Assessment and improvement of digital resilience in the energy crisis caused by missile strikes

Assessment and improvement of digital resilience in the energy crisis caused by missile strikes

V Zubok

G.E. Pukhov Institute for Modelling in Energy Engineering of the NAS of Ukraine, 15 General Naumov Str., Kyiv, 03164, Ukraine

E-mail: vitaly.zubok@gmail.com

Abstract. The relentless penetration of information and communication systems into all spheres of life and the widespread use of digital technologies has been called "digital transformation". Different systems demonstrate a different ability to effectively resist risks of any origin and nature, adapt to changes in the environment, maintain rapid recovery and return to maximally stable functioning. Such properties are generally called resilience. If these properties are acquired or enhanced through the use, application and development of digital technologies, we call them digital resilience. To analyze digital resilience, it is suggested to consider digital subscribers, digital needs, digital tools and their dependencies. Practical examples of such dependencies are given, which are formed under the influence of systematic missile attacks of the aggressor on the power energy system of Ukraine. The foundation was laid for a combined digital resilience assessment methodology that includes a metric approach and the theory of topological spaces.

1. Introduction

A society is being transformed to help individuals and communities use knowledge and ideas that help people realize their potential and realize their aspirations [1]. Digital transformation is a characteristic feature of a digital society whose economy is based on information technologies. The semantic field of digital transformation includes such concepts as the digital economy, digital skills, digital rights, e-government, digital innovations and much more. The digital component of existence acquires significant value and becomes an object of attack. The one's ability to resist a direct or indirect impact on the digital component of their being is known as "digital resilience". By the ability to resist, we mean the dynamic property of the individual or a system, which is embedded in its organization (functional scheme) and which serves as the basis for the ability to overcome negative impacts arising from risks, as shown on figure 1 and well-explained in [2]. Digital resilience characterizes how successfully and constructively one overcomes challenges of any origin and nature, adapts to changes in the environment, maintains stable functioning, quickly recovers to the desired balance and evolves after crisis situations based on the use, application and development of digital technologies. Digital resilience can be a property of an individuals, communities, businesses, society, the state as a whole. It is subject to analysis, measurement and improvement. In [3] authors describe the role of digital social support, digital health, and digital identities in the process of adjusting to a new reality for refugees.

Thus, much attention is spent to the resilience of cyber systems. For example, in [4] authors describe resilience metrics which link national policy goals to specific system measures,

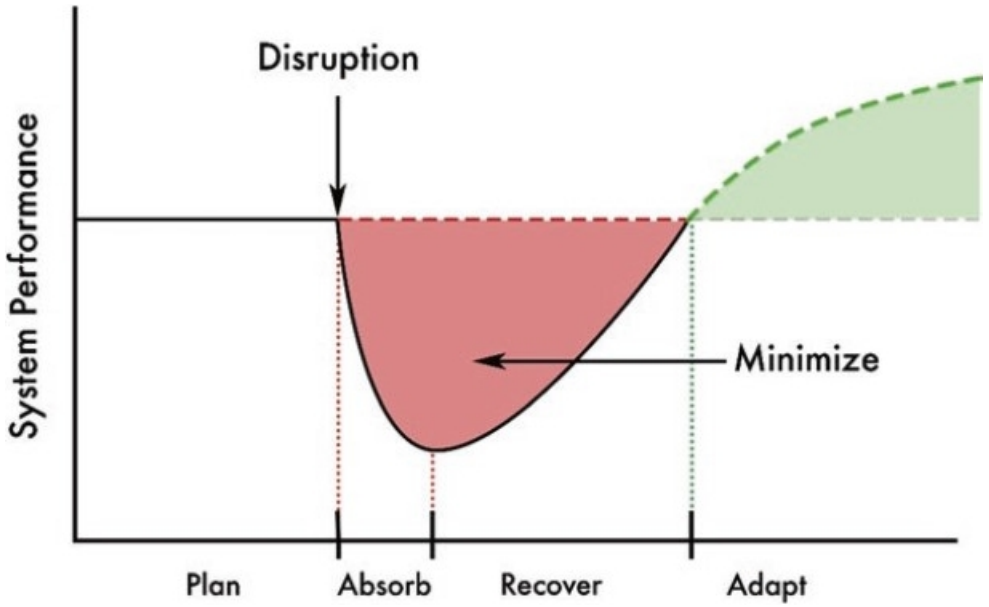

Figure 1. Stages of resilience according to National Academy of Sciences proposal.

such that resource allocation decisions. Being cyber-physical systems, power energy grids have mutual dependencies of their resilience and resilience of both electronic communications and information systems. Clark and Zonouz [5] are noted that resilience of is based on the assumption that a sophisticated intrusion may succeed to evade the deployed protection and runtime detection mechanisms and impact the underlying system services and assets excepting the core functionalities. Based on power systems case study, authors formulate cyber defense policies that ensure the resilience conditions are satisfied.

The experience of Ukraine is extremely valuable for the study of digital resilience. Ukraine is a state that was among the leaders of digital transformation before the large-scale Russian invasion. Unprecedented missile attacks on the main facilities of the power industry lead to massive emergency power outages, which are controlled by the enormous efforts of power network operators. Businesses, telecommunications operators and the general population are trying to adapt to the continuously declining level of electricity supply.

Currently, Ukraine is in transition: instead of scheduled power outages for several hours a day, scheduled inclusions for several hours a day are introduced. In December, 2022 multi-day outages took place. Each business and each household must constantly review their survival options during the growing impact of this negative factor, which directly brings us to the need for resilience analysis. In our opinion, science should contribute to the development of mechanisms for absorption of negative impact, adaptation to the new state and evolution of information and communication systems. This requires the collection, analysis, and systematization of existing experience (especially sectoral) in order to reduce the number of trials and errors in the future when creating resilient information and communication systems in conditions of limitations and uncertainties.

2. Research aim and methodology

To develop methods of increasing the resilience of information and communication systems to threats related to the electric power industry, the following tasks must be solved:

- investigate the most sensitive digital needs of digital subscribers;

- analyze the cyber threats that large-scale power outages pose and how they affect digital needs;
- analyze network architectures, types of electronic communications, data transmission systems, topologies, and determine which combinations can increase the resilience of information and communication systems (ICS) involved in providing the most sensitive information needs of the population and business.

As a result of the analysis, sets of digital subscribers – DS, digital needs – DN, and digital means (or digital tools) – DT will be obtained as depicted on Figure 2. These three sets will form a variety of tuples of three elements each ($ds \in DS, dn \in DN, dt \in DT$), as well as from two elements based on existing and available combinations:

(i) digital subscriber and one's needs: $(ds \in DS, (dn_1, dn_2, dn_3, ..., dn_n) \in DN)$;

(ii) digital subscriber and available digital means$(ds \in DS, (dt_1, dt_2, dt_3, ..., dt_n) \in DT)$;

(iii) digital needs and acceptable digital means for obtaining them $(dn \in DN, (dt_1, dt_2, dt_3, ..., dt_n) \in DT)$;

(iv) digital means and subscribers that can use them $(dt \in DT, (ds_1, ds_2, ds_3, ..., ds_n) \in DS)$;

and this list is not final.

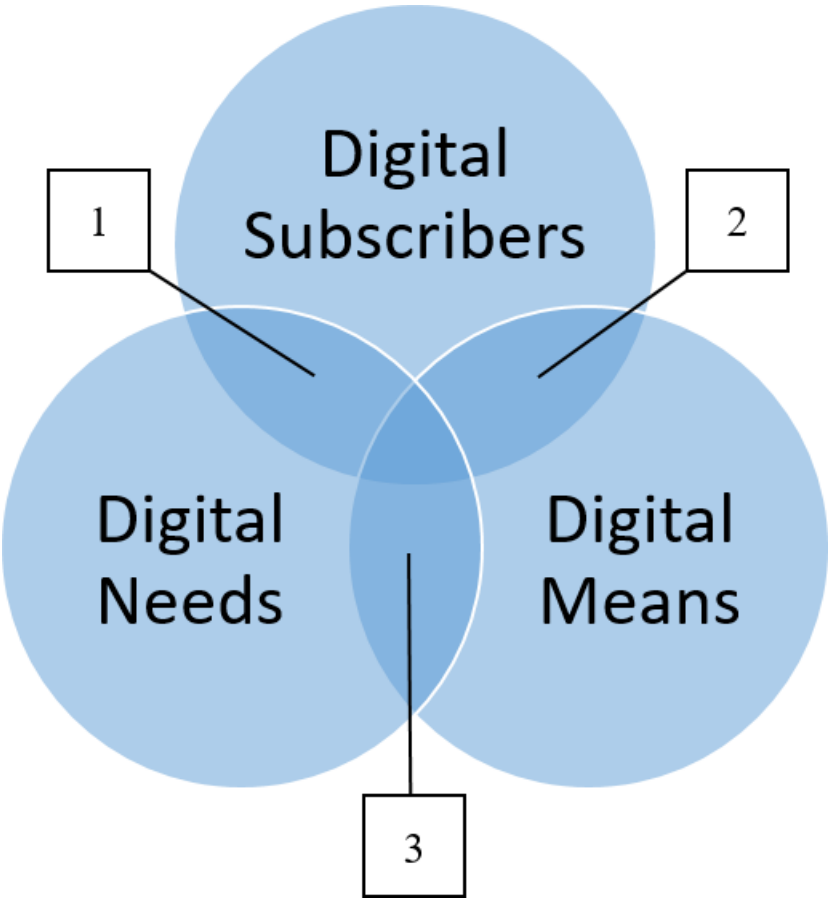

Figure 2. Overlapping sets create tuples: 1 – digital subscriber and one's digital needs; 2 – digital subscriber and available digital means; 3 – digital needs and acceptable digital means for obtaining them.

Let there exist a set $\mathfrak{D}$ such that $\forall ds \in \mathfrak{D}, \forall dn \in \mathfrak{D}, and\ \forall dt \in \mathfrak{D}$. Let there exist a system of elements of this set $\mathfrak{T}$, which includes all possible combinations of these elements, unions and intersections of these sets: $\exists \mathfrak{T} : \emptyset, \mathfrak{D} \in \mathfrak{T}; \forall \mathfrak{D}', \mathfrak{D}'' \in \mathfrak{T} : \mathfrak{D}' \cup \mathfrak{D}'' \in \mathfrak{T}; \mathfrak{D}' \cap \mathfrak{D}'' \in \mathfrak{T}$.

Then $\mathfrak{T}$ corresponds to the definition of topology on the set $\mathfrak{D}$, and a couple $(\mathfrak{T}, \mathfrak{D})$ corresponds to the definition of topological space. Individual elements of the topology represent network structures [6], that can be researched using graph theory, complex network theory, and topological space theory to develop models and methods for enhancing digital resilience.

Let's look inside of those structures. For the operation of an ordinary business, for example, a chain of retail stores, the local ICS of each store, the ICS of the head office, usually the ICS of the operator of the datacenter where ERP system resides, and several more ICSs belonging to the operators of electronic communications may be involved (modern data transmission systems are mostly convergent [7], and therefore have their own information communication systems). The functioning of the mass media (including broadcasting systems), state information services for the society, transport, healthcare, education are connected with ICS. It is also important to realize the main role of ICS in personal communication and the possibility of being in touch. First of all it's about global software platforms of instant messengers and social networks. These examples testify to the existence of an open set of cyber-social systems, the functioning of which is a component of the resilience of the entire society.

In the vast majority of cyber-social systems, the user gets access to digital services via the Internet. Therefore, sufficient connectivity and bandwidth of the global network is the most important factor in the stability of ICS, and therefore in digital resilience. Thus, the availability of Internet access is the most important factor of information security, which affects the availability of information.

3. Examining examples of dependencies between power grid and digital resilience

The Ukrainian power energy industry is unique in Europe due to the presence of a large transport system with nodes whose capacity reaches 3 GVA, as well as unique 750 KV transformers which are custom design equipment. However, these main nodes are the easiest prey to the enemy due to missile terror (figure 3).

Massive Russian terrorist missile attacks on Ukraine's electricity industry lead to massive blackouts that are difficult for power grid operators to control. One of the major missile attacks led to a blackout of the country's entire power grid for 12 hours [9]. Degradation of electricity supply goes through several stages. At the end of November 2022, instead of planned power outages (for several hours per day), planned power-ups for several hours per day were introduced, as shown on figure 4. By weekdays in rows, we can see darkest cells representing planned outages, gray ones show possible outages in case of overloads in the energy system, and pairs of bright cells mark hours of guaranteed provision of power. In fact, the schedule is rarely followed.

Russia widely uses a variety of munitions: from cheap Iranian barrage munitions (Shahed 136 drones) to complex hypersonic missiles of great destructive power. Despite the huge successes of the air defense of Ukraine, during each massive enemy strike, several munitions reach the target, causing new destruction to the energy system [10]. In the future, new missile attacks and regular multi-day outages are expected. This is a real test for the modern digital society based on information technologies and electronic communications.

Figure 5 shows a generalized individual-centric digital chain that connects a digital actor with a set of digital needs using a set of digital means. As we can see, the key element of digital resilience is the means of electronic communications (dt set). The initial element of digital resilience is the digital subscriber (dt set) – consumer of digital services. This is either an individual or a legal entity, the needs of which vary, and the availability of tools for them is also slightly different.

The risks associated with the lack of electricity power affect all elements without exception,

Figure 3. Power autotransformer destroyed by missile strike in Rivne region [8].

but not to the same extent. Let's consider what lessons Ukraine learned during the last few months of 2022.

3.1. Problems on the subscriber's side

The main component that an individual needs to meet digital needs is the electrical power supply of one's office or home or other place where private information communication systems reside. The majority of Ukrainians live in apartment buildings, they have no redundant power supplement systems or local generation facilities. To cover multi-hour power outages, private individuals and small offices massively purchase or construct *uninterruptible power supplies* (UPS). Typical UPS models for home or small office not designed for long-term autonomous operation. Their batteries designed to provide electric current for a maximum of tens of minutes. The use of non-standard batteries of large capacity leads to overheating the UPS both during long-term autonomous operation and during charging of such enormous batteries. Ignoring this danger could result in battery explosion and fire.

The use of systems based on *car batteries* has also gained popularity. Car starter batteries proved to be ineffective as a source of long-term supply of electric current. This is related to the chemical properties of acid batteries. They are prone to sulfation during deep discharge, so they can relatively reliably deliver only 0.3 part of their nominal capacity. In addition, their presence and use indoors causes additional safety problems due to the evaporation of harmful substances from the battery [11].

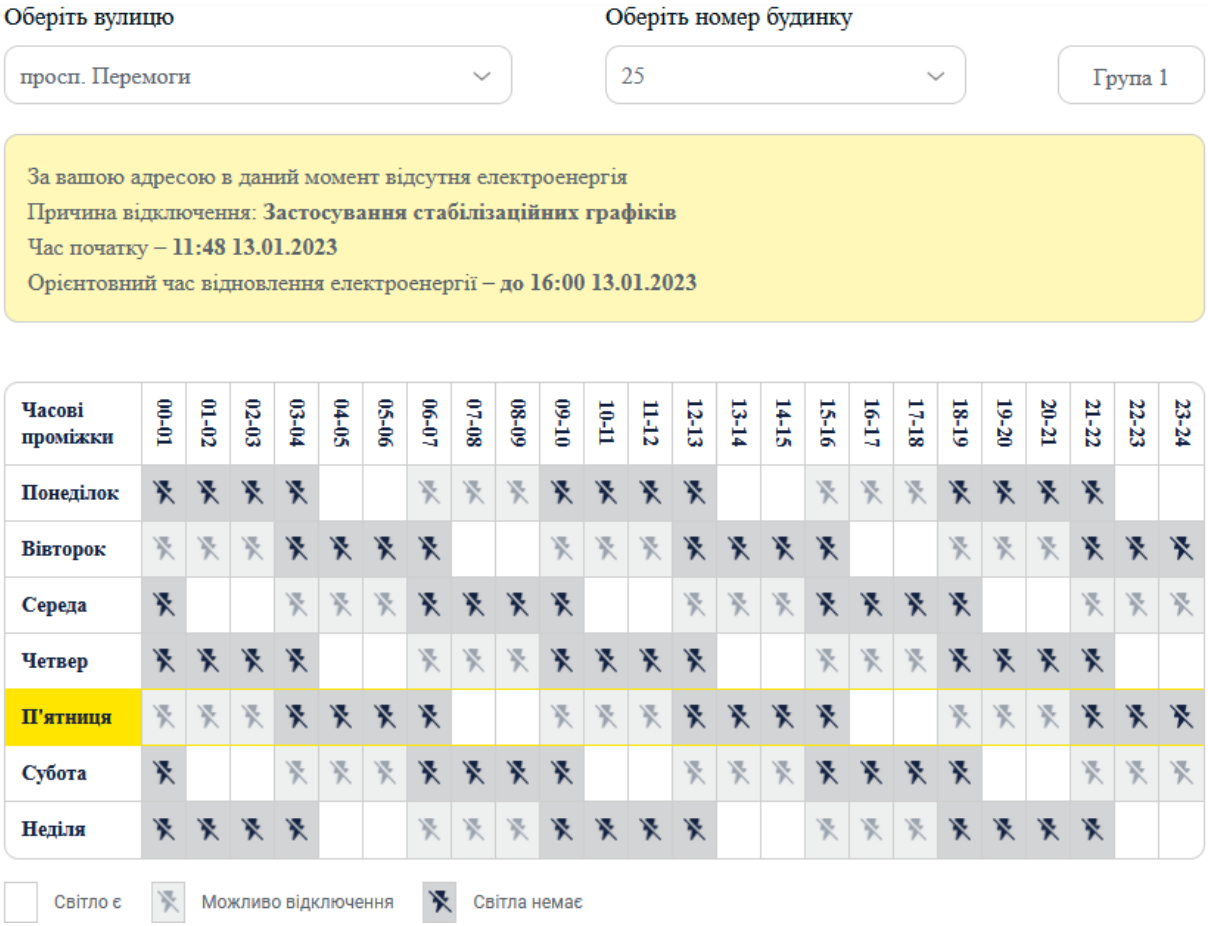

Figure 4. The real-life schedule of planned and emergency power outages for average district of the Kyiv city introduced by power distribution company DTEK (`https://dtek-kem.com.ua`).

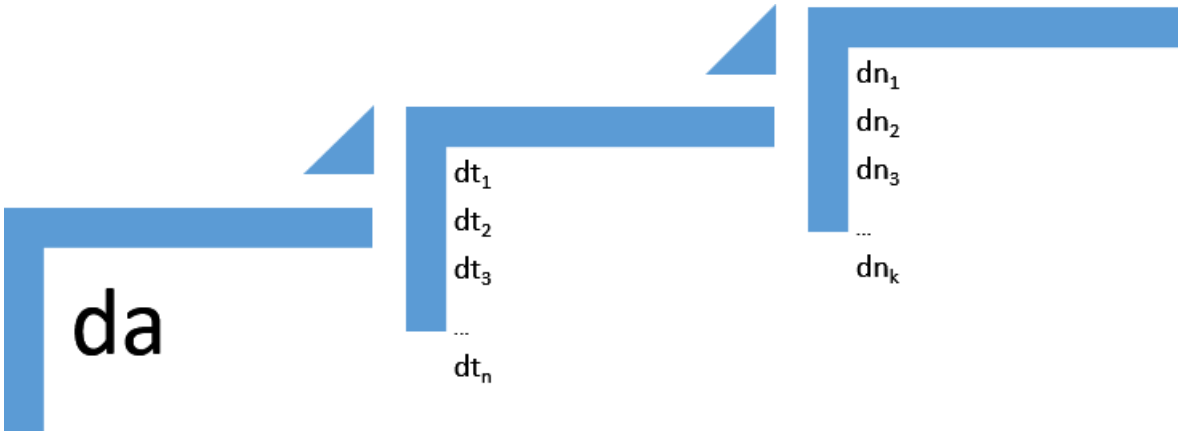

Figure 5. Generalized "digital chain" from digital actor to digital needs.

The use of *specialized low-power UPS* for individual devices, primarily for home wireless routers, has become popular. This makes sense if the local Internet provider has ensured the operation of its network during continuous power outages. The issue of Internet providers will

be discussed below. In terms of human safety, this is a very attractive solution. But it turned out that in the mode of long-term power outages, accelerated degradation of batteries of all main types occurs.

Attempts to use alternative generation (primarily *solar generation*) cause many purely technological difficulties. Residents of individual apartments who are able to place solar panels on the outside and face south can count on partial success. But Russians began their missile terror against critical civil infrastructure in mid-autumn, when the duration of daylight shortens and cloudy days increase. Therefore, the effectiveness of the panels until spring will be very low, even for the lucky ones. Solar panels should be centrally located on the roofs of high-rise buildings. It is clear that such a solution requires large project works at the level of the entire building, not a separate apartment.

The use of *generators based on gasoline or diesel engines* requires major decisions at the level of entire buildings. There are strict sanitary and fire regulations for the installation and operation of such generators. In addition, there is a significant problem of legal storage of fuel stocks, since in Ukraine this type of activity requires obtaining a license.

The use of *mobile Internet* by end users is the most popular. There are two main factors. First is that mobile Internet access in Ukraine is cheap comparing to Europe. Besides, after declaration of martial law mobile operators opened a free roaming between their networks. Second factor is that end mobile devices (4G modems, smartphones, tablets, laptops, POS terminals) have their own batteries, which can be additionally recharged from pocket power banks. However the operators' networks are affected by problems which will be described below.

3.2. Problems of the access to digital needs

Problems of the access to digital needs are mostly related to problems of architecture and topology of local Internet access provider networks. Let's review a few most common ones.

Ethernet – the main technology for Internet access in high-rise buildings. UTP cable and fiber optics are used. A typical network is divided into 2 or 3 layers – core, distribution and access. While the core layer equipment is always located in places with redundant power supplement, the equipment of other layers is closer to subscribers and much more suffers power outages. These are Ethernet switches serving the connection for several apartments (typically from 16 to 48). An attempt to provide them with large-capacity batteries ran into problems of rapid degradation of batteries due to long power outages and insufficient charge as a result. The use of the most modern type of LiFePo4 batteries with charge controllers of the appropriate power has not yet been widely introduced due to the high cost of these devices and insufficient saturation of market [12].

DOCSIS – another "last mile access" technology widely used in Ukrainian cities. DOCSIS is based on the use of coaxial cable (HFC), which used to branch out the terrestrial television signal. The architecture is shown in figure 6 and provides for the presence of a cable management telecommunication system (CMTS) per group of subscribers, as well as repeaters (amplifiers). All these devices require power supply. According to the reviews of users of the operator Volia Cable in Kyiv, this operator does not have any particular advantages in network stability in time of continuous power outages.

ADSL is a technology based on the use of a physical landline telephone network (plain old telephone service). This is a legacy technology for Ukraine, which, however, is still widespread in the developed countries of Europe [13]. Its attractiveness is that the network uses rather long last miles (up to several kilometers) without repeaters, and the operator's equipment is located next to the PSTN (telephone stations), which is always a priority consumer in the power grid and is provided with backup power as critical infrastructure. The main disadvantage of ADSL is the limited speed (usually up to 3 Mbps upstream, and 8 to 20 Mbps downstream). Many Ukrainian Internet users would prefer to return to this technology due to the inability of other

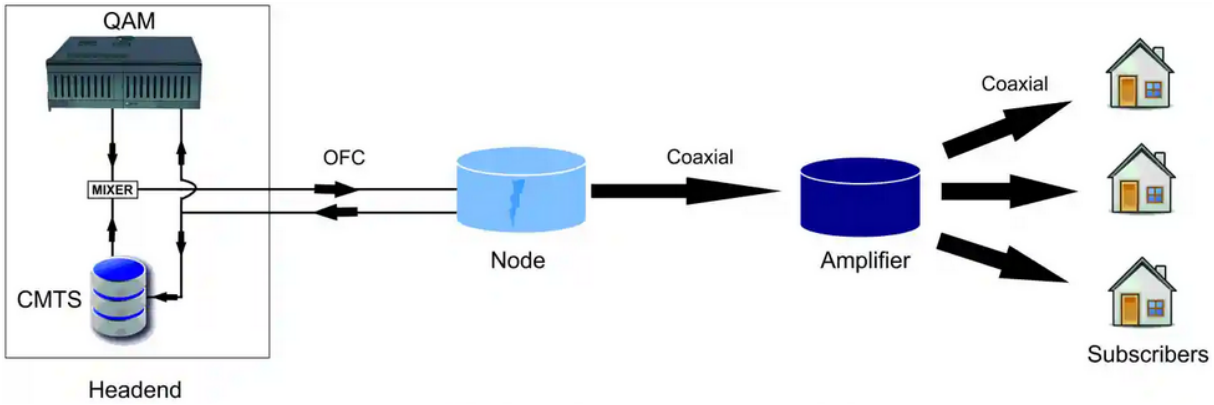

Figure 6. DOCSIS topology requires CMTS at provider's site and amplifiers at customers' buildings to be supported by uninterruptible power supplies.

providers to support networks. But it turned out that in the course of the gradual degradation of landline telephone communication, the infrastructure of copper cables is often broken and destroyed.

Passive optical networks, known as PON, is a widely known and efficient optical network architecture. Its main advantage is coverage of the widest range of subscribers using the minimum number of ports on the operator's side. This achieved by using totally passive devices called optical splitters for creating mixed tree topology, as shown on figure 7. So only optical line units (OLT) at provider's side and optical network terminals (ONT) at subscriber's side require power supply.

The problem with PON is that it is a relatively new technology. It is widely used to build new broadband Internet access networks, while the main urban networks are result of merges and acquisitions of small networks of past and keep growing on old technologies. At the moment, old networks are already physically interfering with the laying of new communications. The process of abandoning Ethernet and DOCSIS will obviously continue for many years.

Mobile (cellular) networks also suffer from power outages. 3G and 4G technologies require a high density of base stations from operators. Their location mostly does not provide for the possibility of using backup generators, and their power excludes the possibility of long-term operation from batteries. In the city of Kyiv, operator networks can be overloaded during power outages, especially in uptowns and suburbs, where the density of base stations is lower. According to the adopted decisions, the mobile operators consider the provision of voice communication as a priority service. Other services may degrade to the level of 20 percent of the nominal [15].

A review of access technologies would be incomplete without *satellite systems*. The use of a fixed or mobile satellite Internet system is also gaining popularity. Several satellite operators do their business in Ukraine. But above all, the leader is Starlink. The supply of Starlink terminals takes place under several international programs at the expense of the state budget of Ukraine, international partners and sponsors. In addition, a significant number of Starlink terminals were purchased by private consumers [16]. The advantages of such a solution are independence from local networks and operators, relative connection reliability and bandwidth which fully meets the needs of a private user or, with some restrictions, a group of consumers. The disadvantages are that in cities with high-rise buildings, users have a problem with the location of antennas (figure 8) and their power supply at the level of a particular residence. Solving problems requires centralized solutions, but Starlink terminals have proprietary limitations that require significant costs to obtain the possibility of collective use of the station for the benefit of several consumers

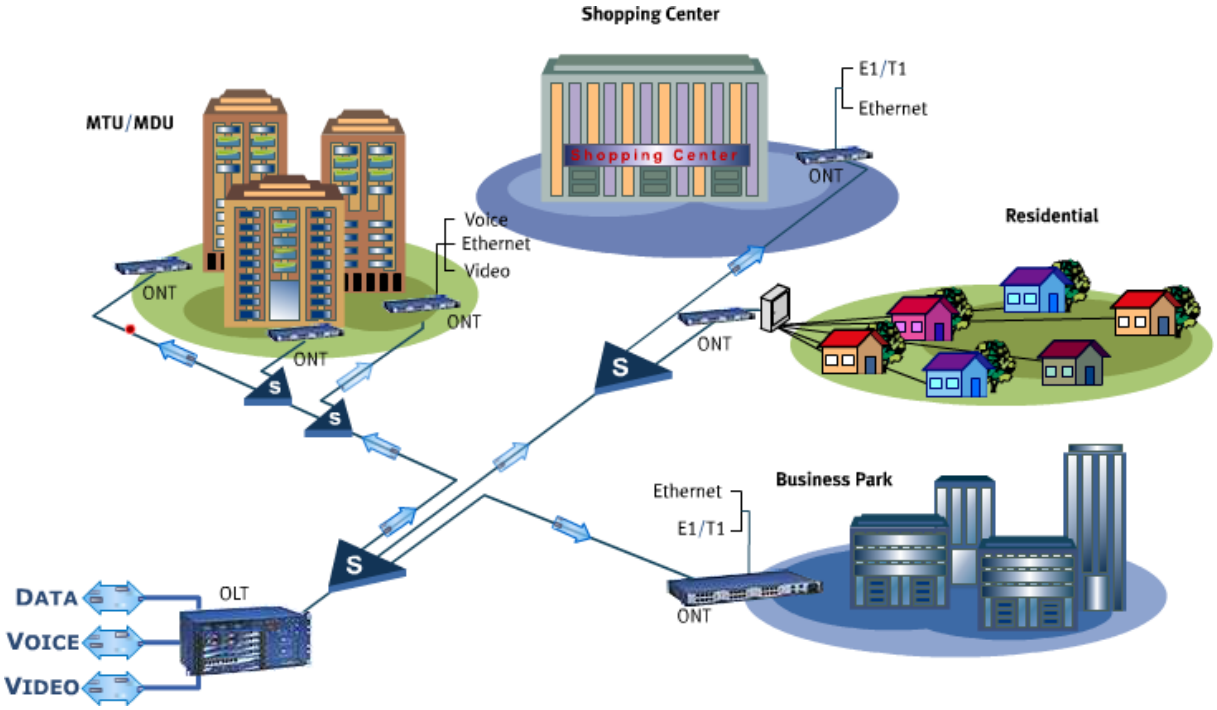

Figure 7. In Passive Optical Network topology passive optical splitters (S) are widely used. Optical line units (OLT) at provider's side and optical network terminals (ONT) at subscriber's side require power supply [14],

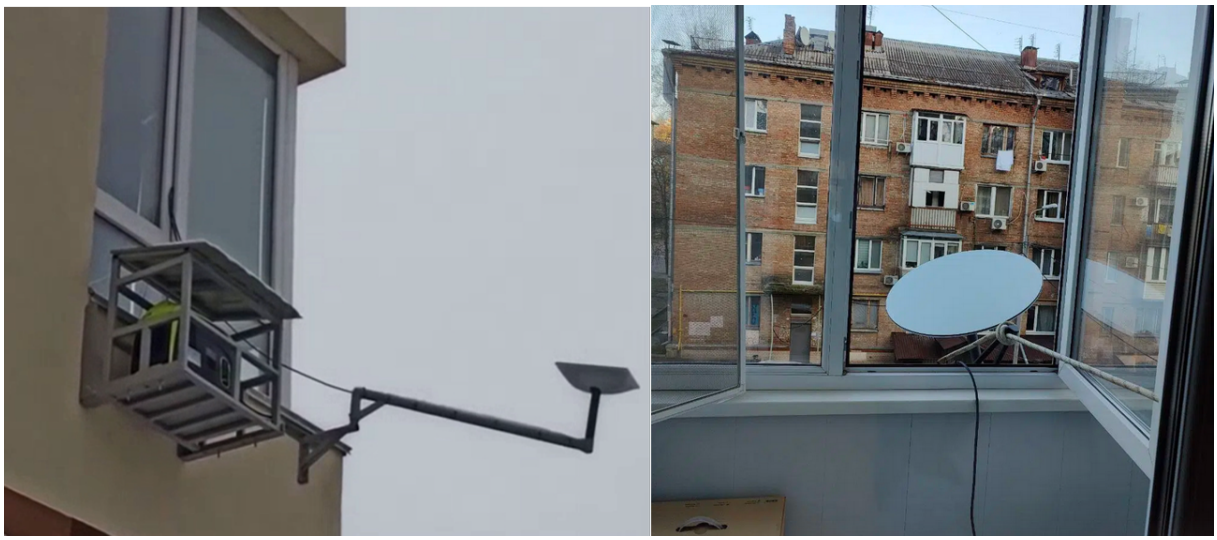

Figure 8. Examples of antenna installation of Starlink stations in cities of Ukraine (photo by `https://highload.today`).

(several apartments or offices).

Also worth noting that Ukraine has widely announced the deployment of so-called "*Invincibility points*", designed to provide heating, hot drinks, electricity for charging private devices and, in some places, Internet access. The following structural elements are necessary for the successful functioning of "Invincibility point":

- professional electric generator capable of working continuously for a long time (which is not provided by widespread household gasoline generators). Its output power capacity must correspond to the expected electricity consumption;
- structured cable system for the possibility of safely connecting several dozen devices with lithium batteries. For instance, the charge of a modern laptop consumes up to 65W, connecting 50-100 laptops requires a serious attitude to the cable system and load calculation;
- reliable Internet access, taking into account the features of operator technologies, which were observed above;
- professional equipment for building a Wi-Fi network capable of serving dozens and hundreds of devices at the same time (home Wi-Fi routers and access points are not suitable for this).

The practical experience of the city of Kyiv is that the premises of catering establishments, schools, etc. receive the status of "Invincibility points". Figure 9 demonstrates this. Each institution independently solves the problems of heating, energy, sanitary requirements, access to the Internet. "Invincibility points" are effective from the point of view of digital resilience, but their impact cannot be called significant.

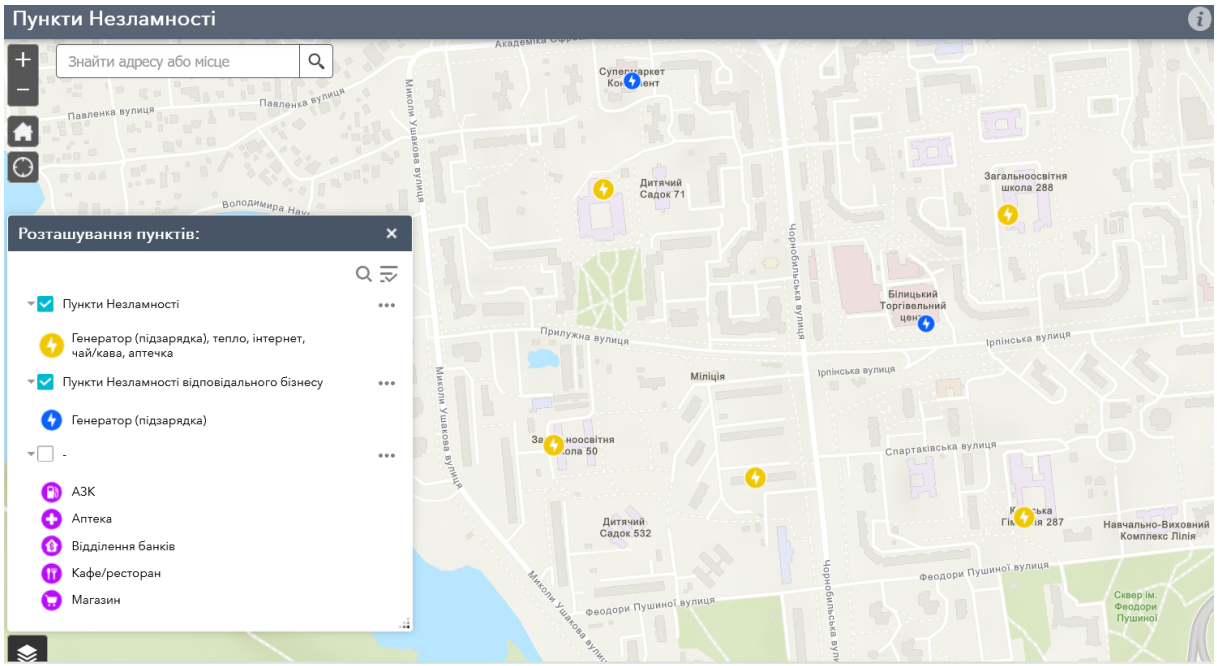

Figure 9. Map of Invincibility points in random Kyiv uptown district with population 45..60 thousand residents. Blue signs point to local stores and tell there is only charging available. Yellow signs mean that Internet access and hot drinks also available, and they point to school buildings and one social services office [17].

3.3. Generalization of the given examples

According to the proposed classification, the chain from a digital subscriber to a digital need at the very initial stage contains a large number of options for ensuring the digital resilience of the subscriber itself and their means. Each digital tool can be analyzed and compared with others that provide a similar result. This can be, for example, a SWOT analysis. But to generalize

the result, the most promising is the development of metrics that characterize the most effective resilience tools, based on their availability, cost, time of implementation, reliability and other properties. Such metric approach approved by many researchers, e.g. Linkov et al [4] and Clark and Zonouz [5]. Whereas this approach was applied for evaluation of most secure paths combination in [18], it was combined with risk management theory applied to global network topology. Such risk-aware metrics can be also introduced to evaluation of digital resilience. For this purpose, we offer to review each property of a digital tool as a component of risk, either a factor of cost or factor of likelihood. For example, let's define some of properties for digital tools as discrete:

- cost c_{dt} – how much does it cost to get this digital tool and use it;
- accessibility a_{dt} – implementation agility, or how easy it is to access this tool (or switch to this tool);
- reliability r_{dt} – a measure of the ability to perform the required functions in the given modes and conditions of this tool's use;
- power autonomy p_{dt} – how much independent this tool is from power outages in comparison to other functionally equivalent digital tools.

Then it's possible to evaluate digital resilience $\mathfrak{R}$ for an average household digital tools, which include redundant power supplies (dt_1), diversified Internet access providers (dt_2), personal awareness how to alternate power source for Internet access equipment (dt_2) and so on:

$$\mathfrak{R} = f(dt_1, dt_2, dt_3, ...dt_n),$$

where dt_n is tied to $(c_{dt}, a_{dt}, r_{dt}, p_{dt})$ in a some way which should be analysed and formalized on future steps of this study.

Similar considerations can be made when analyzing network providers, and data centers, and each element of the entire chain between the consumer and the service. This leads us to generalisation of metric evaluation of digital resilience.

4. Conclusions

Representation of individual components of the digital world in the form of a topological space opens the way to the study of the problem of digital resilience through the study of group properties, characteristics, dynamics of a large number of network structures.

In the future, the study provides an analysis of means and measures to ensure the resilience of digital service providers (from online stores to large data centers) during the crisis of the electric power industry. In addition, it is necessary to develop metrics that characterize the effectiveness of resilience tools, based on their availability, cost, implementation agility, reliability and other criteria.

Acknowledgments

This article is partially funded by the US Army Engineering Research and Development Center. We are grateful to Drs Igor Linkov and Lance Fiondella and Mr Luke Hoguewood for their discussions and assistance in preparing the article.

ORCID iDs

V Zubok `https://orcid.org/0000-0002-6315-5259`

References

[1] Kyushu-Okinawa Summit 2000 (Official Documents) 2000 Okinawa Charter on Global Information Societ URL https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html
[2] Linkov I and Trump B D 2019 *The Science and Practice of Resilience* Risk, Systems and Decisions (Cham: Springer) ISBN 978-3-030-04565-4 URL https://doi.org/10.1007/978-3-030-04565-4
[3] Udwan G, Leurs K and Alencar A 2020 *Social Media + Society* **6**(2) 2056305120915587 URL https://doi.org/10.1177/2056305120915587
[4] Linkov I, Eisenberg D A, Plourde K, Seager T P, Allen J and Kott A 2013 *Environment Systems and Decisions* **33**(4) 471–476 ISSN 2194-5411 URL https://doi.org/10.1007/s10669-013-9485-y
[5] Clark A and Zonouz S 2019 *IEEE Transactions on Smart Grid* **10**(2) 1671–1684 URL https://doi.org/10.1109/TSG.2017.2776279
[6] Zubok V and Mokhor V 2022 *Cybersecurity of the INTERNET Topology* (Ukraine: G.E.Pukhov Institute) ISBN 978-966-02-9929-0 URL https://zenodo.org/record/6795229
[7] Radicella S and Grilli D (eds) 2002 *Evolution and Convergence in telecommunications* (*ICTP Lecture Notes* vol 11) (Trieste: The Abdus Salam ICTP Publications & Printing Services) ISBN 92-95003-16-0 URL https://www.osti.gov/etdeweb/servlets/purl/20909656
[8] Horbachova A 2022 Na Rivnenshchyni okupanty vdaryly po obiektakh enerhosystemy: de vidkliuchat svitlo URL https://www.unian.ua/economics/energetics/raketniy-udar-po-rivnomu-vid-raket-okupantiv-postrazhdali-ob-yekti-energosistemi-12020256.html
[9] Semenova T 2022 Ukraine war latest: Millions still without electricity after Russia's Nov. 23 mass strikes URL https://kyivindependent.com/national/ukraine-war-latest-millions-still-without-electricity-after-russias-nov-23-mass-strikes
[10] Zelenskyy V 2022 Russia still has enough missiles for several massive strikes, we have enough determination and self-belief to return ours – address of the President of Ukraine URL https://www.president.gov.ua/en/news/rosiyi-she-vistachit-raket-dlya-kilkoh-masovanih-udariv-nam-79917
[11] West Virginia University 2007 Lead-Acid Battery Safety URL https://www.ehs.wvu.edu/files/d/0c032a15-ce2c-49b8-8d44-2d6391af0335/lead-acid-battery-safety.pdf
[12] Metaye R 2023 LiFePO4 battery (Expert guide on lithium iron phosphate) URL https://climatebiz.com/lifepo4-battery/
[13] European Commission and Directorate General for Communications Networks, Content and Technology 2022 Broadband Coverage in Europe 2021: mapping progress towards the coverage objectives of the Digital Decade Final report European Commission DG Communications Networks, Content & Technology Luxembourg URL https://doi.org/10.2759/642537
[14] 2019 PON Passive Optical Network URL https://www.reachoptics.com/pon-passive-optical-network-n106.html
[15] Prysiazhna L 2022 U vypadku povnoi dovhostrokovoi vidsutnosti elektroenerhii "Kyivstar" zmozhe pidtrymuvaty lyshe do 20% merezhi u velykykh mistakh [In the event of a complete long-term power outage, "Kyivstar" will be able to support only up to 20 percent of the network in large cities] URL https://tinyurl.com/biz-liga-kyivstar
[16] Sheetz M 2022 About 150,000 people in Ukraine are using SpaceX's Starlink internet service daily, government official says URL https://www.cnbc.com/2022/05/02/ukraine-official-150000-using-spacexs-starlink-daily.html
[17] 2022 Punkty Nezlamnosti URL https://nezlamnist.gov.ua/#map
[18] Zubok V and Kotsiuba I 2020 Empirical Study of New Metrics for the Internet Route Hijack Risk Assessment *Selected Papers of the XX International Scientific and Practical Conference "Information Technologies and Security" (ITS 2020), Kyiv, Ukraine, December 10, 2020* (*CEUR Workshop Proceedings* vol 2859) ed Dodonov A G, Lande D V, Stoianov N T, Tsyganok V V, Snarskii A A, Chertov O and Bozóki S (CEUR-WS.org) pp 199–209 URL https://ceur-ws.org/Vol-2859/paper17.pdf