Policy Research Paper on

Institutional capacity building in the security sector organizations based on the digital transformation experience of Estonia

New Eastern Europe

Author: Lana Turashvili

2022
Krakow, Poland

Content

Introduction

In the modern world, most organizations' future often depends on the level of development of their digital capacities. Aiming at providing effective and efficient governance, state organizations should ensure that they keep up with new digital advances, and in particular, the state security sector organizations (SSOs) - as an important part of good security sector governance (SSG) and reform (SSR) - should take a proactive approach in digital transformation processes.

The idea and the interest in the research topic emerged from the reflections and thoughts during the Internet Governance Forum (IGF), which took place in Katowice (Poland) from 6 to 12 December 2021. The IGF discussions demonstrated that the need to digitally transform and develop governmental institutions became more vital than ever, due to rising technological development and the digital progressions. Contemplating on them and relating to my work experience at the Ministry of Internal Affairs (MIA) of Georgia narrowed down my focus on the digital development in the security sector, and specifically, my past employment at the Tbilisi City Hall in 2015- 2016 allowed me to reflect on the e-governance reform and its positive impacts on citizens, organizations, and employees.

The policy research has been conducted under the fellowship program of the Warsaw Euro-Atlantic Summer Academy (WEASA) and implemented at the office of the „New Eastern Europe" magazine in Krakow, Poland.

In that vein, this policy paper aims at contributing to the policy-relevant and applied knowledge on state digital transformation processes in the SSOs and developing insights related to the digital development of SSOs in Georgia and Ukraine. Those two countries have been significantly progressing on their public sector reform processes alongside with expressing commitments and a strong willingness towards the European and Euro-Atlantic integration, and both countries have been victims of Russia's military attack. Exemplifying the case of Estonia as one of the most progressed and developed countries in the field of digital transformation, the research offers security sector digital transformation for Georgia and Ukraine, as well as the Eastern Partnership (EaP) region, by explaining how Estonia was able to digitally advance and develop SSOs in the country. Therefore, the paper answers the following research question:

How can Georgia and Ukraine enhance security sector organizations digital capacities based on the experience of Estonia?

The study is divided into the following sections:

Introduction part provides a brief presentation of the research goal, content, and the structure of the policy paper. The second part - methodology includes information about the research methods used in

this policy research. The third part of the paper establishes a conceptual framework – security sector reform and good security sector governance – for a systemic approach to the study of the security sector digital transformation. The section on Estonia studies the country's digital advancement and draws parallels with Georgia and Ukraine. It discusses the early stages of digital transformation processes in Estonia, offers ideas based on the Estonian example and practices about how digital penetration in the security sector can contribute to gender equality and create protection of fundamental human rights, discusses the importance of development of cyber security and digital literacy in Georgia and Ukraine and explains challenges around security sector digital transformation processes due to various limitations (including internet accessibility) and discusses legal base and digital governance. In the fifth part the paper presents a questionnaire analysis and their findings for Georgia and Ukraine, answered by relevant employs of the security sector organizations in the two countries, aiming at understanding and presenting SSOs' digital transformation situation and needs in Georgia and Ukraine, based on the conducted survey. The six part presents information about the digital governance in Georgia and Ukraine and some ongoing digital projects. The final section presents specific policy recommendations on the digital transformation, progress, and capacities for the SSOs in Georgia and Ukraine. The policy recommendations provided in this policy research are based on the collected and analyzed findings, including interviews with experts. The recommendations provided are not limited only to the two countries but could also be applicable to other EaP countries.

Methodology

Primary and secondary data have been collected and analyzed, using mainly qualitative research methods.

For gathering the primary data, a survey in the form of the online questionnaire has been distributed to different state security and law-enforcement organizations in Georgia and Ukraine, aimed at understanding and identifying their digital capacities, needs and challenges. Additionally, a semi-structured interview has been held with three field experts, in order to consider their practical expertise, knowledge and know-how for the formulation of the final policy recommendations.

The online questionnaire contained fifteen different questions (closed-ended, open-ended and semi-open.) The questionnaire was prepared and spread in Georgian and English languages, while data analysis was conducted in English. This research method has been chosen of the access it offers to specific knowledge and information limited to those organizations and countries. Even though this research tool has its own limitations – for example, inability to gather the significant number of answers due to the busy, fixed and sometimes restricted schedules and mandates of the civil servants, and the possession of specific knowledge of the employees on their organizations' digital capacities, it has provided the most precise and accurate information and data for analysis.

Interviews held with the digital and cyber security experts of Estonia has provided this research with a precious source of information for more in-depth analyses, reasoning, and formulation of the recommendations.

The secondary data collection has been collected through the data searches on the internet, existing literature, policy-relevant publications, official governmental documents, and other research papers, which together with the primary data allowed for the formulation of enriched response to the research question. Both the primary and secondary data have been crucial for the data analysis and the generation of the policy recommendations.

Security sector reform and good security sector governance: why digital transformation in security sector matters?

The digital transformation processes in the SSOs are the part of the security sector reform (SSR).

Geneva Center for Security Sector Governance (DCAF) defines the SSR as a political and technical process aiming at betterment of state and populational security through providing and managing security in a more effective and accountable way which considers democratic civilian control, rule of law and respect for human rights. SSR aims at incorporating good governance principles to the security sector.[1]

The SSR's role is to strengthen security sector governance (SSG) through transforming security organizations into ones which are capable of providing security to the state and people in an efficient and effective way.[2] The favorable end goal of the SSG is its transformation into the good security sector governance (GSSG). The paper takes the GSSG prism towards the digital transformation processes and thus also as a part of final recommendations. It also proposes a number of initiatives that would foster the GSSG.

GSSG means that the security sector provides state and human security, effectively and in an accountable fashion, in the frames of democratic civilian control, rule of law and respect for human rights, and is a specific type of security governance based on a normative standard for how the state security sector should work in a democracy.[3]

GSSG requires an appropriate development of state digital capacities in the security sector. Due to the need to grow digital infrastructure, technologies, and skills in the security sector institutions to make them function properly, digital transformation is viewed (as both a necessary challenge and an opportunity) in the SSG framework. One of the most important areas of SSG is cyber security. The main principle that GSSG considers is the provision of safe digital space for everyone freeing the critical infrastructure and organizations from digital threats.[4] The digital institutional capacity building of SSOs

[1] Geneva Center for Security Sector Governance (DCAF), "SSG/R," dcaf.ch, accessed on April 12, 2022, https://www.dcaf.ch/about-ssgr .
[2] Heiner Hänggi, "Conceptualizing UN support to security sector reform," dcaf.ch, accessed on April 22, 2022, https://dcaf.ch/sites/default/files/imce/UN%20SSR%20History/01_H%C3%A4nggi_Conceptualizing.pdf .
[3] "Security Sector Governance- applying the principle of good governance to the security sector," SSR Backgrounder, accessed April 23, 2022. https://www.files.ethz.ch/isn/195671/DCAF_BG_2_Security%20Sector%20Reform.11.15.pdf .
[4] Thomas Guerber, "Digitalization and SSG/R: adapting to a new reality", dcaf.ch, October 15, 2021, https://www.dcaf.ch/digitalisation-and-ssgr-adapting-new-reality .

in Ukraine and Georgia needs the protection of digital space and assurance that the cyber threats will not hinder proper utilization of the services.

The recommendations provided at the end of the paper facilitate and contribute to the achievement of current digital goal of the SSG, which is to incorporate the principles of accountability and transparency in the SSOs.

Certainly, the digitalization processes would facilitate inclusivity of reformation processes and will ease the provision processes of security to the citizens. The transformative effect of digital development on SSR is undoubtable in regard to its positive impact on access to vitally important information.[5]

The change that digital transformation brings about is immense, including the creation of new more transparent, open, and inclusive security sector organizations that would provide access to digital services and provide protection in particular to the marginalized or vulnerable groups of people previously excluded from the safety provision.

Digital transformation in SSOs and in particular technologies as a tool would facilitate vulnerable groups of people (including women and the handicapped) inclusion and safety through digital public services and access to information, knowledge, and ensure them their essential rights regarding safety and protection.

Estonia's digital transformation and progress: parallels with Georgia and Ukraine

Digital Transformation - How did it start

In the early 1990s, after Estonia had gained its independence, the country's digital transformation processes started. Estonia faced a scarcity of resources, experience and know how, and there was a pressing need to free the country from its Soviet past.[6] "Estonia managed to regain trust of citizens through living a Soviet era behind where everything was monitored. The government tried to have more or less transparent approach to that."[7] As far as Estonia had an ambition to not to just exist and survive but also thrive, the digital transformation turned to be a tool for Estonia to prove it could sustain and "fit in" the demanding western market and free itself from the Soviet distress.

[5] Thomas Guerber, "Digitalization and SSG/R: adapting to a new reality", dcaf.ch, October 15, 2021, https://www.dcaf.ch/digitalisation-and-ssgr-adapting-new-reality.

[6] Rainer Kattel and Ines Mergel, Estonia's Digital Transformation: Mission Mystique and the Hiding Hand (Oxford University Press, 2019), 145, https://academic.oup.com/book/42635/chapter/358101931.

[7] Rain Ottis, interview by Lana Turashvili, July 14. 2022.

Georgia and Ukraine gained independence in 1991, and their journey to leave behind the Soviet past was not so plain. This journey was filled with a lot of pain, struggles, and hardships. Those two countries found it extremely hard to establish transparent, accountable, and democratic institutions.

The Estonian government was focused on the country's digital development, which became the milestone in its digital progress. The first Prime Minister of Estonia, Mart Laar, elected in 1992, had an important role in heading the country towards a digital advancement. He became successful in getting Western support which enabled him to implement more innovative projects.[8] While Estonia stated its digital transformation journey quite early, Georgia began it only after the 2003 Rose Revolution, in parallel with all other changes and reformation processes in the country. It is noticeable that Ukraine has become a digitally proactive country since 2019, when the Ministry of Digital Transformation was established there.

On 23 August 2021, e-ID cards and passports were approved in Ukraine. In the same month, the law was signed on paperless work for officials,[9] while Estonia went paperless in 2000 and the digital signature and e-ID was introduced there after launching the X-road in 2001.

It is not accidental that president Zelensky and the existing Ukrainian government have announced the availability of digital IDs and passports on 23 August, when the country marked the 30th anniversary of its independence. The Ukrainian state demonstrated its robust digital ambitions and desire to make digital projects an important priority as an essential part of the national agenda. By choosing a symbolic date for the Ukrainian government to introduce significant digital projects, it was demonstrated that the country possesses crucial digital ambitions, goals and fixed digital mindset.

Even though 75% of Georgians are identified as electronic ID card holders, according to 2019 the majority (84%) of them have never applied any electronic procedure using their ID's.[10] The SSOs in Georgia have an opportunity to offer various services for the citizens through ID cards, which are effective to incorporate various functions and create better services for the citizens.

One of the reasons that Estonia became a digital transformation role model for other countries was its primary focus on the citizens and their needs. The Estonian government prioritized creating easy and transparent services for its citizens. For example, the private sector and citizens provide information to government just once, and the necessary data is already provided for the government through X-Road,[11]

[8] Rainer Kattel and Ines Mergel, Estonia's Digital Transformation: Mission Mystique and the Hiding Hand (Oxford University Press, 2019), 148, https://academic.oup.com/book/42635/chapter/358101931.

[9] Slawomir Matuszak, The digitalization of Ukraine: anatomy of a success story'', osw.waw.pl, August 23, 2021, https://www.osw.waw.pl/en/publikacje/osw-commentary/2021-08-23/digitisation-ukraine-anatomy-a-success-story .

[10] Nino Taganashvili, "Digital Services as a Mean of Direct Interaction between the State, Business, and Citizens on the Example of MY.GOV.GE," fighting corruption (blog), Institute for Development of Freedom of Information (IDFI) January 23. 2022, https://idfi.ge/en/digital_services_as_a_mean_of_direct_interaction_between_the_state_business_and_citizens_on_the_example_of_my_gov_ge.

[11] "Building the digital government -Estonia's Digital Transformation," eTrade for all, October 28, 2019, https://etradeforall.org/news/building-the-digital-government-estonia,s-digital-transformation/ .

without any need for a repeated information provision to the government. The X-Road enabled data to be safely connected and exchanged, and through ID cards, the citizens could access the main e-services in Estonia.

The Ukrainian state invites the public prior to launching any digital service to test if it meets the needs of citizens and could be useful.[12] The Ukrainian government is focused on gaining the citizens' trust through offering user-friendly approach and digital innovation,[13] which implies that Ukraine places a higher degree of importance on the service provision to its citizens, and seriously considers the public trust as an integral part of the GSSG. "Ukraine looks like Estonia in 1990 when it has nothing to lose and could innovate."[14]

Ukraine has marked a significant progress on the provision of open data. According to the open data maturity assessment Ukraine moved to the 6th place in 2021 from the 17th in 2020.[15]

Both Georgia and Ukraine are in need to develop and protect their structures to protect their citizens' digitally available personal information and the governments should be able to provide an efficient and effective security and protection to the citizens including their data. "E-governance and security systems will be used by the people if they know and are convinced that it is not a spying tool it is useful for them and good for them accordingly, government will build its credibility."[16]

Alongside with the government, the academia had a great input in Estonia's digital transformation processes. In 1990, the Informatics Council functioned as the primary adviser on Information and Communication Technologies (ICTs), with a focus on cyber security. that supported the X-road developed by the Estonian Academy of Sciences Institute of Cybernetics.[17] Estonia had built partnership and cooperation with Scandinavian countries (Sweden and Finland) that significantly contributed to its ICTs development.

Although Estonia was developing its own capacities, it has demonstrated an ability and willingness to learn and grow based on the experience of foreign countries. For example, the Scandinavian countries were significant contributors to Estonia's digital progression. Accordingly, as "Development cooperation

[12] Nino Taganashvili, "Digital Services as a Mean of Direct Interaction between the State, Business, and Citizens on the Example of MY.GOV.GE," fighting corruption (blog), Institute for Development of Freedom of Information (IDFI), January 23, 2022, https://idfi.ge/en/digital_services_as_a_mean_of_direct_interaction_between_the_state_business_and_citizens_on_the_example_of_my_gov_ge.

[13] Mykhailo Fedorov, "Ukraine's digital revolution is gaining momentum," UkraineAlert (blog), Atlantic Council, September 7, 2021, https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-digital-revolution-is-gaining-momentum/.

[14] Mari-Liis Sulg, interview by Lana Turashvili, July 14, 2022.

[15] Daphne van Hesteren, Raymonde Weyzen and Laura van Knippenberg, "Open data best practices in Europe: Estonia, Slovenia and Ukraine," data.europa.eu, last modified February 24, 2022, https://data.europa.eu/sites/default/files/report/Open_Data_Best_Practices_in_Europe_Estonia_Slovenia_and_Ukraine.pdf

[16] Agnes Kasper, interview by Lana Turashvili, 13 July, 2022.

[17] Rainer Kattel and Ines Mergel, Estonia's Digital Transformation: Mission Mystique and the Hiding Hand (Oxford University Press, 2019), 149, https://academic.oup.com/book/42635/chapter/358101931.

partner countries for Estonia are Georgia, Ukraine and Moldova"[18] this creates significant growth opportunities for those countries in the digital domain.

Estonia's fairly large focus on the ICTs development and infrastructure became an important part of the digital development processes. Estonia currently invests further in its ICT capacity and infrastructure building, including updating and renewing its technologies. Only the ICT strategies and decisions of crucial importance have been made at the higher governmental level, while since 1999 on each governmental agency was responsible for creating and implementing its own digital and ICT development plans. As a result, the need to create data exchange opportunity between IT systems and database emerged and resulted in the X-road system introduction in 2001.[19]

Ukraine already possesses more than 200,000 well-qualified IT specialists,[20] and is willing to invest further in the capacities for its development. Such an attitude together with resources are favorable for a serious and meaningful contribution to the security sector reformation processes.

Apart from being open to the international best practices, the Estonian government considered the experience and know-how of field experts including engineers and technologists mostly in privacy and safety and was able to incorporate that knowledge into the laws as well.[21] "Everything we do need to be based on laws and at the end of the day we need to know who owns those program systems and which laws are behind it."[22]

Another reason why Estonia succeeded in the digital domain was its ability and understanding of the importance of economizing costs, rejecting lust to spend, and minimizing the unnecessary expenses. The Estonian government had a strong awareness of the reality of their resource limitations and the necessity to cut extra expenses. ''It was very expensive to keep bank offices. Banks liked the idea of internet banking and they started to build this infrastructure and the states have realized that they had the same problem."[23] In such a condition, in which the country had serious economic difficulties, it had no other choice but to develop its own industry. In the case of Estonia, the lack of resources sparked creative ideas and added up to a source of inspiration and growth in the digital domain.[24] For economically weak countries to limit foreign purchases and shifting focus on developing local digital resources and capacities is a milestone for digital progress and developments.

---

[18] Mari-Liis Sulg, interview by Lana Turashvili, July 14, 2022.

[19] Rainer Kattel and Ines Mergel, Estonia's Digital Transformation: Mission Mystique and the Hiding Hand (Oxford University Press, 2019), 150, https://academic.oup.com/book/42635/chapter/358101931.

[20] "Modern development centres in Poland and Ukraine", conscensia, accessed April 12, 2022, https://conscensia.com/it-specialists-poland-and-ukraine/#:~:text=Ukraine%20has%20over%20200%2C000%20IT,specialists%20are%20trained%20in%20Lviv.

[21] "Building the digital government -Estonia's Digital Transformation," eTrade for all, October 28, 2019, https://etradeforall.org/news/building-the-digital-government-estonia,s-digital-transformation/ .

[22] Mari-Liis Sulg, interview by Lana Turashvili, July 14, 2022.

[23] Agnes Kasper, interview by Lana Turashvili, 13 July, 2022.

[24] Rainer Kattel and Ines Mergel, Estonia's Digital Transformation: Mission Mystique and the Hiding Hand (Oxford University Press, 2019), 147, https://academic.oup.com/book/42635/chapter/358101931.

Building public-private partnership (PPP) is another example of how the Estonians could successfully develop the country's digital future. The Estonian leadership and private sector were hand in hand building Estonia's digital progress through contributing to the PPPs development. Initiatives and networking within that format have been effectively supported by the government. Free exchange of the information and non-formal and decentralized environment established a unique space for the discussions and new initiatives.

Among the PPPs, one of the most progressive and successful projects in Estonia - the "Tiger Leap" program was launched in 1996, focusing on enhancing IT education at schools, building relevant infrastructure, and enabling all schools to have access to the internet. The program resulted with 99% of the population using the internet regularly.[25]

The talent of the Estonian people to contribute to public-private network development and create links with population and private sector through non-formal talks and interactions is what the Georgian government and population can develop with ease. The sociable nature of the Georgian people and finding value in interactions including non-formal could create the right environment for PPPs development that would positively benefit the digital advancement in the security sector.

The secret of Estonia's digital achievements lies in the country's ability to establish and utilize a large public sphere to network, talk, cooperate, and integrate the citizens on every level of the decision-making and digital progress. A small portion of its population made it realistic to get to know and incorporate people in the processes, that might be hard for such countries with larger populations as Ukraine to fully embody the Estonian experience, but there is a room for improving the SSOs through certain digital projects and practices based on the Estonian example.

Georgia as a small country and a proactive digital changes pioneer, has an important chance to move forward with its digital transformation processes and fully embody Estonia's example, especially regarding the PPPs development that is a crucial contributor to the digital advancement, including in the security sector. Georgia has a population of around 3.714 million and Estonia's is about 1.331 million, while Ukraine is a larger country with 44.13 million people.

Majority of Estonia's population (about 80%) trust government, and the most trusted institutions in the country are the rescue board, police, border guards, and tax and customs,[26] which are reflective of how Estonia managed to successfully reform the security sector and allowed citizens to benefit from the transparent, human centered and accountable security services. Estonia enjoys a regularly good ranking in e-governance, as country ranks third, only proceeded by Denmark and the Republic of Korea,

[25] "This is the story of the word's most advanced digital society, e-estonia," e-estonia, accessed April 25, 2022, https://e-estonia.com/story/ .

[26] "Factsheet E-governance," e-estonia, accessed April 23, 2022, https://e-estonia.com/wp-content/uploads/e-governance-factsheet-sep2021.pdf.

according to the UN's e-governance survey of 2022, while Georgia and Ukraine respectively occupy the 65th and 69th places, among 193 countries.[27]

Notwithstanding some important progress on the side of both countries in e-governance, the e-services development in both countries still needs to be invested more, as the sector is an integral part of the SSR. For example, the MIA of Georgia is the main service provider among the SSOs, and has already created a voice-based portal on its website to facilitate the access of the vision-impaired people to all services. The portal is also adjusted to the needs of people with hearing impairment.[28] But despite those initiatives, more effort is needed to readapt the e-services with the handicapped people's needs and to make digital services more inclusive, as well as a better safety and security provider for all citizens. The new era of digital penetration in security sector will be focusing on providing major services related to the safety for marginalized and vulnerable groups of people, including the handicapped. Finally, digitalization in security sector should serve the larger purpose that is inclusion, protection, and care for the people who need it the most and the modern technologies can serve as a tool to achieve that goal.

How can digitalization of the security sector contribute to gender equality and create protection of fundamental human rights?

The digital inclusion into the security sector and services is an effective tool to limit unfair and unbalanced practices of power dynamics and relationships between the people and government. The trust of the Estonian people in the governmental institutions and the SSOs in the country was a result of a significant effort from the government. The state's focus on providing the safety and security of personal data of the citizens and enabling the tools that would create an equilibrium and balance of power between the government and population resulted in a strong societal trust in the SSOs. For example, the Estonian government implements a data tracker program that allows the Estonians to check online who looks at their data through "RIIGIPOARTAAL EESTI.EE," the official governmental webpage for delivering online public services. "The point is that the government knows a lot of things about us but we also can see how our data is used."[29]

[27] "Georgia in the UN E-Government Review of 2020- Results Survey," Institute for Development of Freedom of Information, July 22, 2022, https://idfi.ge/en/e-governance-e-participation-georgia-index-2020 .

[28] "Public Administration Reform Roadmap," Administration of the Government of Georgia, May 25, 2015 https://www.gov.ge/files/425_49309_322150_15.07.21-PublicAdministrationReformRoadmap2020(Final)(1).pdf .

[29] Agnes Kasper, interview by Lana Turashvili, 13 July, 2022.

The functioning of an analogical data tracker program in Georgia and Ukraine would strengthen the population's trust in government institutions, and especially, in the SSOs. Russia's war against Ukraine has raised the population's trust in the SSOs in Ukraine, especially the police and military, but institutional changes through using such digital tools as data tracker would create a sustainable public trust and a better protection of citizens' rights and data, in the long-term perspective. "This is an additional transparency measure, and this is deterrence against abusing the system."[30]

The establishment of data tracker program would be an effective supporting measure for the Georgian and Ukrainian governments to step up their security sector reforms based on the GSSG principles, following which mean the establishment of state and human security, effectively and accountably, within a framework of democratic civilian control, rule of law and respect for human rights.[31] The tool would allow government to offer its citizens the gift of transparency and protection of their privacy, providing a conclusive answer to the recently vulnerable question within the Georgian society: "who is looking at my data?"

The implementation of the program would also support the elimination of gender inequality in the countries, and one of its extreme manifestations – women's mortality. Because mostly women are targets of unlawful usage of their private data that as a result leads to harsh crimes committed against them, depriving them of their lives or causing them serious physical, moral, emotional, or financial damages. Recently, a lot of women in Georgia have died from the hands of their ex-husbands, boyfriends or partners, and the country still has a high level of domestic violence that in a majority of cases are committed against women. Therefore, there is a significant need for the government to take proactive and transformative measures in order to ensure the safety and security of its citizens and primary the lives and health of women.

To conclude, the implementation of data tracker program would enable protection of the rights of the employees in the SSOs, and especially women who are more inclined to become the victims of the power abuse. Creating the system as the data tracker in Georgia and Ukraine would create more equilibrium, justice, equality, and healthy power dynamics among citizens inside and beyond the countries' security sectors.

[30] Rain Ottis, interview by Lana Turashvili, July 14. 2022.

[31] "Security Sector Governance- applying the principle of good governance to the security sector," SSR Backgrounder, accessed April 23, 2022. https://www.files.ethz.ch/isn/195671/DCAF_BG_2_Security%20Sector%20Reform.11.15.pdf .

Cyber Security and digital literacy

One of the reasons for Estonia's success in the digital government, particularly the digitization in the security sector is that it has been investing regularly in the digital literacy, targeting to raise awareness and enhance the ICTs and cyber security skills of its citizens, of all age groups. The government offers programs for schools for ICT learning and for acquiring essential digital skills. When we talk about digital and cyber literacy, there is a two-sided interaction between the government and citizens. On the one hand, the government initiates ICT and cyber educational programs and opportunities for citizens, and on the other, the Estonians themselves show an interest and enthusiasm to get engaged in those learning opportunities.

In order to strengthen cyber security and ensure a safe and secure utilization of digital platforms supplied by the SSOs throughout the service delivery, well-trained citizens in digital and cyber skills are essential.

For example, in Estonia, such topics as digital safety and digital skills are taught starting from the elementary school classes, and the teaching continues at higher education level. Universities have partnership and cooperation agreements with the Ministry of Defense and Ministry of Education and Research, to enhance the level of understanding of cyber threats.[32]

Alongside with the digital progress, the Ukrainian government aims to enhance digital skills of 6 million people by 2024.[33]

Enabling citizens access to essential and advanced digital and cyber skills is a way towards protecting nations from negative influences of the cyber-attacks. Accordingly, strengthening focus on digital literacy and citizens' ICT skills is one of the ways Estonia has enhanced its cyber resiliency and has built capacities from the distress caused by massive cyber-attack which Estonia experienced in 2007.

"This cyber-attack showed how vulnerable Estonia become because of the reliance on digital technologies."[34] Estonia's cyber security journey led to the understanding that the country was able to learn from the challenges and draw lessons from the hard times. This was proved during a cyber-attack in 2007 when country had to totally disconnect from the internet for about one month, which resulted in Estonia turning into an ever more cyber resilient country with a profound expertise and willingness to share its knowledge and experience with other countries. After cyber-attack the focus on cyber and ICT education significantly increased in Estonia. NATO's cyber security center in Tallinn was created after a cyber-attack and Estonia started to attract talented and well-experienced ICT professionals from

[32] Mark Stone, "How Estonia created trust in its digital-forward government," securityintelligence, September 17, 2021 https://securityintelligence.com/articles/estonia-trust-digital-government/.

[33] Alexander Iosad and Oliver Large "State of Resilience: How Ukraine's Digital Government Is Supporting Its Citizens during the War," institute.global, April 18, 2022, https://institute.global/policy/state-resilience-how-ukraines-digital-government-supporting-its-citizens-during-war .

[34] Agnes Kasper, interview by Lana Turashvili, 13 July, 2022.

the private sector. Ukraine since the outset of the current stage of the war started to incorporate expertise and knowledge from the private sector to help the government cope with the digital security threats, and the country's focus on the cyber resilience elevated significantly.

CyberExer technologies provide cyber security trainings and exercises for enhancing cyber capacities of citizens.[35] In 2020 the company offered free e-learning cyber hygiene training for the Ukrainian National Academy that is part of the Ministry of Internal Affairs.[36] Also, they conducted a joint project with the Estonian Ministry of Defense that offered cyber exercises for school children below age 10. [37]

"After a year from the cyber-attack, in 2008, Estonia drafted its first cyber security strategy that laid down foundations for digital transformation in the security sector including various topics as setting up new processes and procedures, new institutions, information system authorities, focus on critical infrastructure protection (especially the digital part) and reforming legislation and laws become priority.[38] When Russia's war on Ukraine erupted, Ukraine took the state cyber security to another level. The Ukrainian Government adopted the Law on Cybersecurity applied to the companies and institutions listed as "critical infrastructure." The Cybersecurity Strategy defines the actions aimed at strengthening cyber security and fighting cybercrimes and threats.[39] The strategy was adopted on May, 2021 as an update of the 2016 strategy.

Ukraine's National Coordination Center for Cyber Security under the NSSC of Ukraine received the notifications of cyber threats and was responsible for response activities, the primary focus of the office was to ensure the protection of personal data of citizens and to prevent the leakage of it.[40]

During the Russia's war on Ukraine the cyber-security become one of the most important concerns of the Ukrainian government. The state created a layered system of cyber defense for its IT infrastructure and established the Security Service of Ukraine (SBU) hotline, which provided immediate responses during cyber threats to the IT systems. The government has signed agreement between the state archival service of Ukraine and the national archives of the UK on backing up the digital data of Ukraine's state archival institutions in case of its loss.[41] Likewise during the cyber-attack in 2007 in Estonia there was a

[35] Mark Stone, "How Estonia created trust in its digital-forward government," securityintelligence, September 17, 2021 https://securityintelligence.com/articles/estonia-trust-digital-government/.

[36] Sten Hankewitz, "Estonian cyber security company shares free cyber hygiene training with Ukrainian police cadets,"estonianworld, April 6, 2020, https://estonianworld.com/technology/estonian-cyber-security-company-shares-free-cyber-hygiene-training-with-ukrainian-police-cadets/.

[37] Mark Stone, "How Estonia created trust in its digital-forward government," securityintelligence, September 17, 2021 https://securityintelligence.com/articles/estonia-trust-digital-government/.

[38] Agnes Kasper, interview by Lana Turashvili, 13 July, 2022.

[39] "Data protection and cyber security law in Ukraine," CMS, accessed on June 12, 2022, https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/ukraine .

[40] Oleksiy Danilov, "Cyber protection of state information resources is an essential component in the process of digital transformation of the country," rnbo.gov.ua, May 22, 2020, https://www.rnbo.gov.ua/en/Diialnist/4606.html .

[41] "The Ukrainian Digital Resistance: cyber resilience and digital diplomacy at work," ceps.eu, May 18, 2022, https://www.ceps.eu/ceps-events/the-ukrainian-digital-resistance-cyber-resilience-and-digital-diplomacy-at-work/ .

significant focus on data protection. "They were trying to back up their data and move it to another country if something happens. Estonia has back up data bases in another country."[42]

During the war, the Ukrainian government has been attempting to use digital tools to provide safety and security for the citizens crossing the Polish and Moldovan borders, by providing a simplified war time digital ID for the Ukrainian citizens without requiring other official documents for border crossings.[43]

While in the case of Ukraine Russian cyber-attacks proceeded the military attacks[44] in case of Georgia it was the contrary: there firstly Russia started the war in August 2008 and the cyber-attack followed.

In 2008, during Russia's war against Georgia, state services including the servers of the Ministry of Defense experienced cyber-attacks. In reaction the Georgian government introduced a new cyber security strategy and an action plan for its implementation (2013-2015).Today, the Georgian state is highly focused on cyber security and takes proactive measures to strengthen the country's capacities in that domain. The new strategy and action plan for cyber security for 2021-2041 has been introduced by the Georgian government in 2021. This document was Georgia's third strategy on cyber security which defines the vision of safe development of the country, defines the main threats and effective ways to deal with cyber challenges.[45]

In 2018, the 2019-2022 cyber security strategy was drafted in Estonia, which defined the country's cyber security vision and aimed at turning Estonia into the most cyber resilient state.[46]

Internet accessibility and other obstacles to good security sector governance

It is noticeable fact that about 63% of population in Georgia and Ukraine use internet while the number of people in Estonia who benefit from internet access is 89%.

Digital progress requires that a larger part of the population has access to the Internet. Thus 63% is not enough for implementing ambitious digital projects in the security sector and for providing effective services for the citizens. Successful digital transformation processes in SSOs also depend on the citizens' digital participation. The Georgian and Ukrainian governments should take measures to provide internet

[42] Agnes Kasper, interview by Lana Turashvili, 13 July, 2022.

[43] Alexander Iosad and Oliver Large "State of Resilience: How Ukraine's Digital Government Is Supporting Its Citizens during the War," institute.global, April 18, 2022, https://institute.global/policy/state-resilience-how-ukraines-digital-government-supporting-its-citizens-during-war .

44 Zeba Siddiqui,''Russian cyber spies attack Ukraine's allies, Microsoft says," reuters, June 22,2022, https://www.reuters.com/world/russian-hacking-groups-step-up-cyber-espionage-ukraine-allies-microsoft-says-2022-06-22/ .

[45] "Ordinance of Government of Georgia on cyber security 2021-2024 National strategy and Action plan", matsne, April 10, 2021, https://matsne.gov.ge/ka/document/view/5263611?publication=0 .

[46] "Cyber security in Estonia, Digar Estonian articles," DIGAR, July 1, 2019, https://dea.digar.ee/cgi-bin/dea?a=d&d=JVestinformsyst201907.2.7.3&e=-------et-25--1--txt-txIN%7ctxTI%7ctxAU%7ctxTA --------- -- .

to larger segments of the population especially to the regions where statistical data in that regard is even worse. For instance, in some regions of Georgia, only 15% of the population uses the internet and the digital infrastructure at the local government offices is underdeveloped, which hinders the processes of providing efficient digital governance, including service delivery to local population. Only 62% of the households of Georgia own a computer and 46% think that they lack skills to use it. [47]

Since the Starlink satellites appeared in Ukraine in February 2022 in order to facilitate internet accessibility to Ukraine there is high chance that it would significantly enhance the level of internet access in Ukraine in the near future but for now the concern of internet availability remains.

Alongside with that in Georgia, even among some officials, digital transformation is not perceived as a vitally important topic to be incorporated in the public governance and state reform processes because other problems such as poverty and unemployment are considered to be the major concerns in the country.

Legal base and digital governance

Estonia's attitude towards the digital law was also unconventional. Even though all technological and digital procedures are grounded in the legal base, they are flexible enough to change, amend and adjust, in line with the digital needs. "You need the legal framework to allow the entire system to work."[48]

The first drafts of the "Principles of Estonian Information Policy" was presented in 1994 and followed by drafting a first strategic outline for IT development by the Estonian parliament four years later.[49]

Even though Estonia had laws, policies and strategies supporting digital transformation processes in the country, neither of them was the core reason of Estonia's digital success but determined the national choice to progress, as well as the talent to innovate, which brought positive results and developments.[50]

The new digital agenda 2030 introduced by the Estonian Ministry of Economic Affairs and Communications was developed in 2021 focusing on digital development strategies, action plans and

[47] Nino Taganashvili, "Digital Services as a Mean of Direct Interaction between the State, Business, and Citizens on the Example of MY.GOV.GE," fighting corruption (blog), Institute for Development of Freedom of Information (IDFI), January 23, 2022, https://idfi.ge/en/digital_services_as_a_mean_of_direct_interaction_between_the_state_business_and_citizens_on_the_example_of_my_gov_ge.

[48] Agnes Kasper, interview by Lana Turashvili, 13 July, 2022.

[49] "This is the story of the world's most advanced digital society," e-estonia, accessed on 10 June, 2022, https://e-estonia.com/story/.

[50] Rainer Kattel and Ines Mergel, Estonia's Digital Transformation: Mission Mystique and the Hiding Hand (Oxford University Press, 2019), 145, https://oxford.universitypressscholarship.com/view/10.1093/oso/9780198843719.001.0001/oso-9780198843719-chapter-8 .

applying technologies to create better life for the society. During the 1990s the Prime Minister's office was primary responsible for digital matters in the country.

Georgia has incorporated e -governance and e-services development strategies and plans in the strategy and action plan of the public administration reform roadmap 2020 accepted in 2015 and has developed open government partnership action plan of Georgia 2014-2015 and Digital Georgia (E-Georgia strategy and action plan 2014- 2018.)

Now, the government is working on a strategy draft (also incorporating the service delivery strategy) that would cover 2022 -2026 period and would be incorporated in that as well.

Ukraine demonstrates flexibility in speedily changing the legislation and readjusting to digital transformation processes[51] with the focus on developing laws supporting growth of digital economy in Ukraine through adopting the law on stimulating the development of the digital economy in Ukraine in July 2021 and approving the concept of development of digital economy and society of Ukraine by the cabinet of ministers of Ukraine. Ukraine lacks legislation on cloud-based technology and services and is in need to readjust digital agenda and laws with the focus on cyber security after the end of a war.

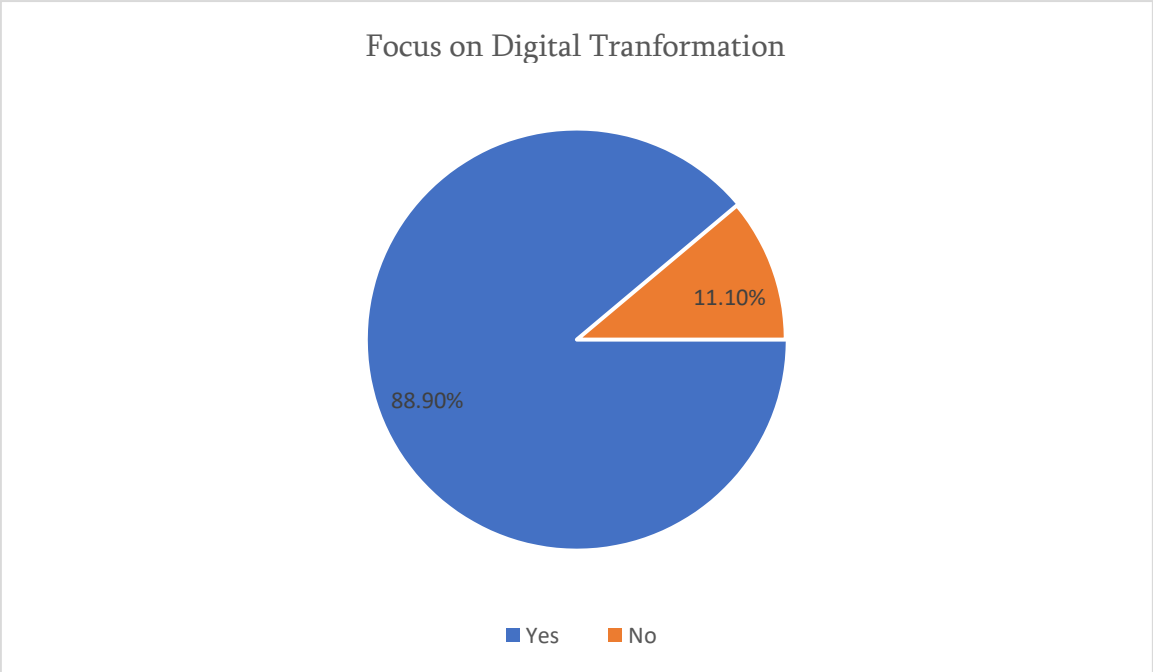
Questionnaire Analyses and Findings

Survey analysis - Georgia

To provide efficient and effective recommendations for the SSOs in Georgia and Ukraine, an online questionnaire was prepared in Georgian and English, and was disseminated to different organizations in those countries. Below, the results and analyses of surveys for Georgia and Ukraine are presented separately.

As many as 88.9% of all respondents from the Georgian SSOs answered that their organization focused on digital transformation, while only 11.1% replied that the digital domain was not the priority for their organizations. Majority of respondents perceive a digital capacity building in organizations as a priority, which points to the inevitability of digital advances for the SSOs.

[51] "Digital country," Ukraine Now, accessed on 23 May, 2022, https://ukraine.ua/invest-trade/digitalization/

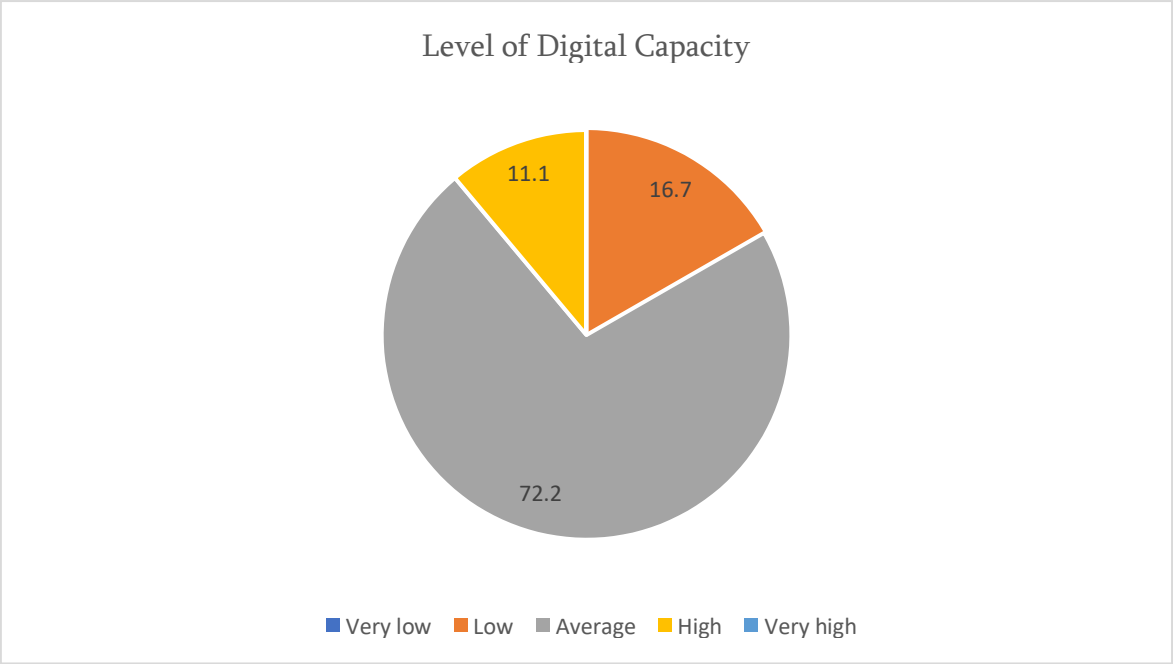


To the question on how their organizations applied digital transformation to their services, various answers have been provided. Among them are: adapting and developing digital technologies including General Packet Radio Services (GPRS) to facilitate developing emergency risk maps, to deal with daily paperwork, to make working processes easier and faster and to keep the data safely stored.

Apart from using the technological innovation to provide a better security and safety to the citizens and to keep the sensitive data protected, public servants in SSOs perceive digital transformation as a tool to facilitate their daily working processes.

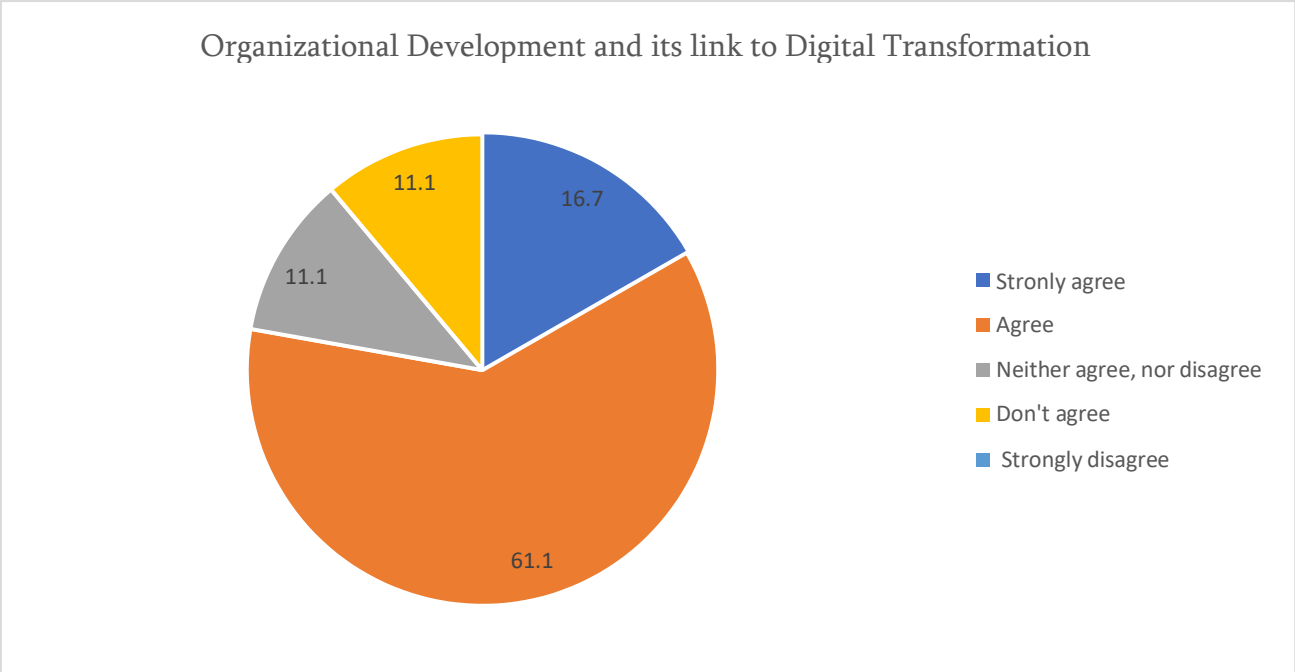
To the question on defining the level of digital development in the country, 72.2% answered that it was average, while 16.7 % of respondents replied that it was low, and only 11.1% replied that their organizational digital capacities were high.

According to that response, we can see that the majority of respondents evaluate digital developments in their countries as moderate, which implies that some SSOs have already experienced digital advances at some level but there is still a space for a further growth in that direction.



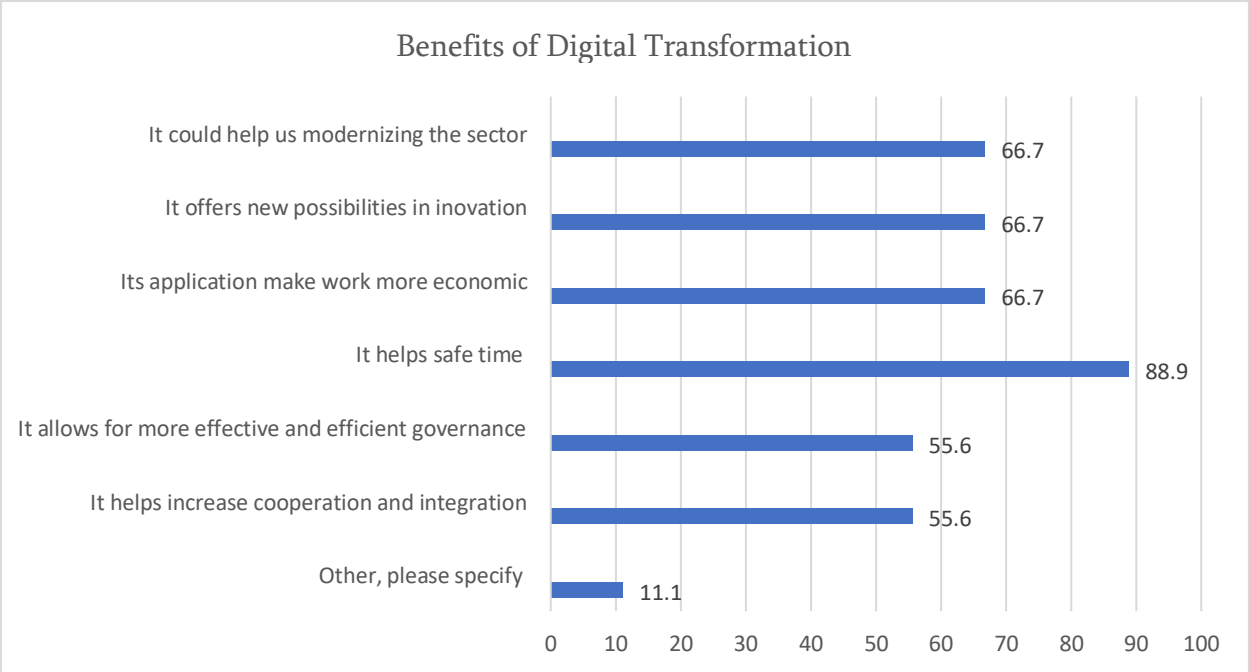
61.1% of all respondents agreed with the statement that the future development of their organizations largely depended on the SSOs digital capacities, while 16.7% replied that they strongly agreed with the statement, and 11.1% responded that they neither agreed and nor rejected the idea and the same percentage of respondents disagreed with the statement.

That tells us that the majority of respondents had awareness about an important link between the digitalization progress and organizational developments that creates space for successful organizational and reform processes to be implemented in the sector.



To the question "what kind of influence the digital transformation can have on your organization," the majority of interviewees, 88,9% replied that it saved time, while 66.7% believe that the digital transformation would modernize the organization, offer new possibilities for innovation and save costs. 55.6% of respondents think that its application makes governance more effective and efficient, and it helps increase cooperation and integration.

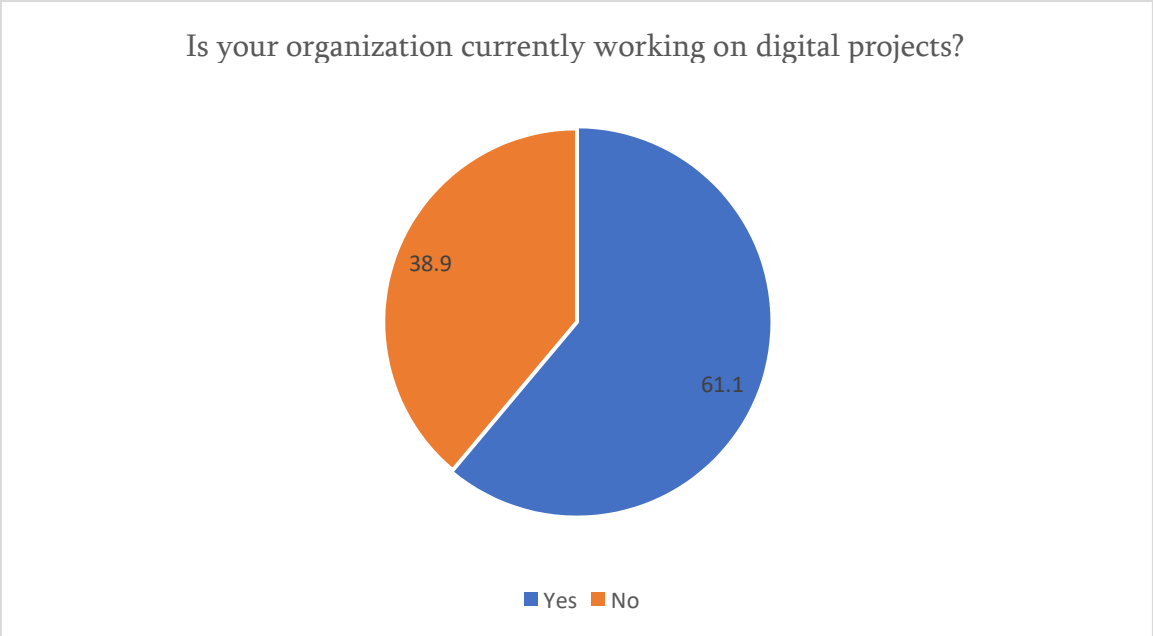
The fact that such a high number believes that digital transformation will save their time means that the security sector perceives digitalization as a tool to facilitate and ease their daily working processes. Incorporating and embracing the approach and the thinking where digitalization is perceived as a tool to provide better services to citizens, would create space for more innovation and advances in that domain.



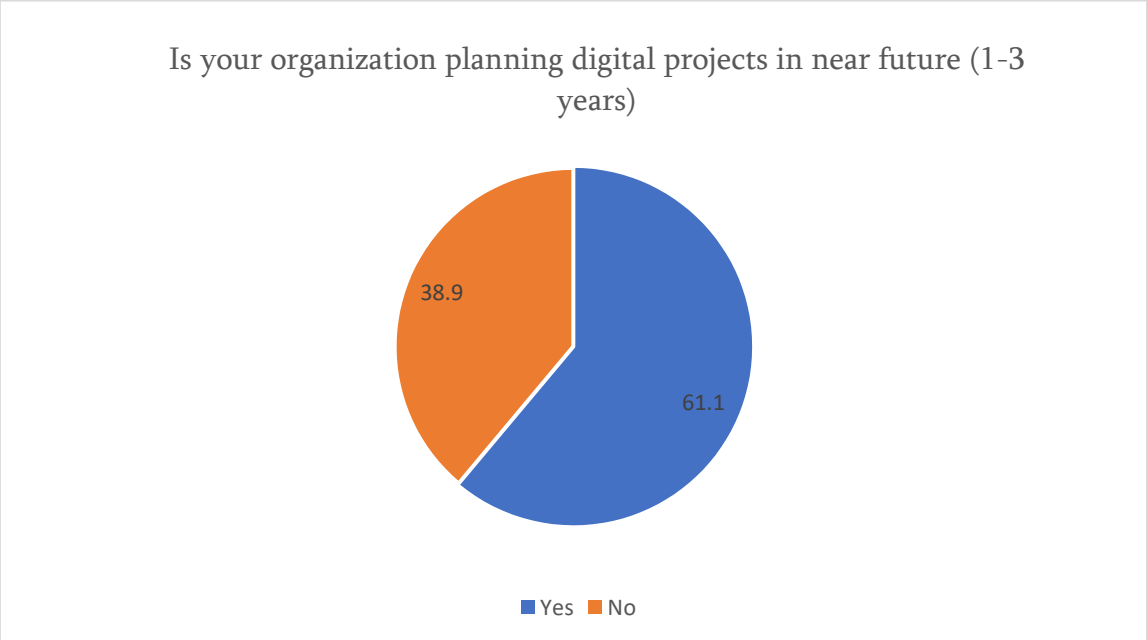
To the question "is your organization currently working on digital projects", 61.1% from all respondents replied 'yes' and 38.9% replied 'no'.

Exactly the same number of responses was received on the closed-ended question if their organization is planning to implement digital projects in the near future (1-3 years).

This shows that there is a number of current and future digital activities and projects planned in the security sector organizations.



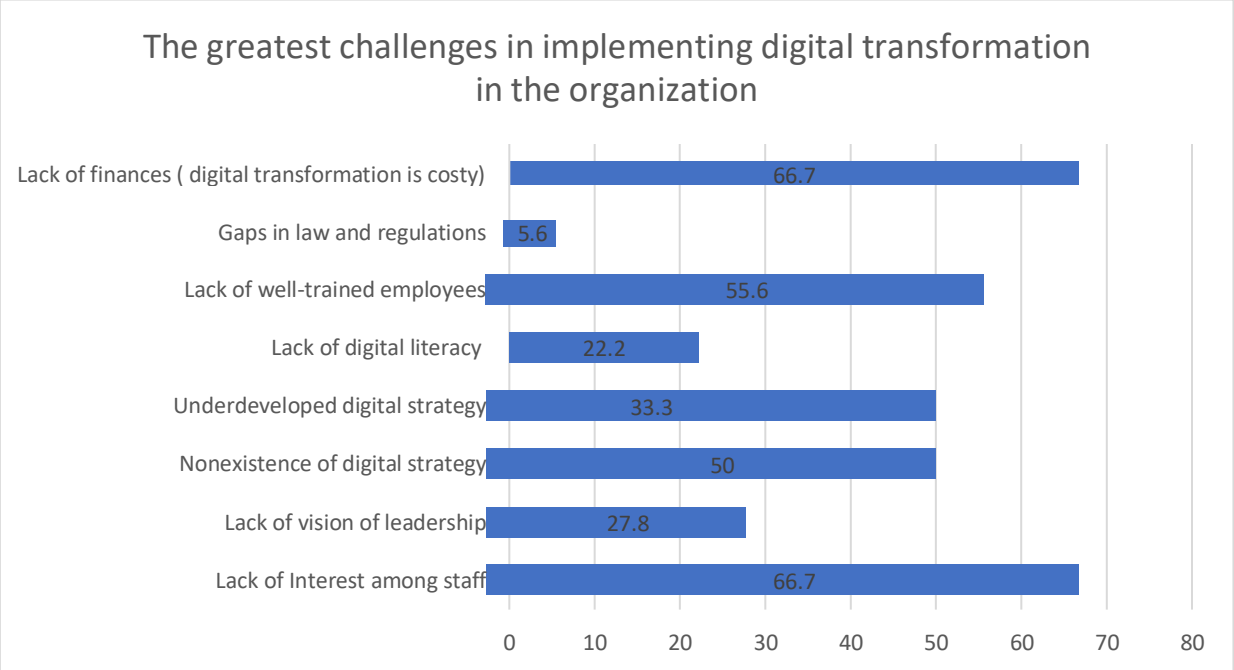
Ongoing digital projects include standardization of data registration, adaptation of digital programs during work process, software development, digitalization of data, utilization of electronic communications during emergencies and creation of digital tools for educational platforms.



Digital projects planned in the security sector organizations in the near future include developing organizational cooperation mechanisms for using the shared digital data and developing risk management maps through using digital technologies.

To the question "in your opinion which of the digital areas listed below need to be used to develop organizational capacities and to what extent," cyber security was the most rated (83.3%) one, followed by mobile devises (72.2%) and e-identities and/or e-signatures (61.1%).

Cyber security as a significant part of the digital developments in organization is a fundamental and integral part of the security sector organization's development. In Georgia, there is a high usage of mobile applications[52]. However, various mobile applications developments in the organizations would be beneficial for the sector development in Georgia.



[52] Nino Taganashvili, "Digital Services as a Mean of Direct Interaction between the State, Business, and Citizens on the Example of MY.GOV.GE," fighting corruption (blog), Institute for Development of Freedom of Information (IDFI), January 23, 2022, https://idfi.ge/en/digital_services_as_a_mean_of_direct_interaction_between_the_state_business_and_citizens_on_the_example_of_my_gov_ge.

We can see that security sector employees in Georgia perceive financial scarcity and the lack of employees' interest in digital affairs as the main obstacle in creating organizational changes and progress through digital developments.

Survey Analysis - Ukraine

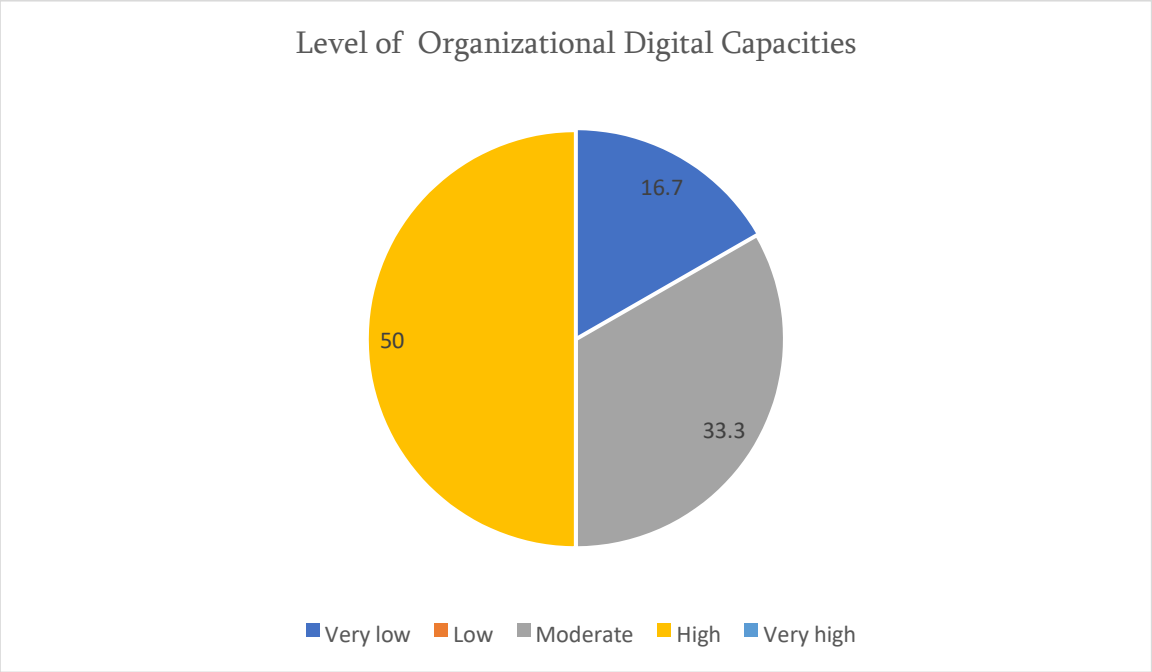
The absolute majority of respondents (100%) agreed that their organization was focused on digital transformation.

Similar to the Georgian case the interest in the digital transformation processes in SSOs is very high.

50% voted that the level of their digital capacities in their organization was very high, while 33.3% wrote that it was moderate and 16.7 % marked it as very high.

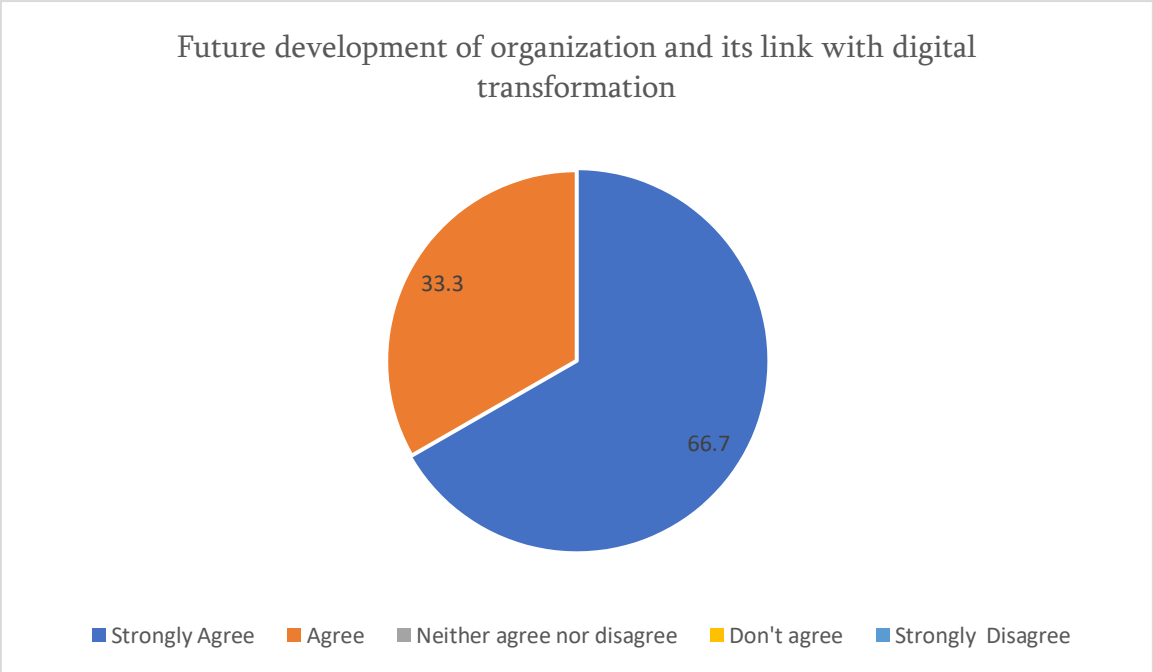
About half of the respondents voted for high digital organizational capacities in the case of Ukraine, while in the case of Georgia only 11.1% voted that their organizational digital capacities were high, and majority (72.2%) voted for average.

In contrast to the Georgian SSO employees, the Ukrainians demonstrate a higher evaluation of digital developments and progress in their organizations.



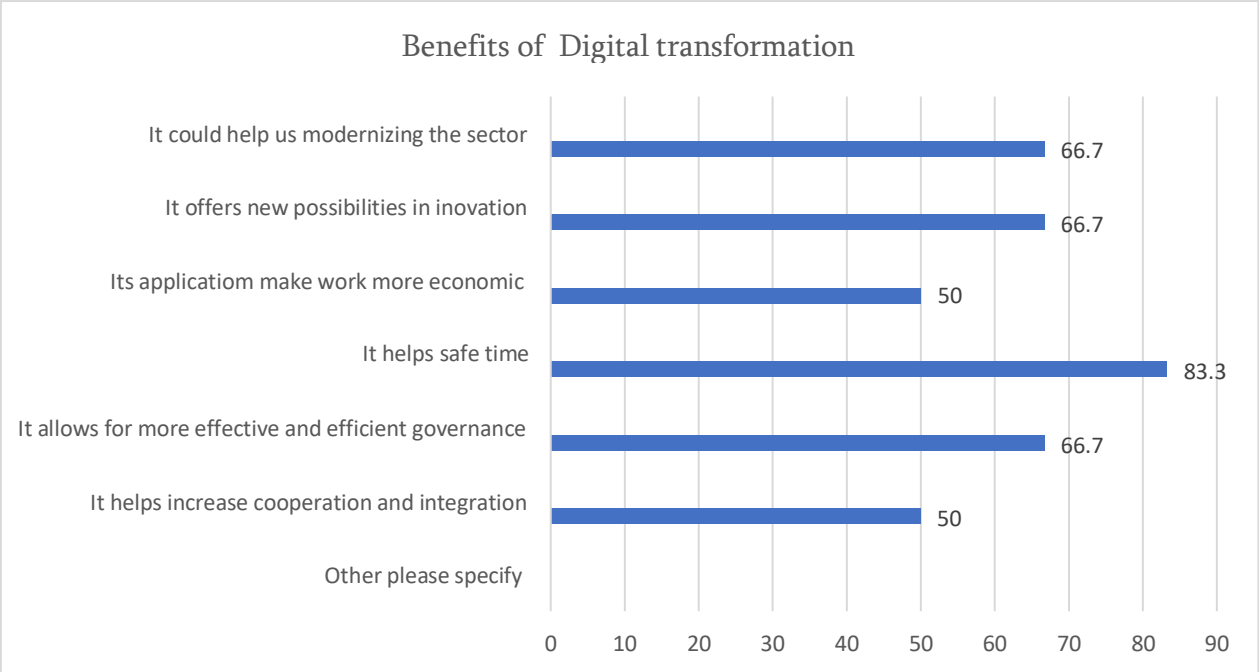
To the question "do you think the future development of your organization largely depends on its digital capacities", 66.7% wrote that they strongly agreed with this statement, while 33.3% indicated a simple agreement.

It implies that more than half of the respondents think that the organizations' future evolution or development is strongly linked to its digitalization, while less than fifth agreed strongly in case of Georgia.



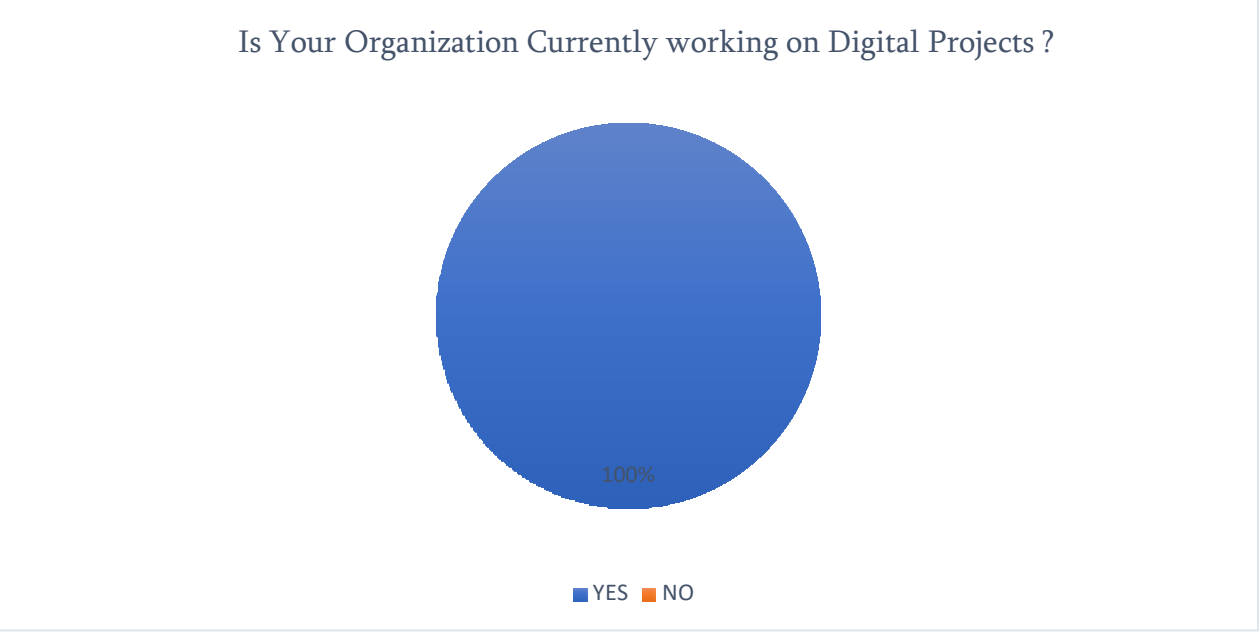
As many as 83.3 % of the surveyed responded that digital transformation in their organizations would help them save time, 66.7% believe that it would help them modernize the sector, offer new possibilities in innovations, and allow for more effective and efficient governance, while 50% replied that its application made work more economic and increased cooperation and integration.

It is observed that both in the Georgian and Ukrainian cases majority of employees of SSOs perceive the digital transformation as a tool that would allow them to save time while implementing their daily tasks, while the primary focus should be on providing more effective services to citizens and strengthening digital cyber resilience.

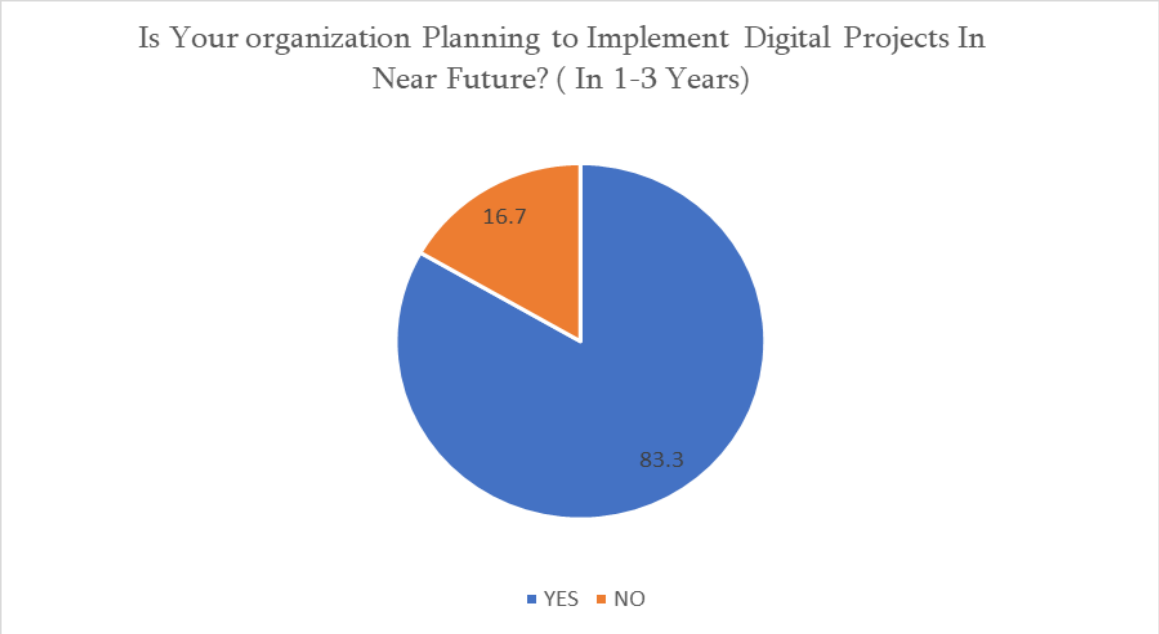


To the question "is your organization currently working on digital projects", the absolute majority of all responders (100 %) replied 'yes'.

The new platform for coordinating communication and internal electronic document management system is functioning in SSO in Ukraine.



To the question “is your organization planning to implement digital projects in the near future?” as many as 83% of the responders replied ‘yes’ and only 16.7% wrote ‘no’. Accordingly, it is high probability that SSOs in Ukraine will have more progress in digital domain.

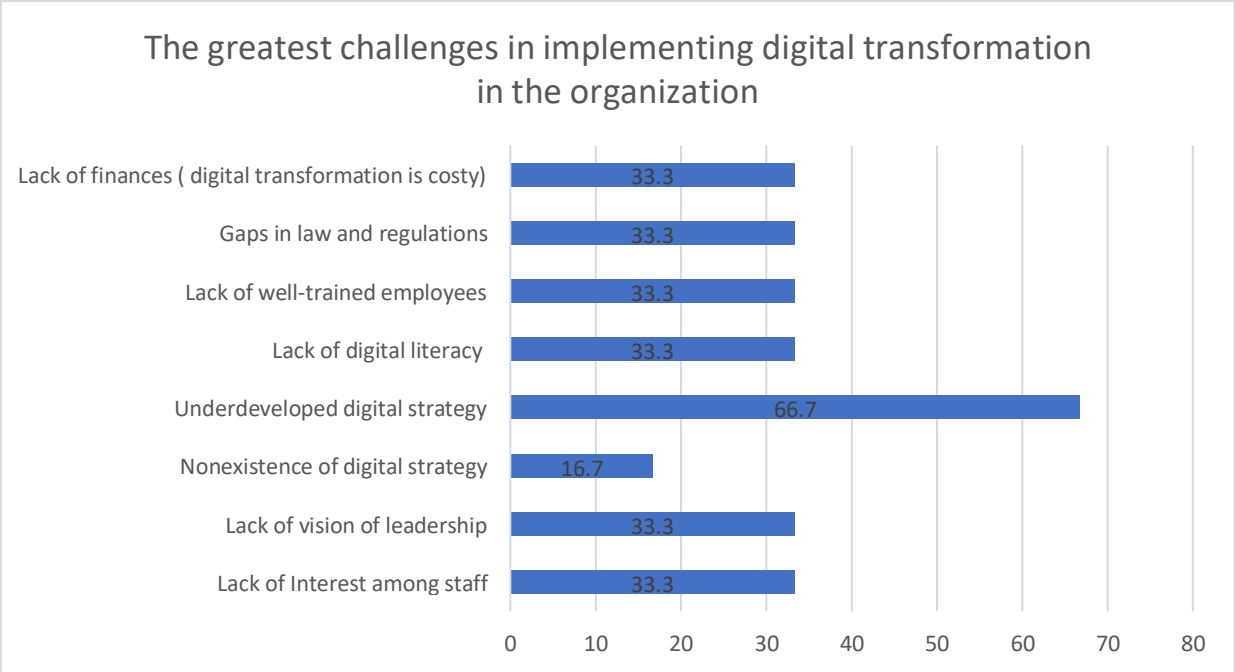


The full integration of law enforcement databanks into internal system alongside with the provision of use of the electronic document management system by every department and unit has been planned in the near future. The security sector employees in Ukraine think that due to the war, it is difficult to determine the scope of digitalization for the coming years.

STEPS Center of the National Academy of Sciences of Ukraine saves their information on cloud storage, regularly makes site updates, manages their server, and communicates and works distantly by the special digital tools.

Cyber security was perceived as the most important field to be digitally developed, according to all of the respondents. Cloud computing and e-identities and/or e-signatures all were marked by 66.7%. While e-governance and development of artificial intelligence were chosen by half of the respondents.

To the question “what are the greatest challenges in implementing digital transformation processes in your organizations”, majority (66.7%) of the respondents pointed to the underdevelopment of digital strategies. All other answers, except the nonexistence of a digital strategy, registered 33.3 %, and the nonexistence of digital strategy as the concern was marked just by 16.7 %.



These findings reveal that there is a space for the Ukrainian SSOs to improve their strategies and legal frameworks to drive forward their digitalization processes.

Digital governance in Georgia and Ukraine

Estonia is a true digital success example – the country is digitalized almost in every area. Georgia and Ukraine are beginners on the digital journey. Even though Georgia and Ukraine take important measures regarding the digital agenda and carry out crucial public sector digital projects, there is still a long way to go.

The Digital Governance Agency, which operates under the Ministry of Justice of Georgia since 2020, is responsible for providing e-governance services to the citizens, supporting, and developing digital governance, strengthening cybersecurity, and in general, contributing to the development of digital transformation processes in Georgia.

Ministry of Economy and Sustainable development of Georgia covers the areas of communication, information, and modern technologies. For example, implementing a project under the EU4Digital

aiming at enhancing the legal frameworks of broadband development aligned with the European Union norms and diminishing digital divide across urban and rural areas. [53]

Provision of transparent data to the citizens is part of good governance, which decreases the level of corruption in public sector and accordingly, its implementation in the security sector has a major importance. Digitalization, including the technological development, is an instrument for the SSOs to provide effective and efficient governance to the citizens that is based on principles of transparency, equality, and safety.

Establishment of GSSG would require the development of secure and safe portal that would allow for an access to and share on all public data in Georgia.

In the digital, and mainly, cyber management, multiple agencies are involved in Georgia. The Digital Governance Agency is responsible for managing the computer emergency response team (CERT-GOV-GE) which is tasked with registering, analyzing, and implementing preventive measures during cyber-attacks on public and private sector's computer systems. The Agency is responsible for raising awareness on cyber topics through trainings, seminars, and joint exercises as well.[54] LEPL Cyber security bureau functioning under the Ministry of Defense is mainly responsible for defining cybersecurity policy and facilitating its implementation. The Ministry of Internal Affairs of Georgia, division for fighting against cybercrimes, which functions under the central criminal police department, deals with investigating the cyber-crime cases. The National Security Council is regularly receiving and preceding information about cybercrimes against national security and through drafting informational-analytical documents provides adequate support to the addressee.[55] In Ukraine, the Ministry of Digital Transformation is mainly in charge of managing digital projects in the country. The ministry is functioning under the Cabinet of Ministers of Ukraine and was created in 2019 on the basis of the State Agency for Digital Administration which was established five years prior to that. The agency is primarily focused on e-services, digital education, building digital infrastructure and cyber security.[56]

Ukraine has a strong cooperation track record with the Estonian e-Governance Academy starting from the year 2016. EGOV4UKRAINE was the project that led to less corrupt and more efficient public services in Ukraine. The data exchange platform "Trembita" became one of the biggest projects of the E-Governance Academy. Through "Trembita", more than million data get exchanged monthly. The platform was created on the model of x-road, and it has a high level of protection around signature.[57]

---

[53] "Communications, information, and modern technologies," Ministry of Economy and sustainable Development of Georgia, accessed on May 25, 2022, http://www.economy.ge/?page=projects&s=18&lang=en

[54] "History," Digital Governance Agency, February 07, 2022, https://dga.gov.ge/?m=articles&id=Br8mYPictY

[55] "Ordinance of Government of Georgia on cyber security 2021-2024 National strategy and Action plan," Legislative Herald of Georgia, October 4, 2021, https://matsne.gov.ge/ka/document/view/5263611?publication=0

[56] Sławomir Matuszak, "The digitization of Ukraine: anatomy of a success story," osw.waw.pl, August 23, 2021, https://www.osw.waw.pl/en/publikacje/osw-commentary/2021-08-23/digitisation-ukraine-anatomy-a-success-story

[57] Justin Petrone "Deployment of Trembita system in Ukraine a milestone for Estonian digitization efforts," E-estonia, April 22, 2021, https://e-estonia.com/deployment-of-trembita-system-in-ukraine-a-milestone-for-estonian-digitisation-efforts/.

The "Diia" website was launched with the support of the US, the UK and Switzerland. Using the webpage, the Ukrainian citizens can access about 50 administrative services. Also, through "Diia", the citizens can change their residential registration.[58] It is used by 8 million people, through both the mobile application and web versions. By 2024, the government aims at providing all services through that webpage.[59]

"My.gov.ge" website, which provides e-services for the Georgian citizens, allows access to electronic documents and citizens, can reassure ID cards, passports, birth and death certificates, has become one of the most popular websites in Georgia. The webpage has far more potential for development, in terms of various services provision and online data protection.

Those e-service portals such as "my.gov.ge" website in Georgia and "Diia" in Ukraine, would facilitate and ease the processes of creation of data tracker system, alongside with the laws on protection of personal data in both countries.

The e-governance has provided a substantial assumption for the government to enhance the role of the SSOs as the trusted and progressive entities. The Estonian government underlines that the e-service development annually saves about 2% of the GDP and more than 800 years of working time for public and private sector in a calendar year.[60] The e-governance development in the SSOs leads to saved costs and contributes to a more rational and effective use of human resources.

The Georgian and Ukrainian governments should reform and enhance the e-governance systems particularly in the SSOs, in order to increase public trust and provide effective public services.

Recommendations

Based on the knowledge and findings as a result of a large study of diverse sources of data from different articles, books, official documents, questionnaire analyses and expert interviews, this section presents policy recommendations for the security sector organizations (SSOs) in Georgia and Ukraine, and they

[58] Sławomir Matuszak, "The digitization of Ukraine: anatomy of a success story" osw.waw.pl, August 23, 2021, https://www.osw.waw.pl/en/publikacje/osw-commentary/2021-08-23/digitisation-ukraine-anatomy-a-success-story.

[59] Alexander Iosad and Oliver Large "State of Resilience: How Ukraine's Digital Government Is Supporting Its Citizens during the War," institute.global, April 18, 2022, https://institute.global/policy/state-resilience-how-ukraines-digital-government-supporting-its-citizens-during-war.

[60] Rainer Kattel and Ines Mergel, Estonia's Digital Transformation: Mission Mystique and the Hiding Hand (Oxford University Press, 2019), 144, https://oxford.universitypressscholarship.com/view/10.1093/oso/9780198843719.001.0001/oso-9780198843719-chapter-8 .

can also be considered for the other Eastern Partnership countries, depending on the country-cases. The recommendations aim at putting forth a number of specific measures that can be useful for the security sector reform (SSR, with a focus on digitalization), and for adjusting the sector in line with the good security sector governance (GSSG) standards through digital transformation. The recommendations' purpose is to support, guide and encourage SSOs to take the necessary actions and apply a number of the best-practice digital tools to strengthen institutional capacities, improve efficiency of governance and provide better protection and services to the citizens.

- Digital development tools and practices from Estonia should be incorporated in the Georgian and Ukrainian cases, very carefully considering the countries' specific cultural specificities, level of digital literacy and digital history.
- Political will, and the leaderships' understanding and proactive approach to the importance of digital transformation processes in the security sector should be present. It is recommended to carefully select a proper leadership style for the security sector leader in digital transformation processes, and maintaining that consistency in each stage - starting from the idea initiation to, projection and execution in the organization, is of pivotal importance.
- Enhancing the level of digital literacy among the leadership and employees. Knowledge that is cultivated in the ICT departments on digital skills, strategies and ongoing and planned activities should be shared with other colleagues with an aim to raise the level of understanding and acquiring the required digital skills that might be useful during implementing their daily tasks.
- Being able to go beyond some organizational limitations and inflexibilities that exist in such bureaucratic structures as the SSOs, to create a basis for digital innovation and progress.
- To learn from the experiences of other countries through arranging official visits, initiating joint projects and trainings. Georgia and Ukraine should be actively engaging in cooperation and synergies and launching mutual projects not only to enhance digital capacities of SSOs but also to enhance the digital literacy in the countries. In this regard, Estonia should have the role of the mentor and expert casting a "digital spotlight" to the organizations in Eastern partnership countries.
- In order Georgia and Ukraine to strengthen cyber security in their countries and ensure safe and secure utilization of digital portals offered by the SSOs during service delivery, both countries should have well-trained public in digital and cyber skills; and in order to achieve that goal, the public (including all age groups) should be involved in digital education and learning programs. The level of digital literacy among people in remote areas and villages both in Ukraine and Georgia bears specific importance.
- Incorporating digital transformation topics and cooperation mechanisms in the bilateral cooperation agendas between the countries, and their relevant SSPs; particularly in already existing international memoranda and agreements (or drafting and signing new ones).
- In the cases of Georgia and Ukraine, both countries should focus more on creating added values of technologies for the benefits of their citizens, rather than focusing on the technology itself.

Accordingly, the attitude towards technologies should be reconsidered and adapted, as both countries lack resources and experience in technological development.

- Georgia and Ukraine should not create and pass vast new laws and rules on digital development, but instead, should adjust, change and update the already existing ones to meet new digital needs and realities.
- While creating and adopting any new legislative, technological and/or digital initiative, the principle of "people come first" should be considered, in order to enable governments to provide effective services to their citizens.
- Georgia and Ukraine should enhance and strengthen public trust in the SSOs and services provided.
- Data tracker program should be created in Georgia and Ukraine, in order to create and deepen public trust in SSOs, enabling the transparency and safety for citizens and diminishing gender inequality within and beyond the security sector.
- In order to promote public trust in SSOs, the government should enquire the provision of citizens' data in order to provide more comfortable services to them.
- Creating public services delivered by the SSOs that are easy and simple to use.
- Georgia needs to create unified data exchange platform that would enable activation of ID cards to receive services as well and would create ground for the creation of data tracker system.
- Creation of the united online data base should consider digital safety of online platform in order to ensure the safety and protection of personal information against cyber-attacks and unlawful leakage of data.
- Enhancing the cyber resilience of "Diia" portal in order to ensure safe and secure protection of citizens data online.
- As a part of GSSG and digitalization processes, Georgia should develop a more secure and safe data sharing system like "x-road", incorporated in security sector covering the data privacy and limitations on its access. The Georgian security services should rely on already existing practices in Georgia (for example from the service provision from the Ministry of Justice) while providing effective digital services for citizens.
- It is necessary to build digital infrastructure in SSOs in regions in order to facilitate provision of safety and security to the citizens.
- Considering the importance of foreign partnerships and cooperation, it is essential to be open to international cooperation, communications, and exchange with academia, foreign partners and private sector.
- Mobile internet use is increasing in Georgia[61] : offering mobile applications to the population in order to increase inclusiveness to public services and ensuring the safety of use are a recommendation to the MIA of Georgia.

[61] Nino Taganashvili, "Digital Services as a Mean of Direct Interaction between the State, Business, and Citizens on the Example of MY.GOV.GE," fighting corruption (blog), Institute for Development of Freedom of Information (IDFI), January 23, 2022,

- To develop PPPs, in order to facilitate and generate new ideas in the security sector digitalization processes.
- Ukraine should develop and improve the organizational strategies and legal frameworks in order to move digitalization processes in security sector forward.
- The improvement and investment in the digital literacy within SSOs in Georgia, and spreading and sharing the knowledge that exists in the ICT departments with other departments: this would improve digital knowledge and skills in the organization.
- Even though both Georgia and Ukraine are looking forward to embracing technological developments and innovations they are both countries with limited resources and developing economies. Thus it is important to consider cost-saving and developing local capacities for expertise and infrastructure with minimum expenses. This can assist those countries in digital and security sector reform. Both countries can follow the Estonian example: spending less on foreign purchases and developing own digital capacities.

https://idfi.ge/en/digital_services_as_a_mean_of_direct_interaction_between_the_state_business_and_citizens_on_the_example_of_my_gov_ge.

Bibliography

Administration of the Government of Georgia. "Public Administration reform roadmap 2020." May 25, 2015. https://www.gov.ge/files/425_49309_322150_15.07.21-PublicAdministrationReformRoadmap2020(Final)(1).pdf.

CEPS "The Ukrainian Digital Resistance: cyber resilience and digital diplomacy at work.". May 18, 2022. https://www.ceps.eu/ceps-events/the-ukrainian-digital-resistance-cyber-resilience-and-digital-diplomacy-at-work/.

CMS. "Data protection and cyber security law in Ukraine." Accessed 12 June, 2022. https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/ukraine.

Conscensia. "Modern development centers in Poland and Ukraine." Accessed April 12, 2022. https://conscensia.com/it-specialists-poland-and-w4ukraine/#:~:text=Ukraine%20has%20over%20200%2C000%20IT,specialists%20are%20trained%20in%20Lviv.

Danilov Oleksiy: Cyber protection of state information resources is an essential component in the process of digital transformation of the country." May 22, 2020, https://www.rnbo.gov.ua/en/Diialnist/4606.html .

Digital Governance Agency. "History" February 07, 2022. https://dga.gov.ge/?m=articles&id=Br8mYPictY.

DCAF- SSR Backgrounder. "Security Sector Reform- Applying the principle of good governance to the security sector." files.ethz.ch. Accessed April 23, 2022. https://www.files.ethz.ch/isn/195671/DCAF_BG_2_Security%20Sector%20Reform.11.15.pdf .

"DIGAR." Cyber security in Estonia, Digar Estonian articles, July 1, 2019. https://dea.digar.ee/cgi-bin/dea?a=d&d=JVestinformsyst201907.2.7.3&e= ------ et-25--1--txt-txIN%7ctxTI%7ctxAU%7ctxTA---------- .

E-estonia. "This is the story of the word's most advanced digital society, e-estonia." Accessed April 25, 2022. https://e-estonia.com/story/.

E-estonia. "Factsheet e-governance." Accessed April 26, 2022. https://e-estonia.com/wp-content/uploads/e-governance-factsheet-sep2021.pdf .

eTrade for all "Building the digital government - Estonia's Digital Transformation." October 28, 2019. https://etradeforall.org/news/building-the-digital-government-estonias-digital-transformation/

Fedorov, Mykhailo. "Ukraine's digital revolution is gaining momentum." UkraineAlert (blog) Atlantic Council, September 7, 2021. https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-digital-revolution-is-gaining-momentum/.

Guerber, Thomas. "Digitalization and SSG: adapting to a new reality." dcaf.ch. October 15, 2021. https://www.dcaf.ch/digitalisation-and-ssgr-adapting-new-reality .

Geneva Centre for Security Sector Governance (DCAF), "SSG/R," dcaf.ch. Accessed April 12, 2022. https://www.dcaf.ch/about-ssgr .

Hänggi, Heiner. "Conceptualizing UN support to security sector reform." dcaf.ch. Accessed April 22, 2022. https://dcaf.ch/sites/default/files/imce/UN%20SSR%20History/01_H%C3%A4nggi_Conceptualizing.pdf.

Hankewitz, Sten, "Estonian cyber security company shares free cyber hygiene training with Ukrainian police cadets." estonianworld. April 6, 2020. https://estonianworld.com/technology/estonian-cyber-security-company-shares-free-cyber-hygiene-training-with-ukrainian-police-cadets/ .

Hesteren van Daphne, Weyzen Raymonde and Knippenberg van Laura. "Open data best practices in Europe: Estonia, Slovenia and Ukraine." data.europa.eu. last modified February 24, 2022. https://data.europa.eu/sites/default/files/report/Open_Data_Best_Practices_in_Europe_Estonia_Slovenia_and_Ukraine.pdf

Institute for Development of Freedom of Information. "Georgia in the UN E-Government Survey – Review of 2020 Results." July 22, 2020. https://idfi.ge/en/e-governance-e-participation-georgia-index-2020 .

Iosad, Alexander and Large Oliver. "State of Resilience: How Ukraine's Digital Government Is Supporting Its Citizens during the War." institute.global. April 18, 2022 https://institute.global/policy/state-resilience-how-ukraines-digital-government-supporting-its-citizens-during-war.

Kattel, Rainer and Mergel Ines. Estonia's Digital Transformation: Mission Mystique and the Hiding Hand. Oxford University Press, 2019. https://oxford.universitypressscholarship.com/view/10.1093/oso/9780198843719.001.0001/oso-9780198843719-chapter-8 .

Legislative Herald of Georgia. "Ordinance of Government of Georgia on cyber security 2021-2024 National strategy and Action plan." October 4, 2021.

https://matsne.gov.ge/ka/document/view/5263611?publication=0.

Matuszak, Slawomir. "The digitalization of Ukraine: anatomy of a success story.'' osw.waw.pl. August 23, 2021. https://www.osw.waw.pl/en/publikacje/osw-commentary/2021-08-23/digitisation-ukraine-anatomy-a-success-story.

Ministry of Economy and Sustainable Development of Georgia "Communications, information, and modern technologies." Accessed May 25, 2021. http://www.economy.ge/?page=projects&s=18&lang=en.

Petrone, Justin. "Deployment of Trembita system in Ukraine a milestone for Estonian digitization efforts." e-estonia. April 22, 2021. https://e-estonia.com/deployment-of-trembita-system-in-ukraine-a-milestone-for-estonian-digitisation-efforts/.

Stone, Mark. "How Estonia created trust in its digital-forward government." Securityintelligence. September 17, 2021. https://securityintelligence.com/articles/estonia-trust-digital-government/.

Siddiqui, Zeba. "Russian cyber spies attack Ukraine's allies, Microsoft says," reuters. June 22, 2022. ''https://www.reuters.com/world/russian-hacking-groups-step-up-cyber-espionage-ukraine-allies-microsoft-says-2022-06-22/

Taganashvili, Nino. "Digital Services as a Mean of Direct Interaction between the State, Business, and Citizens on the Example of MY.GOV.GE." fighting corruption (blog), Institute for Development of National Security and Defense Council of Ukraine. Institute for development of Freedom of Information (IDFI), January 23, 2022. https://idfi.ge/en/digital_services_as_a_mean_of_direct_interaction_between_the_state_business_and_citizens_on_the_example_of_my_gov_ge .

Ukraine Now. "Digital country." Accessed May 23, 2022. https://ukraine.ua/invest-trade/digitalization/.