The Human Side of Service Engineering, Vol. 62, 2022, 342–352
https://doi.org/10.54941/ahfe1002576

Shedding Light on Digital Vulnerability – Challenges and Solutions

Kristina Reinsalu

e-Governance Academy, Estonia

ABSTRACT

The aim of this research paper is to shed light on digital vulnerability, and to understand (a) which are the groups and activities where digital transformation could bring about the biggest change in the quality of life, and empowerment? (b) What are the main challenges they face? (c) What are the recommendations to raise their capacity and empower them? The research collects and analyses data from Ukraine and Georgia through semi-structured interviews and from public sources such as reports, strategy and policy documents. The research paper starts with defining the concept for digitally vulnerable groups and introducing two key groups for both countries which are (a) children and young people; and (b) elderly people. Then, the three main challenges of digital vulnerability (*Geographical challenge; Skills, access and awareness to use digital tools as a challenge; and media literacy challenge)* are analysed. In the context of the studied countries, we have identified the duplicating or even triple amplifying effect of one digital vulnerability on the others. For instance, the geographical difference where digital tools have potential to bridge the digital divide, e.g access to e-services, might even increase the vulnerability if the access to internet in mountainous regions is not guaranteed. The paper also demonstrates how rapidly evolving the vulnerability concept is and how circumstances around digital vulnerability challenges change. At the moment of writing, Ukraine is suffering an unprecedented, terrifying and brutal aggression from the Russian Federation, which also puts the vulnerability and digital vulnerability under a new light and sets the priorities.

Keywords: Digital vulnerability, Digital risks and motivations, Young people, Elderly

INTRODUCTION

There was a hope that digital transformation, in improving public service provision and delivery, and in promoting inclusion – with due regard to the needs of vulnerable populations – would be instrumental in mitigating the effects of exclusion and in improving people's livelihoods (UN e-Government Survey 2012). Also, the rise of social media, with its more inclusive tendencies and lower technical skill requirements, was expected to open new horizons for the inclusion of vulnerable groups. Whereas these hopes have partly become true, we are also witnessing that vulnerable groups are facing new types of risks such as digital harassment, hate speech, disinformation/misinformation attacks and other perils, which hinder those groups from fully benefitting from digital transformation.

While the reasons of the traditional digital divide (lack of access and skills) remain important, motivational reasons have also increased in importance over time. Effective interventions aimed at tackling digital exclusion needs to take into consideration national contexts, individual experience, etc. What worked a decade ago in a particular country might not work currently in a different or even the same country (Helsper, E.J. and Reisdorf, B.C. 2016).

The aim of research paper is to shed light on digital vulnerability, and to understand (a) which are the groups and activities where digital transformation (increase of digital awareness, skills, resources) could bring about the biggest change in the quality of life, and empowerment? (b) What are the main challenges they face? (c) What are the recommendations to raise their capacity and empower them?

Our research collects and analyses data from Ukraine and Georgia. The democratic development of these two countries has been relatively similar. Both countries have also placed lately a strong emphasis on digital development, especially Ukraine. However, the state of democracy is fragile in both countries, there are many inequalities and a great threat to security, which makes the vulnerable groups even more digitally vulnerable with the risks aforementioned having real dramatic consequences. Even though we are looking more closely at these two countries, there is a threat to democracy and societies everywhere, so this focus is universal.

Unfortunately, the biggest fear came true during the preparation of this article, and Russia attacked sovereign Ukraine on February 24, 2022. In addition to stalling our project activities in Ukraine at the moment, this war, and what has happened in cyberspace in this regard, puts digital vulnerability in a completely new light and cannot be also ignored by this article.

The research will make use of primary as well as of secondary data. The primary data was collected using semi-structured interviews with different stakeholders. The secondary data was collected from public sources (strategy and policy documents etc.) The research is part of the project *DRIVE*[1], and the results will be used for preparing recommendations for action, training civil society organisations and public authorities to work on these recommendations and turning two of the recommendations into a pilot project to be implemented during the project[2].

This article presents the theoretical, as well as research activities aimed at surveying the causes of vulnerability in the experience of digitally vulnerable groups in Georgia and Ukraine. Firstly, theoretical standpoints on/around digital vulnerability will be presented.

Secondly, the empirical standpoints (methodology) are introduced and so is a preliminary specification of digitally vulnerable groups in both researched countries.

[1] Project Digital Research and Impact for Vulnerable E-citizens (DRIVE) is implemented by e-Governance Academy, Estonia and funded by the organization Luminate.

[2] Unfortunately, due to the war initiated by the Russian Federation on 24 February 2022, the recommendations for Ukraine will only be further processed and implemented when circumstances allow.

Thirdly, findings from desk research and qualitative interviews, with a sample of subject experts in both countries, are considered. This input also formulates key recommendations to relevant stakeholders dealing with digitally vulnerable groups.

Finally, the conclusions and discussion on whether and how the results and practical recommendations fit into the theoretical framework, are presented.

THEORETICAL STANDPOINTS

Our first challenge was on how to define digital vulnerability. Our assumption and aim were that contrary to the traditional concept of vulnerable groups, digitally vulnerable groups are those that, in the context of rapid digital development, could benefit most from digital development and improve their position, opportunities and conditions for both daily life, and greater social and political engagement. And vice versa, that the digital transformation and potential divide may make groups that are not traditionally so vulnerable even more vulnerable.

However, to be able to identify those groups, we had to define them clearly and there are few challenges even to define vulnerability of different citizens groups as such. First, there is no universally accepted approach for measuring vulnerability, thus is even more challenging to tackle digital vulnerability. Vulnerability can stem from external shocks, and it also depends on historical, cultural, social, environmental, political, and economic conditions of a given setting. It is also clear that vulnerability is dynamic with evolving changes and heterogeneous even within the same vulnerable group.

When it comes to digital vulnerability and how it has been approached, one of the definitions that helped us narrow down this group comes from United Nations E-Government Survey 2012 and states: “The e-government divide in the case of vulnerable populations is thus about how governments of the world fare in facilitating digital access for the illiterate and low-educated, persons with disabilities, the poor, women, children, the elderly, and communities living in rural and remote areas”.

In our view, however, it links digital vulnerability too exclusively to traditional vulnerability (considering social status, education, etc.). We were also looking for a source that would point to some other factors that could make presumably less vulnerable and affected groups more vulnerable in the context of digital development unless some extra activities are designed and implemented to address this problem. As Helsper, E.J. and Reisdorf, B.C. 2016 posit, while traditional digital divide reasons related to a lack of access and skills remain important, motivational reasons increased in importance over time. They point out that effective interventions aimed at tackling digital exclusion need to take into consideration national contexts, changing non-user characteristics, and individual experience with the Internet. What worked a decade ago in a particular country might not work currently in a different or even the same country.

Evidently, the concept itself and context around vulnerability and digital vulnerability is rapidly changing.

The digital divide is no longer confined to counting telephone lines or cellular subscriptions per 100 inhabitants. It is about who has the skills and the means to access information, and then uses it to create new content and engage with other citizens to better respond to their needs and aspirations. For this kind of divide to be bridged, strong economies and healthy governance systems need to encompass a direct and targeted focus on vulnerable groups, including the specific disadvantages that they face and the unique contributions that they can make in bridging the digital divide.

From the above it is clear that digital vulnerability is very dynamic, with evolving changes depending on the changes in the context. Thus, in both target countries of the DRIVE project - in Georgia and Ukraine - the digitally vulnerable groups might vary.

However, the universal characteristic is that Digitally Vulnerable Groups (DVGs) are the potential targets of digital transformation mechanisms that, stemming from a technological divide, may cause wider and deeper new social risks.

Having reviewed the relevant literature, reports, training materials aiming at increasing the digital engagement of different target groups, we defined for further research and the project *digital vulnerable groups* as follows.

Digitally Vulnerable Groups (DVG) are those whose digital engagement in political decision-making and e-services is hindered by their lack of awareness of digital issues, access to technological benefits, and/or digital literacy and skills. Irrespective of the causes (e.g., demographic, socioeconomic and/or health status, living conditions or social position, etc.), these barriers prevent the people from reaping the benefits of digital transformation and as such, have a negative impact on their rights, interests, and everyday life.

EMPIRICAL STANDPOINTS METHODOLOGY

Once the definition was created for this project, we started to collect the data trying to answer to the main research questions:

(a) Which are the groups and activities where digital transformation (increase of digital awareness, skills, resources) could bring about the biggest change in the quality of life, and empowerment?
(b) What are the main challenges they face?
(c) What are the recommendations to raise their capacity and empower them?

Our research was qualitative only and made use of primary as well as of secondary data.

(1) The primary data was collected using semi-structured interviews with different stakeholders – institutionalised and non-institutionalised civil society representatives (CSOs and civic activists), representatives of state authorities and academia, and representatives of media.

(2) The secondary data was collected by project local country partners relying on public sources.

The implementation of the methodology started from the collection of secondary data which allowed to specify the requirements for primary data collection. Our local partners[3] mapped and analysed the previous activities and research carried out for and with these DVG and key stakeholders. The data was collected using public sources such as strategy and policy documents of target countries, reports, online databases, etc.

As the mapping showed, the priority target groups within digitally vulnerable groups according to our definition are similar in both countries – these are (a) children and young people; and (b) elderly people. Evidently both groups have completely different needs, barriers, and enablers for benefitting from digital agenda. However, the digital vulnerability for both target groups in both countries was similarly related to digital awareness and digital literacy including privacy, security (cyber hygiene) aspects, digital skills, and media literacy.

In the second phase of the research the interviews with key stakeholders were conducted. The aim of the semi-structured interviews was to provide a comprehensive view of the key problems and needs of those vulnerable groups to plan further activities in the project (e.g. actions proposals, trainings, pilot projects).

In Georgia we conducted 17 semi-structured qualitative interviews with experts from the public sector, research institutions, unions, and CSOs active in the relevant subject areas.

The interviewees were selected based on the initial mapping and identification of DVGs stemming from the desk research. Once target groups became clear, so did the ecosystem of public and CSOs directly dealing with the target groups and/or the digital transformation and the relevant social groups in the country.

Interviews were carried out in the span of 10 days during the month of January 2021, partly on-site in Georgia and partly via Microsoft Teams.

In Ukraine all the criteria for selecting interviews were exactly the same, and we conducted 11 semi-structured qualitative interviews with 17 experts from the public sector, research institutions, unions, and CSOs active in the relevant subject areas (some interviews were group interviews). However, differently from Georgia, all interviews with Ukrainian exerts were conducted via Microsoft Teams due to the growing security risk in Ukraine already in January 2022.

In both countries we interviewed the representatives of public authorities (Ministries of Education and Science, Ministries of Information Technologies) and civil society organizations which conduct trainings on digital awareness, literacy, media, digital media literacy, etc. Also, the politicians from local parliaments were among the respondents.

[3] In Georgia the local research partner was the Institute for Development of Freedom of Information (IDFI); in Ukraine the partner organization was 2030: Tech for Public Good.

FINDINGS

GEORGIA

In Georgia, 86% of households country-wide enjoyed internet access as of 2021[4]. However, disparities by geography run across the nation, with a net distinction between cities and rural areas (91% and 78.9% respectively).

Regarding our focus groups, the initial mapping of the problems showed that in Georgia the main digital gaps which need further addressing were:

(a) young people in general for whom their digital vulnerability is concerned first and foremost with privacy, etc. issues
(b) younger children whose digital vulnerability is connected to access and digital literacy to education, especially in rural areas
(c) elderly people for whom the vulnerability is hidden in access and literacy, to use the existing e-services.

According to data from Georgia's National Statistics Office[5], up to 9% of children aged 6-14 had either never used the internet or used it over 3 months ago – a *red flag*, in light of the shift to remote learning of most public schools caused by the pandemic. As per the same dataset, 58.4% of people aged 60+ had never used the internet at the time of the survey. The most common uses of the internet among the latter group revolves around social networks, reading online news sites, and making internet calls/video calls. Meanwhile young people aged 15-29 have a more diverse distribution of uses, including finding information about goods and services, looking for employment, and internet banking.

From the 17 interviews carried out, the Georgian subject experts mentioned a total of nine relevant topics that contribute to understanding the diverse instances of vulnerability that DVGs face in Georgia. Most of these apply to the general population, however, there are few which are more characteristic to our priority vulnerable groups - young people and the elderly.

The key challenges regarding digital vulnerability are as follows:

- *Geography as a challenge*

In case of Georgia this is a challenge what has clearly a very wide impact to digital vulnerability affecting young people as well as elderly people. Georgia is a very mountainous country, and as one of the interviewees, a telecommunications expert pointed out, "*Challenges for DVGs are mostly concentrated in the highlands and mountainous regions.*" The lack of solid infrastructure to grant broadband connection keeps several villages in different regions isolated from the web and hinders elderly people to get access to e -services and schoolchildren to access distant learning. Ideally technology should decrease these gaps and empower people who have physical obstacles to e-services. In

[4] https://www.geostat.ge/en/modules/categories/106/information-and-communication-technologies-usage-in-households

[5] https://www.geostat.ge/ka/modules/categories/106/sainformatsio-da-sakomunikatsio-teknologiebis-gamoqeneba-shinameurneobebshi

this case, we can say the opposite, geographical conditions have a so called duplicating effect on digital vulnerability.

Another geographical aspect and duplicating effect is related to the fact that even if families may have internet connection, they might not have the necessary number of devices to allow kids to follow classes or do homework when they need to. Our respondents point out that even if schools have internet, this does not imply, anyway, that the student has access to it all day long and the full potential of equipment is not used for increasing the access, digital literacy etc.

In sum, for both priority groups there is a huge gap in between rural and urban areas – rural youth and rural eldery'sl' digital vulnerability is even bigger than in their traditional vulnerability.

- *Skills, access and awareness to use digital tools as a challenge*

When we talk about skills, access, and awareness, one of the surprising findings is that whereas Georgia advances its ICT infrastructure[6], and these projects are supported also by digital literacy activities to improve the accessibility to e-services, the vulnerable groups, especially elderly aged 65+, display very low interest in using the internet for accessing the services. They use it purely for social media and videocalls.

Considering the high risk of misinformation, disinformation and other threats which are bigger every day in this whole region, the digital almost paradoxically makes those groups this way even more vulnerable to those threats.

Furthermore, it is also obvious from the secondary and primary sources that the awareness on cyber -hygiene and the perception of cybersecurity generally is very low. One of the respondents, a representative of CSOs, mentioned that one of the biggest barriers for e-services is the need to authenticate yourself to be able to start using the e-service. This refers, that the normal procedures for securely consuming e-services for unskilled or unaware and unfamiliar people might be a big barrier.

Talking about the importance of cybersecurity and perception of risks, one of the respondents was sure that young people are the least vulnerable. In the current dramatic security situation, especially in Eastern Europe, this sounds like an understatement, and the fact that our respondents paid so little attention to cyber security, is very alarming.

- *Media literacy as a challenge*

The challenge very much connected to the general awareness to the use of digital, and cybersecurity awareness, is media literacy. We are referring here to the lack of knowledge on how to verify information etc, so all people, but especially young people due to their general lack of experience, as well as elderly people, due to their poor searching skills of information in online spaces, are extremely vulnerable digitally and are potential victims of troll factories what are working in this region to full steam.

[6] Login Georgia project which is funded by World Bank and focuses on infrastructure

Additionally, it is clear, that one of the challenges in Georgia to address the digital vulnerability issues is poor coordination of the activities and lack of clear division of the roles of different stakeholders dealing with digitally vulnerable groups.

UKRAINE

In Ukraine the problems and gaps were generally similar:

(a) For young people, the digital vulnerability is mostly connected to cyber security aspects,

(b) For the elderly, the digital vulnerability is rather related to the access to e-services and awareness and literacy on how to use them.

In the Ukrainian case within these groups, we identified a clearer need to focus on retired people and children (under 15 years). Firstly, these are in fact the two largest digitally vulnerable groups. Secondly, these two groups are at the same time opposite groups in terms of interests, needs, knowledge and experience. Thirdly, the results of a previous study show that these groups are currently not sufficiently covered by the analysis or have a chance to be taken into account in the promoting digitalization processes.

Our work on secondary and primary sources demonstrated that the challenges related to digital vulnerability for identified priority groups are similar in both countries.

Therefore, below is only a quick summary of the findings on key challenges. The most important and similar findings for both countries are analysed in the context of the literature and summarized in the last, conclusions and discussion chapter.

Also in Ukraine one of main *challenges is a geography* - living in rural arears where the connectivity is very poor, automatically makes people digitally vulnerable. This challenge is strongly interlinked with the second main challenge, present also in Georgia, which plays an even more important role in case of Ukraine. 53% of Ukrainians have below *basic level* skills, with 15% of them not holding any at all. By comparison, in this respect, Ukraine lags behind neighbouring Poland (65%) and Hungary (69%), while in Germany the number of people with digital skills is more than 1.5 times higher (78%). Age and the urban/rural divide matter in diversifying the data. Almost 85% of people aged 60-70 years old present below *basic level* digital skills. In addition, 57% of villagers do not have basic digital skills. However, despite the relatively small gap between villages and cities (7-8%) there is a gap in this indicator between regional administrative centres and all other settlements[7].

Like in Georgia, one of the biggest digital vulnerability challenges in Ukraine for young people and children is that lack of availability of devices and access in public areas to the Internet, which limits access to education. Schools, libraries, and other public facilities could compensate for the lack of computerization in households. However, these institutional public areas also do not always have an Internet connection. The disparity between those

[7] Lifelong learning and digital education in Ukraine - Business Law Electronic Resource.

areas that *have* from those that *have not* is higher when regional inequalities are taken into account, as well as the relative situation in villages and settlements.

However, it is worth pointing out very good examples from Ukraine, where we identified many good examples of e-platforms that educate people on important topics, including media literacy, cyber security[8], etc. Ukraine also has very good e-school online platforms for teachers and children[9], etc. Yet, the use of these good examples is hampered by the *geographical and digital access challenges* referred above.

In Ukraine, as in Georgia, nevertheless, the biggest risk is related to both *skills and awareness but also media literacy challenges*. 49.5% of Ukrainian children aged 10-17 years old have been victims of online fraud.

CONCLUSIONS AND DISCUSSION

This chapter presents the main challenges and recommendations on how to approach them. The findings are interpreted in the context of the literature.

First, when we talk about digital vulnerability we can argue, that despite of the fact that internet penetration is rather high in both countries, that there are digitally vulnerable groups who are not necessarily overlapping with traditionally vulnerable groups. For instance, young people – high level of access to internet does not guarantee that young people and/or children are using internet. The data shows that even with pandemic the numbers of schoolchildren who have not accessed internet is relatively high, which shows one clear type of digital vulnerability - limited access to education. There are various reasons for that –digital skills, literacy of parents is low, their awareness of benefits of digital tools is low and technology is rather seen as a risk for their kids. To serve as an example, being a schoolkid in a rural area incidentally creates a condition of double vulnerability, estimated 35,000 schoolchildren in summer 2020 who had never used internet and/or did not have access to distant-learning tools in Georgia. The negative effects have been deepened by the COVID-19 pandemic, with the forced reliance on remote and digital tools it triggered.

One practical recommendation would be to learn from one of the cornerstones of Estonian digital success - the Estonian Tiger Leap Project experience[10] which focused on computer classes with good connection in all Estonian schools back in 1996 and organized free access to students also after classes. The project played a key role in avoiding the digital vulnerability of schoolkids from socially deprived families.

We also identified some serious legislative gaps related to digital access to education. For instance, in Georgia, even now, two years since the start of global pandemic which remarkably hinders access to education globally, the distance learning is unregulated and basically illegal in high education system.

[8] https://osvita.diia.gov.ua/en/courses?theme_id~\protect$\relax=$~32

[9] https://novaukraine.org/prometheus-world-class-online-courses-for-ukrainian-teachers/

[10] https://www.educationestonia.org/tiger-leap/

Thus, we can argue that the pandemic context has very strongly deepened the digital vulnerability for those groups that were not previously traditionally vulnerable - children and young people in general.

Moreover, in the context of the countries studied, it is relevant to talk about duplicating or even the triple amplifying effect of one kind of digital vulnerability to others. For instance, the geographical difference where digital tools have potential to bridge the digital divide, e.g access to e-services, might even increase the vulnerability if the access to internet in mountainous regions is not guaranteed.

Hence, we can state that the hopes expressed by many authors that digital technologies enhance the wellbeing of young people in the way they use it to connect with others who may be distant geographically and build a sense of community that doesn't depend on transport, money or geographic location (Campbell & Robards, 2013, cited by Vichta et al 2018) have not been fulfilled.

Thus, one concrete recommendation for governments to develop their digital agenda would be to pay extra attention to infrastructure developments, supported by digital literacy program in rural areas because the vulnerability factors are duplicated due to these geographical conditions.

Secondly, in the case of elderly people in Georgia, most of the people out of those few who are connected to the internet, use it for social media or internet calls which further increases their digital vulnerability to disinformation, misinformation, cyber-crimes etc. This fear about very limited use of internet and vulnerability concerning using of social media is also expressed by Betts et al 2019 with reference also to many other authors (Hope, Schwaba, & Piper, 2014; Jung, Walden, Johnson, & Sundar, 2017).

Wagner also refers to the clear link between motivational factors and digital vulnerability - older adults who frequently use technology have higher levels of interest in technology, have greater self-efficacy for technology, have also better cognitive abilities and are less vulnerable (Wagner et al., 2010).

Also, Betts et al argue that the less non-users of Internet there are, more important motivational factors will become (Betts et al 2019). Moreover, they argue that the more advanced the country technically is and smaller the non-user group is, more digitally excluded and more marginalized (i.e. there are fewer people like them) and also socially vulnerable they are. Betts et all refer to them as "digital underclass" (see Helsper, 2012, 2014, referred by Betts et al 2019).

This is clear that all policies and interventions have to focus on these hardest-to-reach groups, employing a wider range of interventions addressing multiple reasons for disengagement.

Lastly but not least, the current situation in the region and world demonstrates how dynamic the vulnerability concept can change and how priorities among digital vulnerability challenges can change as well.

Very low awareness on cyber hygiene, media illiteracy, etc. are the number one risks at the moment for our digitally vulnerable groups as well. No illusions here - Russia's aggression in Ukraine has made it crystal clear around the world how important it is to combat troll factories who poison vulnerable groups with fake news, disinformation, and misinformation. This means that media literacy and cyber resistance must be a priority, not only in the studied countries, but globally in order to combat forces hostile to democracy.

To conclude, digital vulnerability for both target groups in both countries is related to digital awareness and digital literacy including privacy, security and cyber hygiene aspects, digital skills, and media literacy. Although the latter is addressed to some extent in both countries, the media literacy - misinformation and related topicsdeserves constant and increasing attention in our target countries, especially in the current geopolitical security situation[11].

REFERENCES

Betts L.R, Hill R., Gardner S. E. (2019) “There’s Not Enough Knowledge Out There”: Examining Older Adults’ Perceptions of Digital Technology Use and Digital Inclusion Classes. *Journal of Applied Gerontology*. 2019; 38(8):1147–1166. doi:10.1177/0733464817737621

Campbell, A. J., & Robards, F. (2013). Using technologies safely and effectively to promote young people’s wellbeing: A better practice guide for services. Young and Well Cooperative Research Centre. Retrieved from https://www.health.nsw.gov.au/kidsfamilies/youth/Documents/better-practice-guide.pdf

Helsper EJ (2012) A corresponding fields model of digital inclusion. Communication Theory 22(4): 403–426.

Helsper EJ (2014) Synthesis report: harnessing ICT for social action. Peer review in social protection and social inclusion. EU Commission, DG Employment report. Available at: http://ec.europa.eu/social/BlobServlet?docId=12437&;langId=en

Helsper, E. J , Reisdorf B. C,(2017), The emergence of a “digital underclass” in Great Britain and Sweden: Changing reasons for digital exclusion Volume 19 Issue 8, page(s): 1253–1270.

Hope, A., Schwaba, T., & Piper, A. M. (2014). Understanding digital and material social communications for older adults. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 3903-3912). Toronto, Ontario: Association for Computing Machinery. doi: 10.1145/2556288.2557133

Jung, E. H., Walden, J., Johnson, A. C., & Sundar, S. S. (2017). Social networking in the aging context: Why older adults use or avoid Facebook. *Telematics and Informatics*, *34*, 1071–1080. doi:10.1016/j.tele.2017.04.015

Olson, K. E., O’Brien, M. A., Rogers, W. A., & Charness, N. (2011). Diffusion of technology: Frequency of use for younger and older adults. Ageing International, 36, 123–145. doi:10.1007/s12126-010-9077-9

United Nations E-Government Survey 2012

Vichta R, Gwinner K, Collyer B. (2018) What would we use and how would we use it? Can digital technology be used to both enhance and evaluate well-being outcomes with highly vulnerable and disadvantaged young people? *Evaluation Journal of Australasia*. 2018;18(4):222-233. doi:10.1177/1035719X18804638

Wagner, N., Hassanein, K., & Head, M. (2010). Computer use by older adults: A multidisciplinary review. Computers in Human Behavior, 26, 870-882. doi:10.1016/j.chb.2010.03.029

[11] Once again it needs to be noted how dramatically the situation has changed during this research. At present, vulnerability has taken on a completely different meaning in the context of Ukraine and, globally as well.