copyrighted work or subject matter of related rights (Art. 199), Unauthorized removal or modification of electronic information on copyright and related rights (Art. 200), Infringement of the right of invention (Art. 201) and Unauthorized use of another's design (Art. 202). When we analyze the criminal sanctions imposed for criminal offenses against intellectual

property, they are a fine or imprisonment for up to three years - for some more serious forms of the crime.

There is a great social dilemma as to whether it is necessary to increase criminal sanctions for such crimes, whether it is necessary to introduce new forms due to the rapid development of technology, bearing in mind the consequences that such crimes can cause. If we look at the examples we mentioned in the previous part of the paper, we can easily see that other crimes can be committed in this or a similar way, or the examples mentioned irresistibly remind us, by their description, of other crimes from other areas. For example, if someone commits a criminal offense that jeopardizes the security of the Republic of Serbia by "demolishing, setting fire to, or otherwise destroying or damaging an industrial, agricultural, or other commercial facility, means of transportation, device or facility, communication system device, public water, heat, gas, or energy utility device, dam, warehouse, building, or any other facility that is of greater importance for the safety or supply of citizens or for the economy or for the functioning of public services" – as was the case with Ukraine – should he be viewed as a cybercriminal or as a person who committed the criminal offense of sabotage, or both? For this type of behavior, the legislator in the Republic of Serbia has provided for a prison sentence of five to fifteen years in prison, so perhaps we should raise social awareness about this a little more. Just as, in the same light, the criminal offense of sabotage should also consider.

In addition to the above criminal offenses, the authorities responsible for high-tech crime also have other related criminal offenses under their jurisdiction, which are: criminal offenses against property (extortion, blackmail), criminal offenses against the economy (counterfeiting money, forgery of securities), criminal offenses against legal traffic (forgery of documents, special cases of forgery of documents), criminal offenses against human and civil freedoms and rights (coercion, abuse and torture, persecution, endangering security), criminal offenses against sexual freedom (sexual harassment, inducing a child to participate in sexual acts), criminal offenses against public order and peace (unauthorized organization of games of chance, causing panic and disorder), criminal offenses against the constitutional order and security of the Republic of Serbia (calling for a violent change in the constitutional order, inciting national, racial and religious hatred and intolerance).

ANALYSIS OF CASES IN THE TERRITORY OF THE REPUBLIC OF SERBIA

Pointing out cases of combating cybercrime in neighboring countries, we did not forget to mention the problems faced by the Republic of Serbia. In the last few years, the Republic of Serbia has also been facing problems in cyberspace that are so well organized and managed that they have managed to shake the foundations of digital security in the Republic of Serbia.

For example, last year, in 2024, a cyber-attack hit the Electric Power Company of the Republic of Serbia, the main and crucial energy factor in the country. This attack aimed to endanger the infrastructure network, which could have led to an interruption in the supply of electricity to users. By the term user, we mean not only households, but also important commercial facilities whose interruption of electricity supply would cause enormous damage to the country's economy. The attack took place via infected email, and on that occasion a huge part of the company's confidential data, contracts, reports, financial documents, stolen. So, the energy system not blocked, its operation not interrupted, but data destroyed and stolen. Is there any greater damage than that?

The first of the major cyber-attacks on the city and its infrastructure occurred in Novi Sad in 2020. In March, unknown perpetrators managed to penetrate the infrastructure of local institutions and block access to all relevant files on the city system. In addition to making the work of the entire administration more difficult, personal data of citizens stolen. Research shows that other countries often meet such attacks (Katagiri, 2023, Hansen, 2024).

The attacks did not stop, they repeated periodically, and one occurred in 2022 when the target of the attack was the cadastre and its entire central system that records data on all property rights and transactions. If we consider the fact that the most important human rights are the right to property, to its unhindered acquisition, disposal, and circulation, then we can see the seriousness of the attack. "Cyber warriors" successfully penetrated the central cadastre system and seriously damaged it, thus causing difficulties in its updating and maintenance. The integrity of property data at that moment seriously violated. The examples clearly show that no one is immune to the potential dangers lurking on the Internet, but it is necessary to understand the seriousness of these threats and take right steps to protect ourselves. At the time of writing this work, the city of Belgrade is also facing this same problem.

We would like to point out that we have listed only those examples where the state is at risk, and that there are endless individual examples of abuse through internet technologies. In addition to all the above, other research is also particularly worrying, as it clearly shows that the Republic of Serbia appointed as a high-risk country in terms of cybersecurity. Research shows that according to the level of risk from cyber threats coming from the internet, the Republic of Serbia and its users ranked in a high ninth place in the world. Which countries are a companion to the Republic of Serbia on this list presented in the picture below:

	Country/territory*
1	Greece
2	Peru
3	Ecuador
4	Qatar
5	Tunisia
6	Belarus
7	Algeria
8	Bosnia and Herzegovina
9	Serbia
10	Sri Lanka
11	Moldova
12	South Africa
13	Bangladesh
14	Morocco
15	Nepal
16	Bolivia
17	Kenya
18	Philippines
19	Argentina
20	Slovakia

Image 1. The TOP 20 countries where users face the greatest risk of online infection

Source: https://www.techzone.rs/2024/12/05/sajber-napadi-u-srbiji-tokom-2024-godine-kaspersky/

CONCLUSION

The authors of the paper started from the assumption that in the era of digitalization, cyber technology is a double-edged sword for the green economy. Neither can do without the other, and no one threatens them more than the other. From one perspective, digital solutions enable a much more efficient functioning of the green economy, and from another perspective, it seems that just one wrong or malicious (often both) step can lead to the collapse, or at least to a slowdown in sustainable development.

Smart networks, remote management of entire systems, digitalization of all processes, digitalization of archives and archival materials, innovations – all of this has come about thanks to digitally literate human resources, but also, all of this can disappear, endanger the existence of the human community, precisely through the misuse of acquired knowledge. Therefore, it is first of all necessary to work on ethics in the digital space, on codes of conduct and honesty of all users of these systems, and especially people responsible for the security of the virtual space. We believe that ethics and responsibility in the cyber world are two key factors that should be insisted on and improved.

The regulation that has been included in the legal system of the Republic of Serbia is good and at a satisfactory level, it follows the obligations that the Republic of

Serbia has undertaken at the international level, but the implementation is of questionable quality, and the level of efficiency and education of people involved in combating cyber-attacks needs to be raised through constant training. Only personnel with a lot of experience and personnel who are up to date with world events and are timely informed and familiar with the latest technological achievements are able to respond to abuses in the cyber world. Of course, in addition to knowledge and experience, appropriate equipment is necessary, which also needs to be improved and innovated. The biggest problem in all of this is the limited budget of the Republic of Serbia, because we are a country that is still in the process of transition and Europeanization.

Cybersecurity is no longer a technical, secondary issue, it represents one of the strategic pillars of sustainable development and if we want to modernize the state and the environment, it is necessary to act towards the development of a secure cyber environment. For this reason, cyber risk must not be separated from the green transformation, because if we want to be a developed state with a green economy, we must not allow cybersecurity to keep pace with cyber risk, but must stay one step ahead. Therefore, preventive action that our criminal justice system proclaims as the last link in protection is also applicable in this area. Digital infrastructure must serve as a carrier of ecological progress, and not represent its "Achilles heel". We are increasingly certain that major wars in the future will be fought in exactly this way (Burton & Christou, 2021, Roche & Blaine, 2023), without the use of conventional weapons, without a bullet fired, but with unforeseeable consequences.

REFERENCES

1. Alevizos, L., & Stavrou, E. (2023). Cyber threat modeling for protecting the crown jewels in the Financial Services Sector (FSS). *Information Security Journal: A Global Perspective*, *32*(2), 134–161.
2. Antczak, J. (2024). Determinants of business management in the digital age. *International Journal of Contemporary Management*, *60*(1), 17–26.
3. Bjelajac, Ž., Matijašević, J., Dimitrijević, D. (2012) *Konvencija Saveta Evrope o visokotehnološkom kriminalu.* Evropsko zakonodavstvo, [Council of Europe Convention on High-tech Crime. European legislation] XI (42). pp. 37-52.
4. Burke, W., Stranieri, A., Oseni, T., & Gondal, I. (2024). The need for cybersecurity self-evaluation in healthcare. *BMC Medical Informatics & Decision Making*, *24*(1), 1–15.
5. Burton, J., & Christou, G. (2021). Bridging the gap between cyberwar and cyberpeace. *International Affairs*, *97*(6), 1727–1747.
6. Chakraborty, A., Banerjee, J. S., Bhadra, R., Dutta, A., Ganguly, S., Das, D., Kundu, S., Mahmud, M., & Saha, G. (2024). A Framework of Intelligent Mental Health Monitoring in Smart Cities and Societies. *IETE Journal of Research*, *70*(2), 1328–1341.
7. De Busser, E. (2025). Human Rights in Technology--A Need for a New Norm. *Case Western Reserve Journal of International Law*, *57*(1/2), 109–138.

8. Hansen, F. S. (2024). The Russian approach to peacekeeping. *International Affairs*, *100*(3), 1023–1042.
9. Katagiri, N. (2023). Hackers of critical infrastructure: expectations and limits of the principle of target distinction. *International Review of Law, Computers & Technology*, *37*(3), 274–293.
10. Krivični zakonik, Službeni glasnik RS,[Criminal Code of the Republic of Serbia, Official Gazette of the Republic of Serbia] br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019 i 94/2024.
11. Ran, Y., Hou, Y., Dong, Z., & Wang, Q. (2022). Moral Observer-Licensing in Cyberspace. *Behavioral Sciences (2076-328X)*, *12*(5), 148.
12. Roche, E., & Blaine, M. (2023). The Folly of Cyber War. *Journal of International Affairs*, *75*(2), 131–143.
13. Wan, A., & Cui, W. (2025). Has the green total factor productivity increased in the early stage of the establishment of smart city? *PLoS ONE*, *20*(5), 1–30.
14. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala Službeni glasnik RS, [Law on the Organization and Competence of State Bodies for the Fight against High-Tech Crime, Official Gazette of the RS],br. 61/2005, 104/2009 10/2023 i 10/2023 - dr. zakon.
15. Zakon o potvrđivanju dodatnog protokola uz konvenciju o visokotehnološkom kriminalu koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko računarskih sistema, Službeni glasnik RS, [Law on Ratification of the Additional Protocol to the Convention on Cybercrime, relating to the criminalization of acts of a racist and xenophobic nature committed through computer systems, Official Gazette of the Republic of Serbia] - Međunarodni ugovori, br. 19/2009.
16. Zakon o potvrđivanju drugog dodatnog protokola uz konvenciju o visokotehnološkom kriminalu o pojačanoj saradnji i otkrivanju elektronskih dokaza, Službeni glasnik RS, [Law on Ratification of the Second Additional Protocol to the Convention on High-Tech Crime on Enhanced Cooperation and Discovery of Electronic Evidence, Official Gazette of the Republic of Serbia]- Međunarodni ugovori", br. 7/2022.
17. Zakon o potvrđivanju konvencije o visokotehnološkom kriminalu, Službeni glasniku RS, [Law on Ratification of the Convention on High-Tech Crime, Official Gazette of the Republic of Serbia], br. 19 od 19 marta 2009.
18. Zhang, J. (2025). Digital economy, green finance, and economic resilience. *PLoS ONE*, *20*(2), 1–24.