DRIVE: Digital Research and Impact for Vulnerable E-citizens Project

Qualitative research, stakeholder interviews and recommendations of Digitally Vulnerable Groups in Ukraine

eGA
e-governance academy

2030
Tech For Public Good

IDFI
Institute for Development of Freedom of Information

This Country Report has been produced within the DRIVE project, supported by a grant from Luminate.

This Country Report is a joint work of several people: written by Federico Plantera, based on the interviews conducted by Kristina Mänd and Kristina Reinsalu from eGA. The research methodology was coordinated by Kristina Reinsalu, and the process and report were supported by Katrin Nyman-Metcalf from eGA. Ukrainian partners, Yaroslav Kotlyarevskyy and Ruslana Rudnitska form 2030: Tech for Public Good (2030TPG) made their contribution to all mentioned phases of joint project. The editing was completed by Radu Serrano and the design by Serhii Buravchenko.

The authors of this Country Report are very grateful for the time, vast knowledge and effort that the interviewees gave to the process.

DRIVE: Digital Research and Impact for Vulnerable E-citizens Project

is led by e-Governance Academy (eGA) in partnership with the Institute for Development of Freedom of Information (IDFI) (Georgia) and 2030: Tech for Public Good (Ukraine).

The vision is the **vulnerable citizen groups in Ukraine and Georgia** to have **a changed quality of life** by being **digitally engaged in political decision-making** (advanced policy development) and **services**, and to have **necessary conditions, awareness and skills** for that.

Though a large number of different elements can contribute to a changed quality of life and digital engagement, **the DRIVE project aims** at two outcomes: **public authorities (PAs)** and **civil society organisations (CSOs)** are **(1) aware of the digitally vulnerable groups**, their needs and gaps in their digital literacy and access (tools and skills), and (2) they are able **to work together** and have **improved skills** to design smart responses to address these needs and overcome the gaps, and implement transparent, accountable and participatory e-governance (e.g. a new tools, platform, etc.) to **prevent the digital divide** (further).

In the DRIVE context, we define the **Digitally Vulnerable Groups** as 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**.

The main activities by the partners to reach the project aim and contribute to the ultimate vision include:

1. an ecosystem building research in Ukraine and Georgia to (1) identify two digitally vulnerable groups in Ukraine and Georgia (per country); (2) map previous activities and research carried out for and with these DVG and key stakeholders involved in the activities; (3) provide a comprehensive view of the key problems and needs of these DVG to plan further activities in the project (actions proposals, trainings, pilot projects); and (4) identify the gaps and needs of the PAs and CSOs;

2. based on the research, prepare and share **recommendations** to CSO and PA stakeholders with hands-on activities on how to improve the situation and work with different digitally vulnerable groups and avoid widening the digital divide, and highlight the best practices;

3. based on the recommendations, create a **training curriculum** and implement (1) two online **trainings for CSOs** and (2) four **seminars for PAs and CSOs**, and (3) prepare a set of **action proposals** for both countries;

4. based on the trainings and the action proposals, facilitate the process of designing one **pilot project** per country and supervise their implementation.

In addition, eGA and local partners work together as competence centres **facilitating communicating and disseminating** the aims and activities in the region, and collaborate to bring more capital to the region for the digital and data rights ecosystem.

The DRIVE project lasts from September 1, 2021 – August 31, 2023 and is supported by a grant from Luminate.

Introduction

Under the evermoving force of digital transformation, technology advances, and so do devices and their relevant use cases. Such dynamic push carries a direct impact on people's lives as the ultimate users and subjects of technological progress. Societies, in the multiplicity of stakeholders that compose them, must take stock of *where it all leads*, who and how benefits from digital transformation, and who and how remains left behind.

Governments and Civil Society Organizations (CSOs) cover a major role in assessing the changing conditions that generate vulnerability for specific social groups. As countries around the world face the opportunities and challenges that come with digital transformation, these stakeholders are tasked also with evaluating the effectiveness of the changes at play in terms of 1) social exclusion; 2) the participation in the wider national economy of at-risk groups; and 3) the prevention from worsening of existing inequalities.

Digitally Vulnerable Groups (DVGs) are those who, due to the technological divide, may potentially be exposed to deeper new social and economic risks from the digital transformation. Broadly defined in this project,

Digitally Vulnerable Groups 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.

In this Country Report, we present the research activities aimed at surveying the causes of vulnerability in the experience of Ukrainian DVGs. First, a preliminary specification of DVGs in Ukraine is presented based on desk research. Secondly, findings from qualitative interviewing with a sample of Ukrainian subject experts contribute to unravel how different factors interplay to deepen people's vulnerability – in the face of increased technological uptake for learning and accessing e-services. Lastly, recommendations to relevant stakeholders are provided, as emerging from the subject experts' input and the authors' own analysis.

It must be specified that research design and qualitative surveying took place previous to February 24, 2022 (United Nations, 2022). On this date, troops of the Russian federation started a full-scale invasion of the territory of Ukraine. Therefore, the research design, questions, and interviewees' answers were formed in times of peace, and with such context in mind they should be read, analyzed, and regarded. Although the ongoing war does not invalidate the findings and recommendations in this Country Report, it shall be kept in consideration that its scope might have to apply to 1) a changed situation in terms of territorial sovereignty, or 2) different possibilities for realizing said actions while the country suffers the foreign aggression, as well as after it.

DVGs in Ukraine, explained: Who and why?

Digital vulnerability is a phenomenon determined equally by existing and new conditions of exclusion or vulnerability in society. While digital transformation pertains predominantly to service delivery in a digital form (from a strictly public administration-related viewpoint), the scope of change and its effects widen when society and the economy as a whole are taken into account.

For reference, as defined by the European Commission in the Digital Economy and Society Index (DESI) methodology, measuring the degree of communities' effectiveness in keeping up with digital transformation must look into 1) connectivity; 2) use of internet and digital tools; 3) a population's digital skills (European Commission, 2021). With such focus, we can assess their degree of access to digital public services, and how well they may reap the market and socialization opportunities that technology enables.

While individuals who might not have previously found themselves at a position of vulnerability may face new setbacks – although for some groups their general situation may improve – previously at-risk groups could see their socioeconomic standing in society fall back even more under the pressure of digital transformation.

Topics in focus across the existing research

Existing research shows that only a limited number of studies have been conducted about the impact of digitalization processes on potentially vulnerable groups in the Ukrainian society. The coverage of such groups is not extensive in scope but allows to initially hint at a series of topics that do highlight salient issues in the way Ukrainians use – or do not have the possibility to use – the internet.

Despite the rapid development of digitalization and big-scale international projects (one of them is EU4DigitalUA* which focuses on the further development of digital government infrastructure, public e-services, cyber security and data protection), there are still many challenges regarding connectivity, digital skills and cyber hygiene in Ukraine.

Connectivity

Today, 35% of all rural residents do not have the possibility to access the internet via fixed broadband. 18% of these simply find the cost of connecting to the internet via fixed broadband too high – about twice the median price in urban areas, while disposable income resources in these settlements are much lower than in cities.

Additionally, 22% of citizens live in settlements where there is no mobile internet access, and 31% do not have the opportunity to connect to mobile broadband internet. Unsurprisingly, the vast majority of these citizens live in rural areas (Government of Ukraine, 2021a).

* The EU4DigitalUA project is funded by the EU, and implemented by the e-Governance Academy (eGA, Estonia) and the International and Ibero-American Foundation for Administration and Public Policies (FIIAPP F.S.P., Spain) in close collaboration with the Ministry of Digital Transformation of Ukraine

Digital literacy and skills

Digital literacy assessments of the population at large show that 53% of Ukrainians have below *basic level* skills, with 15% of them not having any at all. By comparison, in this respect, Ukraine lags behind the neighbouring countries where the number of people with digital skills is higher – such as in Poland (65%), Hungary (69%), and Germany (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 (Government of Ukraine, 2021a).

There is no clear ecosystem for the formation of digital skills throughout life. Digital education and STEM (Science, Technology, Engineering and Math) programs in schools, universities, non-formal education, and further training are not aligned. Moreover, the introduction of digital technologies in public and social services is not always accompanied by parallel training in digital skills on how to use these (for example: e-queue in medical institutions and e-Health in general, e-social services, etc.) (Boychenko et al., 2021).

Availability of devices and access in public areas

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 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.

Reasons for this are to be found in market failure, where operators and providers are insufficiently motivated to implement internet connectivity in commercially unattractive locations and areas. In addition, due to the low level of funding, educational and cultural institutions are not connected to high-speed internet, they are insufficiently computerized, and do not have the necessary software.

Use of internet and risks

According to a study by the Institute of Social and Political Psychology of the National Academy of Pedagogical Sciences of Ukraine, which covered more than 2,800 students, most students (86%) use the internet almost daily and only 4% of them do not use the Internet at all. On average, young people spend 4 hours a day using the Internet (Kostitsky, 2013). There is a clear trend, however, pointing at students using the internet rather for leisure. While this may contribute to develop digital literacy skills, to a lesser extent such intention is explicitly pursued. This happens mostly through becoming familiar with online content, the purpose of its distribution, the subtext, the formation of the ability to select and evaluate such content.

Perhaps in line with such high internet use, young people are often targeted by internet fraud. 49.5% of Ukrainian children aged 10–17 years old have been victims of online fraud – figure that diminished to 34% when taking into account the adult population (18–70 years old) in general (Ionan as in Machuskyy, 2021).

Accessibility in light of disability or impairment

In terms of accessibility for groups with physical or cognitive vulnerabilities, not everyone has the possibility to use state and communal websites, applications, or digital services. Not all government web portals are adapted for use for people with visual, hearing and intellectual disabilities. Though such practice is not entirely absent, it is limited to a small number of examples, and thus may create barriers to accessing socially important information. Consequently, state and communal applications too lack the necessary accessibility tools and framework for people with physical or cognitive disabilities (Government of Ukraine, 2021).

Tests have been conducted on the topic over 82 websites and 7 service platforms (UN Development Program, 2021). Despite such issues having been acknowledged by the government strategies (Government of Ukraine, 2021) and being set to be addressed, the tests carried out show that most government sites are only partially tailored to the needs of people with disabilities. The main issues pertain to the difficulty – if not *impossibility* – for users to identify the presence and functional purpose of certain elements due to inappropriate font sizes, tactile elements, contrast, lack of information or explanations of use.

Age as the common denominator of life stage-related challenges

As it appears, vulnerable groups in Ukraine at large may include a diverse list of categories: internally displaced persons; pensioners; people with disabilities; women with the double burden of professional life and childcare; low-income people and the unemployed; the rural population; veterans; and many others, identified as people in any difficult life circumstance. But when it comes to digitalization, the list expands. A definition of DVGs in Ukraine comes at this point to include, for example, children.

The common denominator among all these groups is that to distinct stages of life correspond different challenges, that manifest in interaction with geographic, social or economic variables to make said issues deeper or more specific. For example, at the stage of life when engagement in formal education happens, children and the youth may be more exposed to become DVGs. Among older, labour market participants instead, digital vulnerability may affect low-earners and people's possibility to put digital skills *to work* for a job search. At the retirement stage, we can find the elderly and pensioners as potential DVGs.

In this report, age spectrum is then assumed as the starting point of the analysis to look into the needs of DVGs. In particular, the focus lies on the two ends of said continuum: children, and the elderly.

Firstly, simply in terms of numbers, these two groups make up about more than a third of Ukraine's population, with 60+ years old seniors and children under 15 years old making up, respectively, 22.9% and 14.8% of residents. Secondly, in many respects, these two groups could be regarded as having a wide range of differences in terms of interests, needs, knowledge, experience, and purpose for the use of internet. Lastly, reviewing the literature shows that these groups are currently not sufficiently covered by research – which is limited on digitally vulnerable groups in general, and lacks a systematic approach to targeting these two specific groups in society.

Methodology

To delve deeper into the experiences of DVGs in Ukraine, in *tandem* with the local consortium partners, we have conducted 11 semi-structured qualitative interviews with 18 Ukrainian experts from the public sector, research institutions, and CSOs active in the relevant subject areas.

Semi-structured interviews prove to be particularly beneficial when it comes to keeping a research agenda open-ended. They give respondents the possibility to hint at areas of inquiry not previously formulated but are eventually fundamental in the deeper understanding of a certain phenomenon (Fedyuk and Zentai, 2018). If the *age group continuum* hypothesis falls short in surveying DVGs experience of vulnerability, we also open to plausible, new theory-generating answers. In our case, indeed, the nuances of the method applied effectively.

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

Following the interview sessions, software application Otter.ai was used to generate transcripts from the full recordings in all but five instances, where this was done manually due to use of the language speakers felt more comfortable with. All transcripts were then checked with their respective original recordings where available, to ensure accuracy of reporting. Direct quotes included in this report have been edited for the purpose of clarity, where needed, and are indicated in an *italic* font format.

Findings from qualitative interviewing

From the 11 interviews carried out with 18 respondents, the Ukrainian subject experts mentioned a total of seven relevant topics that contribute to understanding the diverse instances of vulnerability that DVGs face in Ukraine. The degree to which they affect young people and the elderly varies, in some of such instances negatively affecting more the elderly group. Based on people's need to access different digital opportunities and e-services, and with the stark differences reported across the age spectrum, the skills required also differ along the age continuum.

Here we categorize our findings from the qualitative interviewing sessions according to the seven relevant themes highlighted by the subject experts, delving deeper – where applicable – into the age group specifications of the vulnerabilities experienced by DVGs. The topics are presented in order from the most relevant to the least (but still spontaneously) mentioned, per number of occurrences on the total of the session carried out.

Main issues

1. Cybersecurity (9 mentions)

The most salient and cross-cutting issue identified by our expert respondents is cyber hygiene. It is given priority in the list *ex aequo* with skills, access and awareness based on the number of times it has been brought up as a concrete vulnerability and risk. Not only nine respondents mentioned it, but also proceeded to elaborate greatly – though mentioning explicit similar challenges – on the topic in their respective interviews.

The risks DVGs are exposed to, according to our pool of interviewees, pertain mostly to individuals' behaviour on the internet, rather than national or organizational matters. Thus, issues pertaining to cybersecurity appear to be largely connected to the subdomain of cyberhygiene.

A related issue that cuts across our target age groups is that of personal data protection and awareness. *"The security of personal data and cyberhygiene are important aspects for both groups. This applies to social networks and the display of personal data. In this regard, clarifications and training of people is very important,"* one respondent says. *"Before opening access to new technologies, people must undergo appropriate training. Because the damage that can be done as a result of ignorance and abuse can be greater than that suffered due to lack of access to internet,"* another respondent wisely highlights. In and for themselves, as a consequence, *"people who have no knowledge about cybersecurity become a new vulnerable group,"* the same respondent continues.

While certain threats might be directed at both young and old users, such as frauds and scams, it is believed that more attention should be placed on the younger generations. *"The main threat or challenge* *to children as a vulnerable group is cybersecurity. Especially now that in Ukraine there is a massive digitalization effort going on in all spheres of society, and especially education as a result of the pandemic,"* one interviewee warns. *"I believe the strongest impact in this sense could be on cybersecurity literacy addressing issues relevant to both children and parents – cyberaggression, online bullying, data leaks. We hear a lot about these reports,"* a field-specific respondent says.

Attention must also be drawn to those elderly people who decide to actually use digital services but must do it from a public computer and a public network. *"Consider for example a pensioner applying for digital services at a computer in an administrative centre. It's not very secure, because when you apply on someone else's computer, you can store your password, or insert your USB flash card with your digital signature. I think it's important then to not just teach people digital skills, but also how to be safe on the internet,"* another respondent points out.

2. Geographical location (9 mentions)

One of the biggest issues, unsurprisingly for such a large country with inter- and intra-regional differences, is the geographical location. Nine among our pool of respondents mentioned this as a salient problem determining situations of digital vulnerability for both groups in focus – and beyond. "*Because when you take COVID into account, then we might say that all the population becomes vulnerable*," one respondent begins with. "*In remote villages and mountainous areas there are problems with connectivity, worsened in the case of natural disasters,*" such as floods for example. In the words of the same interviewee, the reasons are two-fold: lack of availability of internet, interacting then with the mentioned issues of access; but also simply a matter of lifestyle, and the different needs of people living in those areas. We shall highlight as well that some territories within the borders of Ukraine are under occupation. Consequently, other salient issues – such as lack of access, skills or awareness – and the way these *weigh on* geographical location might vary from area to area also depending on this factor.

It is worth noting that geographical location is perhaps one of the few factors of vulnerability highlighted to interplay with other issues – mainly skills, access and awareness to use digital tools – and doing so for both the elderly and younger generations. A few respondents hint that the cause of this problem can be found in market failure and return on investments. "*I believe the issue of small towns and remote areas is quite important because, if you look at the Ministry's plans to expand connectivity, then quite logically these proceed with covering areas that take a relatively small investment to become connected. But if we're instead talking about remote areas, or with very low population density, then it becomes more problematic because the return on investment dramatically decreases,*" one interviewee says. The reference is here to the limited investment capacities currently on the market: without a further leap forward or assistance in that sense, vulnerabilities due to geographical location might remain unsolved.

E-commerce, for example, could greatly benefit from increased access to connectivity in rural areas. "*I believe online shopping could work great there, because there is a much wider variety of goods and for a cheaper price. But beyond that, also banking, postal operators.*" The urban/rural gap manifests itself even more strongly in the case of the possibility to use the internet for younger generations. "*Contrarily to the elderly, younger people display a high level of activism* [proactivity] *in using and searching for new tools to use. They seek electronic services that can help them solve everyday problems,*" one respondent says. "*But then you see a big gap* [in vulnerability] *between young people living in cities, and those who reside in rural areas. While this does pertain to digital skills, it's also a matter of infrastructure and access to quality internet,*" another respondent highlights.

Interestingly enough, another group is subject to the geographical disadvantage – but outside the border of the country. "*DVGs, in my opinion, are also people living abroad. Many young people live outside Ukraine but if they have an expired digital signature, for example, they have no possibility of receiving a new one. And with an expired digital signature, they can't apply for digital services. That became clear in the case of my friends, who recently had a baby, and were applying for childcare-related services*," a respondent points out.

In this line of thinking, Ukraine – as well as other countries in a similar situation – has a high and increasing number of displaced people. It must be paid attention to the particular context within which this research is being carried out. In the current context, many find themselves stranded both within and outside the territorial borders of the country. While in the beginning (2014) the issue might have affected mainly citizens in contended eastern regions and Crimea, millions are currently displaced – while life however, as much as possible, goes on. As does the need to access internet and potentially use digital services, essential when even people's own safety and the physical integrity of government buildings are at serious risk. Such context must be kept in mind as, to previous digital vulnerability, geographical displacement adds to existing disadvantage.

3. Skills, access and awareness to use digital tools (8 mentions)

On par with safety on the internet, cyberhygiene, and geographical location, the most mentioned vulnerability for the two target groups in this project pertains to digital skills, access to and awareness of ICT tools. For the elderly, this starts from the very basic: *"Our elderly people who lack digital skills are also very afraid of smartphones or computers, because they think that they could accidentally push some buttons and, you know, destroy the whole world,"* one respondent says.

In that sense, many respondents established a link between lack of skills as a consequence of lack of access or awareness. In relation to the last two elements and the elderly, it has been noted that *"Even if they go to the administrative centre, there is no sense* [for them] *in learning how to apply for a digital service – because they just might not have access to internet, so why should they learn it? Also, to present this application once a year, or even in several years? In their view, of course it's better to apply in person."*

But this introduces the topic of motivation, very much tied to that of awareness. *"When focusing on skills of the elderly, motivation is really important. As an example, my grandma lives in another city. She has learnt to use a tablet, the smartphone, to make online payments – because she needed a way to communicate with us. My grandad, in Kyiv, doesn't need to learn anything because when he needs to apply for the pension in electronic form, he just asks me if I can do it for him. So motivation is very important in teaching people to use digital services, especially when they need these just once or twice a year, or less,"* one respondent recalls. This is consistent with findings from desk research, which are worth recalling here. Young people, in general, seem to lack motivation to develop digital competences and cyberhygiene practices, unless these are somehow connected with using the internet for leisure or entertainment. In the case of elderly people, instead, the lack of motivation is aggravated by that of trust in digital tools.

The issue with digital skills, however, is more widespread and does not stop at the eldest generations. According to recent research in Lviv, carried out in the extended territory of the municipality, about one in five residents (22%) does not possess any digital skills at all. The research proves the point about elderly people being left behind by the country's ongoing digital transformation – among 61+ year old seniors, the percentage raises to 50% in Lviv, and 63% in the suburban area. On the contrary, younger people aged between 16 to 30 years old, are among the most tech savvy – only 2% of them don't have any digital skills at all. The fact that the average percentage of citizens using e-services is 20% tells us, taking Lviv as a case study for large urban areas, that more issues still lie somewhere else.

"We have a project, the 'academia of digital literacy', with a target to increase to 60% by 2025 the proportion of residents whose skill level is above basic. It will entail free offline courses for residents and in this way, we can provide information about the basic practices, as well as some basic skills," we are told.

But who participates in these courses? Another respondent working mostly with young people aged between 18 to 25 years old, refers that *"there is a gender imbalance, most participants in our education courses are women. Particularly when we talk about* [gathering] *knowledge – so awareness – men are not so active in taking part in educational programs."* Something to dedicate attention to, in light of the *motivation* topic already mentioned by another respondent.

It is interesting to note that, if there's the need for such push in terms of motivation, perhaps one way the lack of awareness manifests itself is exactly through a lack of knowledge over *why* citizens need digital skills and to use ICTs. Even before the moment of entering a class or joining a course, the need to make sure that there is a distributed infrastructure and device availability to allow trainings to take place in locations *close* to the end-users emerges (more on geographical location in the next section).

But then, what matters is that the *middlemen* – teachers, lab technicians, educational centre operators – hold already those skills they are tasked to teach. *"The question is, sometimes it looks like even the people who work in digital education hubs lack these skills. That is why we hope we will be able to develop some curricula to train them. It would be the first step because without properly trained people in libraries, it will be impossible to pass knowledge onto others,"* a respondent warns. Same point applies to schools, and teachers in schools. *"The situation is very different, between regions and between schools.* [Those who don't] *They do not use technology because of not knowing* [themselves] *how, or maybe they have fears over using it. This tells us that technology must not only be bought, but* [the knowledge] *transferred to these teachers, and check afterwards that they use it."*

Lastly, an additional point must be made about those people whose access to internet, and communication tools at large, is impaired by other people – both directly and indirectly. This is the case with the LGBTQIA+ community, as highlighted by one respondent on the matter. Community members might indeed not have at their disposal the necessary privacy and space to seek social support and counselling by means of e-services. Abuse and domestic violence, unfortunately, also fall within the realm of such human-caused impairments to access. One respondent highlighted, indeed, how victims' possibility to seek help and support by means of communication tools could be cut off by perpetrators of such violence and restrictions. Though this latter category may pertain rather to vulnerability as a consequence of outright criminal activity, it has come up in the interviews and should then be kept under consideration. On par with access, when such groups do manage to get the information needed, it is possible that this is not suitable to address these specific groups' needs.

4. Disability (4 mentions)

Aside from regional, knowledge and socio-economic inequalities, disability too comes into the picture to deepen digital vulnerabilities. People with disabilities, it seems needless to explicit it, already suffer from disparities in opportunity and life chances compared to the rest of the population. ICTs can be the only way towards being more integrated in society and help them overcome some of the barriers otherwise present. But to this end, digital services must be designed in ways that tap into those needs.

When talking about people with disabilities, *"It's a* [vulnerable] *group less based on age and more on other criteria. It is necessary to make sure that they have at their disposal the tools needed to access* [services], *which is why platforms must be modernized – even the existing ones – to make sure that the right standards are in place,"* an interviewee responds.

Both in the case of children and adults, but particularly with the latter, *"Sometimes internet is the only way for them to communicate with the world of work, or to get information. But I'm not sure if these people have the access and devices that allow them to be integrated in our world. This is a category to dedicate attention to, because thanks to technology, there is a good chance of improving their lives and make them take part in our economy and society,"* another respondent highlights.

Residual issues

1. Need for human interaction (3 mentions)

Somewhat related to the aforementioned need to communicate, one of the DVGs identified *triggers* a cause for digital exclusion of vulnerability out of sheer choice preference. It would not come as a surprise to hear that the elderly do prefer offline options to online or distant ones – among the latter, phone calling for information is still these people's choice. "*This category of residents needs to have a* [physical] *space where they can communicate with the city council, or with city officials. They feel it as a need, so we can't just bypass it with some advertising or an online course. They need this real-life communication*," one respondent says.

According to another respondent, "*There are different instruments available today to present claims or applications. There is a mobile app, there is the website. And maybe these instruments are not perfect, but still quite easy tools to use. Nevertheless, they* [the elderly] *still prefer to go through a hotline. Phone calls are the most popular option"* by public demand in that age group.

2. Socioeconomic situation (2 mentions)

According to two of our respondents, the issue of access to technology (devices and connectivity) may give ground to a more dominant focus on the socioeconomic situation. This takes shape as a form of *inherited* inequality and vulnerability: households' living standards and disposable income might simply be too low for children to see granted their possibility to access online tools.

"*During the pandemic, this emerged particularly in education. For example, with 100,000 children from extremely low-income families enrolled in boarding schools, about 42,000 of them were limited in their distance learning by the absence of technological and networking capabilities once we entered lockdown,"* one respondent highlights. Continuing on the point, "*The same applies when children from low-income families need to submit graduation exams or have to perform tests and applications. They must do it from school, with the support of a teacher, because they lack the necessary devices at home."*

In parallel, children's vulnerability in this sense may manifest through the living conditions they experience with their parents – when these might, altogether, form a vulnerable family. "*For example, in the case of parents with addictions. Or very poor families. In some suburban areas of Kyiv, when entering a house, there is a lot of mess or garbage around, the flats lack proper furniture or food supplies*," the respondent points out. Consequently, it is hard to imagine that such situation wouldn't worsen a child's exposure to increased digital vulnerability (to the end, for example, of education).

3. Digital literacy (2 mentions)

Digital literacy is only marginally mentioned by our sample respondents. But instead of this signalling a lack of attention towards the topic, the issue is considered instead in a more specific way.

While digital literacy matters, it does when in relation with another of the larger talking points brought up by interviewees. This can be observed in particular when the formula itself – "digital literacy" – is made explicit in relation to the two most relevant topics pointed out by the sample respondents: namely, cyberhygiene and digital skills. See above then how digital literacy is as an integral part of vulnerabilities due to cyberhygiene and digital skills.

Stakeholder relations

A whole other topic is represented by stakeholder relations. As emerged from conversation with the interviewees, the stakeholders involved in addressing the digital vulnerabilities of the groups identified result to be the following:

- The state, represented by authorities and government institutions;
- Local authorities;
- Educational institutions and educational establishments;
- International organizations and CSOs.

Interviewees mentioned several projects and initiatives already up and running on same or similar topics, aimed to address the needs of the target groups identified in this research. This might also suggest why, on questions regarding the system of connections and ties between different stakeholders, we rather received a fairly limited amount of input on who should or could do more, be involved in a certain existing or new project, or refocus their actions to better target the groups' needs.

However, such findings might also point at a peculiarity of the Ukrainian context in terms of relations among relevant stakeholders seeking to address digitally vulnerable groups. It is possible that government organizations – of all levels – and CSOs, despite being committed to already active and initiatives towards decreasing the vulnerability of our target groups, might do this in a rather siloed manner. This means that even though many initiatives are operative and being implemented for similar expected outcomes, these might run in parallel without establishing a contact between each other.

Bridging different projects or organizations in tackling digital vulnerability is not a must, if such active projects do manage to have an impact and decrease target groups' disadvantage. However, the issue of *bridging nodes* – creating networks between relevant organizations and stakeholders to achieve set outcomes for relevant groups – could and should be discussed and agreed upon. This would, at least, clear doubts on whether the resulting observation from our interviews is purely coincidental, and the situation is *good as it is*; or whether some involved stakeholders wish – or even demand – for more collaborative practices to take place.

Research note: Cross-cut and additive digital vulnerabilities

The sessions of qualitative interviewing in Ukraine have both confirmed the initial patterns identified in the desk research phase, while highlighting also an issue often overlooked by observers seeking to explore the dynamics of vulnerability.

First, age groups prove to be a relevant interpretative lens through which to analyze digital vulnerability. To distinct stages of life correspond different challenges. With regard to our specific categories in focus, those experienced by the elderly do vary in comparison with those suffered by children and young people. This means that specific attention must be dedicated to specific target groups when designing policies and project interventions, as one-size-fits-all approaches may fall short in addressing each group's actual needs. But while age serves as an initial common denominator, further care must be applied when vulnerabilities *add up*.

The second interpretative lens of our findings leads, indeed, to the topic of *additive* digital vulnerabilities. Though the link between different factors and sources of disadvantage has not often been explicitly established by interview respondents, the issues they highlighted hint at an interaction between the common denominator mentioned above (age and life stages), and specific issues that may worsen the digital vulnerability of the groups in focus (Simien, 2007; Purdie-Vaughns and Eibach, 2008).

As an example of such synthesis, let us consider young people. Though the known vulnerability emerged from desk research, geographic location may deepen the gap between young people's variation in digital skills, access and awareness, between urban and rural areas. Conditions of disability or social exclusion, though obviously not on the same level, may respectively trigger worsening effects on an already comparatively disadvantaged situation. The same interpretative framework, with changed factors and sources of vulnerability, can be applied to the elderly – and so on.

Recommendations

From the analysis of the expert input received from both public sector interviewees and members of CSOs, recommended activities should cover two macro-aspects highlighted – 1) the salient, topical issues DVGs face in their use and experience of digital opportunities, and 2) the lack of collaboration between relevant stakeholders to address digital vulnerabilities.

Recommendations are presented here with a general formulation, to allow and give input for further discussion and planning with Ukrainian public authorities (PAs) and CSOs during the capacity-building events and subsequent action plans and projects.

Specifically, these recommendations contribute to the project objective in a way so that PAs and CSOs are aware of digitally vulnerable groups and their needs, and have improved skills to engage these groups and to prevent the prevalence or deepening of digital divide. They are presented here in the form of desired outcomes, for which specific action lines will emerge during the dedicated workshop activities.

The ultimate objective of developing these recommendations is to improve the quality of life of the groups of vulnerable citizens identified in Ukraine, by increasing their digital engagement in political decision-making (advanced policy development) and services usage, while enjoying the necessary conditions, awareness and skills for that – however, being mindful of the recent and future developments of the ongoing war affecting the country. Such major issue will require project partners and stakeholders to consider different scenarios of implementation for the recommendations introduced here, depending on the circumstances.

Awareness of digital vulnerability and DVGs

PAs and CSOs should be aware of what digital vulnerability is, and who digitally vulnerable citizens and groups are, as well as their unmet needs and salient issues in reaping the benefits of an increased digital economy and society. As shown, issues may pertain cybersecurity, geographical location, access and digital skills, and more.

When planning new policies, services and projects, PAs, CSOs, donors and businesses should scan and scrutinize the policies, services and projects envisioned. The goal is to evaluate the impact – positive, neutral, negative – these could have on digital vulnerabilities and DVGs.

Capacity to plan and implement projects strategically while monitoring and considering the digital divide

On the supply-side of financial help and support to innovative projects, funding organizations and donors active in Ukraine should keep in mind and be aware of issues of digital vulnerability when planning, launching, and implementing grant opportunities and calls. As one respondent highlighted, *"Digital vulnerability is a relatively new topic"* in the Ukrainian context, and developing awareness and sensitivity towards it is among the main aims of this project.

It is suggested to increase local authorities' capacity and awareness towards accessing available funding from donor entities and higher-level institutions, particularly when projects aimed at tackling digital vulnerability may fall under their own level of decision-making and jurisdiction. This, to generate a two-fold outcome: firstly, increasing local authorities' capacity to address digital vulnerabilities, while unlocking the data and concrete information that such local administrations have on context specificities; secondly, and as a consequence, to make local authorities take a more active role in the development of programs and strategies locally – leveraging unique local and context-specific knowledge.

CSOs, by their part, should consider digital vulnerability in order to not worsen, but ideally prevent and/or decrease the digital divide with their projects, particular service provision, and advocacy activities.

CSOs need to be aware of and empowered to advocate for digital rights, need for connection, etc. It is a skill set not limited to only to the digital-related sphere, but more generally about engagement and public policymaking. A skill set that is expected and needed from CSOs in the modern citizen-centred world.

Capacity to cooperate across and within sectors and organizations

In terms of stakeholder relations, PAs and CSOs should be able to co-design effective responses to address unmet needs and gaps in access to digital opportunities of DVGs. Transparency, accountability, and active participation should be the pillars of inclusive e-governance initiatives. Moreover, the creation and growth of multi-stakeholder relations may allow to create an adequate support net to tackle cross-cut and additive digital vulnerabilities, when many of these coexist or add up in worsening people's risks and disadvantages.

This is possible where PAs, CSOs, and other stakeholders involved have a common understanding of the value of engagement and multilevel cooperation when it comes to planning, developing, and implementing projects and activities collaborating across organizations within the same sector, as well as bridging to others in different ones.

Examples could be collaborations between CSOs and local governments, or PAs and private sector entities, and so on. In this line of thinking, it is important to highlight the role public-private partnerships could play towards adopting new approaches and management processes, as well as to unlocking funding opportunities. Together, the public and private sectors can better map out citizens' needs, as well as share the burden of addressing issues large in scope such as digital skills development.

Improved communication and awareness of relevant active projects

Overlapping feedback on stakeholder relations and salient, specific needs of DVGs highlighted in this report show a tendency towards the risk of duplicating activities and outcomes across organizations involved in assisting vulnerable groups. The issue emerges as the consequence of lack of awareness and mapping of what projects are active to tackle a specific issue. Moreover, awareness is required also of the conditions *on the ground,* gaining trusted and accurate knowledge about facts, data and statistics pertaining to digital services, accessibility, skills in the population, and such.

It is necessary to dispose of up-to-date overviews of the initiatives, projects, and services implemented or under implementation that focus on digital vulnerability and DVGs. The scope of such mapping spans across sectors and levels of governance: local administrations, the national government, CSOs, Public-Private Partnerships (PPPs) donors. Interviewees' feedback points at the need for an encompassing repository of all this information, ready-to-check, that surveys and reports of funding opportunities, organizations involved in relevant projects, as well as completed, ongoing and planned activities to tackle digital vulnerability – or that take it into account.

General understanding of salient issues and skills necessary to engage and design policies, develop and offer services

Capitalizing on interviewees' feedback in this survey, it emerges how targeting digital vulnerabilities and training digital skills are activities requiring a high level of specification. From the salient issues highlighted in our Findings, some directions for addressing the unmet needs of DVGs are:

- Paying increased attention to geographical divides, be these between urban and rural areas, or flatlands and mountainous regions, or occupied territories. Infrastructure and connectivity development should remain in focus for watchdog and advocacy activities, as well as the mobilization of further aid sources for comparatively more economically deprived regions;
- Focusing on increasing the access, connectivity, and devices availability in schools, to arrange for students the possibility to freely access such tools even after class. This could prove effective for pupils in the first place, but also to then enable more ambitious programs of awareness-raising and basic skills training in the general population by opening the schools to other digitally vulnerable social groups too. In truth, establishing moments and points of contact between different digitally vulnerable groups may also help tackle common baseline issues – where applicable – that diverse groups face. Indeed, it is possible that this would have

an impact on enhancing the social cohesion between different groups too – a positive *side effect* which should not be disregarded;

- Enhancing people's trust in operators and officials on matters of digital safety, for citizens to see the latter as knowledgeable and competent (in terms of tasks, responsibilities, capacity to act) points of reference in case of specific vulnerability. E.g., young people know who to report to when victims of online bullying;
- Developing critical approaches and lenses towards information consumption and one's own digital responsibility, articulating such focus in an inclusive manner that would account for specific national and regional factors of vulnerability. This would increase the tailoring of programs with such target around more accurately identified issues and groups;
- Focusing on presenting to people so-called low hanging fruits, practical examples where the benefits of digitalization become immediate and easier to grasp. Likely, this will entail creating or enhancing digital solutions that address people's most pressing and salient needs;
- Value-building and human-centred digital services should be developed in order for the government to monitor and address the needs of DVGs. A potential solution could be represented by the appointment of a responsible person/unit (for human resources and digital responsibility) scanning policies, services, and initiatives with such lens and specialized focus;
- The war has created an additional large group in the form of internally displaced people (IDPs), as well as people with refugee status in neighbouring countries. Their need for digital services, whether provided by Ukrainian authorities or those of the current country of residence, is a question of utmost importance. People still need access, need to study, stay connected, etc., and special attention within the DRIVE project can be paid to this particular target category.

Appendix 1

List of references

- Boychenko V. V. et al. (2021). *STEM-education in Ukraine and USA: current trends*. Sumy State Pedagogical University.
- European Commission (2021). *Digital Economy and Society Index (DESI) 2021 – DESI methodological note.* Accessed in February 2022. https://digital-strategy.ec.europa.eu/en/policies/desi
- Fedyuk O., Zentai V. (2018). *The Interview in Migration Studies: A Step towards a Dialogue and Knowledge Co-Production?,* Qualitative Research in European Migration Studies, edited by Ricard Zapata-Barrero and Evren Yalaz, IMISCOE Research Series, p. 176. https://doi.org/10.1007/978–3–319–76861–8_10
- Government of Ukraine (2021). *National Strategy for the Creation of Barrier-Free Space in Ukraine for the period up to 2030.* Accessed in March 2022. https://zakon.rada.gov.ua/laws/show/366–2021-%D1%80#n10
- Kostitsky V. (2013). *Як виховують медіа, або Морально-етичні проблеми інформаційної безпеки дітей,* secondary source. Accessed in February 2022. http://slovoprosvity.org/2013/06/27/iak-vykhovuiut-media-abo-moral-no-etychn/
- Ionan V. as in Machuskyy (2021). *Lifelong learning and digital education in Ukraine*, in Business Law Electronic Resource, secondary source. Accessed in February 2022. https://www.businesslaw.org.ua/lifelong-learning-and-digital-education-in-ukraine-2/
- Purdie-Vaughns V., Eibach R. P. (2008). *Intersectional Invisibility: The Distinctive Advantages and Disadvantages of Multiple Subordinate-Group Identities*, Sex Roles, 59, 377–391. https://doi.org/10.1007/s11199–008–9424–4.
- Simien E. M. (2007). *Doing Intersectionality Research: From Conceptual Issues to Practical Examples*, Politics & Gender, 3(2), 246–271. https://doi.org/10.1017/S1743923X07000086
- United Nations (2022). *Aggression against Ukraine: resolution A/RES/ES-11/1 | adopted by the General Assembly.* Accessed in March 2022. https://digitallibrary.un.org/record/3959039?ln=en
- United Nations Development Program (2021). *Inclusion and human rights at the forefront. Accessibility of e-government services and tools for citizens in Ukraine. Study Report,* UNDP Research and Publications. Accessed in February 2022. https://www.ua.undp.org/content/ukraine/en/home/library/democratic_governance/inclusion-and-human-rights-at-the-forefront.html

Appendix 2

List of interviewees

Name	Position	Institution
Daria Herasymchuk	Adviser-Commissioner of the President of Ukraine for the rights of the child and children’s rehabilitation	Adviser-Commissioner of the President of Ukraine for the rights of the child and children’s rehabilitation
Volodymyr Brusilovskyi	Project manager	UNDP DIA Support Project
Mykola Yabchenko	Digital Literacy Specialist	UNDP DIA Support Project
Oleksiy Zelivianskyi	Senior IT Specialist	UNDP DIA Support Project
Olena Gunko	Head of IT Department	Lviv City Council
Dmytro Zavgorodnii	Director General of the Directorate for Digital Transformation	Ministry of Education and Science of Ukraine
Kateryna Suprun	State Expert for Digital Transformation of Education and Science, Directorate for Digital Transformation	Ministry of Education and Science of Ukraine
Margaryta Noskova	Head of the Center for Innovative Educational Technology	Lviv Politechnical University
Maria Vasyunyk	Specialist, responsible for kids with special needs (inclusion) of the Department of Education and Science	Lviv Oblast State Administration
Myron Pacaj	Head of Cyber Security and IT Unit of the Department of Education and Science	Lviv Oblast State Administration
Igor Komendo	Head of Organization	NGO GoLocal
Olena Mytnyk	Digital and Human Rights Expert	NGO GoLocal
Gulsana Mamedieva	Director General of the Directorate for European Integration	Ministry of Digital Transformation of Ukraine
Anastasiya Dyakova	Founder	Founder of the educational project #stop_sexting
Alina Kuts-Karpenko	Head of the expert group, which deals with the development of e-democracy, digitalization of civil society and internal compliance of information systems	Ministry of Digital Transformation of Ukraine
Oksana Sulima	Directorate of the Social Services Development and Children's Rights Protection of the Ministry of Social Services of Ukraine	Ministry of Social Policy of Ukraine
Inna Hohcharuk	Directorate of the Social Services Development and Children's Rights Protection of the Ministry of Social Services of Ukraine	Ministry of Social Policy of Ukraine
Maryna Shevtsova	Executive Director	Civic Organization Equal Opportunities Platform

Hereby we express our appreciation to all interview participants due to their timely and accurate appointments, as well as for their highly professional and valuable expertise that contributed much to the project aims, especially in situations when enormous tension was accumulating.