SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2023
ORGANIZATION AND MANAGEMENT SERIES NO. 182

TRANSFORMING UNDERGROUND COAL MINE WORKINGS INTO CRITICAL CYBER SECURITY FACILITIES IN THE PERSPECTIVE OF THE EUROPEAN GREEN DEAL PLAN

Robert HILDEBRANDT[1], Ryszard MARSZOWSKI[2*], Zbigniew LUBOSIK[3],
Sylwia JAROSŁAWSKA-SOBÓR[4]

[1] Central Mining Institute National Research Institute Katowice; rhildebrandt@gig.eu,
ORCID: 0000-0001-5700-166X
[2] Central Mining Institute National Research Institute Katowice; rmarszowski@gig.eu,
ORCID: 0000-0002-2855-7121
[3]Central Mining Institute National Research Institute Katowice; zlubosik@gig.eu,
ORCID: 0000-0002-0329-3940
[4]Central Mining Institute National Research Institute Katowice; sjaroslawska@gig.eu,
ORCID: 0000-0003-0920-6518
*Correspondence author

> I believe that if you show people problems and provide solutions,
> you will stimulate them to take action.
>
> *Bill Gates*

Purpose: in the cognitive space, the article focuses on cybersecurity as one of the top priorities of the European Commission and a cornerstone of a digital and connected Europe. The increase in cyberattacks during the coronavirus crisis has shown how important it is to protect hospitals, research centers and other infrastructure. Decisive action is needed in this area to future-proof the EU's economy and society. Therefore, cybersecurity is a key element to ensure the safe and effective implementation of the European Green Deal plan.

Methodology: the theses presented in the article were verified using the following methods: literature review, critical analysis of literature, analysis and comparison of documents and an example of good practices.

Result: the results of analyzes and research clearly revealed that cyberattacks do not stop at state borders, therefore it is necessary to strengthen cooperation between EU Member States, exchange information on threats and develop common standards and best practices in the field of cybersecurity. This allows for effective protection against attacks and minimization of risk to critical infrastructure related to the European Green Deal.

Originality: in the perspective described in the article, important and significant challenges arise in the field of protecting critical infrastructure against cyber threats. One of them is the transformation of underground workings of hard coal mines into facilities critical for national cybersecurity. The theses presented in the article were verified using the following methods: literature review, critical analysis of literature, analysis and comparison of documents and examples of good practices.

Keywords: transforming, coal, cyber security.

http://dx.doi.org/10.29119/1641-3466.2023.182.5

1. Introduction

In recent years, the world has been experiencing an increasing reliance on digital technologies and interconnected systems affecting a wide variety of fields and economic sectors, making cyber security a critical concern across global, regional and national policy dimensions (Gałuszka, Ptaszek, Żuchowska-Skiba, 2016). When writing about cyber security, it is important to note that the term cyber security refers to a set of technologies, processes and practices for protecting and defending networks, devices, software and data from attack, damage or unauthorized access (Bhardwaj et al., 2022). As Jana Pieriegud (Pieriegud, 2016) notes, the digitization of the economy and society is one of the most dynamic changes of our time, which opens up new opportunities in the creation of business models, but at the same time brings with it uncertainty and various risks related to, among other things, the social impact of the automation of manufacturing processes or security in the broadest sense. Digitalization as a continuous process of convergence of the real and virtual worlds is becoming a major driver of innovation and change in most sectors of the economy. The key drivers of the digital economy today are:

- Internet of Things (IoT) and Internet of Everything (IoE).
- Internet of Everything (IoE),
- ubiquitous connectivity (hyperconnectivity),
- cloud-based applications and services (cloud computing),
- big-data analytics (BDA) and big-data-as-a-Service (BDaaS),
- automation (automation) and robotization (robotisation),
- multi-channel (multi-channel) and omni-channel (omni-channel) distribution models for products and services.

A new reality of cyber threats is taking shape in this space. Their dynamic evolution poses a serious challenge to national security. Sophisticated hacking techniques, attacks sponsored by various organisations and cyberterrorism are becoming more common. In this new reality, states, organisations or institutions, faced with the challenge of protecting critical infrastructure from cyber threats, are creating innovative counter-threat approaches and solutions. Cybersecurity centres seem to be an important element of these projects, allowing not only to secure key information systems in the area of proper functioning of the state, but also to collect sensitive data and, through their redundancy, to secure the possibility of restoring data in case of loss (Górka, 2018). In this situation, the aspect of locating such centres takes on particular significance, primarily from the point of view of the possibility of destroying them using conventional methods, e.g. in the event of an armed conflict or terrorist attack. One possibility worth considering is the transformation of underground mine workings of decommissioned hard coal mines into facilities - cybersecurity centres of key importance for the state. It is worth noting here that, in line with the ongoing transformation of the coal mining industry, such initiatives, particularly those concerning new applications for the underground infrastructure of closed mines, are of great interest to decision-makers in this process, as they fit in with the social, environmental and security agendas of the EU.

It should be emphasized that the article was created on the basis of partial financing by NCBiR, grant POIR.01.01.01-00-0180/22 "Center for monitoring industrial installations in underground mining plants and detecting cyber threats".

2. Cyber security in the perspective of the European Green Deal Plan

The European Green Deal Plan is a strategic initiative of the European Union aimed at sustainable economic and environmental transformation (Regional cohesion…, 2022). The plan covers a wide range of areas, such as energy, transportation, agriculture, and waste management. Each of these areas uses increasingly advanced technologies that increase efficiency, improve productivity and contribute to environmental protection. Cyber-security plays an important role, as threats from cyber-attacks can significantly hamper the achievement of sustainability goals. Cyber security is one of the European Commission's top priorities and a cornerstone of a digital and connected Europe. The increase in cyber attacks during the coronavirus crisis demonstrated the importance of protecting hospitals, research centers and other infrastructure. Decisive action is needed in this area to future-proof the EU's economy and society. Therefore, cyber security is a key element in ensuring the safe and effective implementation of the European Green Deal Plan (Joint Communication…, 2020).

Implementing such ambitious goals requires advanced technologies that are linked to the digital economy and extensive use of data. The increase in data and digital technologies comes with a greater risk of cyberattacks. Therefore, protecting critical infrastructure, energy systems, transportation systems, communication networks and personal data becomes extremely important. In the above perspective, a significant challenge is the need to ensure adequate security measures, counter threats and risk management in the context of the activities undertaken within the framework of the European Green Deal Plan (Mielke et al., 2021). The indicated measures should take into account both technical and organizational aspects to minimize the potential risk of cyber incidents. To this end, the European Commission and European Union member states should cooperate and invest in the development of advanced cyber security solutions, training of personnel and strengthening of incident response capabilities. In addition, it is necessary to establish appropriate security regulations and standards to ensure consistency and harmonization of activities at the European level.

In the space described above and in the face of certain challenges, it should be noted that cyber security is an ongoing and dynamic process. With the development of technologies and threats, also the procedures related to the elimination of incidents must be systematically updated (Hoffman, 2018). In this context, it is important to take into account the following aspects related to cyber security - resulting from the European Green Deal Plan. The first is education and awareness. In this regard, those involved in the implementation of the European Green Deal Plan – project managers, employees and communities – should be properly trained on digital risks. The indicated action makes it possible to develop awareness and perception of current digital threats, including minimizing the propensity to succumb to potential cyber-attacks. An extremely important space is the protection of critical infrastructure. Critical infrastructure, i.e. systems and their constituent functionally related objects, including buildings, equipment, installations, services that are key to the security of the state and its citizens and that serve to ensure the smooth functioning of public administration, as well as institutions and businesses, must be adequately protected against cyberattacks (Ustawa z dnia 26 kwietnia 2007 r.). Putting in place strong defense mechanisms, such as intrusion detection systems (IDS – Intrusion Detection System) or attack protection systems (DDoS – Distributed Denial of Service) is a necessary measure. It is worth noting that at the end of 2016, there were three continuous DDoS attacks on domain name system (DNS) provider Dyn. This was a wake-up call about the dangers of targeted DDoS attacks. DDoS attacks have become one of the most serious threats to network security, and the first reported attack was published by Computer Incident Advisory Capability in 1999. Although a number of threat mitigation systems have been developed in academic and industrial environments, DDoS attacks remain serious and are increasing every year (Abu Bakar et al., 2023).

Another area identified by the Green Deal European Plan is data security. Due to the significant increase in the amount of data collected, it is necessary to properly secure the information collected, such as environmental, climate change, energy or mobility data - and to properly store and process it in accordance with data protection regulations (RODO – Data Protection Regulation (Dziennik Urzędowy Unii Europejskiej L 119, 2016)/GDPR – General Data Protection Regulation (Rozporządzenie o Ochronie Danych Osobowych…). In this space, it is important to recognize that data security is the practice of protecting digital information from unauthorized access, damage or theft throughout its lifecycle. It is a concept that encompasses every aspect of information security, from the physical security of hardware and storage devices to administrative and access controls, as well as logical application security. It also includes organizational policies and procedures. Properly implemented, robust data security strategies not only protect an organization's information assets from the actions of cyber criminals, but also protect against insider threats and human error, which remains one of the leading causes of data security breaches today. Data security involves implementing tools and technologies that improve an organization's insight into where its critical data is and how it is being used. Ideally, these tools should enable security features such as encryption, data masking and redaction of confidential files, and should automate reporting to improve audits and compliance with regulatory requirements. In this light, digital transformation is fundamentally changing every aspect of how today's companies operate and compete. The sheer volume of data that companies create, process and store continues to grow, creating a greater need for data management. In addition, computing environments are more complex than ever and routinely include the public cloud, the corporate data center and numerous edge devices, from Internet of Things sensors to robots and remote servers. This complexity creates an expanded attack surface that is increasingly difficult to monitor and secure (www.ibm.com/topics/data-security, 2023).

The European Green Deal plan also centers around issues of international cooperation. Cyber security is a global phenomenon, so it is important for European Union member states to cooperate on an international level. As the European Commission emphasizes, cyber security is crucial to both our prosperity and security. As our daily lives and economies become dependent on digital technologies, we are becoming increasingly vulnerable. Cyber-security incidents vary both in terms of who is responsible and the objective they seek to achieve. Malicious cyber activities threaten not only our economies and the pursuit of a digital single market, but also the very functioning of our democracies, our freedoms and our values. Our future security depends on transforming our ability to protect the European Union from cyber threats: both civilian infrastructure and military capabilities rely on secure digital systems. This was recognized by the European Council in June 2017 (www.consilium.europa.eu/…, 2023), as well as in the European Union's Global Strategy on Foreign and Security Policy (http://europa.eu/globalstrategy, 2023). Cyber threats come from both non-state and state actors: they are often criminal in nature, motivated by profit, but can also be political and strategic in nature. The threat of crime is compounded by the blurring of the line between cybercrime and "traditional" crime, as criminals use the Internet both as a way to scale up their activities and as a source for finding new methods and tools to commit crimes. In this perspective of an increasingly digital and interconnected world, protecting EU citizens from cyber threats is a top priority for the EU. The new proposed measures aim to strengthen cooperation on cyber security in the EU and globally, stimulate innovation and invest in awareness and capacity building. In parallel, the EU and NATO are conducting coordinated exercises to test their ability to respond to cyber and hybrid threats (Wspólny komunikat…, 2017). By sharing information and taking action together, cross-border digital threats can be addressed more effectively.

Research and innovation is another area of intervention of the European Green Deal Plan, which reads that supporting research and innovation in the field of cyber security is key to developing advanced defense technologies. This is evidenced by the following facts. By 2021, cybersecurity will already cost the global economy $6 trillion a year, up from an estimated $3 trillion in 2015. (estimated global GDP in 2020 is $138 trillion) (Cybersecurity Ventures, „2019 Official Annual Cybercrime Report”, 2020). The costs of cybercrime include data corruption and destruction, theft of money, loss of productivity, theft of intellectual property, theft of personal and financial data, disruption of the normal course of business after an attack, and loss of reputation. The European Systemic Risk Board (- hereafter ESRB) estimates that the average cost of a cyber incidents increased by 72% between 2015 and 2020 (ERRS, Europejska Rada ds. Ryzyka Systemowego, 2020). Secondly, according to a 2020 study, cybercrime adversely affects different sectors of the economy in different ways (PWC, Fighting fraud…, 2020). It was the most destructive form of fraud in the government and public administration sector, the technology, media and telecommunications sector, and the health sector. It was also the second most destructive form of fraud in the financial sector and in the industrial and manufacturing sectors.

The objectives and actions indicated above are referenced in the EU Cyber Security Strategy, which aims to ensure a global and open Internet with strong safeguards where there is a threat to the security and fundamental rights of people in Europe. As a consequence of the progress made under previous strategies, it contains concrete proposals for the use of three main instruments, which are regulatory, investment and policy initiatives. These address the following three areas of EU action:

- resilience, technological sovereignty and leadership,
- operational capacity for prevention, deterrence and response,
- cooperation for the development of a global and open cyberspace.

The EU is determined to support this strategy with unprecedented levels of investment in digital transformation over the coming years. This represents a quadrupling of previous investment levels. This demonstrates the EU's commitment to its new technology and industrial policy and reconstruction agenda. The EU's new cybersecurity strategy is a key element of the Shaping Europe's Digital Future strategy (Shaping Europe’s Digital Future…, 2020), the Recovery Plan for Europe (Rozporządzenie Rady (UE) 2020/2094 z dnia 14 grudnia 2020 r.) and the Security Union Strategy 2020-2025 (Komunikat Komisji..., 2020).

Thus, investments in areas such as artificial intelligence, machine learning and big data analytics can help identify new threats and respond quickly to potential attacks. By properly securing digital infrastructure and data, it will be possible to minimize the risk of potential attacks, which will contribute to the successful implementation of the European Green Deal Plan and accelerate the achievement of the set goals related to environmental protection and the fight against climate change. Ultimately, the success of the European Green Deal Plan depends on the effective and secure use of digital technologies. Ensuring an adequate level of cyber-security will avoid potential losses, environmental risks and damage to the long-term implementation of this important plan for the future of Europe and the world.

3. Cyber security in the mining transformation process

The process of transformation of the mining industry is not only the end of mining operations, but also the beginning of a new stage of economic development for regions that have been strongly linked to this economic sector. The decommissioning of mines creates a number of new challenges, among which it seems that the key one is the effort to adapt to changing social, economic and environmental conditions. Mining areas that have based their economies on mining for many years also face the need for adaptation and diversification, which enable them to achieve the following goals (Leininger et al., 2018):

- dissipation of economic risks associated with vulnerability to commodity price fluctuations,
- sustainable development of mining areas,
- development of diverse economic sectors,
- creation of new jobs,
- increase in investment and infrastructure development,
- development of innovation and new technologies,
- environmental protection,
- increasing cultural and social diversity,
- development of new educational programs.

The transformation of mining areas from monoculture to modern, diversified economies is key to ensuring the sustainable development of these regions. Adaptation and diversification respond to the challenges of natural resource depletion, changes in the market for raw materials and the need to protect the environment. Diversity, in turn, contributes to the development of innovation, the creation of new jobs and increased investment in infrastructure and research and development. Transformation, while not without challenges, is opening up opportunities for development and progress in the regions, resulting in sustainable and diversified socioeconomic development. As mining areas undergo transformation and adapt to new functions such as tourism, recreation and new technologies, it is innovative to build new spaces and infrastructure related to cyber security (Nowakowska, Rzeńca, Sobol, 2021).

The process of decommissioning mining poses many challenges, but at the same time opens up new opportunities for growth and adaptation for local communities and industries operating in the transformed areas. As mines close, existing mining spaces and infrastructures can be transformed into new cyber security facilities. As the authors of the Technology Trends Outlook 2022 report note, technology continues to be a major catalyst for change in the world. Technological advances are giving companies, governments and public sector institutions greater opportunities to raise productivity, create and change reality anew, and contribute to humanity's prosperity. And while it is still difficult to predict how technology trends will evolve, world leaders can better plan for the future by tracking the development of new technologies, anticipating how companies can use them and identifying factors that influence innovation and adaptation (Chui, Roberts, Yee, 2022). Second, as the authors of the report, Digital technologies for a new future, note, digital technologies foster eco-innovation that contributes to sustainable development by reducing environmental impact and optimizing resource use. As these technologies develop and converge with biotechnology and nanotechnology, they can generate exponential innovations that will contribute to a sustainable future (The difficult balance…, 2021).

Achieving the above goals requires a number of conditions, among which the key ones may be having adequate resources and infrastructure. This may involve investment in the development of roads, schools, or new technologies, which can be time-consuming and expensive. In the social sphere, the involvement of residents of transformed areas in decision-making processes and increased public awareness of the benefits of diversifying economies may prove to be important factors. Finally, the transition from mining to a different structure of transformed economies may require labor resources to acquire new skills and competencies (Wirth et al., 2018).

In the above-described perspective, the transformation of existing mining spaces and infrastructure into new cyber security facilities has many benefits for both local communities and the economic development of transformed mining regions, including (Marszowski, 2020):

- can determine the influx of investors and regional development. Post-mining areas, thanks to modern infrastructure related to cyber-security, can become an attractive place for IT and cyber-security companies and professionals. This will contribute to the regions' international competitiveness;
- allows diversification of the economy, creation of new jobs, development of innovation and strengthening of digital security. This is an opportunity to minimize the negative effects of mining decommissioning into a positive boost for the development of local communities and the region as a whole;
- areas that previously served as training centers for miners can be transformed into state-of-the-art training centers related to cyber security. They can offer courses, workshops and training for IT professionals and those wishing to pursue a career in cyber security;
- existing facilities and buildings can be adapted into cyber security research and development centers. Such centers can support the development of innovative technologies and strategies to protect against cyberattacks;
- areas after the decommissioning of mines can be transformed into technology parks that will attract companies related to cyber security, IT and IT technologies. Indicated parks can foster the development of the local business ecosystem and create new jobs;
- post-mining facilities can also be used to locate cyber-security monitoring and management centers. These can be places where specialists can focus on detecting threats and responding to attacks;
- large areas after mine decommissioning can be used to build industrial data centers that provide secure data storage and hosting services for various industries.

However, this process also brings challenges related to a lack of resources and infrastructure, as well as resistance to transformation by local communities. Therefore, strategic planning and the involvement of all stakeholders is necessary for the effective and harmonious transformation of mining areas into diversified centers for socio-economic development. Centers can be the basis for transforming underground coal mining pits into cyber-critical facilities. This is a comprehensive approach that combines innovation, critical infrastructure protection and regional development to leverage existing coal mining resources.

Thanks to the rationale described above, accompanying the transformation, mining regions can face the challenges of mining decommissioning and at the same time contribute to strengthening the country's digital security. In conclusion, diversification of mining areas is an integral part of economic transformation. Reduction of economic risk, sustainability, job creation and the development of innovation are key benefits of diversification.

4. Cyber security in the underground workings space

In the European Green Deal Plan, one of the key areas of transformation is mining, and special attention should be paid to transforming underground mine workings into critical cyber security facilities. Their potential stems from infrastructure that can be adapted for new purposes, such as energy storage, data storage or renewable energy installations. Underground mine workings in the cyber security space have a unique advantage over existing infrastructure. These spaces are often characterized by robust construction, flexible power supply and natural environmental isolation. By repurposing these pits, societies can optimize their resources and reduce the need to build new facilities, saving the time and costs associated with building them from scratch. An extremely important element of the space described is that underground mine workings are designed to withstand extreme conditions and ensure physical safety. These features make them ideal for storing critical cyber-security infrastructure, as they provide a level of protection against physical threats such as sabotage, theft or natural disasters. The inherent resilience of these underground structures adds an additional layer of security to the national cybersecurity infrastructure (Pałka, Rizaoglu, 2019).

Transforming underground workings into a cyber security space can contribute to a number of important and significant goals, including (Aligning Policies…, 2015):

- sustainable development, improving the economy in regions that have depended on mining,
- reducing CO2 emissions,
- increasing energy efficiency,
- creating new jobs in the new technology and renewable energy sectors,
- compensate for job losses in mining.

It also has great significance for the transformation process. These unique infrastructures have the potential to attract investment, create jobs and stimulate economic growth. However, in order to achieve these benefits, it is essential to ensure adequate levels of cyber security. Good security of these facilities attracts the trust of investors and users, which is crucial to their success. In addition, cyber-critical facilities can serve as important technology facilities for other sectors, such as banking, healthcare and government. Their reliability and security are integral to the proper functioning of these sectors (Spychała, 2017). In addition, the development of such facilities can contribute to the revitalization of mining areas and improve the living conditions of local communities. The creation of new jobs, investment in digital infrastructure and the development of local technological competence contribute to economic growth and improve the quality of life of local residents (Wariantowe Ramy Transformacji…, 2023). While transforming underground mine workings into cyber-critical facilities brings a number of benefits, it also requires focused efforts aimed at protecting infrastructure and data. The physical and cyber security of these facilities is essential to the success of the transformation process and to ensure investor and user confidence (Cybersecurity strategy…).

Transforming underground coal mine workings into facilities critical to the country's cyber security can also play a number of important roles in the mining transformation process. As mining changes, underground coal mine workings are becoming cyber-critical facilities. Transforming these areas into new, innovative data centers or other technological infrastructures brings many benefits, but also new challenges in protecting against cyberattacks. Transforming underground pits into cyber-critical facilities involves protecting both the infrastructure itself and the data stored there. These facilities can be used as data processing centers that store huge amounts of information of high business or personal value. Their security is crucial, as an attack on these facilities can lead to data loss, service disruptions and even threats to user security and privacy.

Equally important is the regularity that indicates that transforming underground pits into cyber-security facilities can help diminish distributed and redundant infrastructure, increasing the overall resilience of a nation's cybersecurity state. By strategically deploying these facilities in different regions, countries can minimize the risk of a single point of failure and ensure business continuity even in the face of local disruptions or targeted attacks (Michałkiewicz, 2016).

As a result of developing efforts to convert underground mine workings into critical cyber security facilities, their use as energy storage or photovoltaic installations also allows the production of clean energy, thereby reducing greenhouse gas emissions. Secondly, the existing infrastructure in underground mine workings, such as ventilation systems or transportation routes, can be used as the basis for building new facilities, related to related to cyber security – which can significantly speed up the transformation process – saving time and resources. However, it should be remembered that transforming underground mine workings into critical cyber-security facilities requires significant investment. In view of this regularity, governments and European institutions should secure adequate funding and provide support to businesses and local communities to assist them in transforming these areas. As countries face the challenges of protecting critical infrastructure and information from cyber threats, repurposing these pits shapes a unique and innovative approach to ensuring cyber resilience and protecting national interests. With careful planning, cooperation and investment, countries can leverage the advantages of underground mining infrastructure to enhance their cyber security capabilities (The Sustainable Development Goals Report, 2021).

As researchers at the University of Nevada note, another reason why cybersecurity is important is the dramatic increase in the sheer number of cyberattacks, along with the increasing sophistication of cybercriminals' tactics - both of which cause significant financial losses. New malware capabilities, coupled with an increase in data security breaches, have increased the total cost of cybercrime. Potential losses from these reported cybercrimes have exceeded $6.9 billion. Cybercrime magazine estimates that cybercrime will cost the world $10.5 trillion annually by 2025. Hackers are using sophisticated strategies to steal login credentials to gain access to smart phones and computers, hack phones via Bluetooth headsets and spy on people using public Wi-Fi networks. Cybercriminals are becoming increasingly cunning and harder to stop, and cybersecurity professionals must be able to keep up (Why Is Cybersecurity Important? 2023).

In this perspective, underground mine workings that are not used for coal mining can be transformed into special facilities to serve as centers for operations and management of cyber security. Due to their structure and characteristics, such facilities can provide optimal conditions for storing and managing cyber-security resources, such as servers, monitoring systems and threat detection tools. It is also worth noting that underground mine workings have the necessary infrastructure for adapting cyber security operations and management centers in their space, such as power systems, ventilation, resistance to external factors, which can facilitate adaptation and reduce the cost of building new cyber security facilities. The spaces described can help ensure the independence of national systems. Thus, in the event of cyberattacks or other threats, there is a potential opportunity to continue operations and protect the country's key assets. However, this requires very consistent building of a specialized environment associated with highly skilled personnel who can manage these facilities to ensure cybersecurity. Such targeted actions can determine the development of local labor resources in transformed areas and the growth of an education system focused on cyber security competencies and skills. As a result, the dynamic development of digital technologies and the influx of cadres and talents related to cyber security may follow in these areas.

Physical protection of cyber security facilities is also an important aspect. Since they are located in former mine workings, it is necessary to provide adequate security measures, such as monitoring, access control and protection against unauthorized entry. Special attention should be paid to protection against physical intrusion to prevent physical access to these facilities by unauthorized persons. Protecting the infrastructure from cyber-attacks is another important aspect. Ensuring adequate network security, such as firewalls, intrusion detection systems (IDS/IPS) and event monitoring, is key to preventing attacks and identifying anomalies in real time. Regular security audits should be conducted to detect potential security vulnerabilities and take appropriate corrective action. In addition, an important element is the protection of stored data. Data centers in these facilities may store sensitive information, such as financial data, personal data or industrial secrets. Adequate safeguards such as strong data encryption, physical security and authentication systems are needed to prevent unauthorized access to this information. Regularly backing up data and storing it in secure locations are also key to minimizing the risk of data loss.

In this perspective, many coal-related countries are shifting to cleaner and renewable energy sources. With the disappearance of mining-related activities, the repurposing of existing mine workings is in line with sustainable development goals (Sulich, 2021). By transforming them into critical cyber-security facilities, societies can not only address cyber-security challenges, but also promote environmentally friendly activities by repurposing existing mining infrastructure with its consolidation and preservation (Borky, Bradley, 2018).

However, the success of transforming underground mine workings into cybersecurity-critical facilities does not depend only on the technical aspects of protection. Education and awareness of the importance of the transformation among mining employees and local communities is also an important factor. Employees responsible for managing and operating these facilities should be trained in cyber security. They should be aware of the latest security threats and practices, and know the procedures to follow in the event of a cyber security attack or incident. Regular training and awareness of cyber risks are key to building defense capabilities and minimizing risks. In addition, the local community should be involved in the transformation process and aware of the importance of cyber security. Local authorities, community organizations and community representatives should be informed about cyber threats and security measures to protect these facilities. Increased awareness among residents can contribute to reporting suspicious activity and supporting prevention efforts. Finally, collaboration with government agencies, cyber security experts and the private sector is essential to effectively ensure cyber security at these facilities. Coordinated efforts, sharing of threat information and best practices, as well as joint research and development initiatives can help create a strong cyber security ecosystem that is resilient to evolving threats. In this light, he concluded, "transforming underground mine workings into cyber-security critical facilities is a key part of the transformation process. Infrastructure and data protection, employee and community education, and cross-sector collaboration are essential to the success of this transformation. With the right approach, these transformed facilities can be secure technology centers, contributing to socioeconomic development and improving quality of life" (Strategic Agenda ECCC. …, 2023).

As a result, activities aimed at transforming underground coal mining pits into cyber-security critical facilities contribute to the diversification of economies in transformed areas - particularly in areas where coal mining plays or has played a key role. Transforming these areas into cyber security centers can create new opportunities for economic growth and social development. This could include the creation of new jobs related to the management and maintenance of cyber-security facilities, digital security training, and the development of cyber-security-related businesses and services. The indicated positive effects of transformation can thus minimize problems of unemployment, social exclusion and poverty - while contributing to the revitalization of these areas through the creation of new jobs and innovation-related industries becoming a source of economic growth and recovery (Large, 2014).

Transformation in the cybersecurity space can serve as a catalyst for the diversification of transformed mining areas and, as already noted, support their innovation. Achieving the above goals requires cooperation and knowledge sharing. The repurposing of underground mine workings determines the need for cooperation between government bodies, private entities, research institutions and local communities in transformed areas. The outlined challenge fosters knowledge exchange and encourages interdisciplinary and international cooperation. Transformation projects can create a platform for the exchange of expertise, best practices and technological advances, contributing to the overall improvement of capabilities in cybersecurity at the national level (Brunetti et al., 2020).

In conclusion, the need to transform underground coal mine workings into critical facilities for national cyber security is driven by various factors. Evolving cyber threat space, use of existing infrastructure, increased physical security, geographic distribution, synergy with energy transition, economic transformation and opportunities for cooperation are important reasons determining the transformation of underground coal mine workings into critical cyber security facilities (Konieczna-Fuławka et al., 2023).

5. Central Mining Institute National Research Institute Experimental Mine “Barbara" Poland - an example of good practice

The above-described perspective of cybersecurity as a subject of critical concern in terms of global, regional and national policies corresponds perfectly with the concept of adapting the infrastructure of underground excavations and facilities on the surface of the Central Mining Institute (hereinafter GIG) of the Experimental Mine "Barbara" (hereinafter EM Barbara) for the purposes of establishing the Silesian Cybersecurity Center (Analysis of the possibilities…, 2022). The development of the concept of the center - the Silesian Cybersecurity Center based on the underground infrastructure of GIG EM Barbara is part of the plans to transform the mining sector in Upper Silesia. The concept of a potential investment assumes maximum use of the existing infrastructure of EM Barbara and its expansion, modern and alternative to the original function.

As part of the preparation of the work concept, it is planned to create a monitoring system for the mining transformation processes and to build a modern cybersecurity infrastructure on the premises of the GIG EM Barbara. Implementation of the project involves the modernization and equipping of the facilities of EM Barbara with the necessary equipment for: collecting, processing, storing, delivering and securing digital data.

The transformation process monitoring system will consist of thematic quantitative and qualitative databases covering various scopes. The concept of the system assumes that data and quantitative indicators resulting from economic, financial, scientific and other statistics (currently collected and available in various databases) as well as qualitative data will feed the system on an ongoing basis. A special role in the System will be played by data on mining activity and its consequences, important for monitoring the transformation and planning the development of the region, which are a separate competence of the Central Mining Institute. For years, the Institute has been collecting, verifying and sharing:

- data on seismicity in the Upper Silesian Coal Basin (hereinafter referred to as the GZW);
- data for the European Plate Observation System;
- measurement data and measurement network of PM2.5 and PM10 fractions;
- data on current weather conditions and the GIG meteorological station data archive;
- information on the state of basic natural and technical hazards in hard coal mining;
- data on mining and post-mining areas;
- data on shallow exploitation in the areas of liquidated mines in the GZW.

The statutory works, consulting services, expert opinions and projects carried out at GIG provide a stream of data and information that, after integration and development, can supply the database system, among others, in the following areas of mining and post-mining activity:

- information on the risk of loss of surface stability in the areas of closed mines,
- data on mining waste streams and directions of their management,
- methane emissions from active and closed mines,
- qualitative and quantitative data of the GZW mine drainage system and the use of mine water,
- size of the carbon footprint of e.g. Mining Companies,
- heap fire hazard,
- size and structure of employment in mining and mining-related entities.

Structuring and organizing data sets and supplementing them with data collected by other institutions concerning e.g. social, economic, climate and other aspects, which will enable the preparation of in-depth expert opinions and reports on transformation. The wide spectrum of acquired and processed data is associated with the need to secure the appropriate technical infrastructure, provide data sources and develop algorithms for their sharing and processing in the form of reports and/or raw data.

The construction of the Transformation Processes Monitoring System will be carried out on the grounds and buildings managed and used by the Central Mining Institute on the premises of EM Barbara in Mikołów, where the necessary infrastructure (Data Center) will be built.

Figure 1. Visualization of the supercomputer in underground mining workings of EM Barbara.

Compared to traditional solutions, the newly created facility is characterized by the location of the server room. Server rooms being a building consisting of two basic parts: the server chamber and rooms supporting the functionality of the server chamber equipped with IT equipment installed with UPS, energy distribution, technical, telecommunications, operational, cold distribution facilities and areas for the foundation of power generators, cooling aggregates and fuel tanks. In the present project, the existing underground workings of EM Barbara will be used for the construction of the data processing center, which requires their appropriate adaptation - securing, strengthening and enclosing.

The new, pilot approach to the ways of developing post-mining areas means that the project is part of the transformation process and gives the opportunity to give new functions to the existing post-mining facilities.

6. Summary

Cyberattacks do not stop at national borders, so it is essential to strengthen cooperation between member states, share information about threats, and developing common standards and best practices in the field of cyber security. This allows for effective protection against attacks and minimization of risks to critical infrastructure related to the European Green Deal Plan. Finally, cyber security should also be addressed in regulatory and legislative policy.

The European Union should develop an appropriate legal and regulatory framework that will stimulate investment in cyber security and urge companies to implement effective protection measures. Strict sanctions should also be set for individuals or organizations that commit cyber-attacks, in order to ensure accountability and deter potential criminals. In the context of the above-mentioned regularities - it seems - success related to the transformation of underground mine workings into facilities of key importance to the state's cyber security is determined by a number of considerations, among which a particularly important one is the partnership between mining representation, the private sector and local communities. The indicated cooperation of these entities can determine better use of mining resources and ensure sustainable development for transformed mining areas. However, this requires, once again to be emphasized, investment, support and cooperation between different entities. In summary, the transformation of underground mine workings may represent a unique opportunity to use existing resources and infrastructure to build a sustainable future for Europe and prove to be a key element in the transformation of the Polish mining industry and in achieving the goals of the European Green Deal Plan.

References

1. Abu Bakar, R., Huang, X., Javed, M.S., Hussain, S., Majeed, F.M. (2023). An Intelligent Agent-Based Detection System for DDoS Attacks Using Automatic Feature Extraction and Selection. *Sensors, 23, 3333*, pp. 1-22.
2. *Aligning Policies for the Transition to a Low-Carbon Economy (2016). Meeting of the OECD Council at Ministerial Level*. Paris, 3-4 June 2015. Paris: OEDC.
3. *Analysis of the possibilities and the concept of adapting the infrastructure of underground excavations and facilities on the surface of GIG KD "Barbara" for the purpose of creating the Silesian Cybersecurity Center* (2022). Documentation of statutory work. Katowice: GIG.
4. Bhardwaj, A., Alshehri, M.D., Kaushik, K., Alyamani, HJ., Kumar, M. (2022). Secure framework against cyber attacks on cyber-physical robotic systems. *Journal of Electronic Imaging, 061802-1 Nov/Dec, Vol. 31(6)*.
5. Borky, J.M., Bradley, T.H. (2018). Protecting Information with Cybersecurity. *Effective Model-Based Systems Engineering, Sep 9, 345.404*.
6. Brunetti, F., Matt, D.T., Bonfanti, A., De Longhi, A., Pedrini, G., Enna, E., Orzes, G. (2020). Digital transformation challenges: strategies emerging from a multi-stakeholder approach. *The TQM Journal, Vol. 32, No. 4,* pp. 697-724. Emerald Publishing Limited, 1754-2731.
7. Chui, M., Roberts, R., Yee, L. (2022). *McKinsey Technology Trends Outlook 2022*. Report.

8. *Cybersecurity strategy of the Republic of Poland for 2019-2024*. Minister of Digital Affairs.
9. Cybersecurity Ventures „2019 Official Annual Cybercrime Report”. Sprawozdanie finansowane Herjavec Group, 2019 r. za: Cyberbezpieczeństwo w UE i państwach członkowskich UE. Komitet Kontaktowy najwyższych organów kontroli (NOK) Unii Europejskiej. Komitet Kontaktowy najwyższych organów kontroli (NOK) Unii Europejskiej 2020, p. 16.
10. Dziennik Urzędowy Unii Europejskiej L 119 z 4 maja 2016.
11. ERRS, Europejska Rada ds. Ryzyka Systemowego. *Systemic cyber risk, luty 2020* r. za: Cyberbezpieczeństwo w UE i państwach członkowskich.
12. Gałuszka, D., Ptaszek, G., Żuchowska-Skiba, D. (2016). Uspołecznianie technologii u progu czwartej rewolucji przemysłowej. In: D. Gałuszka, G. Ptaszek, D. Żuchowska-Skiba (eds.), *Technologiczno-społeczne oblicza XXI wieku* (pp. 11-33). Kraków: Akademia Górniczo-Hutnicza.
13. Górka, M. (2018). Cyberbezpieczeństwo jako wyzwanie dla współczesnego państwa i społeczeństwa. In: T. Dębowski (ed.), *Cyberbezpieczeństwo wyzwaniem XXI wieku* (pp. 31-51). Łódź/Wrocław: ArchaeGraph.
14. Hoffman, T. (2018). Głowni aktorzy cyberprzestrzeni i ich działalność. In: T. Dębowski (ed.), *Cyberbezpieczeństwo wyzwaniem XXI wieku* (pp. 11-31). Łódź/Wrocław: ArchaeGraph.
15. http://europa.eu/globalstrategy/, 25.07.2023.
16. http://www.consilium.europa.eu/en/press/press-releases/2017/06/23-euco-conclusions/, 25.07.2023.
17. https://www.ibm.com/topics/data-security, 25.07.2023.
18. *Joint Communication To The European Parliament And The Council The Eu's Cybersecurity Strategy for the Digital Decade*. Brussels, 16.12.2020.
19. *Komunikat Komisji w sprawie strategii unii bezpieczeństwa UE*. Komisja Europejska Bruksela, 24.7.2020.
20. Konieczna-Fuławka, M., Szumny, M., Fuławka, K., Jaskiewicz-Proc, I., Pactwa, K., Kozłowska-Woszczycka, A., Joutsenvaara, J., Aro, P. (2023). Challenges Related to the Transformation of Post-Mining Underground Workings into Underground Laboratories. *Sustainability, 15, 10274.*
21. Large, N.G. (2014). *Underground Experiments: Engineering Point of View Pyhäsalmi-Homestake*. Proceedings of the 15th International Workshop on Next generation Nucleon Decay and Neutrino Detectors (NNN14). Paris, France, 4-6 November 2014; presentation by Guido Nuijten-Rockplan/LBNO-DEMO.
22. Leininger, J., Dombrowsky, I., Messner, D., Breuer, A., Ruhe, C., Janetschek, H., Lotze-Campe, H. (2018). Governing the Transformations Towards Sustainability. In: E. Kriegler, D. Messner, N. Nakicenovic, K. Riahi, J. Rockström, J. Sachs, S. van der Leeuw, D. van Vuuren, *Transformations to Achieve the Sustainable Development Goals Report prepared*

by The World in 2050 initiativem (pp. 107-127). Laxenburg, Austria: International Institute for Applied Systems Analysis.

23. Marszowski, R. (2020). *Gminy i powiaty górnicze w Polsce w perspektywie sprawiedliwej transformacji*. Katowice/Jastrzębie-Zdrój.
24. Michałkiewicz, P. (2016). Cyberprzestrzeń a bezpieczeństwo narodowe. *Kultura Bezpieczeństwa, No. 5,* pp. 189-206.
25. Mielke, J., Schütze, F., Teitge, J., Wilk, S. (2021). Europejski Zielony Ład – więcej niż neutralność klimatyczna. *Interekonomia, 2,* pp. 99-107.
26. Nowakowska, A., Rzeńca, A., Sobol, A. (2021). Place-Based Policy in the "Just Transition" Process: The Case of Polish Coal Regions. *Land, 10, 1072*.
27. Pałka, D., Rizaoglu, T. (2019). The concept of a hard coal mine in the perspective of Industry 4.0. *Multidisciplinary Aspects of Production Engineering, vol. 2, iss. 1,* pp. 327-335.
28. Pieriegud, J. (2016). Cyfryzacja gospodarki i społeczeństwa – wymiar globalny, europejski i krajowy. In: J. Gajewski, W. Paprocki, J. Pieriegud (eds.), *Cyfryzacja gospodarki i społeczeństwa – szanse i wyzwania dla sektorów infrastrukturalnych* (pp. 11-39). Gdańsk: Instytut Badań nad Gospodarką Rynkową – Gdańska Akademia Bankowa.
29. PWC (2020). Fighting fraud: A never-ending battle PwC's Global Economic Crime and Fraud Survey. In: *Cyberbezpieczeństwo w UE i państwach członkowskich*.
30. *Regional cohesion in Europe 2021-2022: Evidence from the EIB Investment Survey* (2022). European Investment Bank.
31. Rozporządzenie o Ochronie Danych Osobowych (RODO) - GDPR (General Data Protection Regulation).
32. Rozporządzenie Rady (UE) 2020/2094 z dnia 14 grudnia 2020 r. ustanawiające Instrument Unii Europejskiej na rzecz Odbudowy w celu wsparcia odbudowy po kryzysie związanym z COVID-19.
33. *Shaping Europe's Digital Future* (2020). Luxembourg: Publications Office of the European Union.
34. Spychała, M. (2017). Sztuczna inteligencja w służbie cyberbezpieczeństwu infrastruktury krytycznej – szanse i zagrożenia. In: D. Skokowski (ed.), *Cyberbezpieczeństwo polskiego przemysłu. Sektor energetyczny* (pp. 9-23). Kraków: Instytut Kościuszki.
35. Strategic Agenda ECCC (2023). European Cybersecurity Competence Centre.
36. Sulich, M., Rutkowska, A., Krawczyk-Jezierska, J., Jezierski, P., Zema, T. (2021). Cybersecurity and Sustainable Development. *Procedia Computer Science, Vol. 192,* pp. 20-28.
37. The difficult balance between digitalization and sustainability. In: *Digital technologies for a new futures* (pp. 12-15). Koordynacja prac nad dokumentem S. Rovira we współpracy z W. Peresem i N. Saporito. United Nations.

38. *The Sustainable Development Goals Report 2021* (2021). New York, NY, USA: United Nations Department of Economic and Social Affairs.
39. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Dz.U. 2007, Nr 89, poz. 590.
40. *Wariantowe Ramy Transformacji Przewodnik po zasadach identyfikacji i oceny koncepcji zagospodarowania byłych terenów górniczych i przemysłowych*, https://transformacja.slaskie.pl/content/wariantowe-ramy-transformacji, 20.07.2023.
41. *Why Is Cybersecurity Important?* https://onlinedegrees.unr.edu/ms-in-cybersecurity/resources/why-is-cybersecurity-important/, 26.07.2023.
42. Wirth, P., Chang, J., Syrbe, R.U., Wende, W., Hu, T. (2018). Green infrastructure: a planning concept for the urban transformation of former coal-mining cities. *International Journal of Coal Science & Technology, vol. 5,* pp. 78-91.
43. Wspólny komunikat do Parlamentu Europejskiego i Rady. Odporność, odstraszanie i obrona: budowa silnego cyberbezpieczeństwa dla UE. Bruksela, 2017.