ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Stronger Together? EU Support for Ukrainian Local Authorities Facing Cyber Attacks (2022–2023)

Iryna Fyshchuk | Department of Political Science and Management, University of Agder, Norway | ORCID: 0000-0002-7645-3490

Abstract

This study attempts to explore the extent to which EU support during the decentralisation process in Ukraine facilitates local authorities' digitalisation and strengthens their resilience against cyber attacks. The Ukrainian cyber attack cases are becoming more frequent in 2022 and 2023 in terms of war, especially on the websites of local authorities. The article demonstrates that decentralisation with the support of the EU-funded U-LEAD assistance programme provides an opportunity to bring state services closer to citizens and, accordingly, increase the efficiency of their provision. Decentralisation and digitalisation go hand in hand in the process of implementation in Ukraine. The digitalisation in this direction of local administrations becomes a tool for achieving this goal because it allows local administrations to offer more of their services in a digital format, which ensures the resilience of the development of local authorities. At the same time, the local authorities are less protected against cyber attacks, especially during the war. The article employs a semi-structured interview method to analyse data, revealing that representatives from local authorities participate in various training courses to enhance cybersecurity skills. However, the challenges vary and include issues such as lack of personnel, lack of funding, complex application procedures, lack of coordination, and technical capacity limitations. Indeed, Ukraine is still in the process of improving its own model of cyber defence

Received: 12.02.2024

Accepted: 24.05.2024

Published: 23.07.2024

Cite this article as:
I. Fyshchuk "Stronger together? EU support for Ukrainian local authorities facing cyber attacks (2022–2023)," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190344

Corresponding author:
Iryna Fyshchuk, Department of Political Science and Management, University of Agder, Norway. E-Mail: irafyshchuk@gmail.com;
0000-0002-7645-3490

for local authorities and the country as a whole in terms of countering Russian aggression, using among others practices of NATO and EU countries in the specified field.

Keywords

cyber attacks, cybersecurity, local authorities, digitalisation, decentralisation, EU

1. Introduction

Against the background of the ongoing full-scale Russian invasion of Ukraine and geopolitical tensions, at the same time, Ukrainian local authorities are in the treacherous territory of cyber attacks, as well as fulfilling integration requirements to the European Union. Cyber attacks are increasing, and local governments are often under-resourced and underprepared for them as indicated by Frandell et al. [1]. Moreover, cyber attacks actions aim to obtain sensitive information, disclose it, and threaten to publish or self-publish classified information about the state's information infrastructure [2]. The difficulties that large governments are having in this regard suggest that municipalities, especially small- to medium-sized ones, may also be struggling to protect their and their citizens' data [3]. At the same time, social media platforms, owned and operated by third parties, introduce potential threats such as accidental private data disclosure, misinformation spread, and hacks mentioned by Kenney [4]. As an example, during 13–14 January there was a global cyber attack on Ukrainian government websites. The websites of the Ministry of Education and Science, the Ministry of Foreign Affairs, the State Emergency Service, the Cabinet of Ministers, the Ministry of Energy, and 'Diia' (a mobile application developed by the Ministry of Digital Transformation of Ukraine for Ukrainian citizens) were not working. The attack presented a step towards the imminent Russian invasion on February 24.

Destructive attacks are a component of Russian wartime cyber operations [5]. Cyber attacks continue and threaten the well-being of the civilian population, and their amount is increasing at the local governments and more heavily impacted by cyber incidents than before. The combination of cyber- and physical attacks was aimed at disrupting the functioning of the Ukrainian government, municipalities and the army, undermining the public's faith in these institutions, damaging objects of critical infrastructure, and causing irreversible catastrophic consequences [6]. And under the

conditions of the current decentralisation, local authorities have received more powers, but at the same time this a transitional stage and creates certain challenges. Decentralisation processes are related to digitalisation processes, which started at the same time and take place in parallel. Whereas digitalisation processes are aimed at improving administrative services at the state and the local level where the implementation is main.

The ongoing decentralisation process in Ukraine is considered one of the most successful reforms in the country so far highlighted by Pintsch [7]. Decentralisation of public authorities is a mechanism that ensures the sustainable development of regions of the state on the basis of the legislative and regulatory transfer of functions, powers and budgets from the central executive bodies to the local self-government bodies [8]. The development of the state and decentralisation situation is a transfer of powers and resources to lower levels of public administration. In addition, decentralisation stands out as one of the forms of development of democracy, which allows the state and its institutions to expand local self-government. Also, decentralisation allows to activation of the population for decision-making and implementing solutions for their own needs and interests. Furthermore, decentralisation narrows the sphere of influence of the state on society, replacing this influence with self-regulation mechanisms developed by society itself, which reduces the expenses of the state and taxpayers for the maintenance of the state apparatus indicated by Lukin et al. [9].

A review of the literature proves significant scientific interest researchers to study various aspects of decentralisation of the modern state, challenges and problems of decentralisation processes, and administrative and territorial reform. Rhodes and Bevir determine the general methodological principles of the theory of decentralisation, they proposed by Wagenaar (2014) the 'distinctive interpretive theory' [10]. Some of the scientists such as Dyer and Rose [11] that mentioned the successful implementation of decentralisation depends on strengthening the potential of local bodies' power and the government's capacity for assistance and supporting decentralisation. It is important that local authorities and, communities make the most of their territorial features, even if they are unfavourable that was highlighted by Mikuš et al. [12].

2. Methods

This article is based on the method of qualitative semi-structured interviews with a diverse group of 19 content

experts, which were conducted between May 2023 and May 2024. The participants are established IT and cyber specialists, decision-makers in local authorities and central government bodies, politician leaders, professors, and researchers at universities, community managers, representatives of the cybersecurity charity funds, and NGO managers as shown in Table 1. Also, it was analysed official reports from the State Service of Special Communications and Information Protection of Ukraine (SSSCIPU) [13], Microsoft Digital Defense Reports [14], Cybersecurity Tech Accord [15], and published interviews of leaders of the SSSCIPU, and media reports about cyber attacks in Ukrainian, including the observation of the social network platform as the official telegram channel of the State Special Communications.

The interviews reported in this article were initiated and organised within the framework of the project 'Digital transformation in Ukraine and EU integration', which investigates the EU support for

Table 1. Semi-structured interviews with a diverse group of experts

Interview	Description
I – 1	Decision makers
I – 2	Digital leader of the community
I – 3	IT Manager
I – 4	Cybersecurity specialist
I – 5	Politician
I – 6	Cyber specialist
I – 7	Professor
I – 8	Researcher
I – 9	Manager at the local authority
I – 10	Decision maker
I – 11	Public organisation manager
I – 12	Manager of the NGO
I – 13	IT specialist
I – 14	IT specialist
I – 15	Decision maker
I – 16	Community manager
I – 17	IT specialist
I – 18	Decision maker
I – 19	IT specialist

Ukrainian local authorities facing cyber attacks during 2022–2023. The geographical representation of the respondents is as follows – from the central part of Ukraine and north – 8 local authorities, south – 5, west – 4, and east – 2.

Due to the sensitivity of the topic, it was difficult to arrange interviews. The most commonly given reasons for non-response were restrictions on official duties as public servants and martial law, fear of participating in the interview, lack of time, and refusal without giving a reason. Indeed, almost 85% of the respondents expressed appreciation for its timeliness and relevance. The selection is based on the respondent`s willingness to participate in the interview. Most of the interviews took about one hour. The collection, storage, and analysis of the interview data are based on compliance with ethical standards and protection of the rights of the interview participants regarding voluntary participation, anonymity, and confidentiality.

3. Decentralisation and digitalisation processes in Ukraine

It is worth noting that the process of decentralisation and digitalisation did not begin almost in parallel since 2019. Indeed, in Ukraine, from the very beginning of its declaration of independence in 1991, the issue of decentralisation of power occupied a rather important place, since there was a strong centralisation of power in relation to decision-making. After the Orange Revolution, in 2004, changes were made to the Constitution of Ukraine and the governmental system changed from presidential-parliamentary to parliamentary-presidential. In 2010, the system was changed back to president-parliamentary, and after the Revolution of Dignity in 2014, the issue of changes was raised again, and the form of government got back to parliamentary-presidential. In addition, a thorough decentralisation process started in 2014.

As a matter of fact, Ukraine has established European integration as its main political course and a decentralisation process for making changes inside the country. Practically it chose a 'partnership' model of local self-government, under which the state recognises the increased importance of the territorial community as a carrier of direct democracy and a full-fledged living environment for citizens. According to the European Charter of Local Self-Government, which was adopted in 1985 and entered into force in 1988, the parties must guarantee the political, administrative, and financial independence of local authorities [16]. Additionally, Article 2 of this

charter, it is mentioned that 'the principle of local self-government shall be recognised in domestic legislation, and where practicable in the constitution'. Article 3 of this charter provides that 'local self-government denotes the right and the ability of local authorities, within the limits of the law, to regulate and manage a substantial share of public affairs under their own responsibility and in the interests of the local population' [17]. Ukraine signed the European Charter of Local Self-Government in 1996, and the Charter entered into force in Ukraine in 1998 [18].

According to the constitution of Ukraine, decentralisation is a process of transferring parts of the functions and powers of the central executive bodies to regional and local self-government bodies [19]. The issue of the Ukrainian decentralisation process was investigated by Vasylieva et al. [20], also the decentralisation reform as a domestic development was noted by Keudel and Huss [21], international support for decentralisation and processes of decentralisation as a tool for the advancement of governance and for conflict management was described by Rabinovych and Gawrich [22]. Indeed, decentralisation of public authority is the process of redistributing competencies between the central and local levels with a shift in the focus of implementation on the ground of pre-defined functions guaranteed by the state.

In 2015, Ukraine adopted the Sustainable Development Strategy 'Ukraine – 2020', which provides for the implementation of 62 reforms, including decentralisation [23]. The decentralisation reform involves the creation of a new link in the system of administrative organisation in Ukraine through the introduction of a new administrative-territorial unit – the United Territorial Community (UTC – Hromada). They are formed as a result of the voluntary association of adjacent territorial communities, villages, towns, and cities in accordance with the Law of Ukraine 'On Voluntary Association of Territorial Communities' [24].

Current Ukrainian legislation does not define the concept of the Hromada. It indicates that a Hromada includes a voluntary association of residents of several villages, towns, and cities that have a single administrative centre. According to Article 140 of the Constitution of Ukraine, local self-government is the right of a territorial community to independently resolve issues of local importance within the limits of the Constitution and laws of Ukraine. So, a 'united territorial community – Hromada' is a set of residents united by permanent residents within a certain village, town, or city, which are independent administrative-territorial units with a single administrative centre.

The powers of territorial communities derive primarily from the Constitution of Ukraine and the Laws of Ukraine's 'On Local Self-Government' and 'On Voluntary Association of Territorial Communities'. In particular, the analysis of Art. 140–143 of the Constitution shows that most issues of local importance are not resolved by Hromadas directly but through local self-government bodies created by them.

Under the decentralisation reform, the Hromadas have gained greater powers, resources, and responsibilities, and legislative changes have increased the range of services that they can provide locally. Therefore, citizens of such Hromadas expect to have convenient and high-quality administrative services from their local authorities. With the support of international donor programmes, centres for the provision of administrative services (TSNAPs) have been created. These are premises where, according to the 'single window' principle, citizens can get the necessary administrative services. International donors and programmes, include the Representation of the European Union in Ukraine, 'U-LEAD with Europe', and USAID.

Regarding the U-LEAD programme, it is worth noting that it is financed by the European Union and its member countries Denmark, Estonia, Germany, Poland, and Sweden. In a project description, U-LEAD's thematic priorities are described as follows: 'It improves the capacities of municipalities to carry out the newly assigned tasks and promotes citizen and private sector engagement in local affairs. U-LEAD provides advice on strengthening local self-government (LSG) and regional development to the national level, improving coordination between different ministries and levels of government' [25].

In Ukraine, there is a three-level administrative-territorial system, where the first place is the regional level divided into oblasts, the second place is the subregional level (districts), and the third place is the basic level – which is divided into administrative-territorial units ('Hromadas'), which consist of cities, urban villages, and villages. Nowadays, there are 1470 Hromadas in Ukraine as a result of the decentralisation reform that shown in the Table 2. The decentralisation processes included the following: administrative services, local budgets, health care, social services, cooperation with municipalities, education, and security.

According to the digitalisation process in this paper, it refers to the integration of digital technologies into various aspects of society

Table 2. The new system of administrative and territorial organisation as of October 7, 2021.

Regional level (Oblast)	Number of basic-level administrative-territorial units ('Hromadas')	Number of administrative-territorial units of the subregional level (districts)
AR Crimea	–	10
Vinnytska	63	6
Volynska	54	4
Dnipropetrovska	86	7
Donetska	66	8
Zhytomyrska	66	4
Zakarpatska	64	6
Zaporizhska	67	5
Ivano-Frankivska	62	6
Kyivska	69	7
Kirovogradska	49	4
Luhanska	37	8
Lvivska	73	7
Mykolaivska	52	4
Odeska	91	7
Poltavska	60	4
Rivnenska	64	4
Sumska	51	5
Ternopilska	55	3
Kharkivska	56	7
Khersonska	49	5
Khmelnytska	60	3
Cherkaska	66	4
Chernivetska	52	3
Chernihivska	57	5
Kyiv city	1	–
Total	1470	136

Based on the source [26].

through the public authorities mainly to transform traditional processes, systems, and activities. About the digitalisation technologies, which are used mainly in the sphere of services such as financial, educational, and public was highlighted by Khadzhyradieva et al. [27].

Digitalisation involves the adaptation of digital technologies in public authorities such as computers, mobile devices, and software applications to enhance efficiency, as well as to make effective services and create new opportunities for innovation and growth. And e-government – is about how government organises itself: its administration, rules, regulations, and frameworks set out to carry out service delivery and to coordinate, communicate, and integrate processes within itself digitally noted by Almarabeh and AbuAli [28], regarding the cybersecurity issues, it plays a key role in the success of e-government programmes [29]. In Ukraine, e-government is a requirement for public administration reform on the one hand, and a key tool in the fight against corruption in government (political and administrative corruption) mentioned by Marysyuk et al. [30].

Importantly, the Ukrainian process of digitalisation in public authorities and local bodies as well began mainly in 2019 with the announcement of the 'Digital State' project, and it is still being implemented. The goal of the project is that all government services will be available online; 20% of services will be provided automatically; there will be one online form to fill out to get the package services for any life situation. As part of the project, 14 test services have already been launched: electronic office, mobile app, e-Baby, passport with TIN, child registration online, e-pension, SmartID, MobileID, digital citizenship certificate, e-residency, developer's office, bank account for business online, electronic elections, and ID card with electronic signature. 'The state in a smartphone' is available now in the 'Diia' application, and all online services in the Diia – Government services online, which are divided into two groups for citizens and business.

According to the countries in Europe with the highest E-Government Development Index (EGDI) values, Ukraine in 2022 is in the 46th rank, which means that it improved compared to position 69 in 2020 [31]. This growth is explained by the Ukrainian application Diia as a digital passport and portal where citizens can get a service using this application or site as all data is attached to the person and it is available in digital form.

When the full-scale invasion began, local authorities were decentralised, but not all of them, as the reform was still in the process of implementation, and digitalisation had started almost at the same time and was actively developing, and still it was needed the digital transformation specialists in the regions, that needs time and sources. Additionally, when there is a change in the organisation, everything is in a situation of uncertainty, and in a war situation it increases.

4. Cyber Attacks Definitions

There is no unified definition of the term 'cyber attacks' in the scientific literature. Therefore, in this article, cyber attacks are understood as actions carried out by cyber actors in cyberspace on special targets which lead to violations of (i) privacy, (ii) information availability, (iii) critical infrastructures, and (iv) psychological effects on minds, i.e., confusion about what constitutes the truth, and on the mental state of citizens, such as anxiety and panic.

As mentioned by Michael Kenney (2015) cyber attacks belong to the same metaphorical class or 'genus' of events as cyber-war, 'hacktivism' and terrorists' use of the internet [4].

Cyber attacks can be understood as 'the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population' [32]. They 'pose complex problems that reach into new areas for national security and public policy'. Data and information are getting more vulnerable in this situation of cyber attack, especially if the level of protection is low and local authorities pay little attention to this field.

Inspired by Plotnek et al. and based on the definitions proposed by Al Mazari et al. above the following Figure 1 presents a formation of dimensions which cyber attacks include.

Cyber attacks can be malicious (e.g., trojan horses, computer worms, and sabotage attacks) or unintentional (e.g., incorrect

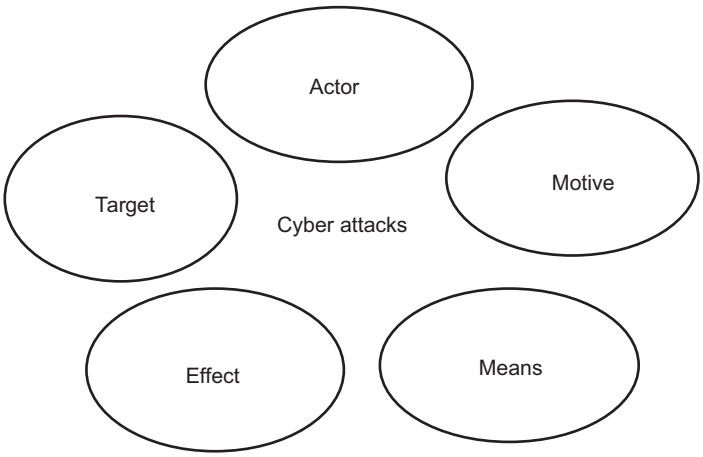

Figure 1. Dimensions of cyber attacks.

software updates, erroneous protocols, or unwanted network connections). The motivation for malicious attacks may among others arise from terrorism, geopolitics, or criminality. According to Stambaugh [33] terrorist cyber attacks are considered 'the premeditated, politically motivated attack against information systems, computer programs, and data to deny service or acquire information with the intent to disrupt the political, social, or physical infrastructure of a target resulting in violence against noncombatants. The attacks are perpetrated by subnational groups or clandestine agents who use information warfare tactics to achieve the traditional terrorist goals and objectives of engendering public fear and disorientation through disruption of services and random or massive destruction of life or property'.

Cyber attacks represent complex problems whose effects reach into new areas for national security and public policy [34]. As mentioned above, cyber actors can use computer network tools to shut down critical national infrastructures (such as energy, transportation, and government operations) or to coerce or intimidate a government or civilian population.

After considering all the keywords related to cyber attacks, a simplified graphical illustration of the dimensions of cyber attacks was compiled with a view to Ukrainian municipalities (see Figure 2).

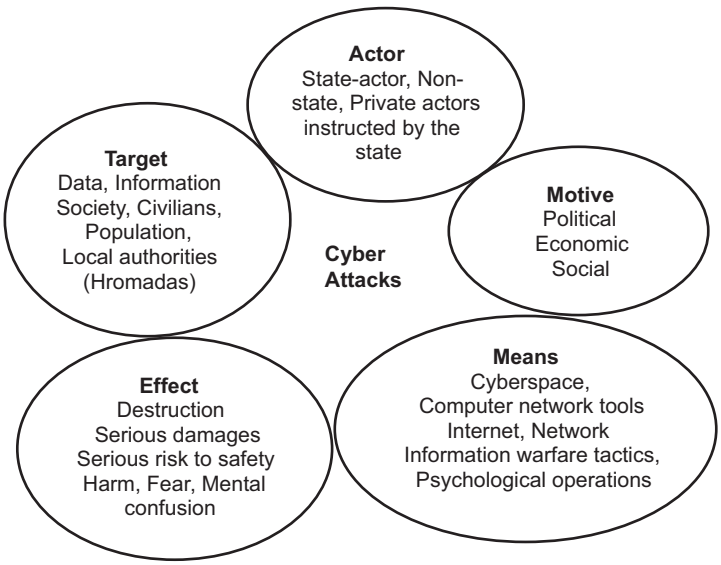

Figure 2. Dimensions of cyber attacks in Ukrainian municipalities.

The key features of cyber attacks can be segmented and contrasted by the relevant components Al Mazari et al. (2018) based on it created dimensions of cyber attacks in Ukrainian municipalities using five key components:

- **Target:** Data, Information society, Civilians, Population, and Local authorities (Hromadas)
- **Motive:** Political, Economic, and Social
- **Means:** Cyberspace, Computer network tools, Internet, Network, Information warfare tactics, and Psychological operations
- **Effect:** Destruction, Serious damages, Serious risk to safety, Harm, Fear, and Mental confusion
- **Actor:** State-actor, Non-state, and Private actors instructed by the state

During analysis, however, it was noted that more recent literature emphasises aspects relating to motive threat investigated by Plotnek and Slay [35], which led to the discovery of a vital gap regarding the threat actor in the cyber-attack dimensions that proposed here.

To analyse the municipalities' protection against potential cyber attacks, the Swiss Cheese Model can be strengthened, which was developed by Reason et al. [36]. The main idea of the model is to explain why accidents and failures sometimes occur even when multiple layers of defence are in place. The model has since been applied to various fields, including aviation, healthcare, and cybersecurity. According to James T. Reason, each slice of Swiss cheese is full of holes and the size, and number of holes will vary from one slice to another. In this model, a slice of Swiss cheese is symbolic of a given measure taken to minimise risk. Each slice of cheese can be thought of as a line of defence level against accidents level. In cybersecurity, this model can be effective to visualise controls and defences that public authorities or municipalities have in place to protect themselves from cyber threats.

These cheese holes can be used by attackers to compromise an organisation's defences. However, the model (Figure 3) also suggests that the chances of an attacker successfully breaching an organisation's defences are greatly reduced if there are multiple layers of protection, as an attacker would need to find a vulnerability in each layer to successfully exploit it. One of the key benefits of the Swiss cheese model is that it encourages organisations to take a holistic approach to cybersecurity and not just focus on one control or protection mechanism. The model encourages organisations

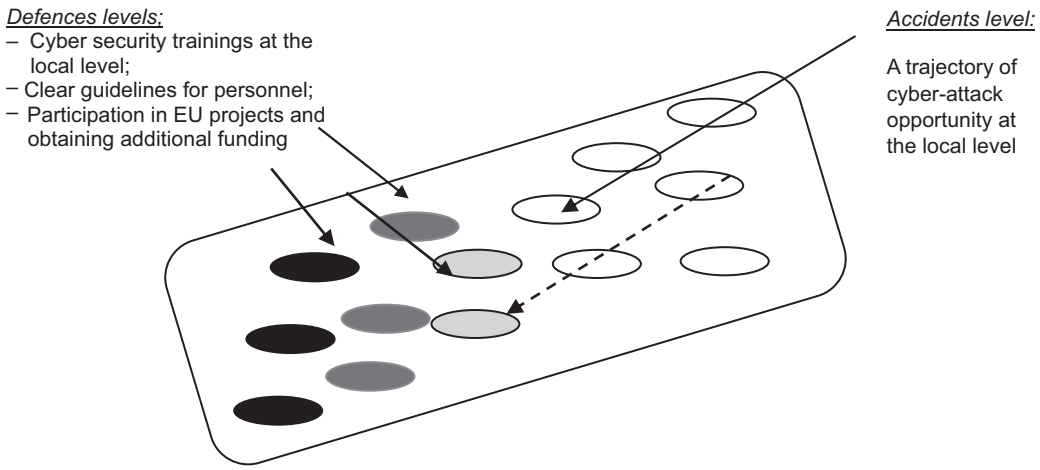

Figure 3. Cyber attacks vulnerabilities at the local level with potential accidents and defences levels based on the Swiss cheese model.

to consider the entire system of controls and protections they have in place and how they can be strengthened.

For example, if employees of the local authorities have listened to training on preventing phishing attacks, not to open unknown links and basic ideas of hygiene on the internet, then one of these slice-levels of protection according to this model is already more protected. However, if employees are not trained in how to detect and prevent phishing attacks, an organisation can still be vulnerable to cyber attacks through this 'hole' in its defences. Another slice that can prevent cyber attacks is the developed guidelines for cybersecurity at the local level.

5. Cyber attack cases in local authorities in Ukraine during 2022–2023

Massive cyber attacks were held on the governmental websites during January 2022 before the full-scale invasion of Ukraine. There were a lot of cyber attacks on the websites of local authorities in Ukraine in spring 2022. According to the State Service of Special Communications and Information Protection of Ukraine Report, cyber attacks took place in different sectors during 2022–2023, but governmental and local authorities were in second place, as shown in Figure 4.

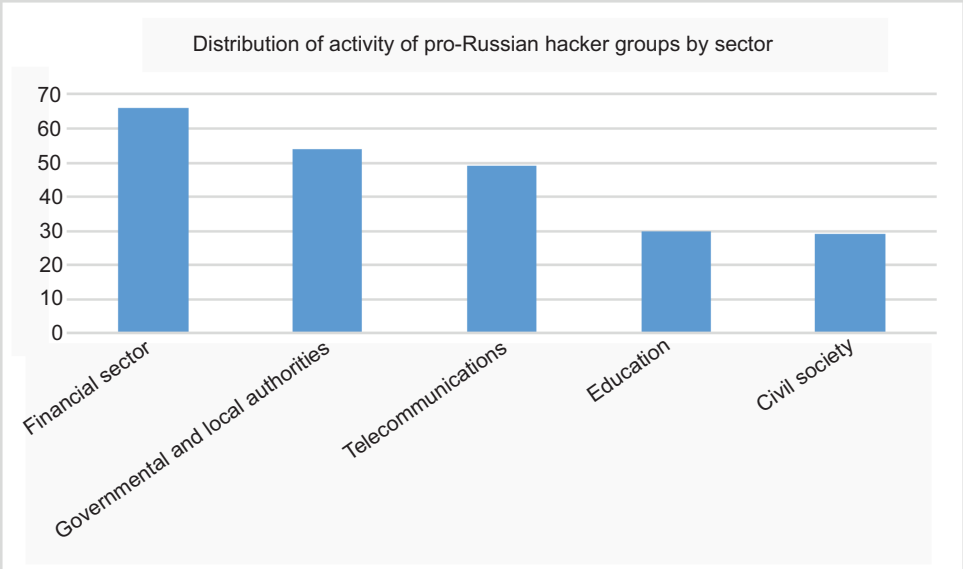

Figure 4. Distribution of activity of pro-Russian hacker groups by sector based on the SSSCIPU data report [13].

Indeed, as mentioned by the manager of the Volyn regional civil administration, the websites of the communities were hacked in the Volyn region on March 3, 2022, and the representatives of the administration of the affected communities asked the citizens not to react and not to spread misinformation.

The spokeswoman of the Security Service of Ukraine in the Zhytomyr region said that a cyber attack was committed on the websites of the community in the Korosten district.

In the same period, the head of the Vinnytsia regional administration, Serhii Borzov, noted that cyber attacks were carried out on the websites of regional state administrations and communities. Borzov also noted that computer algorithms have learned to 'revive' photos, synthesise a person's voice, and replace a face in a certain video.

The press service of the Bereziv city council of the Odesa region reported that the occupiers had hacked the websites of all communities in the Odesa region and published information about the alleged 'surrender of Ukraine'. This was a fake [37]. All these examples from March 2022 were similar in content. Cyber attacks were used to affect the psychological and mental state of the population in the communities.

In April 2023, there was a cyber attack on the official information resources of the Uman community in the Cherkasy region [38]. The rural and town websites are not available to users and administrators themselves. According to IT engineer Oleksandr Lampika:

'Hackers carried out a DDoS attack on the corresponding server, this is a huge number of connections at the same time, and it "went down" a bit. Oleksandr believes that this attack will not bring any benefit to the enemies, except for our temporary inconveniences. These DDoS attacks are the same as bombing fields they just do damage. Our specialists know very well what to do in such cases, everything will be repaired on the servers and the sites will work again. It takes a little time.'

Indeed, some of the representatives of Ukrainian local authorities mentioned about cases facing cyber attacks during the full-scale invasion of Ukraine. As noted, the IT specialist of the Western community:

> The first cyber attack on our community site took place in 2022, after the full-scale war began. The site was down for some time, our technical website developer reacted immediately, and the site resumed operation the next day, so, I would like to note that citizens had access to the site quickly. The second time when we faced the cyber attack it happened in the spring of 2023 and again it lasted up to one day, even several hours and then our technical support restored access to the site.

Thus, this destruction effect spreads anxiety, fear, or mental confusion situations inside society, especially with the full-scale invasion.

According to the research of the Ministry of Digital Transformation of Ukraine, the digital skills of Ukrainians and the level of digital security in 2023, where cybersecurity policies of surveyed Ukrainians do not have policies on cybersecurity and/or cyber hygiene at the workplace 36%; and 26% answered there is no effective protection of confidential information [39]. Hence, this shows the importance of strengthening resilience in the cybersecurity field in the country and in local authorities especially.

6. EU support

Before the full-scale invasion, the EU supported Ukraine in countering cyber attacks by launching a cyber dialogue between

the EU and Ukraine in June 2021, strengthening the operational capacity of the country's telecommunications services and the fight against disinformation. In addition, at the request of the Ukrainian government, the EU activated the PESCO Cyber Rapid Response Teams in February 2022 for the first time in an operational context [40]. In February 2022, the US Cyber Command team assisted cyber rapid response teams in the search for active threats. In March 2022, Ukraine became a contributing member of NATO Joint Cyber Defense Center of Excellence. The European Center of Excellence for Countering Hybrid Threats as well strengthened its cooperation. Also, in March 2022, the EU Parliament called for immediate and full implementation of all decisions that would increase the EU's contribution to strengthening Ukraine's defence capacities, including cybersecurity.

On the local level, the main responsibility for the support from the EU to Ukrainian local authorities provides the U-Lead programme, which includes policy and legal advice to local levels, training support, and consultation. Hence, regarding the interviews with the questions about the EU support for the local authorities that facing cyber attacks during 2022–2024, some of the representatives answered that they cooperate with the U-Lead programme. As mentioned, the IT specialist of the Western community:

> Our community cooperated with the U-LEAD program, they helped us with the opening of the Administrative Services Center (TSNAP), and we also received computer equipment for the TSNAP from them.

Another example of cooperation with the U-Lead programme mentioned the decision maker from the central region community:

> Among EU projects, we cooperated with U-Lead when we opened the Administrative Services Centre (TSNAP). Also, we take part in all training, including cyber security.

The politician representative from one of the eastern communities noted:

> We cooperated with U-Lead programme as part of the opening of TsNAP in our community.

Furthermore, the East Europe Foundation as a non-profit charitable organisation supports local authorities in Ukraine with the aim to build a strong, active civil society, effective, democratic government

at all levels, and institutional development among community organisations and government agencies. Moreover, it provides cybersecurity training, digital for local authorities together with the platform zlozumilo, and some experts have indicated participation in these trainings. For example, an IT specialist of the southern community noted:

> We cooperate a lot with the U-Lead program, and we had support with openning our TSNAP. And we also, participate in the cyber security trainings that conducted by the Eastern European Foundation.

While five experts noted that they lack IT professionals in general to implement digitalisation and also to be aware of cyber incidents. Particularly, one of them from the central region of Ukraine mentioned:

> In our community, there is only one IT specialist who is responsible for whole digital and cyber processes.

At the same time, the decision maker from the northern region highlighted about physical damage in the community and their priority for rebuilding the houses of citizens, which were damaged in the conditions of the full-scale invasion of Russia into Ukraine:

> We have a lot of destroyed houses, citizens are actively using the Diia digital application, recording the damage to their buildings of the war. And in this case, digitalization is very helpful, in terms of processing and recording cases, which is a priority at the moment.

Despite the EU's support to Ukrainian local authorities, which are facing cyberattacks, mentioned by experts, there are certain challenges associated with this assistance. These challenges include a lack of personnel, lack of funding, complex application procedures for the EU projects, lack of coordination, and technical capacity limitations.

Where underfunding is interdependent with understaffing in the digital field, as funding is needed to increase staffing. Regarding the complex application procedures as to gain the EU funding for cybersecurity projects may be excluded by complex application procedures, administrative requirements, and eligibility criteria and local authorities' representatives would need training for this. According to the challenge of as lack of coordination, it may create insufficient processes of communication between Ukrainian local

authorities, national government agencies, and EU institutions, leading to fragmented approaches to cybersecurity governance and implementation. And the lack of a single strategy and coordination mechanism can undermine the effectiveness of EU support efforts and lead to duplication of efforts, and new approaches such as boundary spanning can be the response to this challenge [41]. Concerning technical capacity limitations – Ukrainian local authorities may lack the technical resources and institutional capacity to effectively utilise EU support for cybersecurity initiatives. As mentioned by the decision maker from the northern region in Ukraine:

> The community received technical support from the EU in the form of computers, but their technical capacity.

These and other challenges may be explored in future publications. There are some challenges with cyber attacks and cybersecurity described in scientific publications in the public administration field, and to a lesser extent, those related to the field of local government. Overall, cybersecurity needs to be viewed as a shared responsibility rather than being relegated to IT teams, as highlighted by Brumfield [42], especially when Ukraine has a full-scale Russian invasion of Ukraine and about the war conditions noted Guchua and Zedelashvili [43] the biggest problem is that aggressive states, terrorist organisations, non-state groups, large corporations, etc. are mostly involved in the virtual war as well. The importance of the creation the cybersecurity guidance for public managers in developing and implementing strategies was mentioned by Wirtz and Weyerer [44], and Norris et al. [45, 46] found from the conducted survey in the US that among state and local governments, the two top challenges to achieving high levels of cybersecurity were a lack of skilled personnel and lack of funding. In addition, about the lack of funding at the local level and about the crucial situation to disseminate knowledge about available sources of funding for expenses on cybersecurity, and about good practices in this area, as well as to simplify the rules for using external sources of funding, including EU funds it was emphasised by Choodakowska et al. [47]. As a technical threat, Whitehead et al. [48], indicates that includes weak technical capacities, incompatible technologies, equipment failures, and software failures.

7. Conclusions

The creation of cooperation networks of partnerships with neighbouring communities to share knowledge and cases of cyber attacks, as well as sharing experience in writing and submitting EU

projects will improve integration processes to the EU and strengthen resilience at the local level. A proposed Swiss cheese model for analysing the vulnerabilities of potential cyber attacks in communities and minimising risks to strengthen the resilience of local governments. Furthermore, examining the dimensions of cyber attacks at the local level that proposed in the article such as actor, target, motive, effect, and means would build up better cyber protection.

Consolidating existing cybersecurity training programmes onto a single platform and providing comprehensive information about them for local authorities. Considering that cyber attacks can cause harm to citizens and their data, therefore, state authorities should carry out random audits to identify any irregularities in this regard. Engage veterans, who are ready to work in the cybersecurity field that can be as win-win situation in the country, the minds of veterans will be useful to local authorities, and they will be socially active. Also, active leadership positions in the municipalities may deepen the driving digital transformation at the local level and public administration in general. Ukraine's participation in the Digital Europe programme will provide deeper support for projects on cybersecurity and advanced digital skills and will also ensure the widespread use of digital technologies in the municipalities, including through digital innovation centres. Additionally, the development of training programmes with the aim to enhance the complex application procedures skills of local authority personnel for EU project procedures that would improve the acquisition of possible projects and accordingly, funding.

Acknowledgements

Special thanks to the Scholar at Risk Programme in Norway and the Department of Political Science and Management at the University of Agder for providing the scholarship and the opportunity to conduct this research. The author is grateful to respondents who agreed to be interviewed particularly amidst the challenging wartime circumstances in Ukraine. Also, the author appreciates the generous input of the article reviewers.

References

[1] A. Frandell, M. Feeney, "Cybersecurity threats in local government: A sociotechnical perspective," *The American Review of Public Administration*, vol. 52, no. 8, pp. 558–572, 2022, doi: 10.1177/02750740221125432.

[2] A. Ibrahim, C. Valli, I. McAteer, I. Chaudhry, "A security review of local government using NIST CSF: A case study," *The Journal of Supercomputing*, vol. 74, pp. 5171– 5186, 2018, doi: 10.1007/s11227-018-2479-2.

[3] W. Hatcher, W.L. Meares, J. Heslen, "The cybersecurity of municipalities in the United States: An exploratory survey of policies and practices," *Journal of Cyber Policy*, vol. 5, no. 2, pp. 302–325, 2020, doi: 10.1080/23738871.2020.1792956.

[4] M. Kenney, "Cyber-terrorism in a post-Stuxnet world," *Orbis*, vol. 59, no. 1, pp. 111–128, 2015, doi: 10.1016/j.orbis.2014.11.009.

[5] N. Kostyuk, E. Gartzke, "Why cyber dogs have yet to bark loudly in Russia's invasion of Ukraine (Summer 2022)," *Texas National Security Review*. [Online]. Available: https://tnsr.org/wp-content/uploads/2022/06/TNSR-Journal-Vol-5-Issue-3-Kostyuk-Gartzke.pdf. [Accessed: Jan. 12, 2024].

[6] O. Evsyukova, "Political digitalization for Ukrainian society–challenges for cyber security," *Cybersecurity and Law*, vol. 5, no. 1, pp. 139–144, 2021, doi: 10.35467/cal/142199.

[7] A. Pintsch, "Decentralization in Ukraine and bottom-up European integration," in *Decentralization, Regional Diversity, and Conflict: The Case of Ukraine*, H. Shelest, M. Rabinovych, Eds., Palgrave Macmillan Cham, 2020, pp. 339–363.

[8] V.P. Hordiienko, M.L. Onishchenko, I.S. Malyonkina. (2019). *Foreign experience of decentralization of public power and the possibility of its transformation in Ukraine.* [В. П. Гордієнко, М. Л. Оніщенко, І. С. Мальонкіна. (2019). *Зарубіжний досвід децентралізації публічної влади та можливості його трансформації в Україні*]. [Online]. Available: https://essuir.sumdu.edu.ua/handle/123456789/76912. [Accessed: Jan. 12, 2024].

[9] D.O. Lukin, V.P. Gordienko, G.O. Myroshnychenko, *Fundamentals of Power Decentralization: Methodological Recommendations*, Council of Young Scientists, Sumy, 2015. [Д.О. Лукін, В.П. Гордієнко, Г.О. Мирошниченко, *Основи децентралізації влади: методичні рекомендації*, Рада молодих вчених, Суми, 2015]. [Online]. Available: https://issuu.com/34462/docs. [Accessed: Jan. 12, 2024].

[10] H. Wagenaar, *Meaning in Action: Interpretation and Dialogue in Policy Analysis*, London and New York: Routledge, 2014.

[11] C. Dyer, P. Rose, "Decentralisation for educational development? An editorial introduction," *Compare: A Journal of Comparative and International Education*, vol. 35, no. 2, pp. 105–113, 2005, doi: 10.1080/03057920500129809.

[12] O. Mikuš, M. Kukoč, M. Jež Rogelj, "The coherence of common policies of the EU in territorial cohesion: A neverending discourse? A review," *Agricultural Economics*, vol. 65, pp. 143–149, 2019, doi: 10.17221/229/2018-AGRICECON.

[13] State Service of Special Communications and Information Protection of Ukraine Report. (Jul. 10, 2022). *Report for Q3 2022*. [Online]. Available: https://scpc.gov.ua/en/articles/163. [Accessed: Jan. 12, 2024].

[14] Microsoft Threat Intelligence. (2023). *Microsoft Digital Defence Report. Building and improving cyber resilience*. [Online]. Available: https://microsoft.com/mddr. [Accessed: Dec. 22, 2023].

[15] Cybersecurity Tech Accord. (2023). *Building a voice for peace and security online. The cybersecurity tech accord's first five years*. [Online]. Available: www.cybertechaccord.org. [Accessed: Dec. 22, 2023].

[16] Council of Europe. (Sep. 01, 1988). *Chart of Signatures and Ratifications of Treaty 122 of the European Charter of Local Self-Government.* [Online]. Available: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=122. [Accessed: Dec. 18, 2023].

[17] Council of Europe. (Oct. 15, 1985). *The European Charter of Local Self-Government.* [Online]. Available: https://rm.coe.int/168007a088. [Accessed: Dec. 18, 2023].

[18] Law of Ukraine On Ratification of the European Charter of Local Self-Government of July 15, 1997 [Закон України Про ратифікацію Європейської хартії місцевого самоврядування від 15 липня 1997 року]. [Online]. Available: https://zakon.rada.gov.ua/laws/show/452/97-%D0%B2%D1%80#Text. [Accessed: Dec. 18, 2023].

[19] Constitution of Ukraine [Конституція України]. [Online]. Available: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text. [Accessed: Dec. 18, 2023].

[20] N.V. Vasylieva, O.I. Vasylieva, S.M. Prylipko, S.V. Kapitanets, O.V. Fatkhutdinova, "Approaches to the formation of public administration in the context of decentralization reform in Ukraine," *Cuestiones Politicas*, vol 38, no. 66, pp. 301–320, 2020, doi: 10.46398/cuestpol.38e.19.

[21] O. Keudel, O. Huss, "Polycentric governance in practice: The case of Ukraine's decentralised crisis response during the Russo-Ukrainian war," *Journal of Public Finance and Public Choice*, vol. 39, no. 1, pp. 10–35, 2024, doi: 10.1332/25156918Y2023D000000002.

[22] M. Rabinovych, A. Gawrich, "The conflict in Eastern Ukraine and international support for the decentralization reform (2014–2022): Theory-guided observations," *East European Politics and Societies*, vol. 37, no. 3, pp. 1036–1058, 2023, doi: 10.1177/08883254221139841.

[23] Decree of the President of Ukraine, *On the Sustainable Development Strategy 'Ukraine – 2020'* [Указ Президента України, *Про Стратегію сталого розвитку 'Україна – 2020'*], Jan. 12, 2015. [Online]. Available: https://zakon.rada.gov.ua/laws/show/5/2015#Text. [Accessed: Dec. 16, 2023].

[24] Law of Ukraine, *On Voluntary Unification of Territorial Communities* [Закон України, *Про добровільне об'єднання територіальних громад*], 2015. [Online]. Available: https://zakon.rada.gov.ua/laws/show/157-19#Text. [Accessed: Dec. 20, 2023].

[25] Ministry for Communities and Territories Development of Ukraine (MinRegion). (2022). *U-LEAD with Europe's contribution to a transparent, accountable and responsive multi-level governance in Ukraine, February 2022*. [Online]. Available: https://www.giz.de/de/downloads/giz2022-en-u-lead-four-pager.pdf. [Accessed: Jan. 04, 2024].

[26] *Monitoring of the reform of local self-government and territorial organization of power of the Ministry of Development of Communities and Territories of Ukraine as of October 7, 2021* [*Моніторинг реформи місцевого самоврядування та територіальної організації влади Міністерства розвитку громад та територій України станом на 07 жовтня 2021 року*], Apr. 1, 2024. [Online]. Available: https://www.minregion.gov.ua/wp-content/uploads/2019/01/monitoryng-reformy-misczevogo-samovryaduvannya-ta-terytorialnoyi-organizacziyi-vlady-stanom-na-1-zhovtnya-2021r..pdf. [Accessed: Jan. 04, 2024].

[27] S. Khadzhyradieva, T. Docsenko, M. Sitsinska, Y. Baiun, Y. Pukir, "Prerequisites for process management implementation in the public administration of

Ukraine," *International Journal of Criminology and Sociology*, vol. 9, pp. 2825–2833, 2020, doi: 10.6000/1929-4409.2020.09.346.

[28] T. Almarabeh, A. AbuAli, "A general framework for e-government: Definition maturity challenges, opportunities, and success," *European Journal of Scientific Research*, vol. 39, no. 1, pp. 29–42, 2010.

[29] J.P. Kesan, L. Zhang, "An empirical investigation of the relationship between local government budgets, IT expenditures, and cyber losses," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 2, pp. 582-596, 2019, doi: 10.1109/TETC.2019.2915098.

[30] K.B. Marysyuk, I.O. Tomchuk, M.D. Denysovskyi, I.O. Geletska, B.V. Khutornyi, "Diia. Digital state and E-government practices as anti-corruption tools in Ukraine Institutions," *WSEAS Transactions on Environment and Development,* vol. 17, pp. 885-897, 2021, doi: 10.37394/232015.2021.17.83.

[31] United Nations. (2022). *E-government Development Index*, [Online]. Available: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine. [Accessed: Dec. 16, 2023].

[32] J.A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic & International Studies, Washington, DC, 2002.

[33] H. Stambaugh, *Electronic crime needs assessment for state and local law enforcement*, US Department of Justice, Office of Justice Programs, National Institute of Justice, 2001.

[34] M.S. Mahmoud, M.M. Hamdan, U.A. Baroudi, "Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges," *Neurocomputing*, vol. 338, pp. 101–115, 2019, doi: 10.1016/j.neucom.2019.01.099.

[35] J.J. Plotnek, J. Slay, "Cyber terrorism: A homogenized taxonomy and definition," *Computers and Security*, vol. 102, 2021, doi: 10.1016/j.cose.2020.102145.

[36] J. Reason, E. Hollnagel, J. Paries, "Revisiting the Swiss cheese model of accidents," *Journal of Clinical Engineering*, vol. 27, no. 4, pp. 110–115, 2006.

[37] Dzerkalo Tuzhnya. (Mar. 3, 2022). *In five oblasts, the websites of local authorities were hacked: The Russian Federation spreads fakes on the.* [Дзеркало Тижня. (3 березня 2022). *В п›ятьох областях зламано сайти місцевої влади: РФ розповсюджує на них фейки*]. [Online]. Available: https://zn.ua/ukr/UKRAINE/u-volinskij-ta-vinnitskij-oblastjakh-zlamano-sajti-mistsevoji-vladi-rf-rozpovsjudzhuje-na-nikh-fejki.html. [Accessed: Jan. 12, 2024].

[38] Uman News. (May 25, 2023). *Virtual damage for defeats at the front: a cyber attack continues on the official websites of hromadas of the Uman district.* [Online]. Available: https://umannews.city/articles/289379/virtualna-shkoda-za-porazki-na-fronti-trivaye-kiberataka-na-oficijni-sajti-gromad-umanskogo-rajonu. [Accessed: Jan. 14, 2024].

[39] Ministry of Digital Transformation of Ukraine. (2023). *Research on digital skills in Ukraine.* [Міністерство цифрової трансформації України. (2023). *Дослідження цифрової грамотності в Україні*]. [Online]. Available: https://osvita.diia.gov.ua/uploads/1/8800-ua_cifrova_gramotnist_naselenna_ukraini_2023.pdf. [Accessed: Jan. 04, 2024].

[40] European Parliamentary Research Service. (2022). *Russia's war on Ukraine: Timeline of cyber-attacks.* [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf. [Accessed: Jan. 03, 2024].

[41] A. C. Lindholst, D. O. Torjesen, "Special issue introduction: Boundary spanning in the age of collaborative governance – Insights from Nordic local governments," *Scandinavian Journal of Public Administration*, vol. 28, no. 1, pp. 1–10, 2024, doi: 10.58235/sjpa.2024.22522.

[42] C. Brumfield. (May 06, 2022). *Why local governments are a hot target for cyber-attacks*. [Online]. Available: https://www.csoonline.com/article/3391589/why-local-governments-are-a-hot-target-forcyberattacks.html. [Accessed: Nov. 11, 2021].

[43] A. Guchua, T. Zedelashvili, "Challenges arising from cyber security in the dimension of modern global security (on the example of the Russia-Ukraine war)," *Eastern Review*, vol. 11, no. 2, pp. 79-88, doi: 10.18778/1427-9657.11.18.

[44] B. W. Wirtz, J. C. Weyerer, "Cyberterrorism and cyber attacks in the public sector: How public administration copes with digital threats," *International Journal of Public Administration*, vol. 40, no. 13, pp. 1085–1100, 2017, doi: 10.1080/01900692.2016.1242614.

[45] D.F. Norris, L. Mateczun, A. Joshi, T. Finin, "Cyberattacks at the grass roots: American local governments and the need for high levels of cybersecurity," *Public Administration Review*, vol. 79, no. 6, pp. 895–904, 2019, doi: 10.1111/puar.13028.

[46] D.F. Norris, L. Mateczun, A. Joshi, T. Finin, "Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity," *Journal of Urban Affairs*, vol. 43, no. 8, pp. 1173–1195, 2020, doi: 10.1080/07352166.2020.1727295.

[47] A. Choodakowska, S. Kańduła, J. Przybylska, "Cybersecurity in the local government sector in Poland: More work needs to be done," *Lex Localis*, vol. 20, no. 1, pp. 161–192, 2022, doi: 10.4335/20.1.161-192(2022).

[48] D.E. Whitehead, K. Owens, D. Gammel, J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies." 70th Annual Conference for Protective Relay Engineers (CPRE), College Station, TX, USA, 2017, pp. 1–8, doi: 10.1109/CPRE.2017.8090056.