Developing e-government under cyber threats and Russia's war: Ukraine's Diia platform

Claudiu CODREANU,
Romanian Diplomatic Institute, Bucharest, Romania
claudiu.codreanu@idr.ro

Abstract
Digital democracy used to be an aspiration of the 'old' internet culture. Some saw it as an entirely new system, much more participatory and grounded in libertarian values, while others expected an upgraded democracy and a digitalization of public services and government-citizens interactions. A few decades later, democracy has received a digital upgrade, but mostly for public services. One such remarkable achievement is Ukraine's Diia platform, which launched in 2020 and gained significant public attention in 2023 amidst Russia's full-scale war of aggression. Ukraine has been a target of Russia's hybrid warfare since 2014, from covert military attacks, illegal annexations, disinformation campaigns, to cyberattacks. Despite this, Kyiv managed to promote and implement its e-government platform in the middle of Russia's hybrid war and then full-blown war against the country. Estonia is another relevant example of e-government, having also boosted its efforts for e-government after Russian cyberattacks. This paper analyzes Ukraine's Diia platform and examines the cybersecurity challenges that the country faces in maintaining e-government services online and secure against the multitude of cyber operations and malware targeting them, either from cybercriminals or state actors. This discussion will begin with a brief literature review focused on e-government and cybersecurity. Ukraine's case will be taken into consideration alongside Estonia's example, but the focus will remain on Diia and Ukraine's cybersecurity policies and practices, including international partnerships. Moreover, the paper puts forward several recommendations derived from Ukraine's experience, including strenghtening cybersecurity measures for all e-government developments, bolstering international partnerships, and implementing lessons learned from other countries. The findings offer insights for practitioners, policymakers, and scholars focus on digital governance, e-government, and cybersecurity.

Keywords: Diia, cybersecurity, hybrid warfare.

1. Introduction

Since 2014, Ukraine has been at the forefront of Russia's hybrid warfare as it has been targeted with several groundbreaking cyber operations, ranging from successful cyberattacks against the powergrid and operations that severely disrupted government and private organisations. Despite this, Kyiv bolstered its cyber defences and reinforced its efforts of developing its e-government systems, culminating with the Diia platform. After Russia started a full-blown war of aggression against Ukraine in February 2022, Diia, which means "action" in English [1], became an essential tool of maintaining a robust and trustful relationship between the government and citizens during the war, adapting the platform for the new harsh realities of the conflict. For instance, the app was also used to listen to the radio or watch TV channels during power blackouts caused by Russia's attacks [2].

This paper examines the development of e-government against hybrid and cyber operations, comparing the Estonian and Ukrainian cases and focusing on analysing Diia's role during Russia's war against Ukraine and cybersecurity challenges posed by Russia. Ukraine was chosen for this case study because the country has been a primary target of Russia's hybrid operations, especially cyberattacks. Despite this, the country managed to develop functional e-government services and platforms capable of withstanding a full-blown war. Estonia on its part was chosen because of its long and successful history in

adopting digital services for its government services, and also because of its own experience with Russian cyber operations, being the target of a disruptive cyber campaign in 2007. Moreover, Estonia played an important role in supporting Ukraine's endeavour of developing e-government services, both as a forerunner in this area and with international assistance. In addition to this, the paper puts forward several recommendations derived from Ukraine's experience, including strenghtening cybersecurity measures for all e-government developments, bolstering international partnerships, and implementing lessons learned from other countries.

2. The concept of e-government

E-government essentially refers to governments offering services online through digital means, increasing accessibility and optimizing the relationship between citizens and the state. The UN defines e-government as "the use of ICTs to more effectively and efficiently deliver government services to citizens and businesses" [3]. Thus, it refers to the implementation of digital technologies and software in government operations to "achieve public ends by digital means" [3]. E-government refers to the digitalization of government data and records and of the communication between the government and citizens, or, more plainly, using ICTs within the public sector to optimize governmental and public administration processes [4].

The e-Governance Academy (eGA), a non-profit foundation founded in 2002 by the Estonian Government, United Nations Development Program (UNDP), and the Open Society Institute, provides another definition of e-governance. For eGA, e-governance entails three dimensions – e-administration, e-services, and e-participation – and it refers to the "transparent and efficient use of ICT" in public administration, public services, and citizen participation in decision-making processes [5].

E-government and e-democracy are linked, but as the former refers to digital government services, the latter takes into account different democratic processes and focuses on the idea of public deliberation and participation. E-democracy entails "using ICT in political processes concerning information, discussion, and decision-making" [6]. The difference noted by Gustav Lidén (2013) is that e-democracy also includes democratic political and civil rights [6]. Similarly, OECD uses the term of "digital government" for e-democracy, describing it as transforming government processes and services by using digital technologies to enhance the public sector's activities and relation with citizens [7].

Transparency is a crucial element and benefit of e-government, enabling accessible open governmental data [8]. Transparency and public trust are interlinked, as open information reduces corruption and encourages citizens' participation in democratic processes [8]. Open information, Open Data, or Open Government data, refers to public sector information that is made available to everyone for use and distribution [9]. Therefore, citizens' trust in digital public services depends on the perception that the government is transparent, accountable, and competent in providing online services, which includes clear safeguards for data security and privacy and cybersecurity measures [8].

3. Ukraine and Estonia's e-government development intertwined

3.1. Estonia making the foundation

Estonia started adopting its major e-government policies in 1998, its main goals being reducing bureaucracy by using digital tools, making citizens democratic participation and relations with authorities more accessible and faster, and reforming administrative processes [8]. The e-ID technology was introduced in 2003 for accessing available e-services, which included transport passes and tickets [8].

Now, Estonia is ranked 6 out of 38 countries measured by the OECD 2023 Digital Government Index [7]. 99% percent of government services are online and digital public services have a user satisfaction rate of 82% [5]. Moreover, the Freedom House Net Freedom Index ranks Estonia as one of the top countries regarding internet freedom [5].

The main platform for e-government and online public services is eesti.ee, where the user has to log in with a government-issued electronic ID [5]. Moreover, lawmakers can draft legislation online, and citizens can browse the drafts and get involved in public consultations whilst also propose citizen initiatives [5]. Thus, the e-government services also include a focus on e-democracy facilities. The system for online voting is referred to as 'i-Voting', enabling citizens to cast their votes remotely in an accessible and convenient way [5]. I-voting was adopted in 2005, and, 18 years later, half of the votes registered during the 2023 elections were cast online [5, 8]. Moreover, non-residents gained access to digital identification and business-related e-services in 2014 [8].

3.2. Ukraine's e-government development

Ukraine's development of e-government policies has been closely linked to Estonia since 2012, when eGA began offering assistance, alongside the Organisation for Security and Cooperation in Europe (OSCE) [10]. Estonia has worked closely with Ukraine in developing e-government services, including Diia [11]. Moreover, the Estonian non-profit e-Governance Academy has supported Ukrainian local government digital initiatives since 2012 [11].

Several important landmarks have been achieved after the Euromaidan. In 2015, Ukraine launched the Prozorro ("transparency") platform, an electronic procurement system, and in 2018 it launched the Trembita platform, modelled on Estonia X-road solution, but using cryptography standards tailored for Ukraine's needs and regulation [10]. In the meantime, Ukraine's Parliament, the Verkhovna Rada, adopted laws that aimed at reducing corruption and increasing transparency, such as an electronic asset declaration required for all government employees in 2014 and the 2016 law of public procurement [10].

An important institutional step was taken in 2019 by President Volodymyr Zelenskyy, migrating the 2014-established Center for E-government to the newly-founded Ministry of Digital Transformation [10]. Moreover, the government established the position of Chief Digital Transformation Officers (CDTOs), and now every ministry has a CDTO and almost all oblasts (regions) have one [10]. CDTOs are responsible for increasing digital literacy and internet access for the population, implement e-services, and protecting critical infrastructure [10]. Concurrently, Ukraine continued to build and improve its physical

infrastructure for internet services. In 2022, the coverage of fibre-optic networks in the country reached 90%, with a similar rate for access to 4G mobile connections [10].

As a result, according to UN's E-Government report, Ukraine is ranked 30 out of 193 countries in the E-Government Development Index and 1 of 193 in the E-Participation Index [12]. In just two years, from 2022 to 2024, Ukraine moved up 16 places in the e-government index and 56 places in the participation index [12]. Estonia on the other hand has always been one of the best ranked countries in UN's report since 2003 [13]. The Baltic country is ranked 8 for e-government and 7 for e-participation [13]. Around the world, OECD's 2023 Digital Government Index has shown that most countries have taken steps to boost digital government policies and measures [7].

4. Diia and Russia's cyber, hybrid and conventional warfare

4.1. Diia

Diia is a mobile application and web portal for e-government functioning on the framework provided by the Trembita system [10]. Diia means "action", but it also stands as an acronym for "the state and me" [10]. Launched in April 2020, Diia is operated by the Ministry of Digital Transformation [14]. The launch of the digital platform was also part of President Zelenskyy's plan to reduce government corruption [15].

Diia includes more than 80 e-government services, such as tax payment, registering births or marriages, renewing passports, storing official documents such as passports, apply for unemployment and so on [15, 1, 2]. Citizens can access digital documents such as passports, ID cards, driver's licenses, vehicle registrations, birth certificate etc. [16]. Diia provides access and creation to a digital ID, credential storage (access for personal documents and storing only depersonalised data), communication with government offices, submitting requests and applications, payment for government fees, document management, and e-democracy facilities (surveys of public opinion, communication with citizens) [10].

According to Kyiv, Ukraine has become the first country in the world which made its digital ID valid to use anywhere in the country and all digital documents available in Diia have the same legal power as their physical equivalents [16]. Ukrainian Minister of Digital Transformation Mykhailo Fedorov stressed that the digital platform's development put people first to build trust, making it a human-centred e-government technology [2].

The platform works as a mobile application used a single portal for both citizens and businesses [16]. Ukraine also launched Diia.City in 2022, a platform specifically dedicated to IT businesses [16]. Almost half the country's population has registered on Diia, and more than 1 million entrepreneurs and 14.000 companies have used the app [16].

Support from Kyiv's international partners was a significant element. Ukraine received financial, technical, and legal assistance from USAID since 2019 for the development of Diia [17, 14]. Diia has also received assistance from the United Nations Development Programme (UNDP) and financial support from Sweden [1]. All in all, Kyiv received technical, policy, institutional, and financial assistance from USAID, UKAID, UNDP, and

aid agencies of Germany, Sweden, Switzerland, or Canada, among others [10]. For instance, the basic elements for Ukraine's e-government framework were developed with funding from Sweden's aid agency [10].

4.2. Diia's role after the 2022 Russian invasion

After Russia's full-blown invasion in February 2022, the app has been updated to include new functionalities, such as facilities for donating money, reporting the location of Russian troops on Ukrainian territory or claiming compensation for damaged property and receiving social support in war-torn areas [15, 17]. The app was also used to enable assistance requests for displaced Ukrainians [1]. More than 14 million people, around one third of Ukraine's population, are internally displaced or taken refuge outside the country since the 2022 Russian war of aggression [1]. Moreover, Diia offered the possibility of generating a temporary digital document encompassing all necessary personal information for evacuation and identification at checkpoints inside the country [2].

Thus, Diia became an essential tool for Ukraine's resilience during the war, facilitating contact with the government, offering help for the war effort, receiving support, or following news and official updates in war-torn areas where access to various services was severely affected. Diaa launched several new services, financial assistance to businesses and social assistance for the population, military obligations, grants for veterans, and TV and radio broadcasting, among others [10]. Diia enables Ukrainians who have had their ID cards lost or damaged to create a digital one using a digital signature and biometrics [11].

A significant challenge during Russia's war of aggression is maintaining the physical infrastructure as intact as possible during Russian air strikes and constantly repairing it [10]. However, Ukraine's telecom sector proved resilient and remained functioning during the war without massive longstanding disruptions, as Russian missiles and drones targeted it intensely [10]. Nevertheless, after only one year of war, the Ukrainian telecom sector is estimated to have lost more than 2 billion dollars, most of the damage being recorded in the regions of Kyiv, Kharkiv, and Donetsk [10].

4.3. Ukraine's cyber defence in the face of Russian cyberattacks

Russia started to deploy major cyber operations against Ukraine in 2014, at the beginning of the Russo-Ukrainian conflict. During the first Ukrainian elections after the Euromaidan, Russia deployed malware against the systems of the Central Elections Commission, even trying to alter the results shown on the website [18]. The attacks, however, did not have any significant impact. In December 2015, Russia launched a serious cyberattack against Ukraine's power grid, causing a blackout that lasted 6 hours and affecting more than 250.000 people [18]. The cyber operation was replicated in 2016, but it was neutralized in almost one hour and it affected only the region of Kyiv [18].

Nevertheless, the most disrupting cyberattack used by Russia against Ukraine was NotPetya. In 2017, Russia deployed a self-spreading malware disguised as a 'simple' ransomware, but NotPetya irreversibly encrypted data on affected systems [18]. It had a major impact on almost every government service, banking system, public transport system, airports, and even on Ukraine's private sector, including transnational companies,

causing a significant loss for both the government and companies affected [18]. Thus, Russia deployed a low-intensity series of cyber operations against Ukraine before 2022, using them in the context of the hybrid war against Ukraine [18].

Even though the expectation was that Russia was going to 'unleash its cyber arsenal' against Ukraine at the beginning or during the full-blown war of aggression started in February 2022, Russia did not manage to achieve significant results with cyber weapons [18]. Most cyber operations had low-intensity effects, such as website defacements, DDoS attacks, and data wiping, as more complex attacks failed either from their planning and execution and/or Ukraine's bolstered cyber defences [18].

The most visible cyberattack was launched against the Viasat Satellite network, which was used by Ukraine's army. The attack disrupted the network, causing collateral damage in Europe, but it did not have a tangible impact on the Ukrainian Armed Forces [18, 19]. Other attacks at the beginning of the war include DDoS attack against government agencies and banks, and deploying data wiping malware on infected systems in Ukraine, which did not have the expected impact, but could have disrupted Ukraine's e-government services and systems, for instance [18]. During the January 2022 cyberattack against Ukrainian government systems, Diia was also affected but the disruptions lasted less than a day [20]. Russia has also tried to replicate their cyberattacks on the power grid, but an attempt in April 2022 was neutralized by Ukrainian cyber defenders [18].

Thus, Russia employed a large scale of cyber operations during its full-blown war against Ukraine, its main objectives being influence, sabotage, and espionage [19]. Russia attempted to disrupt government operations and energy infrastructure with data wipers [19]. For instance, in December 2023, one of Ukraine's main mobile network operators, telecom company Kyivstar, was targeted by a serious cyberattack attributed to Russia, causing several days long major connection issues across Ukraine for millions of people, including for air raid alerts and ATMs [10]. In the meantime, Russia deployed extensive cyber espionage campaigns, objectives ranging from intelligence gathering and possible pre-positioning for future cyber operations [19].

Amidst Russian state-sponsored cyberattacks and cybercrime incidents, one of the main challenges for Diia is delivering a functioning user-friendly e-government platform whilst maintaining sound cybersecurity measures [21]. Cyber operations involving data wipers were one of the most relevant incidents that could have significantly affected e-government platforms like Diia, disrupting public services and exposing or destroying citizens' and businesses' data [19]. Diia has been targeted by Russian cyberattacks but the system withstood them, especially after the 2022 full-blown invasion [21].

Ukraine's Parliament acted quick shortly before and in the first few weeks of the invasion to bolster the country's cybersecurity. In February-March 2022, the Verkhovna Rada enacted a law that allowed government data to be stored in the cloud during the war, including in servers outside Ukraine [10]. Moving government data outside Ukraine provided an increased protection from malicious cyber operations and backups outside the country if data centres are bombed [10].

Even though it managed to withstand persistent Russian cyberattacks, Ukraine's cybersecurity framework is ranked in the top half of Tier 3 by ITU's Global Cybersecurity Index 2024, obtaining 84 points [22]. Ukraine's strengths are its legal and technical measures, but still needs to enhance its cooperation and organization measures, as well as capacity development [22]. For instance, the same index ranks Estonia as Tier 1 globally, scoring over 95 points [22]. The Baltic country scored perfect scores for cooperation, organization, and cooperation measures, but should still work on developing technical measures [22].

5. Conclusions

Ukraine's experience with developing Diia offers valuable lessons on balancing digital innovation with fortifying cybersecurity measures, especially for countries facing hybrid operations. Ukraine learned from the events in 2014-2022 and adapted to Russia's hybrid attacks, bolstering its cyber defence. Moreover, Diia became an essential part of Ukraine's resistance against the Russian war of aggression by ensuring uninterrupted access to government services from all around the country.

Key policy measures that should be considered by other governments include moving government data to cloud systems and storing backups in data centres outside the country, upholding cybersecurity at all phases of e-government development and implementation, and focusing on streghtening and expanding international partnership. In doing so, government data should be shielded from both cyberattacks and physical attacks. Moreover, the examples of Estonia and Ukraine should be studied by other countries, especially the case of Ukraine's continuity of delivering digital government services during a war.

Therefore, Diia can be used as an example of good practices. Encompassing both accessible, user-friendly and human-centric services, and robust cybersecurity measures, Diia stands as a potential model for other countries, especially those facing disruptive cyber challenges. Ukrainian officials stated that it started sharing the technology, as other countries have expressed interested in the platform's code, user interface design and/or user experience design [15, 17]. USAID has announced in 2023 that it is aiding several countries, such as Colombia, Kosovo, and Zambia, to adopt local versions of the code, and Estonia has already implemented parts of it [2]. Diia's source code has been made available for other countries in April 2024 [14].

Nevertheless, future studies in this area should also focus on the limits of e-government adoption and on potential risks and shortcomings. Taking into account that digital government systems and services are becoming essential or even unavoidable for citizens, policymakers need to focus on enhancing measures for protecting privacy [23]. Aside from the prospect that governments could abuse data collected by e-government platforms, state-sponsored or criminal cyberattacks can leak online sensitive personal data. Moreover, policymakers should also consider gender issues in developing e-government services [24], ensuring equal access to internet services, and offering facilities tailored for the specific needs and challenges disproportionately faced by women.

References

[1] M. Fouani and V. Brusilovskyy, "A digital lifeline for Ukrainians on the move," UNDP, 24 May 2022. [Online]. Available: https://www.undp.org/blog/digital-lifeline-ukrainians-move.

[2] L. O'Carroll, "Meet Diia: the Ukrainian app used to do taxes … and report Russian soldiers," The Guardian, 26 May 2023. [Online]. Available: https://www.theguardian.com/world/2023/may/26/meet-diia-the-ukrainian-app-used-to-do-taxes-and-report-russian-soldiers.

[3] United Nations, "United Nations E-Government Knowledgebase," 2024. [Online]. Available: https://publicadministration.un.org/egovkb/en-us/Overview#whatis.

[4] F. Björklund, "E-government and moral citizenship: the case of Estonia," *Citizenship Studies,* vol. 20, no. 6-7, pp. 914-931, 2016.

[5] E-Government Academy, "Factsheet e-Governance," 2024.

[6] G. Lidén, "Technology and democracy: validity in measurements of e-democracy," *Democratization,* vol. 22, no. 4, pp. 698-713, 2015.

[7] OECD, "2023 OECD Digital Government Index," OECD Public Governance Policy Papers, 2024. [Online]. Available: https://www.oecd.org/en/publications/2023-oecd-digital-government-index_1a89ed5e-en.html.

[8] V. I. Espinosa and A. Pino, "E-Government as a Development Strategy: The Case of Estonia," *nternational Journal of Public Administration,* vol. 48, no. 1, pp. 1-14, 2024.

[9] R. Zdjelar, A. Musa and N. Ž. Hrustek, "Open data availability in Croatian local government: Improving the quality of life," *Smart Cities and Regional Development Journal,* vol. 5, no. 3, pp. 21-40, 2021.

[10] G. Ingram and P. Vora, "Ukraine: Digital resilience in a time of war," Brookings, 30 January 2024. [Online]. Available: https://www.brookings.edu/articles/ukraine-digital-resilience-in-a-time-of-war/.

[11] e-Estonia, "Estoniain Ukrainian Digital Cooperation," 2024. [Online]. Available: https://e-estonia.com/estonian-ukrainian-digital-cooperation/.

[12] United Nations, "UN E-Government Knowledgebase Ukraine," 2024. [Online]. Available: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine.

[13] United Nations, "UN E-Government Knowledgebase Estonia," 2024. [Online]. Available: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/57-Estonia.

[14] EU4Digital, "Ukraine's 'Diia' state app is now available worldwide as open source code," 11 April 2024. [Online]. Available: https://eufordigital.eu/ukraines-diia-state-app-is-now-available-worldwide-as-open-source-code/.

[15] D. Krasnolutska and O. Tammik, "Ukraine Pushes Diia App Used to Counter Russia as Global Tool," Bloomberg, 16 March 2023. [Online]. Available: https://www.bloomberg.com/news/articles/2023-03-16/ukraine-pushes-diia-app-used-to-counter-russia-as-global-tool.

[16] Ukraine UA, "Digital Country," 2024. [Online]. Available: https://ukraine.ua/invest-trade/digitalization/.

[17] U.S. Agency for International Development (USAID), "A U.S.-Supported E-Government App Accelerated the Digital Transformation of Ukraine; Now Ukraine is Working to Scale the Solution to More Countries," USAID , 18 January 2023. [Online]. Available: https://www.usaid.gov/news-information/press-releases/jan-18-2023-us-supported-e-government-app-accelerated-digital-transformation-ukraine-now-ukraine-working-scale-solution-more-countries.

[18] L. Maschmeyer and M. Dunn Cavelty, "Goodbye Cyberwar: Ukraine as Reality Check," *Policy Perspectives,* vol. 10, no. 3, 2022.

[19] T. Grossman, M. Kaminska, J. Shires and M. Smeets, "The Cyber Dimensions of the Russia-Ukraine War," European Cyber Conflict Research Initiative, 2023.

[20] A. Lapatina, "Major cyberattack hits Ukrainian government websites (UPDATED)," Kyiv Independent, 14 January 2022. [Online]. Available: https://kyivindependent.com/major-cyberattack-hits-ukrainian-government-websites/.

[21] . A. Motkin, "Ukraine’s Diia platform sets the global gold standard for e-government," Atlantic Council, 30 May 2023. [Online]. Available: https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-diia-platform-sets-the-global-gold-standard-for-e-government/.

[22] International Telecommunication Union, "Global Cybersecurity Index 2024 5th Edition," ITUPublications, 2024.

[23] K. Allman and R. Radu, "Digital footprints as barriers to accessing e-government services," *Global Policy*, vol. 14, no. 1, pp. 84-95, September 2022.

[24] B. Zankova, "Smart societies, gender and the 2030 spotlight - are we prepared?," *Smart Cities and Regional Development Journal*, vol. 5, no. 3, pp. 63-76, 2021.