

# Apps at War: Army+, Reserve+ and the Rise of Digital Defence Governance in Ukraine

MATTHEW B. ARNOLD, VIKTORIIA ROLLER AND KHRYSTYNA ZHYVOGLIAD



## The Authors



**Matthew B. Arnold** is Programme Director of LSE IDEAS' Democratic Resilience in a New Age of War Programme. He holds doctoral and master's degrees from the London School of Economics and Political Science.



**Viktoriia Roller** is Head of the Analytical Unit, Defence Policy Sector at Better Regulation Delivery Office (BRDO). She holds a doctoral degree in law from Taras Shevchenko National University of Kyiv.



**Khrystyna Zhyvogliad** is Senior Defence Policy Analyst, Defence Policy Sector at BRDO. She holds a master's degree from Kyiv National University of Trade and Economics.

## Acknowledgements

This paper is a co-publication of **LSE IDEAS** and **BRDO**. The co-authors would like to thank the leadership of both institutions for their support in launching this collaborative partnership and this report. We are also grateful to those who provided invaluable insights through expert interviews, as well as to the many **BRDO staff** who reviewed drafts and offered thoughtful feedback throughout the process. A deep appreciation goes to the **LSE IDEAS publications team** for their exemplary support. The authors are grateful to the **Ministry of Defence of Ukraine** for its cooperation and for providing access to data that informed this research. BRDO would also like to thank the **Ministry of Defence of Germany** for its financial assistance. The views expressed in this paper are those of the authors and do not necessarily reflect those of the institutions involved. Final responsibility for the content rests with the authors.

The **Democratic Resilience in a New Age of War (DRNAW)** programme is a three-year, multidisciplinary initiative supporting democracies amid escalating drone-enabled warfare and hybrid conflict. Ukraine is both a core partner and a hub for operational learning and knowledge exchange. Leveraging LSE's global expertise, direct Ukrainian partnerships, and practitioner engagement, the programme delivers real-world solutions for democratic resilience against accelerating authoritarian threats and technological disruption.

**May 2026**

Editor: **Stuart Austin**

Design, Typeset and Layout: **Indira Endaya**

Cover image: **pngtree.com**

DOI: <https://doi.org/https://doi.org/10.21953/researchonline.lse.ac.uk.00138317>

## Contents

The Authors	2
Acknowledgements	2
Contents	3
Abstract	4
Glossary of Key Terms	5
Section 1. Introduction: Why Digital Defence Governance Matters	6
Section 2. From Digital State to ‘Digital Army’	7
Section 3. Legal Foundations of Ukraine’s Digital Defence Governance	10
3.1. <i>Oberih</i> : The Digital Backbone	10
3.2. Reform Waves to Maximize <i>Oberih</i>	12
3.3. Ukraine’s Digital Door to Defence Governance	14
3.4. Data Governance in Army+ and Reserve+	15
Section 4. What Army+ and Reserve+ Do	16
4.1. How Reserve+ Works	17
4.2. How Army+ Works	20
4.3. Data Security and Privacy Protections	23
Section 5. Adaptive Governance in a High-Intensity War	24
5.1. Turning Adaptive Governance into Combat Power	25
5.2. Sustaining Consent in a Hard War	27
5.3. Hard Political Choices and the Reach of a Wartime Digital State	29
Section 6. Implications for EU and NATO allies	31
References	34
Interviews	37
Annexes	38
Annex 1. Legal Framework Underpinning Army+ and Reserve+	38
Annex 2. Legal Provisions for the Defence Portal	39
Annex 3. Reserve+: Privacy and Safety Standards Notice	40
Annex 4. Army+: Privacy and Safety Standards Notice	41

# Apps at War: Army+, Reserve+ and the Rise of Digital Defence Governance in Ukraine

## Abstract

Ukraine's Army+ and Reserve+ applications show how digital tools can transform mobilisation and military administration by re-engineering core governance processes, not simply adding apps on top of bureaucracy. By achieving a high degree of digital defence governance, Ukraine is reshaping the structural conditions under which it can sustain its defence effort – from how it mobilises people to how it supports serving personnel – and, in doing so, expanding what is politically and administratively possible in a long war. Army+ and Reserve+ are central to an adaptive governance approach that seeks to sustain a protracted war under democratic constraints, using digital channels to make mass military service more rule-bound, transparent, and legible to citizens and servicemembers, while constraining arbitrary bureaucratic discretion. Ukraine's democratic allies should study its model to identify elements that could be adapted within their own national contexts.

## Glossary of Key Terms

Ukrainian Official Definitions, further explanation in italics where useful.

<b>Conscript</b>	Persons enrolled for military registration (Verkhovna Rada, 1992). <i>In practice, this is mainly men aged 18–25 who are assigned to a conscription station and subject to basic military service rather than mobilisation.</i>
<b>Oberih</b>	(Ukrainian for ‘Safeguard’) The Unified State Register of Conscripts, Persons Liable for Military Service, and Reservists is an information and communication system designed for the collection, storage, processing, and use of data on conscripts, persons liable for military service, and reservists, established to ensure the military registration of citizens of Ukraine (Cabinet of Ministers, 2024a).
<b>Persons Liable for Military Service</b>	Persons who are in the reserve for the staffing of the Armed Forces of Ukraine and other military formations during a special period, as well as for carrying out work to ensure the defence of the state. They may be called up for military service, as a rule between the ages of 25 and 60, with specific categories of men under 25 also becoming liable once they have completed conscript service, signed a contract, or obtained an officer’s rank (Verkhovna Rada, 1992).
<b>Reservist</b>	Persons serving in the military reserve of the Armed Forces of Ukraine and other military formations and designated for their staffing in peacetime and during a special period. <i>To become a reservist, a person must sign a contract for this type of military service</i> (Verkhovna Rada, 1992).
<b>Servicemen</b>	Persons undergoing military service (Verkhovna Rada, 1992). <i>Active-duty personnel.</i>
<b>State Web Portal for Electronic Public Services in the National Security and Defence Field (Portal)</b>	An organised set of interrelated information technology tools that, in interaction with other information and communication systems, registers – including public registers – and databases/data banks, operate as a single entity for the purpose of providing and receiving electronic public services in the field of national security and defence (Cabinet of Ministers, 2024b).
<b>Territorial Recruitment and Social Support Centres (TRSSCs)</b>	Military administration bodies that ensure the implementation of legislation concerning military duty and military service, as well as mobilisation preparedness and mobilisation; TRSSCs are established, liquidated, and reorganised by the Ministry of Defence (Cabinet of Ministers, 2022).

## Section 1. Introduction: Why Digital Defence Governance Matters

Russia's full-scale invasion in 2022 forced Ukraine to resist a larger enemy in a long war whilst maintaining democratic norms (Panasiuk, 2024). Sustaining that effort has pushed digital defence governance to the centre of how the Ukrainian state mobilises people and manages military service. Two mobile applications, Army+ and Reserve+, now sit at the heart of Ukraine's efforts by serving core defence needs in ways that are faster, more rulebound, and more visible to citizens and servicemembers.

An early surge of volunteers helped Ukraine resist Russia's initial onslaught, but that wave began to ebb over 2023 as the war settled into a grinding fight (Schlegel, 2024). Ukraine then had to find ways to both bring in new troops and better serve forces spread across a vast frontline. The inherited Sovietstyle defence bureaucracy had become a liability: its slow, paperbased routines disrupted mobilisation and clogged everyday administration for those already serving, fuelling a sense that the burden of service was uneven and the state was struggling to meet its obligations to its soldiers.

In response, Ukraine's Ministry of Defence launched Army+ and Reserve+ over 2024. Together, they directly connect the state to more than seven million people essential to sustaining the war effort: over six million citizens liable for mobilisation and one million activeduty personnel (Ministry of Defence, 2025a). Army+ is a secure, allinone service hub for servicemembers, digitising reports, approvals, information feeds, training and feedback mechanisms, while Reserve+ provides citizens of military age with a single channel for registration data, electronic IDs, deferments, summons verification and recruitment pathways.

Together these applications bolster Ukraine's defence governance: how defence is run and overseen. By achieving a high degree of digital defence governance, Ukraine has begun to reshape the structural conditions under which it can sustain its war effort – from how it mobilises people to how it supports serving personnel. In doing so, it is expanding what is politically and administratively possible in a long war. In this sense, Army+ and Reserve+ embody a potential model of digital defence governance in which interoperable data registers and individualised user interfaces are designed to redistribute agency, increase transparency, and entrench more equitable, rule-bound treatment of citizens and servicemembers.

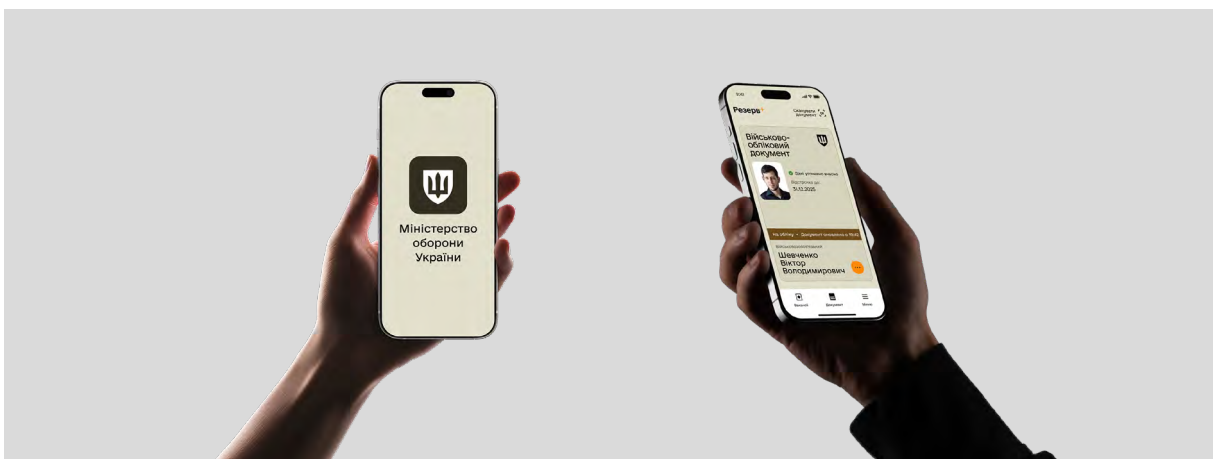


Image credit: Ministry of Defence of Ukraine

Drawing on key informant interviews, legal analysis and implementation reportage, this report maps why and how Army+ and Reserve+ were built by examining the policy problems they seek to address, the legal reforms that enabled them, and how those choices are coded into the apps' workflows and services.<sup>1</sup> It then uses that empirical base to assess what they contribute to Ukraine's national defence, from citizens facing mobilisation to soldiers at the front and the institutions running the war. A core inquiry is whether these tools materially sharpen Ukraine's ability to innovate and adjust under fire – what this report terms its adaptive governance. Finally, the report assesses which elements of Ukraine's digital administration and mobilisation model merit consideration by EU and NATO allies, particularly how these apps encode governance choices about discretion, equity and transparency.

## Section 2. From Digital State to 'Digital Army'

*We started with the goal of convenience.  
But in wartime, digital became the  
only way to keep the country functioning.*  
(Digital State UA, 2025)<sup>2</sup>

**T**his section explains how Ukraine's wartime pressures intersect with earlier digital state reforms and shows how those reforms were repurposed into a 'Digital Army' by digitalising core parts of defence governance.

After more than a decade of war, and four years of full-scale invasion, Ukraine faces a persistent manpower dilemma conditioned by democratic imperatives. It must sustain large-scale fighting over time without pushing existing cohorts beyond what they can endure at the front. To keep popular support behind national defence, mobilisation must continue but also must be seen to operate through clear, rule-bound and transparent procedures. At the same time, the government must strip out bureaucratic friction inside the armed forces so that scarce personnel and resources are used as effectively as possible.

Amid an ongoing, high-intensity war, digitalising defence governance is no longer a side project about efficiency; it is one of the few realistic ways to balance scale, available resources, and speed with the political imperatives of sustaining democratic legitimacy (Mamediiieva, 2025). The sheer volume of decisions involved in mass mobilisation and force sustainment under democracy risks quickly overwhelming legacy systems in an era defined by social media, intense public scrutiny, and the relative ease of mass emigration (Danish Immigration Service, 2024). Digital tools offer realistic ways to maintain scale, cut arbitrary discretion, and help keep people's attitudes towards the war effort anchored in transparent, predictable rules.

- 
- 1 Eight key informant interviews were conducted, including programme managers in the Ministry of Defence, database experts, parliamentary staffers and sectoral/legal experts.
  - 2 Valeriya Ionan, Advisor to the First Deputy Prime Minister of Digital Transformation on accelerated digital reforms during wartime: "[...]not just to maintain public services, but to reimagine what a state can be in the 21st century."

### Box 1. Ukraine's Approach to Mobilisation

Ukraine operates a hybrid mobilisation system that has evolved from a Soviet-legacy draft into a mixed framework combining compulsory service with incentivised voluntary contracts. Since the full-scale invasion in February 2022, mobilisation has taken place under martial law and general mobilisation, under which men aged 18–60 are generally prohibited from leaving the country and can be called up for service, subject to limited exceptions. The system is anchored in the Law on Mobilisation Preparation and Mobilisation and the Law on Military Duty and Military Service, which place men on the military register from age 17 to 60; active mobilisation focuses mainly on those aged 25–60 following a 2024 reform that lowered the previous threshold of 27 years. A major reform package adopted in 2024 tightened obligations and procedures, clarifying duties to keep personal data up to date and appear when summoned, strengthening penalties for evasion, and streamlining how deferments, reservations, and fitness for service are recorded. These reforms laid the groundwork for a gradual shift from mandatory conscription towards a more recruitment-led model. Young adults, aged 18–24, can sign fixed-term military contracts – often for one year – rather than serving indefinitely until the end of martial law, as part of a wider post-2024 expansion of contract options available across the force. This recruitment-driven tier allows citizens to apply for specific roles, such as drone operators or technical specialists, while compulsory mobilisation continues to provide the backbone of manpower. Despite these recruitment-related reforms, a fully developed demobilisation framework for all cohorts has not yet been put in place, so the length of service for many mobilised personnel still largely depends on the evolving demands of the war. Structurally, the Ministry of Defence's Territorial Recruitment and Social Support Centres (TRSSCs) function as the essential local interface for mobilisation.

Ukraine's wartime approach builds on nearly a decade of digital statebuilding to rebuild trust in institutions long seen as inefficient and corrupt.<sup>3</sup> By overhauling policy, institutions, and technology together, Ukraine created nearseamless digital services for its citizens (Ingram and Vora, 2024). Most significantly, the *Diia* (The State and Me) portal is a 'state in a smartphone' application, but also accessible via desktop. Since 2020, it has regularised digital public services for over 20 million citizens. Beneath *Diia's* user-facing services lies an architecture of interoperable base registers, so ministries work from shared, regularly updated datasets rather than isolated files (Vyhovska *et al.*, 2024).

Enabled by laws giving full legal force to electronic documents and signatures, together with a strengthened cybersecurity and data-protection frameworks, core state functions – such as taxation, social benefits, identification, and civil registration – moved online while maintaining strong safeguards for integrity and confidentiality (OECD, 2022). These efforts have been driven by a politically empowered Ministry of Digital Transformation focused on enabling large-scale governance to function online in the form of a digital ecosystem.<sup>4</sup> Cumulatively, these efforts transformed how Ukrainian citizens interact with the state and raised public expectations that services should be easily accessible and largely free of paper-bound bureaucracies.

3 Ukraine now ranks 5th globally in the UN EGovernment Index for digital public services, rising from 102nd place in 2018 and underscoring the rapid pace of its digital transformation (United Nations, 2022).

4 Established in August 2019, the ministry coordinates a wider state digital ecosystem, including flagship platforms such as *Diia* for public services, *Mriia* for digital education, and CodeUA for promoting Ukrainian IT firms.

When Russia escalated to full-scale war in 2022, this digital ecosystem gave Ukraine a distinct starting point to re-engineer mobilisation, military administration, and civil–military relations around the same principles: digitalising defence governance not just to fight the current war more effectively, but to lock in more transparent, rules-based governance for the long term. For many who began serving from 2022 onwards, including large numbers from Ukraine’s IT sector, encountering paper-based military administration felt like a step backwards and generated bottom-up pressure on the MoD to modernise.<sup>5</sup>

Over 2023, as mobilisation pressures sharpened, digitalisation was the most obvious modality to underpin wider reforms.<sup>6</sup> As the MoD noted, digitalisation allowed Ukraine to preserve resources, strengthen military effectiveness, and achieve ‘advantage over the enemy’, a logic that aligned with wider efforts to build digital frontline tools, most notably the DELTA battlefield management system (Ministry of Defence, 2025a). Taken together, these efforts to deeply embed digitalisation across the war effort came to be known as Ukraine’s ‘Digital Army’ initiative.<sup>7</sup> As one recent assessment argues, Ukraine is now building ‘one of the most advanced defence governance models of the digital age’ (Bondar, 2025).

Within this context, the technical design of both Reserve+ and Army+ began in 2023 while legal reforms were drafted in parallel to mandate their functionality. The roll-out and implementation by the public began in May and August 2024, respectively. This concurrent development, with teams of software developers and lawyers working together under the exigencies of the war, allowed Ukraine to move quickly to strengthen defence governance on digital foundations, making mobilisation and administrative processes faster, more transparent, and less exposed to corruption or arbitrary discretion.

More broadly, the apps are intended to function as instruments of democratic resilience in wartime: by giving citizens and servicemembers direct, trackable access to their own data and to the decisions that affect them, these platforms seek to build trust in government and defence institutions and embody Ukraine’s emergence as a more transparent European democracy despite the pressures of full-scale war.

While later sections unpack the detailed functionality and governance design of each application, their policy goals are straightforward. With its focus on military personnel, Army+ is intended to de-bureaucratise internal military administration by replacing paper reports and approval chains with standardised digital workflows and a single platform for routine administrative services.<sup>8</sup> The intent is to reduce the time military personnel must

5 The significance of volunteer cadres of IT experts cannot be understated: “The 2022 injection of civilians into the army liquefied the Soviet mood of the armed forces -- and made everything possible” (Romaniukov, 2026, interview).

6 A Brookings Institute report (Ingram and Vora, 2024) argued of Ukrainians’ experience since 2014: “War rallied citizens to the government and made essential the ability of government to perform citizens’ services outside of physical offices, which in turn demonstrated the efficiency and efficacy of e-government and consequently contributed to citizen trust in government.”

7 The Digital Army is Ukraine’s initiative to redesign defence institutions around connected, datadriven systems and is now hosted in a state-owned enterprise of the same name. It uses interoperable digital platforms to manage mobilisation, personnel, logistics, and frontline services in near-real time (Volokita, 2025).

8 At its peak, Ukraine’s military was generating nearly 20 million paper requests a year, consuming enormous time and institutional capacity. Each request took around 100 minutes to prepare, with personnel then waiting weeks for updates, while commanders spent up to 70% of their time on clerical work, and processing this volume of reports cost an estimated USD 48 million annually (Bondar, 2025).

devote to administrative paperwork and lessening associated stress.<sup>9</sup> As such, then Prime Minister Denys Shmyhal launched Army+ by saying it was like ‘*Diia* for the military’ – most services for active personnel run through a traceable, auditable and more corruption-resistant digital channel that also gives commanders clearer, real-time visibility over their units (Denisova, 2024). While Army+ launched with a core set of services, new functions are added regularly to create an ‘ecosystem of products for the military’ (BRDO, 2024a).

Complementing this, Reserve+ covers all those liable for military service and is built around interlinked aims. Initially, the most urgent task in 2024 was solving ‘one single problem’: cleaning up and completing mobilisation records by giving every liable citizen a personal electronic cabinet to update their data directly into the *Oberih*, the national military registration register (Romaniukov, 2026, interview). Beyond that, Reserve+ supports key functions such as managing deferments and supporting more targeted recruitment. In doing so, Reserve+ seeks to make mobilisation more visibly rules-based and sustainable, relying on digital convenience and transparency rather than escalating coercion. In this way, Reserve+ helps close the loop between Ukraine’s pre-war digital state and its wartime ‘Digital Army’.

### Section 3. Legal Foundations of Ukraine’s Digital Defence Governance

*We redesigned the logic of mobilisation  
for a country at war.*

– Kateryna Chernohorenko (2025)<sup>10</sup>

**T**he shift from a ‘digital state’ to a ‘Digital Army’ described in Section 2 rests on three core capacities of Ukraine’s digital transformation: interoperable base registers, the legal force of electronic documents and signatures, and a modern digital security framework. Building on this foundation, a concerted legislative push built out the unified military register *Oberih*, linked it to key civil registers, established a dedicated Defence Portal with electronic cabinets for millions of civilians and servicemembers, and set core rules for accessing defence-related personal data. This section sets out the legal scaffolding behind *Oberih*, the reform waves that established the Portal, and the data arrangements that now shape Ukraine’s digital defence ecosystem.

#### 3.1. *Oberih*: The Digital Backbone

Ukraine’s unified electronic database for military registration, *Oberih*, covers those citizens who are conscripts, persons liable for military service, and reservists (roughly ages 17–60). Created in 2017, the register primarily covers men, as only they are subject to conscription,

9 As Commander-in-Chief of the Armed Forces of Ukraine, Colonel General Oleksandr Syrskyi, explained: “Innovations are the defining factors in contemporary warfare, determining the winners of wars. The innovations of the Army+ application aim to improve the efficiency of military personnel, creating more comfortable conditions for solving service issues and performing combat missions as assigned. Army+ simplifies service and reduces wasted time” (Ministry of Defence, 2024a).

10 Former Deputy Minister of Defence for Digital Development, Digital Transformation and Digitalisation, Ukraine (2023-2025).

though women in certain specified professions (including many medical specialties) are also required to register. Establishing *Oberih* required migrating existing paper military records into the digital register, after which it gradually expanded in scope and interoperability.<sup>11</sup>

Multiple reforms in 2021 and 2022<sup>12</sup> set detailed rules for maintaining military records and exchanging data with other state registers, including a wide array of civil ones.<sup>13</sup> Together, these reforms laid the groundwork for digital military registration documents and more automated registration processes based around *Oberih*. Notably, a further major reform is underway to establish a parallel registry for military personnel. While Reserve+ draws on comprehensive military registration data from *Oberih*, this new register will provide the first unified dataset on active service members, enabling additional services.<sup>14</sup>

*Oberih* aggregates detailed personal and service data – such as full name, place and date of birth, place of residence, registration number, and (where applicable) rank and specialty – into a single, centrally managed database, replacing fragmented paper records. Together, the three legal categories – conscripts, persons liable for military service, and reservists – define who appears in *Oberih* and how they are tracked over time, allowing the state to manage conscription and reserve obligations through a common digital register rather than dispersed local files. Upon reaching conscription age, many men are registered automatically, with *Oberih* pulling data from other state registers, marking a shift toward automated military registration rather than purely in-person enrolment (Ministry of Defence, 2025b).

Importantly, a key feature of *Oberih* is its interface with over a dozen other state registers, used to understand, for instance, marital status, family size, disabilities, and education and employment status. The granular profile provided is essential to applying the legal provisions determining conscription eligibility, deferments, and exemptions, as well as more generally supporting workforce planning. Cross-register interoperability makes it possible, for instance, to automatically verify eligibility for some deferments and exemptions and to streamline their extension, reducing in-person paperwork (Romaniukov, 2026, interview). These functions have turned *Oberih* from a basic register into a unifying node of digital defence governance.

11 *Oberih* was established in law in 2017 as the Unified State Register of Conscripts, Persons Liable for Military Service, and Reservists, and moved into active operation in stages from March 2022 onward.

12 These were the Law of Ukraine ‘On Public Electronic Registers’ (2021) and the Cabinet of Ministers Resolution No. 1487 of December 2022, ‘On approval of the procedure for organising and maintaining military records of conscripts, persons liable for military service, and reservists, and regulating data exchange with state registers’.

13 These include at least 14 sources: registers of civil status, legal entities and sole proprietors, war veterans, and individual taxpayers, as well as the e-health system, the *Diia* eservices portal, registers of territories of hostilities or occupation, education and employment databases, social protection information systems, and other electronic resources (Novyny, 2024b).

14 The Military Personnel Register is being created as a distinct database from *Oberih*, with its own legal basis, to record service histories and current status of active-duty personnel – including unit affiliation, role, deployments, and benefits eligibility. Whereas *Oberih* directly covers conscripts, reservists, and all those liable for military service, the new register is intended to function as a single, authoritative source on serving personnel, allowing Army+ to offer more tailored services – for example, automating entitlements and further streamlining transfers.

### 3.2. Reform Waves to Maximize *Oberih*

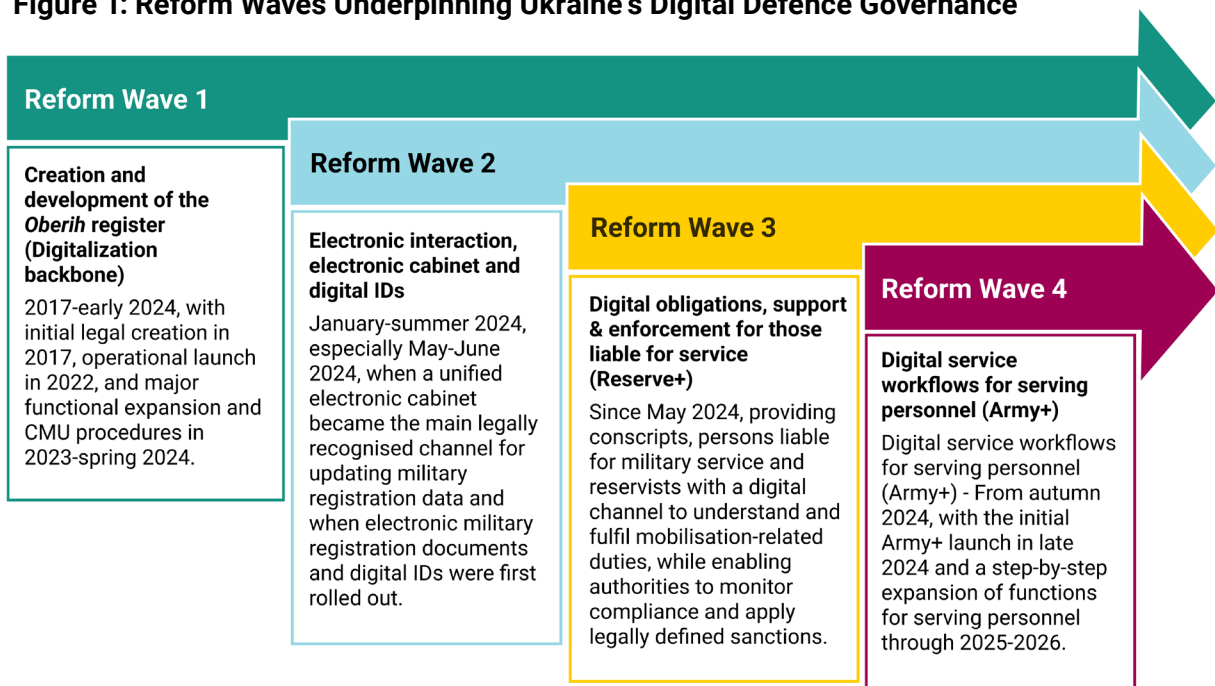
While *Oberih* evolved into the core data backbone, other reforms were necessary to translate its potential into digital tools for mobilisation and military administration. After independence in 1991, Ukraine adopted its own basic laws on defence, military service, and mobilisation, but the underlying systems remained largely Soviet-style: paper-based registration, territorially organised recruitment offices, heavy reliance on local officials' discretion, and top-heavy bureaucratic procedures for routine administrative services.

These foundational laws created the core categories that still matter today – conscripts, persons liable for military service, and reservists – and defined the state's authority to register citizens, call them up, and organise the reserve. What has changed since is less the categories themselves than the way they are administered and connected to citizens' rights and services.

As Russia's war against Ukraine intensified after the full-scale invasion, Ukraine began applying its accumulated digital and legal infrastructure to core tasks of defence governance: mobilisation and personnel management. From 2024, as the government sought to stabilise and strengthen the human resources needed to sustain the country's war effort, Ukraine launched a major push to digitalise mobilisation and military administration, building on the earlier creation of the *Oberih* register.

As such, this reform momentum unfolded in successive waves: first consolidating *Oberih* as described previously, then making electronic cabinets and digital IDs the primary legal channel for interaction, then extending digital obligations and support mechanisms to all those liable for service via Reserve+, and finally digitalising everyday service workflows

**Figure 1: Reform Waves Underpinning Ukraine's Digital Defence Governance**



for active personnel through Army+.<sup>15</sup> Crucially, implementation of both apps has entailed continuous upgrades backed by legal amendments. Across these reform waves, there have also been efforts to embed these tools within broader safeguards, oversight arrangements, and governance standards as part of Ukraine's wider digitalisation agenda, discussed below.

Given the extensive reforms that enabled both Army+ and Reserve+, it is important to recognise the government's systematic approach. While one experimental resolution under martial law authorised specific transfer procedures in Army+, none of the core legal measures establishing either app relied on emergency provisions.<sup>16</sup> Rather, successive laws and Cabinet resolutions expanded electronic processing of military records, introduced personal electronic cabinets and digital IDs, obliged men of mobilisation age to update their data through digital channels, and established data sharing between electronic registers, with Army+ and Reserve+ as key interfaces for millions of individuals. For the full legal evolution and timeline, see Annex 1.

In this context, Army+ and Reserve+ operationalised these legal changes into concrete administrative practice despite some pushback, including within the military.<sup>17</sup> Rather than stand-alone apps, they are policy instruments that express the state's intent to handle sensitive data at scale and its desire to do so in a manner that respects privacy. They also embed transparency and accountability into system design through audit trails based on time and user stamps, standardised workflows, and rights to view and partially correct one's own data within delimited parameters, so that digital systems can both constrain bureaucratic discretion and align everyday governance more closely with legal norms and citizen oversight.<sup>18</sup> Both policy assertions will be assessed below.

---

15 May 2024 marked a key milestone, as the launch of Reserve+ coincided with the enactment of interdependent legal provisions on mobilisation obligations, digital identification, and deferments. This alignment avoided a gap between legal mandate and practical compliance, making the 16 May 2024 package a model of synchronised legal and technical implementation.

16 The legal framework for Army+ and Reserve+ was primarily established through ordinary legislation and Cabinet of Ministers resolutions. An exception is Resolution No. 1297 on experimental transfer procedures in Army+, adopted under martial law as part of a broader practice of experimental resolutions and acts rather than a defence-specific measure.

17 Pushback included scepticism from some commanders and staff who feared losing discretion, added reporting burdens, and reliability or security risks. Army+ and Reserve+ also faced early adoption glitches and user complaints, fuelling concern among some TRSSC staff and commentators about shifting sensitive mobilisation processes into app-based channels. As one official put it: "Getting the data is hard. Processing it is harder. But selling it to the stakeholders and actually making the change – that's where the most important task lies" (Zahorodnii, 2026, interview).

18 In Reserve+, this primarily covers basic personal and contact information (address, phone and email), while allowing users to see how their wider military registration data are recorded in *Oberih*, even where changes require verification or can only be made by authorities.

### 3.3. Ukraine's Digital Door to Defence Governance

For most of Ukraine's post-independence period, military registration and routine military administration ran through dispersed TRSSCs and files spread across the military's bureaucracy, with no single place for people to see or manage their status or engage in 'public services' related to defence. As *Oberih* consolidated data and linked with civil registers while digital records acquired legal force, a front-end limited to TRSSCs and paper files turned into a bottleneck. Created in July 2024 by Resolution 879, the *State Web Portal for Electronic Public Services in the National Security and Defence Sphere* establishes a legal framework for holistic electronic defence-related services. Subsequent amendments in 2025 formally consolidated Army+ and Reserve+ as its core (Cabinet of Ministers, 2025).

The significance of the Portal lies in establishing a legal mechanism that allows *Oberih*-based data to be used in online defence services, thereby transforming a fragmented paper-based administrative model into a single digital channel. As such, the Portal breaks the deadlock between older systems and the newer digitalisation reforms by extending Ukraine's 'digital-first, accounts-based' model, pioneered from *Diia*, into the defence domain.

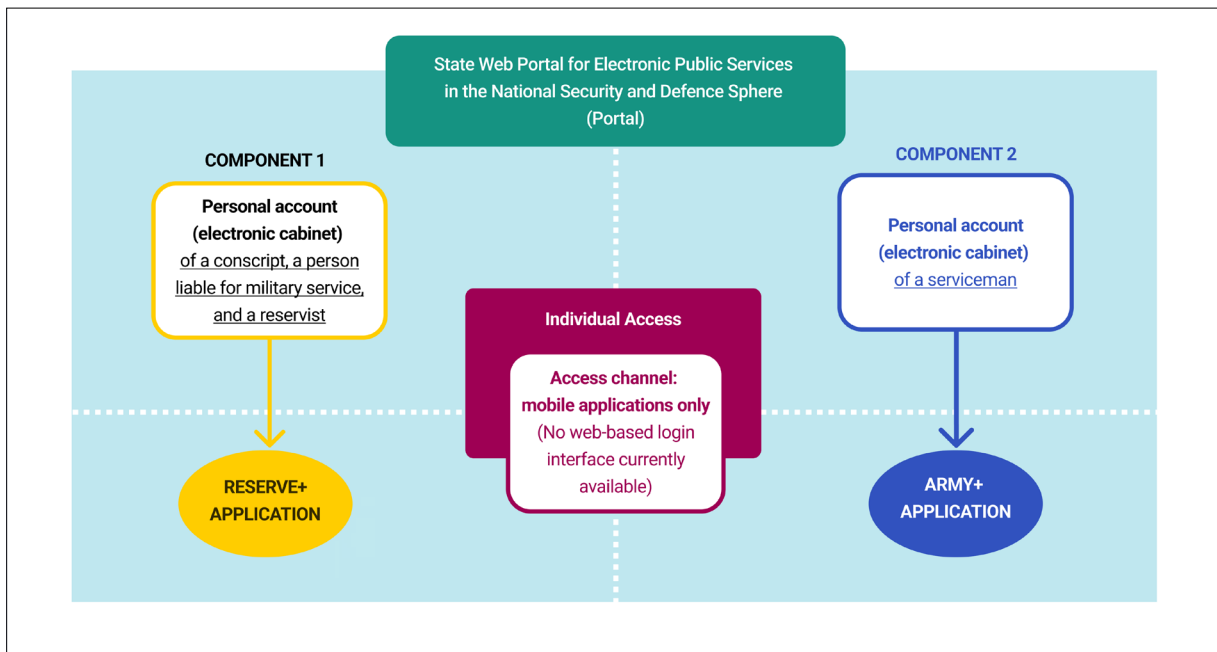
By law, the Portal has two core components each linked to an app: (1) a personal account (electronic cabinet) of a conscript, a person liable for military service, and a reservist and (2) a personal account (electronic cabinet) of a servicemember (see Annex 2). Reserve+ is the primary front-end for citizens to view and update *Oberih* data, while Army+ connects more indirectly until the Military Personnel Registry becomes fully operational, using *Oberih* to identify servicemembers.<sup>19</sup> In effect, the Portal provides one legally defined online doorway where conscripts, reservists, those liable for service, and servicemembers all access defence-related services through personal electronic cabinets.

By doing so, it legally reduces the need and scope for local discretion in TRSSCs and streamlines routine administrative practices for serving personnel. As such, the Portal and its tools both facilitate and mediate electronic interaction between state data registers and individual user accounts. By acting as a horizontal integration layer between *Oberih* and more than a dozen other state registers, it makes large-scale automation of mobilisation, services, and verification legally and technically feasible. In effect, the Portal, via Army+ and Reserve+, gives every conscript, reservist, and servicemember a single digital channel to update data, receive decisions, and present a verifiable status without going through local offices each time.

In contrast to *Diia*, which also has a 'State Web Portal' accessible via both website and app, the Portal, for now, currently remains accessible only through the Army+ and Reserve+ applications.<sup>20</sup> The Portal's structure is illustrated on the next page.

19 As noted by one of the registry's designers, the Military Personnel Registry will be able to answer additional questions: "Army+ right now doesn't know whether [a person] is a major or a lieutenant, whether he serves for the Defence Ministry or a different unit, how much government materiel he has – what kind of weapon and so on – what his rights are, how much money he's received and how much they still need to pay me so on" (Post, 2025).

20 *Diia* itself is formally defined as a 'Unified State Web Portal of Electronic Services "*Diia*" with a web portal plus a mobile app' (State Enterprise *DIIA*, 2019). Hence, both *Diia* and the defence Portal follow a similar architecture: a unified state web portal defined in resolutions, combined with mobile applications that provide personal electronic cabinets linked to underlying state registers.

**Figure 2: Components of Defence Portal**

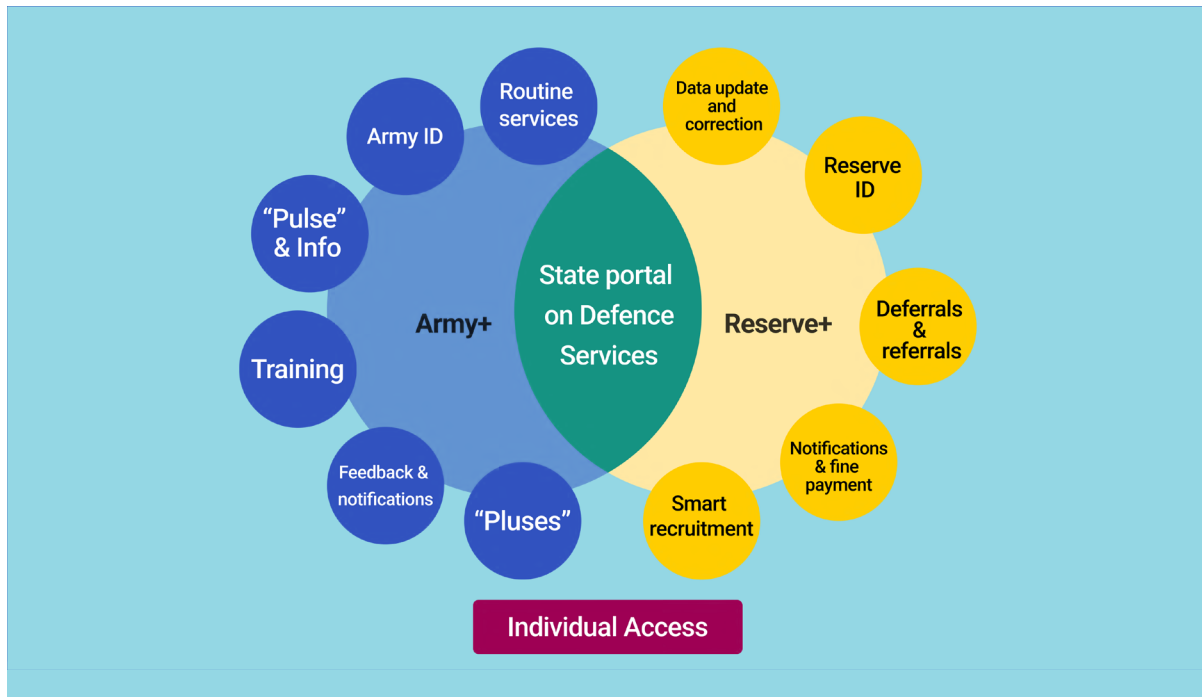
### 3.4. Data Governance in Army+ and Reserve+

Because Army+ and Reserve+ handle large volumes of highly granular, personspecific data, their operation and safeguards are governed by each app’s dedicated legal provisions. Their privacy notices define which categories of information they collect and process, but they do so using noticeably different grouping logics.

Reserve+ organises personal data into three main groups: authorisation data, data refined directly by the user, and data received from the Unified State Register and displayed in the application. Within this structure, it covers core identification and contact details, military registration and specialty data, medical and deferment information, and the user’s registration status with the relevant territorial recruitment centre and social assistance offices (Ministry of Defence, 2024b).

The Army+ Privacy Notice, by contrast, distinguishes between data required for authorisation and data processed for the provision of services (Ministry of Defence, 2024c). The first category covers basic identification details and status, while the second covers information needed to deliver services, track the progress and outcomes of applications and appeals, handle complaints and email communications, draw on relevant registry data, and support authentication and software operation.

In essence, Reserve+ provides a more detailed, categorybased breakdown – especially of registry data – while Army+ adopts a broader, functionoriented approach that links data processing directly to service delivery and system functioning.

**Figure 3: Accessing a Holistic Range of Services across the Defence Sector**

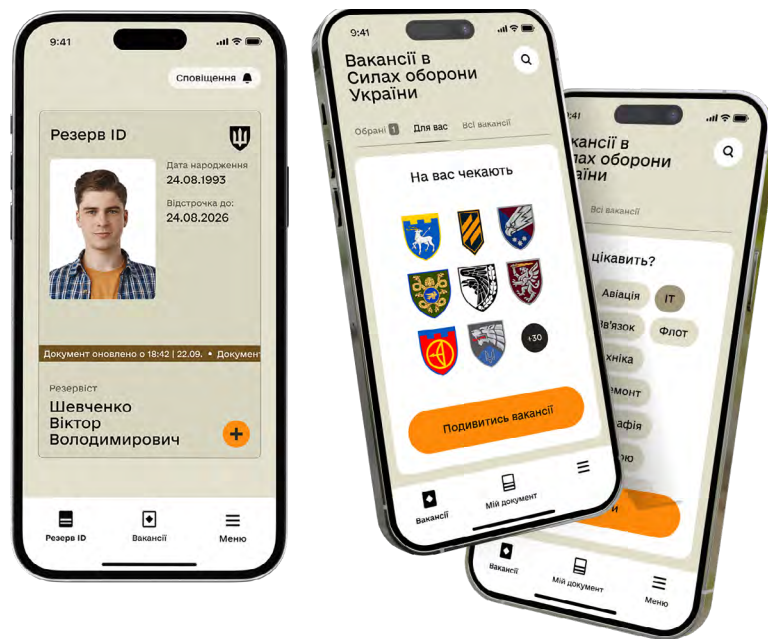
The formal governance of *Oberih*, the Portal, and their associated applications sits primarily with the Ministry of Defence, which is legally designated as the register holder and overall responsible body.<sup>21</sup> Other state institutions play defined roles: some operate the underlying registers and infrastructure; others set access rights or issue dataprotection and cybersecurity standards; and specialist regulators conduct inspections to ensure compliance with national law.<sup>22</sup>

#### Section 4. What Army+ and Reserve+ Do

**H**aving set out the legal and institutional foundations in Section 3, this section examines how Army+ and Reserve+ together form a digital layer of defence governance that reaches from conscription and reserve management to everyday life in uniform. Rather than narrow ‘HR apps’, the section shows how they address core needs for sustaining Ukraine’s national defence: from updating mobilisation data and holding digital IDs to handling transfers, accessing benefits, lodging applications, and interacting with commanders.

21 Under the Law of Ukraine on the Unified State Register of Conscripts, Persons Liable for Military Service and Reservists, the Ministry of Defence is defined as the Register Holder (legal owner) responsible for *Oberih* and the Defence Portal; the General Staff of the Armed Forces acts as the Register Manager; and the Security Service of Ukraine together with Ukraine’s intelligence agencies are designated as bodies responsible for administering and maintaining the Register (Verkhovna Rada of Ukraine, 2017).

22 For example, civil registries and tax authorities supply underlying population and employment data; specialised state IT enterprises host and administer the relevant databases; and dataprotection and cybersecurity regulators issue technical standards and conduct inspections to ensure compliance with national law.



#### 4.1. How Reserve+ Works

*If you want to build something like this: create your register first.  
Then give people a useful instrument to communicate with it.  
(Korzh, 2026, interview).*

By early-2026, Reserve+ provides registration services for over six million citizens of mobilisation age (17–60), allowing them to manage their conscription and reserve status (Mazur and Lanchukovska, 2025). It pulls data directly from *Oberih* and shows an up-to-date digital ID with their category – conscription-age, liable, reservist, deferment, reservation – and the date of the last update, turning an opaque paper file into a visible digital profile that can be shown to state authorities when needed. Identity is verified via secure authentication (e.g., BankID), after which users access a personalised interface with their status, key data fields, and an auditable trail of changes, including partial self-corrections. Reserve+ provides five core functions to citizens of mobilisation age.

1. **Self-service data update and correction:** the app allows users to view key personal data (see Annex 3) and submit partial corrections if information is missing or incorrect, all without visiting a TRSSC aside from limited circumstances.<sup>23</sup> Requests are sent to the TRSSC automatically for verification and once approved, changes are reflected in *Oberih* and hence the app.
2. **'Reserve ID' – electronic military registration document with QR code:** Reserve+ lets users generate an electronic military registration document that has the legal force of a paper document and includes a photo and QR code. Reserve ID is the main document for conscripts and reservists. The QR code can be scanned by TRSSC staff or police to instantly verify a person's registration status, and the

<sup>23</sup> For example, users may still need to visit a TRSSC in person to resolve complex status issues (such as when data are not found in *Oberih*, multiple conflicting records exist, or a change affects their legal mobilisation category), or where law requires physical verification of identity or documents before a change can be confirmed.

system automatically invalidates non-active IDs (those with missing or outdated data) when QR codes are scanned.

3. **Deferment requests, medical referrals, and summons validity:** Users can submit electronic requests for deferments or extend existing deferments through the app, with many categories now automatic, such as for students and people with disabilities.<sup>24</sup> The app allows users to request and receive an electronic referral to the Military Medical Commission without personally visiting a TRSSC. Users can also check the validity of a paper summons via a QR code accessed by the app, helping distinguish genuine documents from fakes.
4. **Notifications on violations with fine payment:** Reserve+ informs users about possible violations of military-registration rules (e.g., out-of-date data) and clarifies their obligations under current legislation. This makes enforcement more rules-based: the system shows what is required and flags issues before they become legal problems. Where applicable, Reserve+ also allows users to pay fines directly, offering a discount for timely digital payment.
5. **'Smart recruitment' – vacancies and pathways into the Armed Forces:** Reserve+ includes a job-search function that lets users browse vacancies in the military and apply for roles that match their skills and status. This reframes part of mobilisation as matching people to roles rather than only as compulsory call-up. As Ukraine expands the range of contract types offered for military service, Reserve+ also supports those applying to better understand their options.<sup>25</sup>

---

24 By illustration, other categories eligible for automatic extension include single parents of children under 18, parents of seriously ill children without disability status, spouses of military personnel with a child, parents of three or more children in one marriage, close relatives of posthumously awarded Heroes of Ukraine, and persons whose spouse has a disability

25 For example, Ukraine's evolving contract system now includes the experimental '18–24' one-year contract with enhanced pay, bonuses, and social guarantees for young volunteers, alongside a broader framework of fixed-term contracts (typically ranging from one to five years) with differentiated financial terms and benefits. These options are a national priority intending to support a more recruitment-led mobilisation model, help attract critical skills, and offer clearer, timebound service commitments compared with open-ended mobilisation.

Reserve+ provides wider institutional services to the state. For TRSSCs, it delivers cleaner, regularly updated data into *Oberih* without manual data entry, as citizens can view their records and correct contact details digitally. Routine handling of deferments and medical referrals is partly automated and standardised, reducing front-office workload at TRSSCs and helping align decisions with national rules (SUD. UA, 2026). Easier status verification through Reserve ID saves time for enforcement officers out in communities and cuts in-person disputes around paper documents. System-generated notifications and integrated fine payment make enforcement of registration obligations more systematic and predictable, rather than ad hoc. Lastly, the vacancies module functions as a recruitment funnel, surfacing candidates and matching them to open roles across the Armed Forces.

For Ukraine's national leadership, those entrusted with a strategic perspective, Reserve+ is a key interface enabling the *Oberih* register to be continuously updated with cleaner, more timely data.<sup>26</sup> This situational awareness of the mobilisation pool is fundamental to designing national strategies to manage and utilise it.<sup>27</sup>

26 As one interviewee noted, a key merit of Ukraine's approach is that it can plan in detail, including for the future: "Data should be used for forecasting, not just for accounting" (Pravdyvets, 2026, interview).

27 As one interviewee noted: "The old paper system was a Soviet legacy -- the information authorities held was outdated. You simply could not know the correct numbers. The key purpose of Reserve Plus was to see how many people were actually still in Ukraine and how to reach them" (Shestakov, 2026, interview).

## Box 2. Reserve+ and Managing the Complexity of Deferments

Deferment from conscription during mobilisation means a temporary exemption from military service granted in cases explicitly provided by law; it does not permanently eliminate the possibility of conscription but only postpones its potential activation. Managing deferments, of which there are 35 grounds, is an inherently complex process given that they cover a wide range of personal circumstances (Mezha, 2025). Justifications for deferments can be clustered into four main areas: health-related, family-care and parenthood, education, and professional-activity grounds, specifically 'reserved' employees in critical sectors. Previously, managing deferments consumed a significant amount of administrative capacity given the need to collect hard-copy documents from a wide range of government agencies. Reserve+, using the backend depth of *Oberih* and its automatic data sharing with other digitalised state registers, provides significant efficiency and transparency gains to an otherwise cumbersome, obtrusive process by digitalising deferment processes, specifically initial requests and extensions. As of early February 2026, more than 60% of new applications for deferment now start via Reserve+ rather than through in-person TRSSC visits (Korzh, 2026, interview). Moreover, approximately 90% of granted deferments were extended automatically (Ministry of Defence, 2025c). This represents a major time savings for both TRSSCs and individuals as there is no need for additional supporting documents or an in-person visit to TRSSCs. In terms of interactions, users of Reserve+ receive a push notification indicating a scheduled extension. After processing, a confirmation of extension is displayed.



## 4.2. How Army+ Works

Army+ is a secure, all-in-one service hub for Ukrainian servicemembers, acting as a key interface between each individual soldier and the state (Bondar, 2025). As of February 2026, Army+ had approximately 1 million users spread across over 1,700 units (Ministry of Defence of Ukraine, 2026). By providing a wide range of routine services and information sources, the app aims to reduce the daily burden on servicemembers as they manage their administrative interactions with the defence bureaucracy.<sup>28</sup> Institutionally, it enables the military to process large volumes of data digitally, replacing paper-based systems that previously constrained operations (see Annex 4). Army+ provides six core services to individual military personnel.

- 1. Routine services and report workflow:** Army+ replaces paper reports with standardised electronic forms that soldiers can fill, sign and submit directly in the app. By February 2026, over 50 standard electronic report types were provided, covering most everyday interactions a soldier previously handled through paper and in-person visits (ArmyInform, 2026). Army+ organises its functions in a 'Services' section, grouped to cover leave, payments, health, document issuance, training, change of duty station, and discharge from service. In 2025, over 1.5 million reports were submitted on Army+ (Ministry of Defence of Ukraine, 2026).

<sup>28</sup> As noted by Rustem Umerov, then Defence Minister: "Excessive paperwork that slows down the efficiency and quality of service is one of the most frequent complaints I hear from the military. Efficiency and quality help us to hold our own in the war against the Russians. I believe that Army+ and the digitalisation of the army, in general, will significantly strengthen these components" (BRDO, 2024b).

A guided 'constructor' helps individuals select the appropriate report type and complete the required fields (Novyny.live, 2024a). Commanders receive reports in-app, approve or reject them, and must give reasons for any rejection. All users apply e-signatures, creating a transparent, traceable workflow. A dedicated notification area lets servicemembers track messages and outcomes, reinforcing the app's role as a central interface for their administrative and service-related interactions with the military.

Notably, transfers can now be requested and are required to be processed within 72 hours by the relevant commander.<sup>29</sup> Transfers permissible within Army+ are limited to certain circumstance, notably from non-combat to combat units and between the latter.<sup>30</sup> Moreover, personnel can withdraw submitted reports if circumstances change, and commanders can view the full approval chain and prior decision stages. Given this capacity, the Army+ generates important contextual information around requests. For example, per unit, Army+ generates data that shows how many requests were made and how many were approved, effectively highlighting concerns about incompetent commanders (Post, 2025).

A built-in 'Army ID Directory' lets users view the IDs of commanders, acting commanders, and administrative officers, enabling one-click insertion of the correct addressee when filing a report. Document capture is integrated: servicemembers can upload supporting documents via a camera, with automatic recognition and scanning plus duplicate-document warnings, which improves data quality and reduces administrative clutter.

Digitised reports, for illustrative purposes, include service certificates (to access benefits such as priority kindergarten placement), leave requests for travel outside the garrison, healthbased duty exemptions, and onetime payment requests for a first contract. They also cover postcaptivity leave requests, onetime financial assistance linked to disability or partial loss of working capacity, blood donation and income certificates, certificates on injury circumstances, dismissal upon reaching the age limit, family circumstances and childcare-related leave, and requests to update bank details for salary and bonus payments. As of February 2026, the most popular reports were annual leave, medical rehabilitation benefits, and transfer requests<sup>31</sup>

29 72 hours is the timeframe permitted for the commander to approve or reject the request. Moreover, moving to the new unit takes on average two weeks, which is much quicker than the three to nine months previously (Ministry of Defence of Ukraine, 2026).

30 A soldier submits a transfer request in Army+ with basic credentials and, where applicable, a recommendation from the receiving unit or a medical commission; the report goes directly to the Armed Forces Personnel Centre, which must issue a reasoned decision within 72 hours and may seek the commander's opinion in sensitive cases such as moves between combat and rear brigades or for officers. Transfers are limited to one per year and can be refused on operational grounds (for example, if the unit's manning is deemed critical), so while the app standardises the procedure and timelines, final decisions remain constrained by commanders' assessments of staffing needs and combat readiness.

31 The specific breakdown (to February 2026): Annual leave – 29%; Report on health leave – 20%; Change of place of service – 13%; Report for obtaining a F5 certificate – 11%; Return from vacation, business trip or recovery/ sick leave – 4% (Ministry of Defence of Ukraine, 2026).

2. **'Army ID':** The Army+ app provides a basic digital military ID showing a photo and limited data. For now, its functionality is still under development. Over time, it is expected to link directly to official personnel records, allowing servicemembers to prove their status comprehensively. At present, the digital ID in Army+ is mainly used to route reports to the correct commander. As such, Army ID complements but does not yet replace the paper identification documents necessary for enabling secure military access.
3. **Information and 'Pulse' feed:** Through its 'Pulse' news feed and a collection of reference materials, Army+ functions as an information channel about rights, obligations, and practical service issues. For instance, informational videos can be shared quickly to explain day-to-day insights for soldiers on the frontline. Moreover, soldiers can see official explanations of benefits, procedures, key updates, and typical problem cases, reducing dependence on informal word-of-mouth explanations and helping to standardise how rules are understood in and across units (InterfaxUkraine, 2025). A notifications section aggregates important administrative messages and reports reminders over time.
4. **Training courses:** Army+ integrates online training courses directly into soldiers' smart phones, starting with modules on cybersecurity. This allows commanders and the MoD to push targeted learning content into units and track completion, effectively turning the app into a lightweight education platform for everyday use. Training modules include skillsets – such as basics of UAVs, financial literacy, mental health, and battlefield communications – as well as training on other components of the MoD's digital ecosystem, including DELTA, DOT-Chain Defence, and Impulse.<sup>32</sup> By the end of 2025, 18 training courses were provided; 200,000 personnel had started at least one course over 2025, with 90,000 courses being completed during the year (Ministry of Defence of Ukraine, 2026).
5. **Surveys:** Army+ also has survey functions allowing the military to conduct routine surveys to gauge morale and assess priority needs of its forces. By the end of 2025, 20 surveys had been conducted, based on 494,000 responses, covering pressing topics such as perceptions regarding medical care and service standards in hospitals, Basic General Military Training, and options for improving transfers (Ministry of Defence of Ukraine, 2026). Alongside meeting wider policy interests, these surveys directly inform further development of Army+, for instance adding electronic forms, survey topics, and training courses.
6. **Pluses Discounts:** With support from large Ukrainian firms, Army+ displays discounts offered to servicemembers, who in turn can share them to their families, covering a range of everyday needs, such as petrol, food and beverages, clothing, cinema and transportation tickets, field kit, pharmaceuticals, and access to business loyalty programmes.<sup>33</sup> By the end of 2025, Pluses discounts were supported by 15 partners, and discounts were used over 8 million times (Ministry of Defence of Ukraine, 2026).

32 DELTA is a digital situational awareness system; DOTChain Defence is an eprocurement and logistics platform; and Impulse is an internal communication and workflow tool within the Ministry of Defence's digital ecosystem.

33 Pluses discounts are a very popular function of Army+. The feature was designed to ensure confidence in users, as one interviewee noted: "We didn't want soldiers to feel that humiliation of asking, 'Do you have a discount for military?' Your whole perception shifts when there's a sticker that simply says: we're happy to have you here" (Romaniukov, 2026, interview).

While Army+ provides many services direct to individuals, it also plays a larger institutional role for the military (Sukhankin, 2024). For commanders and the wider military institution, Army+ provides a set of concrete services beyond easing individual soldiers' administrative burdens. First, it standardises and digitises routine workflows, giving commanders a single channel to receive, track, approve, or reject reports with full visibility over the approval chain and better evidence for decisions. Second, it improves data quality and timeliness: electronic reports, integrated document capture, and automatic checks (for duplicates and missing fields) feed cleaner information into personnel systems and reduce errors from manual paperwork. Third, the Pulse feed, training modules, and survey tools give senior leadership a direct communication and sensing layer into the force, allowing faster dissemination of guidance and more structured collection of bottom-up reactions concerning equipment, logistics, and unit conditions.

### 4.3. Data Security and Privacy Protections

Army+ and Reserve+ apply layered security protocols and privacy safeguards. They handle highly sensitive personal and service data and operate under the MoD's cyber-defence architecture.<sup>34</sup> The apps work as secure interfaces to protected state registries (notably *Oberih*) rather than standalone databases, pulling only the data needed for specific services and avoiding unnecessary storage on personal devices. Security is enhanced through cryptographic data encryption, and public announcements stress installing the apps only from official sources to avoid malicious clones and malware (New Voice of Ukraine, 2024).

Privacy in Army+ and Reserve+ rests on minimising data exposure and tightly controlling who can see what. Access to the apps is mediated through strong 2-factor authentication, using Bank ID, and role-based permissions, reducing the risk that commanders, clerks, or third parties can browse data beyond their remit. On the backend, all actions that change personal records are logged with timestamps and user identifiers, creating an audit trail that can be checked in case of abuse or suspected unauthorised access. This design aims to ensure that any misuse can be traced and sanctioned.

*Oberih* is central to both apps' privacy and security. As a national critical-infrastructure asset, it is subject to strict role-based permissions, limited to authorised bodies, and carries strict legal liability for misuse.<sup>35</sup> In practice, Army+ and Reserve+ serve as narrow, user-facing

“

Ukraine's ability to adjust without losing its democratic soul is a strategic asset, not just a technical one.

”

34 Army+ and Reserve+ operate in a high-threat environment where Russian state and aligned actors use fake military-themed apps, malware, DDoS and intrusive probing to steal data, disrupt services, and track users, yet available evidence suggests no publicly reported major or lasting compromises of Ukraine's core defence digital services, with key registers and applications, including those linked to Army+ and Reserve+, continuing to function.

35 Under Ukraine's Law 'On Critical Infrastructure', systems whose disruption could significantly harm national security and mobilisation capacity qualify as critical infrastructure, such as *Oberih*. Illegal interference (e.g., entering fictitious deferrals or falsifying medical commission results) is prosecuted under severe Criminal Code provisions, with cases already opened against TRSSC officials for unauthorised modification of records (Office of the Prosecutor General, 2026).

‘tunnels’ into different registers, including *Oberih*, accessing only the specific fields needed for a given service (Romaniukov, 2026, interview).<sup>36</sup> This architecture lets the apps minimise what they store locally and instead rely on a system that is tightly regulated by law, has controlled institutional access (MoD, General Staff, TRSSCs), and logs every data change with an electronic signature to reduce human error and corruption. Despite Russian cyberattacks, *Oberih*’s security has been fully preserved, ensuring that critical services, including Reserve+ and Army+, continue functioning. Overall, MoD registries provide a hardened central ledger with strong legal, technical, and audit controls, while apps such as Army+ and Reserve+ add API-level safeguards on top, so security rests on a combined, defence-in-depth design rather than any single component (Zahorodnii, 2026, interview).

“

This sense of fairness is a critical driver of morale: soldiers and their families are more likely to accept ongoing deployment if they believe the rules of service are applied broadly and transparently.

”

## Section 5. Adaptive Governance in a High-Intensity War

*Ukraine’s most strategic asset has been its capacity to learn, evolve, and rewire its defence institutions under the pressures of full-scale, high-tech combat*  
(Bondar, 2025).

In protracted wars, countries win or lose not only on the battlefield but in how they mobilise and manage human resources. For democracies, these pressures cut deeper, because consent and legitimacy must be sustained even as the state demands more from its citizens. One solution is adaptive governance: continually adjusting rules, allocations, and procedures as the war evolves, while still operating within legal, transparent, and accountable bounds.

Ukraine’s digital defence governance tries to hard-wire adaptive capacity into day-to-day warfighting, with an emphasis on maintaining asymmetric advantages against a larger enemy (Ministry of Defence, 2024d). Moreover, the country’s ability to adjust without losing its democratic soul is a strategic asset, not just a technical one.

This section unpacks these dynamics in practice: how Ukraine uses digital tools to bolster its war effort in a recognisably democratic fashion while making defence governance more sustainable in a long war, and where the limits lie when technology cannot substitute for hard political choices.

<sup>36</sup> Army+ and Reserve+ secure user sessions, communications, and app logic but only touch subsets or limited ‘views’ of the data that reside in *Oberih*, which reduces exposure if a device or account is compromised.

## 5.1. Turning Adaptive Governance into Combat Power

**Real-time policy responses in a long war:** The biggest policy challenge Reserve+ addressed was the lack of complete, reliable data in *Oberih* after the full-scale invasion. Using the app from mid-2024 to update and then maintain records for millions of people was a major achievement.<sup>37</sup> With personnel data consolidated in a single authoritative system, government leaders see in real time who is available, where they are, and in what condition – giving them live visibility into manpower readiness (Chernohorenko, 2025).

Built on legal reforms and the *Oberih* register, Army+ and Reserve+ act as instruments of continual policy adjustment: new laws, Cabinet decisions, and MoD orders become updated workflows and forms, enabling ‘policy prototyping’ in which changes – such as new transfer procedures – can be tested, tuned, rolled back, or extended in days rather than months, helping to prevent overload and reform fatigue. This infrastructure creates a ‘policy-to-user’ pipeline: when a new law or cabinet decree is issued, it is operationalised as a digital workflow rather than a manual routine. This is adaptive governance in practice: strategic decisions rapidly become operational rules at scale.

**Matching people to roles at scale:** Digitalisation gives Ukraine a realistic pathway to smarter mobilisation by adding the ability to directly recruit via Reserve+. The app features more than 13,000 vacancies at any one time, including on civilian platforms like Lobby X and Work.ua, allowing users to filter roles based on civilian expertise such as IT or UAV piloting (Ministry of Defence of Ukraine, 2026). Reserve+ also allows a ‘direct-to-unit’ pathway for citizens to apply directly to specific brigades or technical roles via Reserve+, rather than entering through a generic mobilisation pool. While this feature is still limited in scale, it can be expanded and builds combat power by ensuring that high-value specialists – such as engineers or drone pilots – are placed according to their civilian expertise rather than assigned randomly by TRSSCs (Volovina, 2026, interview). Similarly, the training courses provided via Army+ turn it into a channel for upskilling, with over 200,000 service members started specialised courses by the end of 2025 (Ministry of Defence of Ukraine, 2026).

Army+ is steadily replacing the slow, paper-based system for transfers, transforming the process into a more transparent digital workflow. This shift narrows the scope for unchecked discretion through real-time status tracking.<sup>38</sup> While this feature is limited to certain categories of service members and maintains commanders’ ultimate authority, it demonstrates the military’s greater openness to placing individuals where they feel they

37 By the end of 2024, approximately 3.5 million people had registered in Reserve+, followed by another 2.5 million by the end of 2025 (Ministry of Defence of Ukraine, 2026). These figures suggest that Reserve+ enabled an unprecedented largescale ‘cleansing’ and completion of *Oberih* in a matter of months which, if attempted through inperson visits alone, would likely have taken years. Given this, Reserve+ significantly narrowed the mobilisation ‘data gap’ opened by Russia’s 2022 full-scale invasion.

38 Transfers have become one of the most contentious issues in Ukraine’s Armed Forces because they determine soldiers’ exposure to risk, quality of leadership, and proximity to family support, so blocked or arbitrary moves are felt as questions of basic fairness and survival. Complaints centre on opaque, inconsistent handling of requests, suspicions of favouritism or ‘connections’ shaping who gets moved, and the experience of being trapped in frontline units under weak or dysfunctional commanders while others appear to cycle out more quickly.

are best used.<sup>39</sup> The aim is to mitigate longstanding tensions about fairness in transfers, including over command performance. This digitalisation has slashed processing times from months to, in many cases, just a few days. Even though transfers aren't allowed from combat to support units, by successfully moving over 55,000 personnel by the end of 2025, this capacity nonetheless helps improve morale across extensive frontlines in a protracted war, what has been one of the most contentious issues of service in Ukraine's military (Ministry of Defence, 2025d).

**Cutting administrative drag:** Under a design ethos of 'let[ting] technology manage processes, so people can manage missions', both apps have significantly reduced administrative burdens.<sup>40</sup> Army+ has fundamentally altered the daily administrative burden for Ukrainian service members by digitising the traditional report. Fifty different templates cover the bulk of routine administrative needs. For commanders, multi-signature functionality allows them to process dozens of leave or equipment requests simultaneously rather than signing individual paper files by hand (Ministry of Defence, 2025e). At the same time, a mandatory response rule obligates them to respond within 72 hours. This 'anti-ghosting' mechanism prevents applications from being lost in bureaucratic delays as the system provides transparent tracking. By early 2026, this accountability loop had processed over 1.2 million electronic reports, representing major savings in man-hours per month across the force (Ministry of Defence, 2025d).

Most significantly, TRSSCs' front office workload has fallen markedly because of Reserve+'s efficacy (BRDO, 2025).<sup>41</sup> Key to this was replacing millions of annual physical visits with digital processing of the most common types of interactions: deferment requests, contact updates, and the issuance of paper documents. Deferments, especially medical, had been especially onerous to manage as well as susceptible to corruption (Fornusek, 2023). By lightening the bureaucratic load on TRSSCs, the policy intent is to allow staff to concentrate on more complex cases and shift from policing routine process enforcement towards recruitment. Digitalisation also reduces a major tension of civilians fearful long fearful of visiting recruitment centres even if they want to comply with mobilisation obligations.<sup>42</sup>

39 Maintaining this sense of fairness and purpose is also essential to reducing desertions. As one interviewee noted: "80,000 people applied for transfers. We estimate roughly 30,000 desertions probably were prevented. That's one Army Corps. That's not a small number" (Zahorodnii, 2026, interview).

40 As Kateryna Chernohorenko, former deputy minister of defence, noted: "Reserve+ and Army+ saved Ukraine over 70 million hours of administrative time for both soldiers and government staff, the equivalent of over 8 billion UAH (\$200 million) in direct and indirect economic value, and eliminated billions more in potential corruption risks by closing loopholes for unofficial 'expedited payments'" (Chernohorenko, 2025).

41 As one interviewee noted: "The conscription centres' job is to make new soldiers -- not to process deferments. Yet 70 % of their workload was exactly that. We changed it" (Romaniukov, 2026, interview).

42 As one conscript noted after Reserve+ went active in 2024: "I was not so much afraid of the potential service in the Armed Forces as much as the bureaucratic hell that I had to face in the enlistment office" (Khalilova, 2024).

## 5.2. Sustaining Consent in a Hard War

*The best thing you can do for your army  
is care about your soldiers -- and don't be afraid  
to throw out processes that are 20 or 30 years old.*

– Roman Zahorodnii (2026, interview).

In a long war, the democratic legitimacy of a state hinges on whether mobilisation and service feel equitable, legible, and more participatory. When these traits are present, citizens are more likely to accept prolonged mobilisation and its costs. This section explores how Ukraine's digital defence governance seeks to make mobilisation and service more legible and rule-bound, while giving citizens and servicemembers greater capacity to understand and, at times, shape what happens to them. In this sense, adaptive governance is about illuminating and moderating state power to preserve consent.

**More Equitable:** Improving a sense of fairness is imperative as war stretches on across a fatigued society. Reserve+ and Army+ redistribute authority and discretion through digitally defined workflows, so that decisions following rule-bound processes become more predictable for all and therefore easier to accept. The use of electronic signatures within Army+ creates an auditable trail of identifiable, traceable decision points for every request.<sup>43</sup> To reinforce this, the Ministry of Defence introduced a mandatory 72-hour response rule for commanders in late 2024: if a digital report is not addressed within three days, the system flags the delay, tying personnel decisions to documented rules rather than arbitrary preferences. Standardising routine processes is essential for maintaining the social contract during a high-intensity war.

By narrowing opportunities for petty corruption and 'ad hoc' bargains, the state reduces the perception that the system is being gamed by the wealthy or well-connected.<sup>44</sup> Automated deferments through Reserve+ for most eligible categories sharply cut perceptions of favouritism at TRSSCs. This sense of fairness is a critical driver of morale: soldiers and their families are more likely to accept ongoing deployment if they believe the rules of service are applied broadly and transparently. Enforcement mechanisms – including summons, fines, and compliance checks – are also moving into rule-bound and app-mediated channels, replacing opaque street-level encounters with clearer and less arbitrary procedures.<sup>45</sup> Between those

43 One interviewee noted: "Before, a report could disappear -- deliberately or accidentally. Now it's in the system, and there is a defined response time and a specific person. That changes everything" (Zahorodnii, 2026, interview).

44 "You cannot change anything quietly – all changes are logged in the system, so any illicit action will be noticed. The system is smarter than people" (Korz, 2026, interview).

45 A mid-2025 reform allowed citizens to resolve military registration violations directly via Reserve+, offering a 50% discount on fines if settled within 20 days, and replacing opaque street-level encounters with a more transparent digital process in which sanctions are clearer and less arbitrary. The universal QR code gives citizens a verifiable ID to instantly prove their legal status, reducing the risk of wrongful detention. Adaptive governance here lies in recalibrating enforcement tools so that they remain firm but predictable, keeping coercion inside a visibly legal and reviewable frame.

facing mobilisation and those already in service, perceptions of fairness are mutually reinforcing. Failures on either side risk undermining willingness to sustain the war effort.<sup>46</sup>

“

Even the best-designed digital systems risk feeling like tools for locking people into endless service rather than mechanisms for managing finite commitments.

”

**More Legible:** In a long and difficult war, people are more likely to accept mobilisation when they clearly understand the ‘rules of the game’. Through personal cabinets in Reserve+ and Army+, individuals can now track and increasingly trigger decisions on their status, deferments, and benefits. The universal QR code in Reserve+ allows citizens to prove their legal status instantly to any official, replacing vulnerable paper documents with a single, verifiable source of truth. Audit trails and standardised workflows in Army+ and Reserve+ record who accessed which data, when and on what basis, making it harder for local officials to bend rules for personal gain. By early 2026, the *Oberih* register’s integration with over a dozen other national databases means that compliance is checked against real-world information such as tax and residency records, providing leaders with defensible evidence when asking society to bear the war’s costs and giving citizens clearer grounds to judge whether mobilisation is being applied fairly.

**More Participatory:** As Ukraine has moved to a mixed model of mobilisation, digital defence governance aims to shift citizens and soldiers from being purely passive subjects to playing an increasing role in how their obligations are organised and met. By allowing users to comprehensively view and partially update their own data – something over six million Ukrainians now do through Reserve+ – the state grants a form of ‘functional agency’ that keeps records accurate without intermediaries. This is adaptive governance turned inward: the state continually re-tools its interfaces to keep individuals engaged rather than alienated. By treating the soldier as a stakeholder, the digital state seeks to reinforce a sense of participation that underpins legitimacy in a high-intensity war rather than mere compliance born of fear or confusion. Digitalisation also lets the state to identify and address problems – such as training gaps – before they erode morale. The Army+ survey module enables large-scale, anonymous participation in polls on contentious issues like basic training and transfer access. Here, adaptive governance means not just changing rules from above but doing so in response to structured feedback from below.

<sup>46</sup> As one sectoral expert noted: “The main communicator of any army is the soldier, not the press officer. Information from the front spreads instantly – and this shapes whether people are willing to serve” (Muraveinyk, 2026, interview).

### 5.3. Hard Political Choices and the Reach of a Wartime Digital State

*The issue of mobilisation is a matter of fairness, conditions of service, and trust in the state -- digital applications alone cannot solve this.*  
 – Liliia Oleksiuk (2026, interview).

Even as Reserve+ and Army+ make mobilisation and military administration more streamlined and rule-bound, they also deepen the everyday reach of Ukraine’s digital defence governance into citizens’ lives. In this role, they concentrate public concerns about how far control can extend and how safely data are handled, especially during wartime.<sup>47</sup> On their own, digital products cannot resolve the deeper political and human pressures of a long war, most pressing being that of trust and the primal fear of war itself (Méheut, 2025).<sup>48</sup> Ukraine’s manpower situation, despite its significant efforts, remains pressing, as acknowledged by its senior most leadership.<sup>49</sup> This section examines the operational strains and societal concerns that now surround Ukraine’s digital defence governance.

Technology cannot replace hard political decisions: Ukraine may sit at the global forefront of digital mobilisation, but its efforts are constrained by mounting societal fatigue, pervasive fears about inadequate training and equipment at the front, equity problems in ‘reservations’ for critical industries, and growing economic worries as households and employers lose working-age men (Hedenskog and Umland, 2025). Each new wave of call-ups feels less like a temporary emergency and more like an open-ended drain on families, communities, and key sectors, sharpening questions about who serves, for how long, and on what terms.

Most pressing is the absence of a clear demobilisation policy for those who have already served for years on brutal frontlines. This uncertainty corrodes consent: people who volunteered or accepted early call-ups now face effectively indefinite service until the war’s end.<sup>50</sup> In that context, even the best-designed digital systems risk feeling like tools for locking people into endless service rather than mechanisms for managing finite commitments. Without a credible demobilisation horizon, adaptive, app-mediated defence governance cannot answer the core question that weighs most heavily: whether service has become a one-way street.

47 In many ways, fears over Army+ and Reserve+ also match earlier, but still ongoing discussions, about Ukraine’s wider ‘digital state’ approach (Bohdanova, 2021).

48 As one interviewee noted: “The issue of trust in the state is the main challenge for the entire digital system” (Oleksiuk, 2026, interview).

49 As Mykhailo Fedorov, newly appointed Minister of Defence, noted at the start of 2026, two million Ukrainians were wanted for mobilisation evasion, while another 200,000 servicemen were listed as absent without official leave (Struck-Feshchenko, 2026).

50 As of early 2026, the official term of service remains ‘until the end of martial law’, a legal status extended over a dozen times.

At the same time, sometimes-aggressive TRSSC tactics persist in places, so digital channels coexist with coercive street-level encounters, reinforcing the sense that, regardless of the interface, the hardest questions about who is compelled to serve, and how, are still being answered through power and politics rather than technology.<sup>51</sup>

Fears about state overreach, privacy, and data protection: concentrating mobilisation and military services in digital systems raises concerns about privacy and state surveillance. These fears are sharpened by the sense that a single, integrated infrastructure now mediates some of the most sensitive relationships between citizens and the state, giving the latter an unprecedented capacity to consolidate and track individual data. For a country still traumatised by past autocratic rule and Russian manipulation, what works well under a democratic government could become highly problematic if political trajectories shift.

“

As Ukraine has moved to a mixed model of mobilisation, digital defence governance aims to shift citizens and soldiers from being purely passive subjects to playing an increasing role in how their obligations are organised and met.

”

Reliance on this single digital backbone also creates worries about brittleness and systemic vulnerability. As more decisions depend on the same core infrastructure, a major outage or successful cyberattack could paralyse mobilisation and military administration overnight, turning a key asset for adaptive governance into a critical point of failure in a high-intensity war. This fear lingers even though, over several years of implementation, the system has remained functional under constant Russian attack, one of the world’s most adept users of cyber operations.

Not everyone can or wants to manage mobilisation and service through apps, and early roll-outs brought glitches, access problems, and confusion that left some feeling excluded or punished by a ‘digital-first’ approach. The long-term success of digital defence governance therefore depends on whether Ukraine can convincingly guarantee data security and address public concerns over privacy.

51 Over 2025, Ukraine’s Human Rights Ombudsman, Dmytro Lubinets, received 6,127 complaints – an exponential increase over earlier years. The most common complaints involve restrictions on freedom of movement during detention, superficial medical examinations by military medical commissions, violations in processing conscription deferrals, illegal confiscation of personal belongings, and unlawful detention in enlistment offices (Hodunova, 2026).

Ukraine has made rapid accession to the European Union a strategic priority, which puts its digital defence governance under the lens of EU standards on data protection and good administration. To move from wartime expedients toward durable alignment, Ukraine's digital defence governance will need not only strong technical safeguards but also oversight, audit powers, and redress mechanisms compatible with the EU acquis and data-protection framework.<sup>52</sup> The challenge is to hard-wire these guarantees into mobilisation systems so they continue to meet urgent military needs while eventually satisfying European expectations of privacy, proportionality, and accountability.

If strong safeguards, encryption, and independent oversight make it clear that personal data are tightly protected and narrowly used, these systems can underpin trust and democratic resilience. If citizens doubt how their information is stored, shared, or monitored, the same tools risk being seen as soft surveillance and efficient coercion, undermining consent for mobilisation and service rather than reinforcing it. In practice, that balance is still being worked out in Ukraine.

## Section 6. Implications for EU and NATO allies

*I hope our experience will be useful for European partners - they will face many complex questions, and these questions concern not so much technologies as approaches to organising defence.*

– Liliia Oleksiuk (2026, interview).

Ukraine's experience with Army+ and Reserve+ demonstrates how digital defence governance can be operationalised in practice. By rebuilding core processes in code, Ukraine has sought to create an integrated regime of digital defence governance that reshapes the conditions under which it can sustain a long war, from how people are mobilised to how serving personnel are supported.

Significantly, as digital systems become the default, they allow continual adaptation and expand the realm of what is politically and administratively possible, supporting stable mobilisation during a difficult war. At the same time, Ukraine has paired these efforts with a growing emphasis on unmanned systems to offset frontline manpower constraints, reinforcing a broader effort to reduce the human burden of sustained mobilisation (Frich, 2026).

EU and NATO allies do not face high-intensity war on their own territory and operate under stricter peacetime data and privacy-protection regimes, but this does not make Ukraine's model an exceptional wartime anomaly. Some dynamics – above all the scale and tempo of wartime mobilisation – are specific to Ukraine's circumstances, but most of the underlying

52 This refers in particular to alignment with the EU's dataprotection and administrative standards, including the General Data Protection Regulation (GDPR), the Law Enforcement Directive, and broader 'good administration' norms. In practice, this implies clear legal bases for processing, purpose limitation, dataminimisation, strong security and encryption, independent supervisory authorities, effective audit powers, and accessible remedies for individuals whose rights may be infringed.

design choices are compatible with peacetime governance. Much of the underlying architecture – interoperable base registers, legally recognised electronic documents and signatures, defence-specific portals, and embedded audit trails – already exists, in many cases, in civilian government systems.

Ukraine's approach is fundamentally about strengthening democratic governance even during war, rather than slipping into the comfort of wartime autocracy, for example by using digital records and audit trails to constrain arbitrary discretion rather than to expand it. The main challenge for allies is not whether they can adopt similar approaches but how to adapt them to their own legal frameworks, mobilisation models, and levels of political appetite.

Ukraine's experience should inform allies' choices, not be copied wholesale. Every country has its own registry architecture and legal framework for data exchange, interoperability, and cybersecurity, so what can travel across borders are governance principles. Ukrainian officials themselves caution against 'copy Ukraine' thinking, stressing that digital transformation in defence is first a governance project – about building public trust and working through institutional needs – not simply rolling out apps. For EU and NATO states, the central lesson is to treat Ukraine not as a provider of exportable apps but as a pioneer of digital defence governance.

This report has sought to understand what Ukraine has tried to do – reengineer mobilisation and military administration while maintaining democratic norms under extreme pressure – and to identify which elements democratic allies can build in peacetime, so they are not forced to improvise under crisis. The argument is not that Ukraine has perfected a response. Rather, it has made a goodfaith attempt to address an exceptionally daunting challenge, and the lessons from this attempt merit serious attention.

Equally important for EU and NATO allies is to learn from Ukraine's mistakes and constraints. No system of this scale, built under wartime pressure, can be free of flaws. Ukraine's efforts have revealed real challenges – from gaps and errors in underlying registers, to frictions between central systems and local implementation, to initial confusion and mistrust around how mobilisation rules and exemptions were communicated. Some design choices risk creating new concerns, for instance by rolling out enforcement tools faster than visible service improvements and, at times, by routing sensitive or contested cases through standardised workflows that leave little room for individual circumstances.

Against that backdrop, several elements of Ukraine's approach stand out as practical steps that allies can consider in peacetime.

1. **Prioritise the governance strategy, not just the apps.** Focus on how Ukraine designs and governs core defence needs (mobilisation and services to active personnel), not on cloning Army+ or Reserve+ as stand-alone products.
2. **Reframe mobilisation as a core strategic capability.** Use peacetime to review existing legal frameworks, force structures, and political red lines, and decide in advance how to move from a volunteer-heavy model to expanded conscription if required, rather than treating mobilisation as secondary and improvising under crisis.

- 3. Invest in interoperable base registers.** Establish the legal and technical foundations for civil–military registry interoperability and systematically address barriers such as restrictive cross-agency data rules, incompatible technical standards, and institutional resistance to sharing or ceding data control.
- 4. Align legal reform and digital system design from the outset.** Where possible, develop laws, organisational changes, and digital tools in parallel, with policymakers, lawyers, and IT engineers working to a shared problem definition so that code, procedures, and legislation reinforce each other.
- 5. Build role-specific digital entry points into defence governance.** Create dedicated portals that give citizens liable for service and active personnel direct, self-service access to key processes – such as status tracking, deferments, and transfers – and embed them in the core workflows of the institutions that handle these cases.
- 6. Embed oversight into system architecture.** Bake logging, audit trails, role-based access, user visibility of decisions, and redress channels into the code and database design from day one.
- 7. Balance enforcement tools with service improvements.** Pair any digital enforcement or fine-collection features with visible improvements in services, information, and options to serve, to avoid perceptions of growing coercion.
- 8. Feed frontline experience back into governance.** Design digital channels, like surveys, so that complaints and feedback from servicemembers flow directly into personnel and policy decisions, allowing rules and resource allocations to adjust under fire.
- 9. Use digital governance to uphold obligations to serving personnel.** Treat digital tools as core instruments for meeting the state’s duties to soldiers on benefits, transfers, and leave, so that reforms reinforce the social contract and make the state’s responsibilities more visible and reliable.
- 10. Make privacy protection a core design principle.** Treat personal data protection as foundational to user rights and use digital systems to increase transparency around data use, access rights, and system rules – including through userdriven data cleansing that lets citizens review and partially correct their own records.
- 11. Make strategic communication the anchor of digital mobilisation.** Use it to provide clear information on legal requirements, digital services, and the specific actions citizens are expected to take. Public-facing communication should also highlight how digitalisation benefits citizens as well as the state. ■

## References

- ArmyInform (2026) 'More than one million reports via Army+: Ministry of Defense names leading brigades', *ArmyInform*, 12 January. Available at: <https://armyinform.com.ua/en/2026/01/12/more-than-one-million-reports-via-army-ministry-of-defense-names-leading-brigades/>.
- Bohdanova, T. (2021) 'Security concerns and legal ambiguities threaten the future of Ukraine's "State in a Smartphone"', *Global Voices Advox*, 11 February. Available at: <https://globalvoices.org/2021/02/11/security-concerns-and-legal-ambiguities-threaten-the-future-of-ukraines-state-in-a-smartphone/>.
- Bondar, K. (2025) *How and why Ukraine's military is going digital*. Center for Strategic and International Studies (CSIS). Available at: <https://www.csis.org/analysis/how-and-why-ukraines-military-going-digital>.
- BRDO (2025) 'Reserve+: one year of digital solutions used by over 4 million persons liable for military service', *Better Regulation Delivery Office (BRDO)*, 2 June. Available at: <https://brdo.com.ua/en/news/rezerv-rik-tsyfrovyyh-rishen-yakymy-skorystalysya-vzhe-4-mln-vijskovozobov-yazanyh/>.
- BRDO (2024a) 'Армія+ – папери мінус: Міноборони презентувало застосунок для військових', *BRDO*. Available at: <https://brdo.com.ua/news/armiya-papery-minus-minoborony-prezentovalo-zastosunok-dlya-vijskovykh/>.
- BRDO (2024b) 'Армія+ – папери мінус: Міноборони презентувало застосунок для військових', *BRDO*, 7 August. Available at: <https://brdo.com.ua/news/armiya-papery-minus-minoborony-prezentovalo-zastosunok-dlya-vijskovykh/>.
- Cabinet of Ministers of Ukraine (2025) *Pro vnesennia zmin do postanovy Kabinetu Ministriv Ukrainy vid 30 lypnia 2024 r. № 879* [On amendments to the Resolution of the Cabinet of Ministers of Ukraine of 30 July 2024 No. 879]. Postanova No. 1010, 20 August. Available at: <https://zakon.rada.gov.ua/laws/show/1010-2025-%D0%BF#Text>.
- Cabinet of Ministers of Ukraine (2024a) 'Ministry of Defence explains what *Oberih* register is and why it is needed'. *kmu.gov.ua*, 17 March. Available at: <https://www.kmu.gov.ua/en/news/minoborony-poiasnylo-shcho-take-reiestr-oberih-i-dlia-choho-vin-potriben>.
- Cabinet of Ministers of Ukraine (2024b) *On certain issues of the State web portal of electronic public services in the field of national security and defence "Army+"*. Resolution No. 879, 30 July. Available at: <https://zakon.rada.gov.ua/laws/show/879-2024-%D0%BF#Text>.
- Cabinet of Ministers of Ukraine (2022) *On approval of the Regulations on territorial centres of recruitment and social support*. Resolution No. 154, 23 February. Available at: <https://zakon.rada.gov.ua/laws/show/154-2022-%D0%BF#Text>.
- Chernohorenko, K. (2025) 'Digitize or die: Ukraine's war is a wakeup call for 20th century militaries', *Breaking Defense*, 11 July. Available at: <https://breakingdefense.com/2025/07/digitize-or-die-ukraines-war-is-a-wake-up-call-for-20th-century-militaries/>.
- Danish Immigration Service (2024) *Ukraine – mobilisation*. Danish Immigration Service. Available at: <https://us.dk/media/t1ihlhsq/ukraine-mobilisation-2024-til-usdk.pdf>.
- Denisova, K. (2024) 'Ukraine launches new military app, aims to make soldiers' service "paperless"', *The Kyiv Independent*, 8 August. Available at: <https://kyiv-independent.com/ukraine-launches-new-phone-app-aims-to-make-soldiers-life-paperless/>.
- Digital State UA. (2025) *Ukraine's digital transformation is making international headlines*. Available at: <https://digitalstate.gov.ua/news/govtech/ukraines-digital-transformation-is-making-international-headlines>.
- Fornusek, M. (2024) 'Defense Ministry: 1.6 million draft-aged men update military registration data', *The Kyiv Independent*, 5 June. Available at: <https://kyiv-independent.com/defense-ministry-1-6-million-draft-aged-men-update-military-registration-data/>.
- Fornusek, M. (2023) 'SBU detains military medical commission official for corruption', *The Kyiv Independent*, 29 August. Available at: <https://kyiv-independent.com/sbu-detains-military-medical-commission-official-for-taking-bribes/>.
- Frich, K. (2026) 'Ukraine reveals new plan to revolutionize the frontline: "We are replacing 30% of soldiers"', *Dagens.com*, 22 March. Available at: <https://www.dagens.com/war/ukraine-reveals-new-plan-to-revolutionize-the-frontline-we-are-replacing-30-of-soldiers>.
- Hedenskog, J. and Umland, A. (2025) *The Ukrainian mobilization challenge: military and society during full-scale war*. SCEEUS Report No. 13, Stockholm Centre for Eastern European Studies (SCEEUS), Swedish Institute of International Affairs. Available at: <https://sceeus.se/en/publications/the-ukrainian-mobilization-challenge-military-and-society-during-full-scale-war/>.

- Hodunova, K. (2026) 'Ukrainian ombudsman gets over 6,000 complaints against enlistment officers in 2025 – 333 times more than at all-out war's start', *The Kyiv Independent*, 9 February. Available at: <https://kyivindependent.com/ukrainian-ombudsman-receives-over-6-000-complaints-against-enlistment-officers-in-2025/>.
- Ingram, G. and Vora, P. (2024) 'Ukraine: digital government is central to resilience', *Brookings Institution*, 7 February. Available at: <https://www.brookings.edu/articles/ukraine-digital-government-is-central-to-resilience/>.
- InterfaxUkraine (2025) 'New Army+ version launched with digital ID and news feed – Ministry of Defense', *InterfaxUkraine*, 21 December. Available at: <https://en.interfax.com.ua/news/general/1130422.html>.
- Khalilova, D. (2024) 'Ukraine is digitalizing its military ahead of a new mobilization wave', *The Kyiv Independent*, 25 May. Available at: <https://kyivindependent.com/aiming-to-mobilize-thousands-of-new-troops-ukraine-is-digitalizing-its-military/>.
- Mamedieva, G. (2025) 'Ukraine's digital transformation: innovation for resilience', *Center for International Development, Harvard Kennedy School*, 1 April. Available at: <https://www.hks.harvard.edu/centers/cid/voices/ukraines-digital-transformation-innovation-resilience>.
- Mazur, Y. and Lanchukovska, T. (2025) 'How many Ukrainians use Reserve+ and Army+?', *LIGA.net*, 7 December. Available at: <https://news.liga.net/en/politics/news/reserve-has-about-6-million-users-and-1-million-military-joined-army-shmyhal>.
- Méheut, C. (2025) 'Its forces worn down, Ukraine moves to revamp military service', *The New York Times*, 4 November. Available at: <https://www.nytimes.com/2025/11/04/world/europe/ukraine-war-military-contracts-conscription.html>.
- Mezha (2026) *Reserve+ App scheduled maintenance on February 20, 2026*. Available at: <https://mezha.net/eng/bukvy/reserve-app-scheduled-maintenance-on-february-20-2026/>.
- Mezha (2025) "Reserve+": digital enlistment for military service in Ukraine. Available at: <https://mezha.net/eng/bukvy/reserve-digital-enlistment-for-military-service-in-ukraine/>.
- Ministry of Defence of Ukraine (2026) Direct communication, 28 February.
- Ministry of Defence of Ukraine. (2025a) *Digitalization as the foundation of systemic change in the military: results for 2025*. Available at: <https://mod.gov.ua/en/news/digitalization-as-the-foundation-of-systemic-change-in-the-military-results-for-2025>.
- Ministry of Defence of Ukraine (2025b) *Government decides on automatic military registration of citizens*. Available at: <https://mod.gov.ua/news/uryad-uh-valiv-rishennya-pro-avtomatichnij-vijskovij-oblik-gromadyan>.
- Ministry of Defence of Ukraine (2025c) *Automatic extension now applies to 90% of deferments for Ukrainians*. Available at: <https://mod.gov.ua/en/news/automatic-extension-now-applies-to-90-of-deferments-for-ukrainians>.
- Ministry of Defence of Ukraine (2025d) *Ukraine's MoD presents comprehensive update on defense digital transformation efforts*. Available at: <https://mod.gov.ua/en/news/ukraine-s-mo-d-presents-comprehensive-update-on-defense-digital-transformation-efforts>.
- Ministry of Defence of Ukraine (2025e) *Kateryna Chernohorenko: Army+ introduces a multi-signature feature for commanders*. Available at: <https://mod.gov.ua/en/news/kateryna-chernohorenko-army-introduces-a-multi-signature-feature-for-commanders>.
- Ministry of Defence of Ukraine (2024a) *MOD introduced a novel mobile app for the military*. Available at: <https://mod.gov.ua/en/news/army-the-ministry-of-defence-introduced-a-novel-mobile-app>.
- Ministry of Defence of Ukraine (2024b) 'Reserve+ notification on the processing of personal data' [in Ukrainian], *Reserve+*. Available at: <https://reserveplus.mod.gov.ua/privacy/>.
- Ministry of Defence of Ukraine (2024c) 'Повідомлення про обробку персональних даних / Privacy notice' [Army+ Portal Privacy Notice], *Army+*. Available at: <https://aplus.mod.gov.ua/privacy> (navigate to 'Обробка персональних даних' link in the footer).
- Ministry of Defence of Ukraine (2024d) *Zelena knyha: stratehichni napriamy, vyklyky ta nova arkhitektura oborony* [Green Paper: strategic directions, challenges and a new defence architecture]. Available at: [https://mod.gov.ua/assets/Zelena\\_knyha\\_Ministerstva\\_oboroni\\_Ukrayini\\_4f0eaf9850.PDF](https://mod.gov.ua/assets/Zelena_knyha_Ministerstva_oboroni_Ukrayini_4f0eaf9850.PDF).
- New Voice of Ukraine (2024) 'Reserve+ app: three fake applications were found in Ukraine – how to distinguish fakes', *The New Voice of Ukraine*, 4 August. Available at: <https://english.nv.ua/nation/reserve-app-three-fake-applications-were-found-in-ukraine-how-to-distinguish-fakes-50440288.html>.
- Novyny.live (2024a) *How to submit a report to Army+ – detailed instructions*. Available at: <https://mobilizatsiya.novyny.live/elektronii-raport-v-armii-pokrokovaya-instruktsiia-z-video-214831.html>.

- Novyny.live (2024b) "Oberig" to take data from four more registers in 2025: details. Available at: <https://mobilizatsiya.novyny.live/oberig-bratime-dani-shche-z-chotirokh-reiestriv-u-2025-rotsi-detali-216161.html>.
- OECD (2022) *Digitalisation for recovery in Ukraine*. Available at: [https://www.oecd.org/en/publications/digitalisation-for-recovery-in-ukraine\\_c5477864-en/full-report.html](https://www.oecd.org/en/publications/digitalisation-for-recovery-in-ukraine_c5477864-en/full-report.html).
- Office of the Prosecutor General of Ukraine (2026) *A military officer of the RTCC and SP will be tried for interference in the "Oberig" system*. Available at: <https://en.gp.gov.ua/en/posts/za-vtrucannya-v-sistemu-oberig-suditimut-viiskovosluzbovcyu-rtck-ta-sp>.
- Panasiuk, K. (2024) 'Ukraine's wartime democrats battle conscription crisis', *Center for European Policy Analysis*. Available at: <https://cepa.org/article/ukraines-wartime-democrats-battle-conscription-crisis/>.
- Post, K. (2025) 'The military branch behind Ukraine's battlefield apps turns to weapons bureaucracy', *The Kyiv Independent*, 7 October. Available at: <https://kyivindependent.com/the-military-branch-behind-ukraines-battlefield-apps-turns-to-weapon-buying-bureaucracy/>.
- Schlegel, S. (2024) 'Mobilisation, peacemaking and deterrence in Ukraine', *International Crisis Group*, 17 December. Available at: <https://www.crisisgroup.org/qna/europe-central-asia/eastern-europe/ukraine/mobilisation-peacemaking-and-deterrence-ukraine>.
- Struck-Feshchenko, J. (2026) 'Fedorov: 2 million Ukrainians wanted for draft evasion, 200,000 listed as AWOL', *Kyiv Post*, 13 January. Available at: <https://www.kyivpost.com/post/68067>.
- State Enterprise DIIA (2019) *Unified State Web Portal of Electronic Services Diia*. Available at: <https://se.diia.gov.ua/en/unified-state-web-portal-of-electronic-services-diia>.
- SUD.UA (2026) *Автоматична відстрочка від мобілізації – Мініборони додало 7 нових категорій*. Судово-юридична газета [Automatic deferment from mobilization – the Ministry of Defense has added 7 new categories]. Available at: <https://sud.ua/ru/news/ukraine/352531-avtomaticheskaya-otsrochka-ot-mobilizatsii-minoborony-dobavilo-7-novykh-kategoriy>.
- Sukhankin, S. (2024) 'New military app is set to revolutionize how Ukraine runs its army', *The Kyiv Independent*, 3 September. Available at: <https://kyivindependent.com/new-military-app-is-set-to-revolutionize-way-ukraine-runs-its-army/>.
- United Nations (2022) *Ukraine – EGovernment Development Index country data, UN E-Government Knowledgebase*. Available at: <https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine>.
- Verkhovna Rada of Ukraine (2017) *Zakon Ukrainy "Pro Yedynyi derzhavnyi reiestr pryzovnykiv, viiskovozobov'iazanykh ta rezervystiv"* [Law of Ukraine "On the Unified State Register of Conscripts, Persons Liable for Military Service and Reservists"]. No. 1951VIII of 16 March 2017, as amended. Available at: <https://zakon.rada.gov.ua/laws/show/1951-19#Text>.
- Verkhovna Rada of Ukraine (1992) *Law of Ukraine on military duty and military service*. No. 2232XII of 25 March. Available at: <https://zakon.rada.gov.ua/laws/show/2232-12>.
- Volokita, V. (2025) 'Ukraine's Defence Ministry establishes Digital Army company', *Ukrainska Pravda*, 25 February. Available at: <https://www.pravda.com.ua/eng/news/2025/02/25/7500059/>.
- Vyhovska, V., Sholudko, V., and Balytska, M. (2025) 'State digital transformation in Ukraine: 2019–2024 review', *VoxUkraine*, 3 July. Available at: <https://voxukraine.org/en/state-digital-transformation-in-ukraine-2019-2024-review>.

## Interviews

- Korzh, Sergiy; Product Manager, ReservePlus (Ministry of Defence), 25 February 2026.
- Muraveinyk, Anton; Come Back Alive, 10 March 2026.
- Oleksiuk, Liliia. Advisor to the Committee of the Verkhovna Rada of Ukraine on National Security, Defence and Intelligence, 10 March 2026.
- Pravdyvets, Oleksandr, PhD; Head of the Department of Financial and Economic Security at KROK University, 20 March 2026.
- Romaniukov, Artem; Ministry of Defence, 18 February 2026.
- Shestakov, Vadym; Legal Expert, Defence Sector Legal Team Lead (BRDO) 26 February 2026.
- Volovina, Halyna; BRDO, 23 March 2026.
- Zahorodnii, Roman; Head of Product, ArmyPlus (Ministry of Defence), 3 March 2026.

## Annexes

### Annex 1: Legal Framework Underpinning Army+ and Reserve+

Law No. 3549-IX, adopted in January 2024, amended the Law on the Unified State Register and several related acts on mobilisation and military service to expand electronic processing of military registration data, strengthen *Oberih*'s interaction with other key state registers, and introduce electronic cabinets through which persons on military registration can access and update their data. This reform accelerated procedures such as recognition of combatant status and enabled remote interaction with TRSSCs via an electronic cabinet linked to the *Oberih* register. Taken together, these changes marked a shift from *Oberih* being used primarily as a back-end register toward also serving as the legal basis for citizen-facing digital services, particularly those implemented through Reserve+.

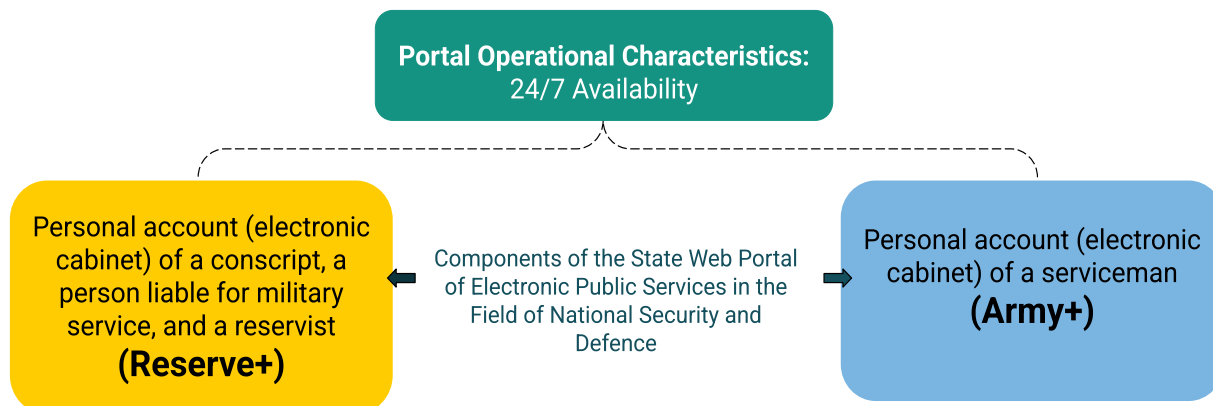
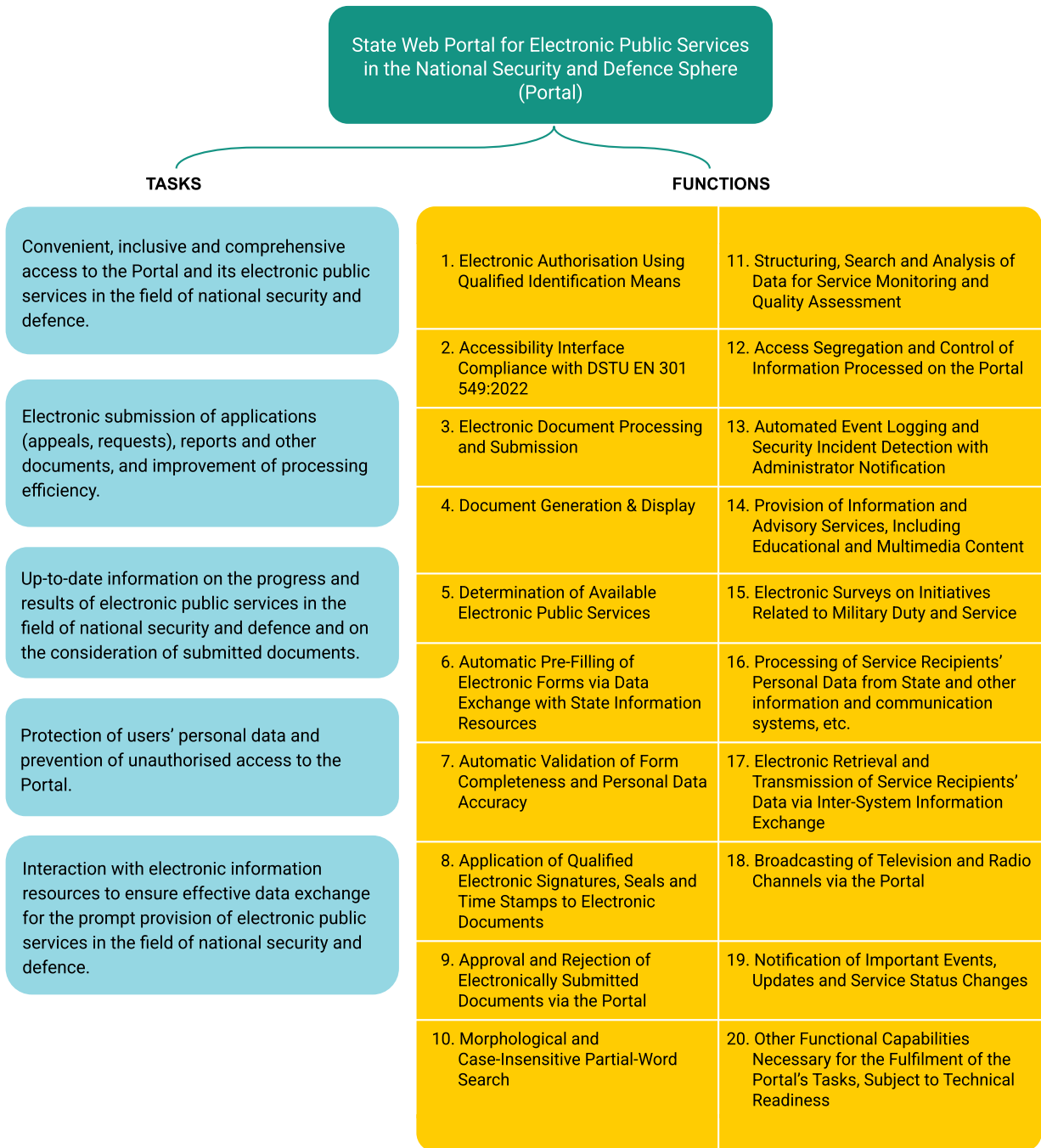
From the spring of 2024, successive measures turned these foundations into concrete app-based tools. Law No. 3633-IX of 11 April 2024 ('On Amendments to Certain Legislative Acts of Ukraine on Certain Issues of Military Service, Mobilisation and Military Registration'), which entered into force on 18 May 2024, required men aged 18–60 to update their data within 60 days and made a range of changes to mobilisation ages, basic military service, and document verification. The government implemented this obligation via the creation of the Reserve+ application alongside existing channels, effectively positioning Reserve+ as a principal way for conscripts and reservists to comply with data-update requirements.

Cabinet of Ministers Resolution No. 559 of 16 May 2024 introduced an electronic military registration document and approved the procedure for its formation and use, allowing such a document to be generated through Reserve+ or *Diiia*. The Reserve+ app itself was launched on 18 May 2024, enabling remote updating of personal data, access to information from the *Oberih* register, and generation of an electronic document with a QR code for verification.

In July 2024, the Cabinet of Ministers adopted Resolution No. 879 ('On Certain Issues of the State Web Portal of Electronic Public Services in the Sphere of National Security and Defence'). In effect, it acts as the 'operational manual' for this State Web Portal, setting out how it should be structured and how it should interact with other state information systems. This Resolution introduced the Army+ application as the main user interface of the portal. On this basis, subsequent acts and technical decisions also brought Reserve+ into the same portal architecture, so that Army+ and Reserve+ now function as a single digital tool for servicemembers and those liable for military service.

On 12 November 2024, an experimental Resolution of the Cabinet of Ministers No. 1291 was adopted, allowing certain categories of military personnel to initiate a transfer to another place of service by submitting a report through Army+. Because this Resolution is experimental, its validity period is set at two years. Based on the results of the experiment, the Ministry of Defence must propose to the government a permanent regulatory procedure.

## Annex 2. Legal Provisions for the Defence Portal



### **Annex 3. Reserve+: Privacy and Safety Standards Notice**

Резерв+ - Повідомлення про обробку персональних даних

Personal data may include:

#### **1. Data required for authorisation of the person in the application:**

Name, surname, patronymic (if any); registration number of the taxpayer's account card from the State register of individuals - taxpayers; data of the identity document (type, series, number, date and issuing authority, validity period, country of issue); address of residence/registration; date of birth; place of birth; gender; phone and e-mail and citizenship.

Collection of the aforementioned type of data is performed during the authorisation (electronic identification) via receiving these data from the BankID service.

#### **2. Data which can be refined by the user (after successful authorization in the application):**

Phone number; address of residence; e-mail (if any).

Data refinement is defined as a confirmation of information received during authorisation (electronic identification) from the BankID service, or amendment of such data.

#### **3. Data received from the Unified state register of conscripts, persons liable for military service and reservists (hereinafter - the Register) and may be displayed in the RESERVE+ application:**

Surname, information about the change of surname; full name (all full names), information about changes to the full name; patronymic (if any); date of birth; registration number of the taxpayer's account card; digitised image of the person's face; code of military specialty; name of the military specialty; category of registration (conscript, person liable for military service, reservist); type of registration (registered, deregistered, excluded); reason for deregistration/exclusion; availability of the reservation; reservation expiration date (if any); fitness for military service; date of the last military medical examination; availability of a deferment; the final date of the deferment; whether you are wanted by the National Police of Ukraine; place of actual residence; communication numbers and e-mail addresses; unique number in the Register; and the territorial centre of recruitment and social support where he/she is registered.

The said personal data is collected to form a military registration document in electronic form or display information about a person, which is carried out by obtaining information from the Register and may be stored on the user's mobile device. The Manager does not have access to the data transferred from the Register.

#### **Annex 4. Army+: Privacy and Safety Standards Notice**

Повідомлення про обробку персональних даних | Армія+

Personal data may include:

##### **Data required for authorisation:**

Surname, first name, patronymic (if any); the registration number of the taxpayer's account card or the series and number of the valid passport of a citizen of Ukraine (for persons who, due to their religious beliefs, rejected to accept the registration number of the taxpayer's account card and reported this to the relevant supervisory authority); date of birth; and the status of the person (whether he is a military serviceman).

##### **Data processed for the provision of electronic public services:**

Personal data necessary for the provision of electronic public services; data about the progress and results of the provision of electronic public services, consideration of appeals, other user notifications about the provided electronic public services; data about complaints based on the results of electronic public services provision; data provided in e-mails during the provision of electronic public services, consideration of appeals, for the purpose of decisions making on individual action, as well as other issues raised by the user; other data obtained from the Unified State Register of Conscripts, Persons Liable for Military Service and Reservists.

##### **Other personal data:**

Data provided by users when using Portal "Army+" software, including the use of Portal "Army+" (Army+) mobile application.

##### **Technical data:**

Technical data necessary for user authentication and authorisation; data on monitoring and evaluating the quality of electronic public services provided using Portal "Army+"; and other technical data necessary for the proper functioning of Portal "Army+" software, including Portal "Army+" (Army+) mobile application.





THE LONDON SCHOOL  
OF ECONOMICS AND  
POLITICAL SCIENCE ■

# A Unique Programme in Strategy Designed for Decision Makers

**LSE IDEAS**, a centre for the study of international affairs, brings together academics and policy-makers to think strategically about world events.

This one-year **EXECUTIVE MASTERS PROGRAMME** is at the heart of that endeavour. While studying in a world-leading university you will be able to learn from top LSE academics and senior policy practitioners.

The programme will sharpen your ability to challenge conventional thinking, explore new techniques for addressing risk and threats, and coach you in devising effective strategies to address them.

Residential and non-residential options allow students to learn while holding demanding positions in the public, private and non-governmental sectors.

*'Right from the first week I was able to apply the lessons I had learnt to our operational and policy work and to coach my teams to look at issues differently.'*

–**Dame Karen Pierce DCMG**

UK Special Envoy to the  
Western Balkans, Former  
UK Ambassador to the  
United States

## CONTACT US

[ideas.strategy@lse.ac.uk](mailto:ideas.strategy@lse.ac.uk)

+44 (0)20 7955 6526  
[lse.ac.uk/ideas/exec](https://lse.ac.uk/ideas/exec)





**LSE IDEAS** is the LSE's foreign policy think tank. Through sustained engagement with policymakers and opinion-formers, IDEAS provides a forum that informs policy debate and connects academic research with the practice of diplomacy and strategy.

The views and opinions expressed in this publication are those of the author(s) and do not represent those of the London School of Economics and Political Science (LSE) or LSE IDEAS. This publication is issued on the understanding that if any extract is used, the author(s) and LSE IDEAS should be credited, with the date of the publication. While every effort has been made to ensure the accuracy of the material therein, the author(s) and/or LSE IDEAS will not be liable for any loss or damages incurred through the use of this publication..

**LSE IDEAS**  
Floor 9, Pankhurst House  
1 Clement's Inn, London  
WC2A 2AZ+44 (0)20 7107 5619  
ideas@lse.ac.uk  
lse.ac.uk/ideas

