Policy Paper

An E-Integration Marathon

The Potential Impact of Ukrainian Membership on the EU's Digitalisation and Cybersecurity

| Merle Maigre |

January 2024

RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI • ESTONIA

Title: An E-Integration Marathon: The Potential Impact of Ukrainian Membership on the EU's Digitalisation and Cybersecurity
Author: Maigre, Merle
Publication date: January 2024
Category: Policy Paper

Cover page photo: A man near the national flag mural in Kyiv, 10 April 2022 (EPA / Oleh Petrasyuk / Scanpix)

Keywords: connectivity, critical information infrastructure, cybersecurity, Diia, digital ecosystem, e-governance, electronic identification, enlargement, information and communications technology, Ministry of Digital Transformation, open data, public services, resilience, EU, Russia, Ukraine

ISSN 2228-2068

63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee, www.icds.ee

Acknowledgements

This paper is the fourth publication of the project on "The political and economic impact of Ukraine's EU accession on the EU and Estonia" conducted by the ICDS in cooperation with the Centre for European Policy Studies (CEPS) in Brussels and the Ukrainian Institute for Economic Research and Policy. The multi-disciplinary research team assesses the potential political, security-related, institutional, economic, and budgetary implications of Ukraine's EU accession. The project is led by Dr Kristi Raik, Deputy Director of the ICDS, and supported by the Estonian Ministry of Foreign Affairs.

About the Author

Merle Maigre

Merle Maigre is the Programme Director of Cybersecurity at Estonia's e-Governance Academy. Previously, she was the Executive Vice President for Government Relations at CybExer Technologies. In 2017-18, she served as the Director of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn and as a member of the NATO CCDCOE International Advisory Board in 2018-22. In 2012-17, she worked as a Security Policy Adviser to Estonian Presidents Kersti Kaljulaid and Toomas Hendrik Ilves. In 2010-12, Merle Maigre served in the Policy Planning Unit of the Private Office of NATO Secretary General. She is currently a chosen Member of the Advisory Group of the European Union Agency for Cybersecurity (ENISA) and a non-resident fellow of the Centre for European Policy Analysis (CEPA).

List of Abbreviations

3G	third-generation
4G	fourth-generation
AFU	Armed Forces of Ukraine
BEREC	Body of European Regulators for Electronic Communications
CERT-UA	Ukrainian Computer Emergency Response Team
CII	critical information infrastructure
CRRTs	Cyber Rapid Response Teams and Mutual Assistance in Cyber Security
DCFTA	Deep and Comprehensive Free Trade Areas
DDoS	Distributed-Denial-of-Service
DSM	Digital Single Market
eIDAS	electronic Identification, Authentication, and trust Services
ENISA	European Union Agency for Cybersecurity
FIRST	Forum of Incident Response and the International Cybersecurity Security Teams
FSB	Federal Security Services (*federal'naya sluzhba bezopasnosti*)
GRU	Military Intelligence Directorate (*glavnoye razvedyvatelnoye upravlenie*)
ICT	information and communications technology
ID	identification
IDP	internally displaced person
IT	internet technology
LTE	Long-Term Evolution
NCCC	National Coordination Centre for Cybersecurity
NCEC	National Commission for State Regulation in the Fields of Electronic Communications, Radio Frequency Spectrum, and the Provision of Postal Services
NCRCI	National Commission for State Regulation in the Field of Communication and Informatisation
NIS	network and information system
PESCO	Permanent Structured Cooperation
SIM	Subscriber Identity Module
SSSCIP	State Service for Special Communications and Information Protection
SVR	Foreign Intelligence Service (*sluzhba vneshney razvedki*)
UMTS	Universal Mobile Telecommunications Service

Introduction

Digitalisation is neither a one-size-fits-all solution nor a turnkey project like building a bridge or a tunnel. It requires the active participation of all stakeholders – political leaders, lawmakers, and public servants – to ensure the effort is appropriate for the country's legal system and administrative culture. For an effective digital transformation, leaders must realise how revolutionary digitalisation can be, completely rethinking governance.[1]

This paper envisages the future of Ukraine in Europe, focusing on the areas of digitalisation and cybersecurity. The war has pushed Ukraine to seek membership in the European Union and thus access to the EU Digital Single Market (DSM), which presupposes an alignment with international regulations and standards. On 17 June 2022, the European Commission recommended that the EU Council accept Ukraine's candidacy. The official Commission opinion noted the "particularly good results" achieved by Ukraine in the area of information society and media (within the "Competitiveness and inclusive growth" cluster).[2] It referred to the "in-depth sectoral reform and approximation to EU DSM *acquis,*" the adoption of laws on electronic communications and telecommunications regulator, and their enforcement since the beginning of 2022.[3] This paper explores the potential impact of Ukraine's accession on digitalisation and cybersecurity of the European Union and looks at how Ukraine can contribute to the EU's performance in this field. Faced with Russia's aggression, the Ukrainian government has shown a remarkable level of institutional strength, determination, and ability to function. Joining the world's most successful club of peaceful and prosperous democracies will set Ukraine on a new and promising path.

Ukraine's future EU membership will certainly have far-reaching implications for the future of the European political, economic, and security order.[4] The integration of candidate countries in the digital and cybersecurity sphere will be increasingly important for the future of the EU. In this area, the EU is committed to the DSM and the internet which is open, stable, free, inclusive, global, interoperable, reliable, and secure.[5] People and their rights are at the centre of this digital transformation. As a comprehensive framework established to guide all digital sections, Europe's Digital Decade policy programme revolves around four cardinal points: digitalisation of public services, secure and sustainable digital infrastructure, skills, and digital transformation of businesses. The EU's new digital partnerships – including with Ukraine – have been aimed at boosting connectivity and digital and cyber cooperation.

1 Toomas Hendrik Ilves, *Twenty Years of Building Digital Societies: Thinking about the Past and Future of Digital Transformation,* ed. Peeter Vihma (Tallinn: e-Governance Academy, 2023).

2 European Neighbourhood Policy and Enlargement Negotiations (DG NEAR), "Opinion on Ukraine's application for membership of the European Union," European Commission, 16 June 2022

3 "Digitalisation for recovery in Ukraine," OECD Policy Response on the Impacts of the War in Ukraine, 1 July 2022

4 See Kristi Raik and Steven Blockman, "Accelerator for a Geopolitical Europe: Potential Impact of Ukraine's Membership on EU Foreign, Security, and Defence Policy," *International Centre For Defence and Security (ICDS),* 27 November 2023; Steven Blockmans, "The Impact on Ukrainian Membership on EU's Institutions and Internal Balance of Power," *ICDS*, 9 November 2023; Michael Emerson, "The Potential Impact of Ukrainian Accession on EU's Budget," *ICDS*, 25 September 2023.

5 The EU digital transformation is guided by the eGovernance regulation, including on digital identity, and Digital Identity EWallets (2020), European Data Governance Act (2022), Europe's Digital Decade and Path to the Digital Decade (2022), and the Gigabit Infrastructure Act (2023). EU cybersecurity main legal documents include Network and Information Security Directives (the so-called NIS 1 (2016) and NIS 2 (2022)), Cyber Solidarity Act (2023), Cybersecurity Act (2019), Critical Entities Resilience Directive (2022), and the General Data Protection Regulation (2016).

Building on these components of EU policy, this paper:

- looks at the connectivity and the development of digital public services in Ukraine over the last decade with a focus on its breakthrough in digitalisation following the 2019 presidential elections, as well as their wartime adaptation;
- assesses the extent to which President Volodymyr Zelensky's presidency and Russia's war of aggression have served as the turning points for digitalisation and provides insights into the share of the digital sector in Ukraine's economy and its economic growth;
- analyses cybersecurity in Ukraine by studying the factors that have contributed to its effective cyber defence against Russia;
- measures the prospects of further development of digitalisation and cybersecurity in Ukraine.

It thereby seeks to find answers to the following questions:

- What further progress could Ukraine achieve in these fields by 2030?
- What are the lessons learned from Russia's full-scale war of aggression in Ukraine and how relevant is Ukraine's model for cyber conflict scenarios of the future?
- What will be the impact and contribution of Ukraine to the EU's performance in digitalisation and cybersecurity?

1. Connectivity

1.1. Peacetime Functions

The deployment of broadband infrastructure and the availability of broadband access to internet networks are key to successful digital transformation. Despite commitments in the Association Agreement (and the Deep and Comprehensive Free Trade Areas, DCFTA), the political leadership of Ukraine did not pay sufficient attention to the development of electronic communications until 2020, while the state administration stayed involved. For the initial development of telecommunication services, the National Commission for Communications Regulation was established in 2004 and focused mainly on public radio frequencies. In 2011, the agency was reorganised into the National Commission for State Regulation in the Field of Communication and Informatization (NCRCI). In 2015, the NCRCI issued licenses for the UMTS(3G) standard to the three largest mobile operators; in 2018, the NCRCI started selling licenses for the 4G(LTE) standard.

The government under Zelensky's presidency sought to improve connectivity, particularly in rural areas. In 2020, the parliament adopted the Law on Electronic Communications and the Law on Regulator.[6] These two core laws represent an important step forward in Ukraine's harmonising of its legislation with the EU norms. However, financial constraints make it difficult for the central executive body – the State Service for Special Communications and Information Protection of Ukraine – to perform its functions as defined by law.[7]

The political leadership of Ukraine did not pay sufficient attention to the development of electronic communications until 2020, while the state administration stayed involved

In July 2020, the Ministry of Digital Transformation announced a four-year programme to increase high-speed internet availability in all schools and along main

[6] Verkhovna Rada of Ukraine, *Закон України про електронні комунікації* [Law of Ukraine on Electronic Communications] (Kyiv: Verkhovna Rada of Ukraine, July 2023).

[7] European Commission, *Commission Staff Working Document Ukraine 2023 Report Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 2023 Communication on EU Enlargement policy* (Brussels: European Commission, November 2023).

highways.[8] In 2022, the national regulatory authority responsible for electronic communications was further re-organised from the NCRCI into the National Commission for State Regulation in the Fields of Electronic Communications, Radio Frequency Spectrum, and the Provision of Postal Services (NCEC). According to the NCEC's 2022 report, the number of active SIM cards in the mobile network in Ukraine at the end of 2022 was 49.3 million.[9]

1.2. Wartime Adaptations

Since the beginning of a full-scale invasion, connectivity and communication have become the most critical aspects. Currently, access to high-speed internet in Ukraine is provided by using fibre-optic communication lines, television cable, phone lines, mobile communication (3G, 4G, 4.5G, and LTE), and satellite communication. By October 2022, Russia had destroyed or taken over 4 000 telecommunication stations and over 60 000 kilometres of fibre-optic internet lines.[10] However, the real challenge for connectivity and communication was the blackouts that started in October 2022 and were caused by the shelling of energy infrastructure facilities. During the winter of 2022-23, Russia carried out massive missile attacks on the energy infrastructure of Ukraine with about 270 recorded hits. As a result of that shelling, 24 power generation facilities, such as thermal and hydropower plants and storage plants, were damaged and Ukraine's overall energy system lost almost half of its capacities.[11] Ukrainians started buying backup power supplies (generators, power stations, power banks, etc.) and changing communication channels (switching to fibre-optic communication channels or acquiring Starlinks). The telecommunication operators began to accumulate electricity reserves for their networks to be ready to provide communication during longer periods of network power failures. This process continues to this day.

For Ukrainians to stay connected when one of the telecommunication operators lacks coverage, a solution was developed by the largest mobile providers (Kyivstar, Vodafone Ukraine, and Lifecell). Together with the Ministry of Digital Transformation of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the NCEC, and the Association of Communications Operators, they implemented a simple algorithm for selecting an available network to allow for a free network switch to another telecommunication company. On 7 March 2022, Ukrainian mobile operators launched a national free roaming service providing voice services and minimum internet speed. At times of power outages, about 2.2 million Ukrainians used the national roaming service every day.[12]

The SpaceX Starlink system satellite terminals – both supplied to Ukraine by the US Department of Defence and purchased by individual households – have become invaluable during the war, with Ukraine becoming the world's top country by the number of Starlinks. Residents and businesses were able to access the internet during blackouts. Additionally, mobile operators used Starlink technology instead of damaged transport networks and ensured the availability of communication for subscribers.

[8] "Міністерство цифрової трансформації України [Ministry of Digital Transformation of Ukraine]," Ministry of Digital Transformation of Ukraine, accessed in December 2023; Cabinet of Ministers of Ukraine, *Розпорядження від 8 вересня 2021 р. № 1069-р Київ Про затвердження плану заходів з розвитку широкосмугового доступу до Інтернету на 2021-2022 роки* [Order dated September 8, 2021 No. 1069 Kyiv On the approval of the plan of measures for the development of broadband access to the Internet for 2021-2022] (Kyiv: Verkhovna Rada of Ukraine, September 2021).

[9] National State Regulatory Commission In The Fields Of Electronic Communications, Radio Frequency Spectrum And Provision Of Postal Communication Services, *Звіт про діяльність Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку за 2022 рік* [Report On The Activities Of The National Commission Executing State Regulation In The Spheres Of Electronic Communications, Radio Frequency Spectrum And Provision Of Postal Communication Services] (Kyiv: National State Regulatory Commission In The Fields Of Electronic Communications, Radio Frequency Spectrum And Provision Of Postal Communication Services, 2023).

[10] Romina Bandura and Janina Staguhn, "Digital Will Drive Ukraine's Moderinzation," *Center for Strategic and International Studies (CSIS),* January 2023.

[11] Halyna Yalivets', "Ніхто не готовий на 100%: Як мобільні оператори будуть працювати під час блекаутів [No one is 100% ready: How mobile operators will work during blackouts]," *Biznes.Censor*, 29 September 2023.

[12] National State Regulatory Commission, *Report On The Activities Of The National Commission*.

In February 2022, Ukraine became one step closer to the free-roaming zone when the European Commission adopted a proposal to include it in the Association Agreement between Ukraine and the EU.[13] With the support of the European Commission, the European Parliament, the NCEC, and the Body of European Regulators for Electronic Communications (BEREC), national operators concluded a Joint Agreement to support Ukrainian refugees in Europe wishing to stay in touch with their relatives back home.[14] Namely, EU and Ukrainian telecommunications operators offer affordable or charge-free calls between the EU and Ukraine on a voluntary basis. Twenty European mobile and fixed communication operators entered into the agreement with seven Ukrainian partners (Kyivstar, Vodafone, lifecell, Ukrtelecom, Data Group, Vega Telecom, and 3Mob). Consequently, the wartime adaptation solutions have also strengthened the processes of European integration of Ukraine.

The wartime adaptation solutions have also strengthened the processes of European integration of Ukraine

2. Digital Public Services

2.1. Peacetime Functions

Since the independence of Ukraine, state authorities have started to compile and maintain public registers, which indirectly form the basis for providing electronic public services. While the appeal for a secure data exchange between information systems extended back to 2010, the decision-makers in Ukraine were not seriously committed to digitalisation until 2014. Only after the Revolution of Dignity in 2014, e-governance and the development of e-services began to draw more attention, whereas the digitalisation hubs moved from several municipalities to the central government. As the core group of digital enthusiasts relocated to Kyiv, the country was given a head start.

Only after the Revolution of Dignity 2014, the digitalisation hubs moved from several municipalities to the central government

Acknowledging that transparency and open data are important for they promote economic growth, the parliament of Ukraine in 2011 adopted the Law on Access to Public Information. In 2015, the Cabinet of Ministers approved Resolution No. 835 on Approval of Regulations on Data Sets Subject to Publication in the Form of Open Data. In 2016, the Unified State Open Data Web Portal was officially launched. Since then, government bodies have been keen to publish data as required by the legislation. The opening of data in various areas contributed to the creation of services that helped entrepreneurs avoid corruption-related risks. In particular, data from the Unified State Register of Legal Entities, Individual Entrepreneurs and Public Organisations, as well as registers of court decisions, notaries, taxpayers, and tax debtors, was made publicly available. Along the same lines, ProZorro – an electronic system for asset declarations and a public procurement system – was launched in 2016. President Petro Poroshenko used to underline how it increased transparency and reduced corruption. Open data allowed private organisations and volunteers to develop other useful services. In particular, YouControl, Opendatabot, Liga Contr Agent, Ring, and Vkursi.Pro services allow checking potential contractors, thus enabling businesses to avoid financial losses, fraud, and defaults.[15]

In June 2014, the State Agency for E-Governance of Ukraine was established. During the six years of its existence, the foundations for the modern digital

[13] Verkhovna Rada of Ukraine, *Угода Про Асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони* [Association Agreement between Ukraine, on the one hand, and the European Union, the European Atomic Energy Community and their member states, on the other hand] (Kyiv: Verkhovna Rada of Ukraine, November 2023).

[14] "Joint Statement by EU and Ukrainian operators to help refugees from Ukraine stay connected," European Commission, 5 April 2022.

[15] "Безцінні та безоплатні. Як відкриті дані допомагають українському бізнесу [Priceless and free. How open data helps Ukrainian business]," *Ekonomichna Pravda*, 11 February 2022.

transformation of Ukraine were laid. The launch of the information and communication systems empowered the state authorities and local governments to develop, in particular, a public services portal; an electronic interaction system for executive authorities; Trembita, a state electronic information system; and an integrated electronic identification system.

The State Agency for E-Governance of Ukraine laid the foundations for the modern digital transformation

- In 2014-19, the **public services portal** acted as an aggregator of links to various public services web pages such as the online House of Justice, the taxpayer portal, and the portal of construction-related administrative services. In addition, Vulyk (meaning a 'beehive' in Ukrainian), a modern information system for roughly 600 administrative service centres across Ukraine, was created.[16] The development of electronic public services during this period was active yet mostly chaotic. Meanwhile, the decentralisation reform was seen as an ideal tool by policymakers to strengthen regions and empower local municipalities, called *hromadas*. In a similar decentralised manner, each agency set up its own registers and developed the functionality for its own systems. Insufficient attention was paid to data interoperability, resulting in a chaotic architecture of data registers and poor quality of data.

- In order to create a single information space for registration, analysis, and storage of documents of executive authorities in electronic form using a qualified electronic signature, the **electronic interaction system for executive authorities** was launched in 2015-16 by the State Agency for E-Governance of Ukraine and the State Enterprise State Centre of Electronic Information Resources.[17] This system was a prerequisite for the transition to fully electronic interdepartmental document circulation, which helped reduce state budget costs.

- As part of the international technical assistance financed by the EU and its member states (Denmark, Estonia, Germany, Poland, Sweden, and Slovenia), the **Trembita** system was created and launched.[18] Trembita, as a system, is a nod to Ukraine's pastoral roots: a traditional *trembita* is a long wooden horn used by Ukrainian highlanders to gather people to announce births, funerals, weddings, etc. Similarly, the new electronic Trembita was meant to serve as an interoperability system that provides secure data exchange between information systems, mostly between government agencies. For citizens and businesses, Trembita enables unified access to data in state registers. Its basic functionality was developed in 2018; it was deployed on servers and passed security certification in 2019; and starting from January 2020, it was put into industrial operation. The set-up of Trembita was implemented by the e-Governance Academy of Estonia, a foundation-based international development cooperation implementer.

- Significant progress was achieved in trust services and electronic identification. In 2019, Ukraine adopted changes to the law that harmonised legislation with the EU requirements of the eIDAS regulation and submitted a request for mutual recognition of electronic trust services.[19] Additionally, Ukraine has been deployed to the Third Countries Trust List for electronic signatures that meet EU requirements and are technically validated on the

[16] "Інформаційна система «Вулик» [Information System Vulyk]," Vulyk.Gov.ua, accessed in December 2023.

[17] "Система електронної взаємодії органів виконавчої влади (СЕВ ОВВ) [System of electronic interaction of executive authorities (SEV OVV)]," Diia.Gov.ua, accessed in December 2023.

[18] "Трембіта. Система електронної взаємодії державних електронних інформаційних ресурсів [System of electronic interaction of state electronic information resources], Trembita.Gov.ua, accessed in December 2023.

[19] eIDAS (electronic Identification, Authentication, and trust Services) refers to a range of services that include verifying the identity of individuals and businesses online and verifying the authenticity of electronic documents. The eIDAS Regulation established the framework to ensure that electronic interactions between businesses are safer, faster, and more efficient, no matter the European country they take place in. It is a European Regulation that created one single framework for electronic identification (eID) and trust services, making it more straightforward to deliver services across the European Union. See: "Discover eIDEAS," European Commission, accessed in December 2023.

European Commission portal.[20] In the first half of 2019, an **integrated electronic identification system** was launched in an experimental operation mode.[21] This system integrated various methods of electronic identification of individuals and legal entities. It was built upon Ukraine's own Public Key Infrastructure based on local cryptographic algorithms. Ukraine also tested eIDAS NODE with the European Commission and several Member States (e.g., Austria and Estonia), enabling it to authenticate Ukrainians in the EU and Europeans in Ukraine based on the EU rules and processes. The next steps foresee moving towards the full recognition of Ukraine's qualified electronic signature by the EU and the use of eIDAS NODE in real-life situations to receive services online.

After the 2019 parliamentary and presidential elections, a Ukrainian digitalisation breakthrough occurred. President Volodymyr Zelensky deemed digital transformation to be a priority by establishing the Ministry of Digital Transformation and appointed his campaign manager Mykhailo Fedorov as the minister. The Minister of Digital Transformation also serves in the position of a Vice Prime Minister, which empowers the officeholder to comprehensively coordinate all the digitalisation processes in Ukraine.[22] Some re-organisation within the government structure was needed, including a new position of the Chief Digital Transformation Officer at the national (a Deputy Minister) and regional (a Deputy Governor) levels.

After the 2019 parliamentary and presidential elections, a Ukrainian digitalisation breakthrough occurred

Before assuming the ministerial position, Mykhailo Fedorov travelled to Estonia for inspiration.[23] The visit encouraged him to pursue digital transformation in Ukraine. He was particularly impressed with the e-residency programme, as well as the fact that Estonia was among the first countries to launch electronic interaction of registers and ID cards, achieved an online service rate of 90%, and held elections electronically. Once in office, Minister Fedorov was keen to implement the basic functionalities of a successful e-government: legal framework, data exchange environment, security principles, and electronic identity.

In addition, the newly established Ministry of Digital Transformation aimed to:

- transfer 100% of all public services for citizens and businesses online;
- provide 95% of transport infrastructure, settlements, and their social facilities with access to high-speed internet;
- teach digital skills to 6 million Ukrainians;
- increase the share of IT in the country's GDP to 10%.

Establishing a uniform persons registry for the whole of Ukraine proved to be a challenge, as different oblasts used to register people on a different basis: for example, either by birth or when eligible for taxation. However, given that leadership was there, the coordination hurdles were eventually overcome.

In 2019, the Ukrainian government launched its vision for electronic public service design and delivery. Minister Fedorov was set to build the "most convenient digital state in the world without bureaucracy" or "a state in a smartphone."[24] Several fundamental laws were adopted to accelerate digital transformation in Ukraine: e.g., the Law on Electronic Trusted Services, the Law on Electronic Communications, the Law on Cloud Service, and the Law on Administrative Procedure. Perhaps the most notable amongst the digital reforms is the standardisation and unification of e-Services within a single efficient, user-facing digital ecosystem Diia (a Ukrainian word

[20] European Commission, "Third Countries Trusted List Browser," European Commission, eIDEAS Dashboard, accessed in December 2023.

[21] "Інтегрована система електронної ідентифікації ID.GOV.UA [Integrated system of electronic identification ID.GOV.UA]," ID.GOV.UA, accessed in December 2023.

[22] Valeriya Ionan, "Digital Transformation in Ukraine: Before, During and After the War," *Harvard Advanced Leadership Initiative*, 29 November 2022.

[23] Vihma (ed.), *Twenty Years of Building Digital* Societies, 112-3.

[24] Ionan, "Digital Transformation in Ukraine."

for "action" and an acronym for "the State and Me"). The Diia web portal and mobile application form the basis for the provision of electronic public services in Ukraine. The Diia ecosystem primarily includes the following elements.

The most notable amongst the digital reforms is the standardisation and unification of e-Services within a single efficient, user-facing digital ecosystem Diia

- **Diia** portal is an online portal of public services for citizens and businesses. All electronic public services entering the Diia ecosystem are subject to re-engineering, which aims to make it simple and convenient for the end-users.[25]

- **Diia.Engine** platform was launched due to the joint efforts of Ukraine's Ministry of Digital Transformation and the State Service for Special Communications and Information Protection. This solution allows ministries and state bodies to create and manage registries enabling them to store data in a systematic and safe manner, as well as to automate and digitise government services. This aims to speed up the launch of online services and digitalisation in general. [26]

- **Diia mobile** application provides personal electronic documents and data from the registers. It offers several useful services: an option to submit a tax return declaration, to order a replacement for one's driver's license, to extend one's car technical passport, and to submit a request for a certificate, as well as a possibility to find out information about fines and enforcement proceedings. The application is the main form of identification for millions of Ukrainian citizens.[27]

- **Diia.Osvita** portal offers digital literacy courses.[28]

- **Diia.Business** portal assists small and medium-sized businesses.[29]

- **Diia.Center** is a platform for administrative service centres that operate under a unified procedure and meet unified quality standards.[30]

- **Diia.City** is a special legal regime for the IT industry.[31]

To simplify the navigation through multiple options, the Ministry of Digital Transformation has launched a public services guide that explains the content of these public services and how to obtain them.[32]

People in Ukraine have welcomed and quickly adapted to the use of digital documents: e.g., ID cards, biometric international passports, driver's licenses, vehicle registration certificates, student ID cards, child's birth certificates, etc. All the digital documents available in Diia have the same legal status as their paper version, which was made possible due to the adoption of the so-called "Paperless Law" introducing the concept of an electronic document in July 2021.[33] Doing business has become more convenient with the launch of document sharing in Diia which synchronised the copies of digital documents with a company's system.[34] Documents can be shared both offline (when visiting an organisation) and online (via a website or application). This service is particularly popular in the hospitality and insurance industries (e.g., purchasing a "Green Card" insurance policy via

25 "Державні послуги онлайн [Public Services Online]," Diia.Gov.ua, accessed in December 2023.

26 "В Україні запустили платформу Дія. Engine для нових державних онлайн-послуг [In Ukraine, the Diya. Engine platform was launched for new state online services]," Ukrinform, 21 September 2023.

27 "Дія 4+ Ministry of Digital Transformation of Ukraine Preview," Apple Store, accessed in December 2023; "Дія Ministry of Digital Transformation of Ukraine," Google Play, accessed in December 2023.

28 "Дія.Освіта [Diia.Education]," Osvita.Diia.Gov.ua, accessed in December 2023.

29 "Дія.Бізнес [Diia.Business]," Business.Diia.Gov.ua, accessed in December 2023.

30 "Дія Центр [Diia Centre]," Center.Diia.Gov.ua, accessed in December 2023.

31 "Дія.City [Diia.City]," City.Diia.Gov.ua, accessed in December 2023.

32 "Гід з державних послуг [Public Services Guide]," Guide.Diia.Gov.ua, accessed in December 2023.

33 Verkhovna Rada of Ukraine, *Закон України Про особливості надання публічних (електронних публічних) послуг* [Law of Ukraine "On the Peculiarities of Providing Public (Electronic Public) Services] (Kyiv: Verkhovna Rada of Ukraine, March 2023).

34 "Diia.Paperless," Paperless.Diia.Gov.ua, accessed in December 2023.

finance.ua).[35] Ukrainian companies have been transitioning to the **Diia.Signature** as a means for authorisation. [36]

2.2. Wartime Adaptations

The Ukrainian state has been able to function during the war due to having moved government services to the cloud and having actively developed Diia, the Trembita system, and electronic identification. To ensure the transfer of digital state information resources to the cloud after the war had broken out, the Cabinet of Ministers on 12 March 2022 adopted a special Resolution No 263.[37] It empowered the authorities to locate public information resources and public e-registers, as well as their encrypted copies, on the cloud resources or data centres outside of Ukraine's physical borders.

During the 18 months of the large-scale war, the Ministry of Digital Transformation introduced about 70 new services

During the 18 months of the large-scale war, the Ministry of Digital Transformation introduced about 70 new services.[38]

- **eDocument** is a temporary digital document that is valid for the duration of martial law and used to identify people, for example, at military checkpoints when other documents have been lost.

- **Military bonds** are issued by the state to support the country's economy and are available for purchase via Diia.

- **eVorog** (eEnemy) is a chatbot that allows a user to report the movement of Russian troops and equipment (e.g., share their geolocation and attach photo and video evidence) to the Armed Forces of Ukraine (AFU).

- **Diia TV** and **Diia Radio** provide access to news in areas where traditional broadcasting is unavailable because of jammed signals.

- **Army aid** facilitates donations to the AFU.

- **eOselia** (eHousing) helps military personnel, healthcare workers, and educators apply for a mortgage on preferential terms.

- **Services for internally displaced persons** (IDPs) include registration to receive various forms of assistance, change one's place of residence, and cancel the registration for the IDP status once the person has returned to the place of permanent residence.

- **Damaged property service** facilities the reporting of real estate that has been destroyed or damaged as a result of the Russian military aggression and the subsequent application for compensation.

- **eRobota** (eJob) allows small- and micro-business owners to apply for micro-grants (i.e., up to UAH 250 000).

Hence, Diia helps patriotic citizens to donate to the war effort and report the enemy's positions to the state and struggling businesses to receive support from the state. With the war having made visiting government offices in person more difficult, the ability to conduct official business online has been a welcomed development. Similarly, people living in the regions affected by the hostilities can verify their eligibility for financial support and apply directly via the Diia application.

The service delivery system has also evolved during wartime, starting from almost no services available during the first days of the full-scale invasion to resuming all significant services in the following three months as the system adapted to the new risks. Currently,

[35] Vladyslav Nadashkivskyi, "Як працює шеринг документів у Дії [How Diia document sharing works]," *Finance.ua*, 3 October 2022.

[36] "ID.Gov.ua," ID.Gov.ua, accessed in December 2023.

[37] Cabinet of Ministers of Ukraine, *Постанова від 12 березня 2022 р. № 263 Київ Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану* [Resolution of March 12, 2022 No. 263 Kyiv Some issues of ensuring the functioning of information and communication systems, electronic communication systems, public electronic registers under martial law] (Kyiv: Cabinet of Ministers, March 2022).

[38] Lia Ilchenko, "У "Дії" запущено 70 нових сервісів від початку повномасштабної війни [70 new services have been launched in "Diia" since the beginning of the full-scale war]," Ekonomichna Pravda, 19 December 2023.

the Diia portal enables access to a total of 120 most popular electronic public services, and 25 are available in the mobile application. Unfortunately, wartime operational security measures have restricted access to many open data sets. Since the full-scale invasion, the number of Diia mobile application users has increased by more than 4 million. 17.3 million users have installed it on over 32 million devices, whereas Ukraine's estimated population is now approximately 37 million.

Diia helps patriotic citizens to donate to the war effort and report the enemy's positions to the state and struggling businesses to receive support from the state

Ukraine's latest wartime solutions follow the basic principles of the European interoperability framework and, thereby, the direction of the digital services development in the EU – sometimes even surpassing that of EU countries.[39] Diia, the Trembita system, and the cloud-based electronic identification have guaranteed that taxes are being collected, social benefits are being paid, and the customs and border services are functioning. In hindsight, Ukrainian officials have been vocal in acknowledging the impact that the cloud migration had on the continuity of core government services and the functioning of the economy. For instance, they claim that "not a single registry has stopped operating" as a result of Russia's cyber offensive.[40]

Ukraine's latest wartime solutions follow the basic principles of the European interoperability framework and the direction of the digital services development in the EU

3. Cybersecurity in Ukraine

3.1. Peacetime Functions

Ukraine's long-term commitment to improving its cyber defences and investment in talent and resources, combined with its capacity for institutional adaption, has made a real difference in its cyber defence capability.[41] The Law on the Protection of Information in Information and Telecommunication Systems laid down the initial principles of information security in 1994 and remained the foundational piece of legislation for many years. In 2016, the National Cybersecurity Strategy was adopted, setting out strategic objectives and formulating actions needed to build resilience and reduce cybercrime. The strategy was supplemented by annual action plans issued by the Cabinet of Ministers.

With the adoption of the Law on the Basic Principles of Cybersecurity, which came into force in 2018, Ukraine established a comprehensive governance system for information and communication technology (ICT) security. The law defined key principles and objects of cybersecurity and cyber defence; assigned cybersecurity roles, responsibilities, and tasks; developed principles for the protection of Critical Information Infrastructure (CII) and guidelines for international cooperation. In 2019, the Cabinet of Ministers of Ukraine approved a resolution on the general cybersecurity requirements for critical infrastructure.[42]

The key public agencies mandated to deal with cybersecurity in Ukraine are the National Security and Defence Council with its National Coordination Centre for Cybersecurity, the Parliament of Ukraine with its Standing Committee for Informatisation

[39] European Commission, *New European Interoperability Framework* (Luxembourg: Publications Office of the European Union, 2017).

[40] Tim Anderson, "Russian missiles can't destroy the cloud: Ukraine leader describes emergency migration," *The Register*, 30 November 2022 quoted in Dan Black, *Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences,* (International Institute for Strategic Studies, March 2023), 13.

[41] Black, *Russia's War in Ukraine*.

[42] Cabinet of Ministers of Ukraine, *Постанова від 19 червня 2019 р. № 518 Київ Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури* [Resolution of June 19, 2019 No. 518 Kyiv On the approval of General requirements for cyber protection of critical infrastructure objects] (Kyiv: Verkhovna Rada of Ukraine, September 2022).

and Communications, the State Service for Special Communications and Information Protection, the Security Service of Ukraine, the Department of Cyber Police within the National Police, the Ministry of Defence and the General Staff of the Armed Forces, intelligence agencies (that assume greater roles during military aggression in cyberspace), and the National Bank (responsible for cyber defence system in the banking sector).

- The **National Coordination Centre for Cybersecurity** (NCCC) of the National Security and Defence Council coordinates and supervises the activities of the entities responsible for cybersecurity. Set up in 2016, the NCCC's board comprises the heads of multiple organisations: the First Deputy or Deputy Minister of Defence, the Chief of the General Staff of the Armed Forces, the Head of the Security Services, the Head of the Foreign Intelligence Service, the Head of the National Police, the Head of the National Bank, the Head of the Main Directorate of Intelligence of the Ministry of Defence, the Head of the Office of Intelligence of the Administration of the State Border Guard Service, and the Head of the State Service for Special Communications and Information Protection. The NCCC is guided by an action plan that is prepared every few months and assigns practical tasks to all institutions represented in the body. In February 2023, the NCCC approved general rules for exchanging information about cyber incidents, following a Traffic Light Protocol recommended by the European Union Agency for Cybersecurity (ENISA), and the Forum of Incident Response and the International Cybersecurity Security Teams (FIRST).[43]

- The **Standing Committee for Information and Communications** initiates legislation and reviews draft laws on cybersecurity that are submitted to the Parliament.

- The **State Service for Special Communications and Information Protection** (SSSCIP) is the technical security and intelligence service under the control of the President of Ukraine. It takes care of the technical protection of state information resources and information in cyberspace. The SSSCIP maintains and operates the national telecommunication network, which provides secure communications to public authorities and functions as an emergency communications network. The SSSCIP also has a coordinating role at the operational level, it sets requirements and oversees information security audits of critical infrastructure. The SSSCIP licenses companies that have the right to provide cryptographic protection and technical information protection services. It issues compliance certificates to the information protection systems: e.g., compliance with administrative and engineering measures, techniques, and methods of information protection.

- In May 2021, the SSSCIP opened the **State Cyber Protection Centre** (also known as UA30). It is a headquarters for the national cyber incident response teams and security operations centre and a focal point for national cyber defence efforts.

Since the martial law was enforced in 2022, the SSSCIP has assumed additional responsibilities. For example, it was charged with designing the cyber defence policy and ensuring the implementation of the CII protection in Ukraine.[44] Since April 2023, the SSSCIP has maintained the national register of CII assets, along with a single database of threats and vulnerabilities shared by the SSSCIP and the

The unified command structure enables the SSSCIP to operate an extensive ecosystem of cyber defences throughout Ukraine

[43] "Загальні правила обміну інформацією про кіберінциденти [General rules for exchanging information about cyber incidents]," Computer Emergency Response Team of Ukraine, 31 March 2023.

[44] Державна служба спеціального зв'язку та захисту інформації України [State Service for Special Communications and Information Protection of Ukraine], "Кабінет Міністрів прийняв постанову про розроблення та погодження паспортів безпеки на об'єкти критичної інфраструктури [The Cabinet of Ministers adopted a resolution on the development and approval of safety passports for critical infrastructure facilities]," Government Portal, 5 August 2023.

sectoral responsible points of contact, allowing for the compilation of updates for the CII cyber defence requirements.[45] This unified command structure has thereby enabled the SSSCIP to design and operate an extensive ecosystem of cyber defences throughout Ukraine.

3.2. Wartime Adaptations

Russia's cyber war in Ukraine demonstrates that cyber attacks are an extension of the conflict. During the first months of the large-scale invasion, analysts were quick to conclude that cyber dimensions were absent from the battlefield.[46] Some even interpreted it as a sign of the ineffectiveness of cyber operations in kinetic conflicts.[47] That narrative, prominent in the first stages of the full-scale invasion, that "there is no cyber war in Ukraine" risks leading to excessive optimism and complacency. Since then, more granular reporting from threat intelligence researchers and practitioners has shed light on multiple cyber dimensions in the ongoing war.[48] Between July and December 2022, the average number of cyber incidents where the Ukrainian Computer Emergency Response Team (CERT-UA) had to get involved was 57 per month (i.e., 2 incidents per day). In the first half of 2023, this number increased to 128 per month and 4-5 per day.[49] While still relatively little information is available from the field due to operational security, Ukraine appears to have adapted well and proven successful in achieving cyber resilience. Offensive and defensive actions in wartime can largely be divided into the following phases: [50]

1. The preparation phase (prior to January 2022) involved the long-running operations by various Russian intelligence services that focused on cyber espionage and pre-positioning to gain access to Ukrainian critical infrastructure. Since the annexation of Crimea and the outbreak of the conflict in Donbas in 2014, Russia has been launching cyber attacks against Ukraine, which involves the use of proxies, networks, and organised crime.[51] The most notable attacks targeted the election IT infrastructure in 2014 and electricity networks in Western Ukraine in 2015 and Kyiv in 2016. The former aimed to portray the vote as illegitimate and rigged and frame Ukraine as a failed state. The impact of attacks such as Not-Petya in 2017 caused substantial economic damage globally, thereby demonstrating that cyber attacks do not recognise national borders.[52]

The impact of attacks such as Not-Petya in 2017 caused substantial economic damage globally, thereby demonstrating that cyber attacks do not recognise borders

Prior to January 2022, the Russian Federal Security Services (FSB) and the Russian military intelligence (GRU) used simple but reliable tactics – such as credential harvesting, brute-force techniques, and exploitation of known vulnerabilities – to gain access. Reportedly, several months before the invasion, the GRU had

[45] Cabinet of Ministers of Ukraine, *Постанова від 28 квітня 2023 р. № 415 Київ Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього* [Resolution dated April 28, 2023 No. 415 Kyiv On approval of the Procedure for maintaining the Register of critical infrastructure objects, inclusion of such objects in the Register, access and provision of information from it] (Kyiv: Verkhovna Rada of Ukraine, April 2023).

[46] See: Nadiya Kostryuk and Erik Gartzke, "Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invation of Ukraine." *The Strategist* Vol 5, Issue 6 (Texas National Security Review,2022): 113-26; Lennart Maschmeyer and Nadiya Kostryuk, "There is no Cyber 'Schock and Awe': Plausible Threats in the Ukrainian Conflict," *War on the Rocks*, 8 February, 2022.

[47] Taylor Grossman, Monica Kaminska, James Shires, and Max Smeets, *The Cyber Dimension of the Russia-Ukraine War* (European Cyber Conflict Research Initiative April 2023).

[48] Such analysis was conducted by Microsoft, Mandiant/ Google, etc.

[49] State Service for Special Communications and Information Protection, *Russia's Cyber Tactics H1 2023 Lessons Learned: Shift in the Patterns, Goals, and Capacity of the Russian Government and Government-Controlled Groups* (State Service for Special Communications and Information Protection, September 2023).

[50] Dan Black and Gabby Roncone, "The GRU Disruptive Playbook," *Mandiant*, 12 July 2023; Black, *Russia's War in Ukraine*; Taylor Grossman et al., *The Cyber Dimension of the Russia-Ukraine War*.

[51] Shane Huntley, "Fog of War How the Ukraine Conflict Transformed the Cyber Threat Landscape," *Google Threat Analysis Group*, 16 February 2023.

[52] For more information about this period, see: Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York, 2019); David Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (London 2018); Laurens Cerulus, "How Ukraine became a test bed for cyberweaponry," *Politico,* 14 February 2019.

re-activated intrusions dormant since 2019.[53] During the same period, Ukraine was consistently implementing basic protection measures. Those efforts most probably included hardening remote entry points into the CII networks; supplementing passwords with multi-factor authentication; threat hunting to detect instances of long-term access gained through legitimate compromise credentials; and rapid application of security patches.[54]

2. During the opening phase of the full-scale invasion (February to April 2022), Russia aggressively used pre-positioned access points to facilitate attacks. It leveraged hard-to-detect, compromised public internet-facing infrastructure – such as routers, virtual private networks, firewalls, and mail servers – to gain initial access into targets, which then became a foothold for lateral movement.[55] At least a dozen unique malware modifications were used in this opening campaign.[56] In early March 2022, Ukrainian authorities suspended all inbound roaming, phone calls, and SMS from Russia and Belarus.[57]

3. The Donbas Offensive (May to September 2022) phase was characterised by sustained targeting and attacks using built-in tools (such as operating system components or pre-installed software for reconnaissance), as well as lateral movement and information theft on target networks, likely meant to limit Russian malware footprint and evade detection.[58] Intruders aimed to create persistent, privileged access from which wipers could be deployed, using the tried-and-true PowerShell script.[59] Prior knowledge of the victim organisation's network infrastructure, defensive measures, key personnel, and communication patterns provided the returning attackers with a substantial advantage by exploiting organisations that had already been compromised.[60] To supplement Russia's custom-made tools, the GRU tactics factored in the increasing volume of malware from open sources and criminal marketplaces.

4. The renewed campaign phase (October 2022 to January 2023) involved re-occurring disruptive attacks. Based on an analysis of the GRU playbook, Mandiant also calls this period a "disrupt and deny" phase: the GRU deployed "pure" wipers and disruptive tools disguised as ransomware, including some commercially sourced variations. These disruptive tools were lightweight in design and intended for immediate impact, aiming only to disrupt or deny access to the targeted organisations and sometimes erase the evidence of the attacker's presence. It increased the overall speed and scale at which they could be used to achieve operational objectives.[61]

5. From February to June 2023, the Russian cyberwarfare refocused on strategic espionage and pre-positioning. The CERT-UA encountered espionage operations where the primary objectives of the GRU, along with FSB and the foreign intelligence (SVR), were to identify Ukrainian law enforcement agencies' plans, as well as learn about witnesses and evidence to be presented to the International Criminal Court, to issue arrest warrants, and to impose sanctions.[62] Successful disruption narratives were amplified by hacktivist personas on Telegram, regardless of the actual impact of the operation.

[53] Gabby Roncone and John Wolfram, "Cyber war on the edge: a balance of access and action," *Cyberwarcon'22*, November 2022, quoted in Black, *Russia's War in Ukraine.*

[54] Black, *Russia's War in Ukraine*, 12.

[55] Black and Roncone, "The GRU Disruptive Playbook."

[56] Black, *Russia's War in Ukraine*, 9.

[57] Black, *Russia's War in Ukraine*, 14.

[58] Black and Roncone, "The GRU Disruptive Playbook."

[59] PowerShell is a cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework. As a scripting language, PowerShell is commonly used for automating the management of systems. PowerShell runs on Windows, Linux, and macOS.

[60] State Service for Special Communications, *Russia's Cyber Tactics H1 2023.*

[61] Black and Roncone, "The GRU Disruptive Playbook."

[62] State Service for Special Communications, *Russia's Cyber Tactics H1 2023,* 10.

These phases demonstrate that wartime offensive cyber operations, in practice, are cyclical by nature, where active periods alternate with gaps. Ukraine continues to absorb a sustained and intensive campaign of network attacks and cyber espionage operations from Russia. Several more factors warrant special attention in this regard.

First, the IT Army of Ukraine. It was borne out of an idea that emerged from a meeting convened by Digital Minister Mykhailo Fedorov to consider creating a "volunteer corps" to defend Ukraine's digital infrastructure from Russian cyber attacks. Minister Fedorov announced this offensive IT volunteer initiative with a tweet on 26 February 2022. In one month, it had recruited 300 000 members, uniting committed IT professionals, amateurs, and interested observers.[63] The primary tool of the IT Army is the Distributed-Denial-of-Service (DDoS) attacks, whereby an attacker attempts to overwhelm a site with traffic, thus obstructing its operation. Over the past 20 months, the IT Army of Ukraine has transformed from an ad-hoc force of volunteers into a tightly organised operation. It has become a smart construct with an organisational setup and operational impact, which will likely inform and shape the art of cyber and information warfare in future conflicts. However, the legality of foreign volunteers in cyber attacks raises several lingering questions. For instance, experts worry that the IT Army, a government-created entity, has been willing to form and openly advertise its partnership with a cybercriminal DDoS enterprise such as IPStress.[64]

The IT Army of Ukraine has transformed from an ad-hoc force of volunteers into a tightly organised operation which will shape cyber and information warfare in future conflicts

Second, the foreign assistance**.** The Ukrainian government first began to reach out to foreign partners with calls for assistance in cybersecurity already under Petro Poroshenko's presidency in 2018, ahead of the presidential and parliamentary elections of 2019, and continued under President Zelensky.

- In May and September 2021, the e-Governance Agency of Estonia, as an implementing actor for an EU-financed project that supports digital transformation in Ukraine, organised task-driven threat-hunting exercises for cybersecurity agencies. In particular, it taught what indicators of compromise attackers leave behind and how they move between the network systems.[65]

- Ukrainian cyber personnel also hosted their counterparts from the US Cyber Command to hunt for evidence of Russian cyber units pre-positioning themselves in critical infrastructure networks. American cyber forces provided support beyond direct countermeasures, such as remote analytic and advisory support to enhance the resilience of priority networks. This joint operation reportedly led to the removal of pre-positioned destructive malware in the Ukrainian Railways' networks prior to the invasion.[66]

- In addition, Kyiv benefitted from the defence capabilities elaborated under the EU PESCO framework. In February 2022, the Lithuanian-led Cyber Rapid Response Teams (CRRTs) and Mutual Assistance in Cyber Security were enacted in an operational context at the request of Ukraine for the first time.[67]

Third, public-private partnerships. Immediately after the invasion, the Ukrainian government began to elicit support from the private sector to supplement the state's

[63] For more on Ukrainian IT Army, see: Stefan Soesanto, „The IT Army of Ukraine", Centre for Security Studies, ETH Zürich, June 2022.

[64] Stefan Soesanto, *Cyberdefense Report The IT Army of Ukraine Structure, Tasking, and Ecosystem* (Centre for Security Studies, ETH Zürich, June 2022), 27.

[65] For more on this, see: "Cyber trainings to enhance Ukraine's skills to respond to cyberattacks," *eGa*, 22 September 2021.

[66] "Before the invasion: hunt forward operations in Ukraine," US Cyber Command, 28 November 2022; Mehul Srivastava, Madhumita Murgia, and Hannah Murphy, "The secret US mission to bolster Ukraine's cyber defences ahead of Russia's invasion," *Financial Times*, 9 March 2022.

[67] "Activation of first capability developed under PESCO points to strength cooperation in cyber defence," European Defence Agency, 24 February 2022.

cyber capabilities. This provided Ukraine's cyber defences with expert personnel on top of cutting-edge detection and response capabilities. Cooperation with companies such as Microsoft, ESET, and Google added a defensive depth to Ukraine's critical information infrastructure. Within several days following the invasion, key CII assets and services were put under the protection of Western technology companies, thereby allowing Ukrainian authorities to maintain access to and control over vital state functions. Banking systems continued performing transactions, and trains were arriving on schedule. Whereas Ukraine's military remained connected to vital situational awareness data.

Cooperation with companies such as Microsoft, ESET, and Google added a defensive depth to Ukraine's critical information infrastructure

In May 2023, after the Cabinet of Ministers had approved the procedure for searching and identifying potential vulnerabilities in information (automated), electronic communication, and ICT systems, the Ukrainian authorities adopted the "Bug Bounty" mechanism.[68] It provides for the recruitment of external specialists who would, for a fee, search for errors and vulnerabilities in software products, ICT systems, etc. in order to eliminate them.

Although it is difficult to measure the exact impact of external support, the involvement of outside parties in supplementing the efforts of national cyber defenders has been a critical factor in Ukraine's resilience. As the Russian cyber groups show no signs of exhausting their operational capacity, further support of Ukraine remains crucial, especially with a layered defensive posture that can sustain attack surface reduction, network detection, and basic cyber-hygiene practices. Building an effective cyber-defence posture is a marathon, not a sprint.

Building an effective cyber-defence posture is a marathon, not a sprint

Conclusion and Recommendations

According to the European Commission's 2023 report, presented in the context of the enlargement package, Ukraine is assessed to be in between a moderate and a good level of preparation in the domain of digital transformation. It has made substantial progress during the last 18 months.[69] Ukraine has a well-advanced e-government system that provides citizens with easy access to public services. Although fighting the war of defence has strained its digital infrastructure, Ukraine's IT sector overall is still in good health, having undergone rapid growth in the pre-war years. The government has also organised a strong response to tackle the digital challenges of the war.[70] Although Ukraine has performed admirably in sustaining much of this progress, the war has highlighted the need to physically protect digital government infrastructure, achieve greater integration between government agencies, and improve data governance.[71]

The war has highlighted the need to physically protect digital government infrastructure, achieve greater integration between government agencies, and improve data governance

[68] Cabinet of Ministers of Ukraine, *Постанова від 16 травня 2023 р. № 497 Київ Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж* [RESOLUTION dated May 16, 2023 No. 497 Kyiv On approval of the Procedure for searching and identifying potential vulnerabilities of information (automated), electronic communication, information and communication systems, electronic communication networks] (Kyiv: Verkhovna Rada of Ukraine, May 2023).

[69] European Commission, *Commission Staff Working Document Ukraine 2023 Report*.

[70] Richard Grieveson, Branimir Jovanovic, Miriam Kosmehl, et al., "Outlier or not? Ukrainian economy's preparedness for EU accession," *The Vienna Institute for International Economic Studies* No 2023-11(November 2023).

[71] "The Patch to becoming a Data-Driven Public Sector," OECD, 28 November 2019.

- Regarding cybersecurity, Ukraine should further align itself with the EU Directive on the security of network and information systems (NIS).

- As the war continues, Kyiv needs to focus on ensuring that citizens, businesses, and public agencies can connect to the internet, as well as continue modernising its communications and public service infrastructure.

Determined legislative efforts previously allowed the government to back up and safeguard vital state registers and databases with key cloud service providers. It also paved the way for emergency migration of critical services to European data centres, thereby putting them outside the reach of conventional attacks, such as missile strikes on data centres.

- Looking beyond the war, Ukraine should focus on further enhancing its omnichannel approach and on supporting the resilience of the government as a platform ecosystem to ensure that all Ukrainian citizens, including refugees, can access public services.

- As roads are being rebuilt, Ukraine should consider laying fibre cables and thereby connecting more people (even if operators may not be able to provide such services for the next several years, especially in rural areas). To this end, the regulator could also stimulate broadband providers to deploy more fibre deeper into the networks and gradually phase out Digital Subscriber Line technologies.

- The destruction caused by the war should be leveraged as an opportunity to rebuild, modernise, and extend the uptake/access of the communication and digital infrastructure (e.g., by laying fibre cables), as well as put all unused spectrum to service and reduce current gaps across oblasts.

- Other immediate measures could focus on supporting teleworking practices and facilitating digital access to public services, for instance, for the IDPs and refugees.[72]

[72] "The Patch," OECD.

Likewise, there are steps that the EU can take to help Ukraine while helping itself.

The EU should continue with the dedicated financing instrument to support Ukraine's access to the EU's digital market

- To further bolster Ukraine's digital transformation, the EU should continue with the dedicated financing instrument to support Ukraine's access to the EU's digital market in terms of integration and connectivity. The EU should make as many of the temporary liberalisation measures as possible.

- In 2024-27, the Ukraine Facility (EUR 50 billion) should help not only to resist further aggression but also rebuild a modern, prosperous country and support the transition towards a digital economy.

- For the EU to meet the Digital Decade targets, collective efforts should be made by all member states. Each member state should contribute to this ambitious goal from a different starting point, determined by its resources, comparative advantages, and other relevant factors such as the population size, the scale of the economy, and the areas of specialisation.

- Digital technologies and data should play an important role in the post-war recovery. Ukraine's move towards integration into the Digital Single Market brings a progressive alignment with international regulations and standards on digital practices, which could add important benefits in terms of the reduction of cross-border barriers to digital trade and acceleration of Ukraine's digital economy.

- Ukraine's digital journey should serve as an example for other aspirant countries to harvest the benefits of digitalisation and thus move the Union's enlargement policy forward. Successful digitalisation in Ukraine should contribute to greater convergence with member states and reinforce their collective competitiveness and resilience in the global context.

- Ukraine's labour force skilled with experience in using e-governance, as well as with practical cyber defence through membership in the IT Army, could be beneficial to member states and the digital single market. In the future, Ukraine should become a frontrunner in pushing for the implementation of more digital services on the EU level.

Ukraine should become a frontrunner in pushing for the implementation of more digital services on the EU level

If the EU wants to have a functioning Digital Single Market, it will need more use cases. The precondition for that is that data can move freely across the EU in a secure and privacy-friendly manner. Ukraine is progressing well in that direction. It has opted for a model where it first provides digital public services, which, in return, increases trust through usability. By pushing for more digital public services, citizens have been able to see the added value and how digitalisation has simplified lives.

- The Ukrainian government should, in the future, pave the way for the establishment of a digital ecosystem that would allow the private sector and start-ups to thrive.

- It should also focus on improving digital skills in the population to support the prospects of future growth.

The current geopolitical context and Russia's invasion of Ukraine render the implementation of innovative digital solutions, technologies, and infrastructures based on the EU's values and principles only more relevant.

- Providing more digital services and guaranteeing their interoperability across the EU should become a priority area whereby Europe could become a global leader.

- Dreadful as the circumstances of war are, they have created the prospect for an EU that will be both bigger and better. The war in Ukraine offers a chance to enlarge and improve the European Union and externalise benefits through the Global Gateway strategy, which should not be wasted.

The war in Ukraine has brought into focus the necessity of digital identity solutions. Access to reliable public services remains fundamentally important during the conflict. Despite the challenges posed by the war, the Ukrainian government has relentlessly continued its effort to provide, expand, and digitise its public services. IDPs may have lost access to their physical identification papers, while those who have sought refuge overseas urgently need their Ukrainian documents to be recognised in their host countries. Hence, a critical need for portable and internationally interoperable digital identity solutions has emerged.

- Efforts to develop such cross-border solutions to ensure people can prove they are who they say they are, despite the loss of critical documentation or displacement across borders, should continue.[73]

Even with limited insights into the cyber dimensions of the war, we can conclude that Kyiv has been successful in defending against Moscow's cyber offence.

- Yet, we should not let Ukraine's success in this area engender a false sense of security about offensive cyber operations in future conflicts.

- Institutional adaptation, proactive defensive actions, capacity to absorb external support, and expanding to the cloud require further research into Ukraine's experience in cyber defence.

- Policy makers and practitioners should pay more attention to cyber capacity building that has provided the necessary push for legislative reforms during the earlier years of Zelensky's presidency and has been a crucial enabler for Ukraine's long-term success.

Measures taken to increase external and private sector support have driven much of Kyiv's defensive success. Ukraine's emergency

[73] The OECD's "Recommendation on Broadband Connectivity" (adopted in 2004 and revised in 2021) provides a reference for policymakers and regulatory authorities to unleash the full potential of connectivity for people, firms, and the government. See: "Digitalisation for recovery in Ukraine," OECD, 1 July 2022.

migration to the cloud has conferred immeasurable benefits. Kyiv's cyber defence has been capable of consolidating different forms of technical assistance and incorporating volunteer defenders.

- Cooperation and coordination with external actors – be it from the private sector, civil society, or international states and non-governmental organisations – appear to have been pivotal for many state agencies' capabilities. It has proven to have a defensive reach far beyond what Ukraine could have achieved alone and thus needs to be bolstered.

As a result of Russia's war in Ukraine, the EU institutions and national authorities have intensified cooperation and information sharing in relation to cybersecurity.

- Ukraine's strong focus on cybersecurity should set an example for other countries to follow and thus ensure that public digital services remain resilient, especially in uncertain times and with cyber threats growing.

Ukraine's strong focus on cybersecurity should set an example for other countries to follow and thus ensure that public digital services remain resilient

- The defence against a military invasion now requires, from the national authorities, an ability to disburse and distribute digital operations and data assets across borders and into other countries.

The cyber warfare between Russia and Ukraine may define future rules of engagement in cyber wars. The primary goals of wartime operations – i.e., sabotage, influence, and espionage – have remained unchanged. Cyber operations provide new opportunities to achieve age-old objectives.[74] The GRU's disruptive operations in Ukraine have revealed a series of tactical choices that Russia's military has made to achieve its wartime objectives. This indicates that the GRU has a playbook that is likely to be used in future crises and conflict scenarios.[75]

- Careful analysis of the Russian target selection, manipulation of attribution, maintaining of deniability, examining how cyber is integrated into Russian hybrid tactics, and identifying the advanced malware and techniques employed by Russian cyber actors should begin now.

- By learning from Ukraine, EU member states should be able to better sustain investments to boost visibility, detection, and resilience, which will surely remain relevant and helpful in the conflicts to come.

Drawing lessons from Russia's and Ukraine's cyber warfare will help Europe forecast and prepare for the development of new tools and methods in future cyber attacks.

[74] Taylor Grossman et al., *The Cyber Dimension of the Russia-Ukraine War.*

[75] Black and Roncone, "The GRU Disruptive Playbook."

RECENT ICDS PUBLICATIONS

REPORTS

Raik, Kristi, and Eero Kristjan Sild. ***Europe's Broken Order and the Prospect of a New Cold War***. October 2023.

Iwama, Yoko, Tetsuo Kotani, Sugio Takahashi, Tony Lawrence, and Henrik Praks. ***Allies Help Those Who Help Themselves: How Estonia and Japan Approach Deterrence***. September 2023.

Jermalavičius, Tomas, and Alice Billon-Galland. ***British Power in Baltic Weather: The UK's Role in Nordic-Baltic Security and UK-Estonia Defence Cooperation***. July 2023.

Gretskiy, Igor. ***Is There Life in the Desert? Russian Civil Society After the Full-Scale Invasion of Ukraine***. May 2023.

Idarand, Tõnis, Kalev Stoicescu, and Ian Anthony. ***The Future of Arms Control: Ready to (Dis)Agree?***. May 2023.

Jermalavičius, Tomas, Veli-Pekka Tynkkynen, Andrian Prokip, Christian Egenhofer, Edoardo Righetti, Arūnas Molis, Priit Mändmaa, Tony Lawrence, and Oleksandr Sukhodolia. ***War and Energy Security: Lessons for the Future***. May 2023.

Stoicescu, Kalev, Mykola Nazarov, Keir Giles, and Matthew D Johnson. ***How Russia went to war: The Kremlin's Preparations for its Aggression against Ukraine***. April 2023.

Klyszcz, Ivan U K. ***How Russia Brings Its Aggression Against Ukraine to The Global South***. April 2023.

POLICY PAPERS

Raik, Kristi, and Steven Blockmans. "**Accelerator for a Geopolitical Europe: Potential Impact of Ukraine's Membership on EU Foreign, Security, and Defence Policy**." November 2023.

Blockmans, Steven. "**The Impact of Ukrainian Membership on the EU's Institutions and Internal Balance of Power**." November 2023.

Emerson, Michael. "**The Potential Impact of Ukrainian Accession on the EU's Budget – and the Importance of Control Valves**." September 2023.

Kvamladze, Tato. "**Conscription in Estonia and Georgia: Lessons from and for Small-State Peers**." March 2023.

ANALYSES

Arjakas, Merili. "**A Tale of Two Populists: The Foreign Policy of PiS and Fidesz**." October 2023.

Peterson, Annabel. "**From Shadows to Spotlight: The Kremlin's Not-So-Covert Gambit for Ukraine**." October 2023.

Leveque, Arthur. "**The New Geopolitical Landscape in the EU's Eastern Neighbourhood: Fragmentation of Economic Ties Post February 2022**." September 2023.

Teperik, Dmitri. "**The Glass of Societal Resilience – Half Empty or Half Full? Perceptions of Socio-Economic Threats and Wellbeing in Estonia**." September 2023.

Jüris, Frank. "**China and Rare Earths: Risks to Supply Chain Resilience in Europe**." May 2023.

Hurt, Martin, Mārtiņš Vargulis, Liudas Zdanavičius, and Tomas Jermalavičius. "**Baltic Defence Development: Adding Value to the Defence of the Baltic Sea Region**." March 2023.

Idarand, Tõnis. "**Reining In Autonomous Weapons. Impact on Military Innovation – An Estonian Perspective**." February 2023.

Fedosiuk, Tetiana. "**The Stolen Children: How Russia Attempts to Kidnap Ukraine's Future.**" February 2023.

BRIEFS

Verville, Francesca, and Catarina Buchatskiy. "**In a State of Denial: The Air War in Ukraine**." October 2023.

Adeoti, Kristin. "**New Frontiers: Estonia's Foreign Policy in Africa**." October 2023.

Lawrence, Tony, Toms Rostoks, Margarita Šešelgytė, Henrik Larsen, Mārtiņš Vargulis, Gintaras Bagdonas, and Iro Särkkä. "**NATO's Vilnius Summit**" (Series of ICDS Briefs). July 2023.

Watkins, Peter. "**British Nuclear Policy.**" May 2023.

Blockmans, Steven. "**The EU's Magnitsky Act: Obsolete in the Face of Russia's Crimes in Ukraine?**" May 2023.

All ICDS publications are available from https://icds.ee/category/publications/.

ICDS.Tallinn
@ICDS _ Tallinn
ICDS-Tallinn
www.icds.ee

International Centre for Defence and Security
63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee

ISSN 2228-2068