Dual-use GovTech and Civilian Protection

How digital public services evolve into security infrastructure, a story of Ukraine and Estonia

Malte Benda and Iasmina Stoian

Highlight sentence: Dual-use GovTech turns citizens into “security sensors”: civilians supplying security-relevant data. While they can boost resilience and improvement, they may also raise DPH and cyber-reprisal risk.

1. Introduction

Who would have imagined 15 years ago that booking an ID appointment, paying taxes, or receiving a hazard alert could be just one click away? This is now becoming a routine across Europe and around the world. And yet, who would have imagined only 7 years ago that citizens could also report damage to destroyed buildings, or relay real-time alerts about approaching enemy forces in conflict zones through the same digital governance ecosystem? In recent years, this kind of dual-use civic infrastructure has become increasingly visible and implemented in countries, platforms and apps built for everyday public administration that can also serve national security and civilian protection. In principle, ‘dual-use’ refers to an object or service that can be used to serve both civilian and military purposes (Cséfalvayová, 2025). This raises a moral dilemma: how can states mobilise their society digitally without turning civilians into a risk-bearing extension of the security system?

Building on earlier research on Total Defence that compared Ukraine’s Diia app with potential adaptations for the German government, this article extends the analysis by focusing on a comparison between Ukraine’s Diia app and Estonia’s digital state ecosystem. Estonia is selected not only for its functional similarities and highly developed digital infrastructure, but also because it has been one of Ukraine’s key long- term digital partners, supporting major e-governance and digital infrastructure initiatives now used in Ukraine, one notable initiative being the development of the Diia

app. This pairing of the two countries shows a contrast in how similar governance tools work under opposite security conditions, namely wartime and peacetime.

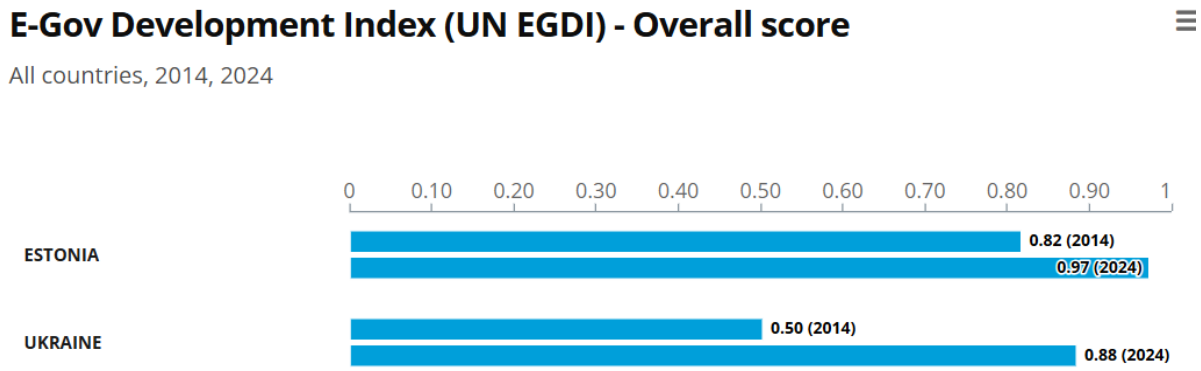
Therefore, the central research question of this essay is simple: to what extent, and through which functions, do Ukraine's Diia ecosystem and Estonia's digital state app ecosystem transform civilians from service users into contributors of security-relevant information, and what legal and national-security risks follow from this shift?. The essay will start with a brief outline of the two digital ecosystems, Diia's wartime use and Estonia's peacetime model, followed by the legal implications for citizen protection and state responsibility, an assessment of the cyber and operational risks, and will conclude by summarising the findings through the "citizen-as-client vs. citizen-as-sensor" perspective.

To structure the comparison, this article applies a conceptual distinction between the citizen-as-client and the citizen-as-sensor. In the citizen-as-client model, individuals interact with digital platforms primarily as service users within an administrative relationship. In the citizen-as-sensor model, civilians provide information that carries operational or security relevance. This distinction serves as the analytical lens throughout the essay, allowing the legal, cybersecurity, and ethical implications of digital participation to be assessed under two different logics of state-citizen interaction.

2. Two digital state models

Ukraine and Estonia represent structurally similar digital ecosystems operating under opposite security conditions. Both rank among Europe's leading digital governance innovators. Estonia's E-Government Development Index (EGDI) rose from 0.82 in 2014 to 0.97 in 2024, while Ukraine's increased from 0.50 to roughly 0.88 over the same period. This development trajectory suggests that digital infrastructure in Ukraine evolved not only as administrative modernisation but also increasingly as a resilience mechanism embedded in the national security strategy, from 2014 until today.

To structure the comparison, this article applies a conceptual distinction between the citizen-as-client and the citizen-as-sensor. In the citizen-as-client model, individuals interact with digital platforms primarily as service users within an administrative relationship. In the citizen-as-sensor model, civilians provide information that carries operational or security relevance. This distinction serves as the analytical lens throughout the essay, allowing the legal, cybersecurity, and ethical implications of digital participation to be assessed under two different logics of state-citizen interaction.



Source: [United Nations E-Government Knowledgebase]

2.1 Ukraine: Diia during wartime

Launched in 2020 by Ukraine's Ministry of Digital Transformation, Diia (meaning "action") was originally conceived as a comprehensive digital governance platform designed to create a "state in a smartphone" (Ministry of Digital Transformation of Ukraine, 2020).

Before 2022, Diia functioned primarily as an administrative interface, providing digital IDs, business registration, tax services, and document verification. However, following Russia's full-scale invasion in February 2022, Diia rapidly expanded into a dual-use infrastructure that integrated wartime capabilities.

Key features included:

1. eVorog (eEnemy) chatbot, enabling citizens to report geolocated information on Russian troop movements (Interfax-Ukraine).

2. eRestoration program, allowing civilians to report damaged property and receive compensation (Cabinet of Ministers of Ukraine, 2023).

Defence bond purchases, facilitating civilian financial participation in the war effort (Ministry of Finance, Ukraine).

This rapid functional expansion reflects characteristics of wartime policy: acceleration, centralisation, and prioritisation of operational efficacy over procedural perfection. As the OECD notes, Ukraine's digital governance reforms were crucial in maintaining continuity of state services during active conflict (2023).

In doing so, Diia partially shifted from a citizen-as-client logic toward a citizen-as-sensor logic, where civilian-generated data may acquire direct operational significance. However, centralisation also introduces cybersecurity vulnerabilities. Highly centralised digital systems may create single points of failure and increased attack surfaces (ENISA, 2023).

Thus, Diia embodies a paradox: it enhances societal resilience while simultaneously expanding systemic risk exposure.

2.2 Estonia: Digital state under threat

Estonia represents a peacetime digital state model embedded within a long-standing security awareness shaped by historical tensions with Russia, and by the current threat in the ongoing war. Unlike Ukraine, Estonia's digital transformation was not crisis-triggered but strategically institutionalised since the early 2000s.

Estonia's digital governance ecosystem rests on three pillars:

1. X-Road interoperability framework, enabling secure decentralized data exchange (Information System Authority of Estonia, 2022).
2. e-Identity system, providing legally binding digital authentication (e-Estonia, 2024).
3. Data embassies, ensuring continuity of government services in case of territorial disruption (Republic of Estonia, 2018).

Estonia's model remains predominantly anchored in a citizen-as-client logic: digital tools facilitate service access and state continuity, but civilians are not operationalised as real-time contributors to military intelligence.

Unlike Diia, Estonia's model emphasises decentralisation and layered redundancy. After experiencing large-scale cyberattacks in 2007, Estonia institutionalised cybersecurity as a national security priority (Ottis, 2008). Therefore, Estonia demonstrates how a digital state can integrate preparedness logic without transitioning civilians into direct wartime participation roles. While Estonia maintains crisis alert systems and secure authentication tools, it has not operationalised its civilian digital infrastructure for real-time military intelligence reporting.

This distinction marks a structural difference: Ukraine's Diia reflects wartime mobilisation logic, whereas Estonia's ecosystem reflects deterrence and continuity logic.

3. Legal Implications

3.1 Civilian participation & protections

From an international law perspective, in times of armed conflicts, individuals can (in limited circumstances) be lawfully targeted, meaning an enemy force may direct hostile measures against them. This happens only if the individual is found to be engaged in the hostile conduct. More simply, civilians can become subject to attack for such time as they take part in fighting. This is especially important for our comparison when discussing the situation in Ukraine. Under international humanitarian law (IHL), which applies in armed conflicts, and since Russia's occupation falls within this category, civilians as a general rule are protected, both as a matter of treaty law and customary rules. But there are exceptions. One of them is that civilians may lose that protection if, for example, they take a direct part in hostilities, for short - DPH. Hence, in this context, to lose civilian status under International Humanitarian Law (IHL), it does not necessarily mean that people take up arms and attack Russian forces, but it can also include providing the state with militarily valuable information that is closely linked to military operations. Following this logic, the mere existence of an app, or general

state encouragement to use it, is not in itself unlawful under IHL. Therefore, according to the ICRC's interpretive guidance, direct participation in hostilities requires three cumulative criteria:

1. Threshold of harm: the act must be likely to adversely affect enemy military capacity
2. Direct causation: a sufficiently close causal link between the act and the harm
3. Belligerent nexus: the act must be specifically designed to support one party against another (ICRC, 2009)

As a result, using the Diia app to file compensation claims, report general damage, or use it for personal administrative matters would not meet these requirements. The legal risk therefore would depend on the specific act and context, not on merely using the Diia app. For instance, only activities resembling the eVorog-type reporting model raise meaningful targetability concerns. Therefore, this distinction is essential. However, today the line between lawful targets under humanitarian law and the civilian character becomes more and more blurred, making it very difficult to assess what is lawful and what is not, leaving this matter in a grey area.

3.2 State responsibility

A pertinent question that follows from this is whether states bear any degree of responsibility towards citizens who are targeted, or made vulnerable to targeting, because of their support for, or cooperation with, their government. In the context of Ukraine, where civilian engagement with state institutions and the war effort has exposed individuals to heightened risk, this is crucial to assess.

First, under the International Law Commission's Articles on State Responsibility (ARSIWA):

1. Conduct of state organs is attributable to the state (Article 4)
2. Conduct of persons acting under state instruction, direction, or control may also be attributable (Article 8)

Applied to our cases, a digital governance app will usually be a state function. This means that failures in design, verification, or safeguards can engage responsibility where they breach a primary obligation, such as the security of their citizens, and are attributable. However, attribution thresholds are strict. The key issue is **not** that civilians become state organs simply by using an app, but that the state creates a participation that, even if voluntary, may result in harm or infringement of individual rights, such as targeting, retaliation risks, or individual sanctions. In this sense, the legal exposure is often indirect but real: if the state uses civilian input as a security contribution, it strengthens the point that the state must anticipate and mitigate the individual risks. Consequently, this is where human rights protections come into play.

3.3 Other human rights safeguards

Since both Estonia and Ukraine are parties to the European Convention on Human Rights (Donald & Grogan, 2022), they are further protected by international law. Hence, the Convention provides a set of legal safeguards for both conflict-time and peacetime. For instance, Article 8, which protects private life (including personal data), is particularly relevant for large-scale state databases and app-based participation by civilians. Together with Article 13 (effective remedy), these provisions require meaningful oversight over how data is used within Diia and Estonia's app ecosystems, including requirements of how data is collected, for what purposes, how it is retained, and how it is used. The ECHR framework also implies that states must take measures to protect individuals against serious risks, especially where targeting risks may arise, given the right to life under Article 2.

The bottom line is that dual-use civic infrastructure and the two examples of ecosystems are legally safeguarded for predictable harms only: where civilian participation through these apps could create exposure to threats from foreign states or other actors. However, international and national legal frameworks are intended to cover these gaps, by providing standards and accountability mechanisms for citizens' data.

4. National security implications

The transformation of digital governance platforms into dual-use security instruments produces both strategic advantages and systemic vulnerabilities. First, such platforms enhance societal resilience. For example, NATO increasingly emphasises the role of civilian infrastructure in modern hybrid warfare, highlighting that resilience is as critical as military capability (NATO, 2022).

Yet a data breach involving identifiable civilian reporters could expose individuals to reprisals in occupied territories or contested regions. Hence, if geolocated reporting data were accessed by hostile actors, individuals who contributed security-relevant information might face targeted retaliation, harassment, or sanctions. Consequently, the risk is not merely abstract data loss, but physical endangerment. Indeed, in citizen-as-sensor architectures, data protection becomes inseparable from personal security.

Second, digital mobilisation may create cyber escalation risks. For instance, civilian participation in cyber activities, such as through the IT Army of Ukraine, blurs the boundary between combatants and civilians (Maurer, 2018).

A further vulnerability lies in the risk of manipulated civilian reporting. If adversaries were able to inject spoofed geolocation reports into systems such as eVorog, they could deliberately misdirect defensive resources or saturate verification channels. On the other hand, even if individual reports are verified, a high volume of fabricated inputs could create analytical overload, delaying responses to genuine threats. In this sense, citizen-as-sensor systems are exposed not only to hacking, but to information warfare tactics designed to weaponise trust in civilian input.

Third, centralised platforms increase data concentration risk. Indeed, according to the European Commission's Cybersecurity Strategy, resilience depends on distributed architectures and secure interoperability standards (European Commission, 2020).

A highly centralised application such as Diia may become an attractive single-point-of-failure target. For example, a coordinated cyberattack disabling authentication

systems or corrupting central registries could temporarily paralyse access to identity verification, financial transfers, or emergency notifications. In wartime conditions, such disruption could generate cascading operational effects, including delayed mobilisation, misallocation of emergency funds, or erosion of public trust. The more governance and security functions converge within one interface, the higher the strategic value of its disruption.

Thus, the national-security value of digital state ecosystems must be weighed against systemic vulnerabilities, including data breaches, misinformation manipulation, and infrastructure targeting.

5. Citizen-as-Client vs Citizen-as-Sensor

The distinction between “citizen-as-client” and “citizen-as-sensor” offers a conceptual framework for understanding the legal and ethical implications of digital participation. In the citizen-as-client model (typical of Estonia), individuals interact with digital platforms to access services. Their relationship with the state remains transactional and administrative. In the citizen-as-sensor model (partially reflected in wartime i.e.: Diia), citizens provide information that may carry security relevance.

This model introduces three risks:

1. Targetability risk under International Humanitarian Law, as discussed by the ICRC (2009)
2. Attribution risk under Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), where civilian contributions could be attributed to the state (International Law Commission, 2001)
3. Data protection concerns under the European Convention on Human Rights (ECHR) and General Data Protection Regulation (GDPR) (European Union) (European Court of Human Rights)

The shift from client to sensor does not automatically violate international law, but it alters the civilian-state relationship by embedding citizens within security ecosystems. As Cséfalvayová (2025) argues, dual-use innovation creates moral dilemmas where civilian engagement becomes security leverage.

Thus, the ethical core question becomes not whether digital mobilisation is lawful, but how states mitigate predictable harm to participating civilians.

6. Conclusion

This comparative analysis demonstrates that Ukraine and Estonia represent two structurally similar digital ecosystems operating under fundamentally different security logics. Ukraine's Diia evolved from a service platform into a wartime resilience instrument. Its success was enabled by centralised leadership, accelerated reform, and high public buy-in under existential threat. However, this mobilisation model introduces legal ambiguities and cybersecurity vulnerabilities.

On the other hand, Estonia's model illustrates an alternative pathway via decentralised interoperability, layered redundancy, and institutionalised cybersecurity preparedness without civilian intelligence mobilisation.

The distinction between citizen-as-client and citizen-as-sensor encapsulates the broader transformation of digital statehood in Europe. While digital governance enhances resilience, its securitization reshapes civilian status, risk exposure, and state responsibility.

For Germany and other EU Member States, the key lesson lies not in replicating Diia's wartime model, but in designing interoperable, rights-compliant, and resilient digital infrastructures before crisis conditions arise. Preparedness in peacetime allows legal clarity and technical safeguards to be embedded without emergency overreach. In this sense, dual-use civic infrastructure is neither inherently destabilizing nor automatically protective. Its normative legitimacy depends on transparency, safeguards, and proportional integration into national security strategy.

List of references:

•Cséfalvayová, K. (2025, June 9). The dual-use dilemma: Why Europe must rethink civil-military innovation. Institute for Central Europe. https://iceoz.eu/the-dual- use-dilemma-why-europe-must-rethink-civil-military-innovation/

•Donald, A., C Grogan, J. (2022, June 24). The European Convention on Human Rights. UK in a Changing Europe. https://ukandeu.ac.uk/explainers/the-

european-convention-on-human-rights/

•European Court of Human Rights. (2021). *European Convention on Human Rights*. Council of Europe. Retrieved January 31, 2026, from https://www.echr.coe.int/documents/d/echr/convention_ENG

•International Law Commission. (2001). Draft articles on responsibility of States for internationally wrongful acts, with commentaries. United Nations.

https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

•International Committee of the Red Cross. (2009). Interpretive guidance on the notion of direct participation in hostilities under international humanitarian law. https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc- 002-0990.pdf

•United Nations. (2024). E-Government Development Index (EGDI) https://data360.worldbank.org/en/indicator/UN_EGDI_EGDI

•Ministry of Digital Transformation of Ukraine (2020). “ Diia – Digital State Platform.” Thedigital.gov.ua, thedigital.gov.ua/. Accessed 8 Feb. 2026.

•Interfax-Ukraine. “Ministry of Digital Transformation Launches EVorog Chatbot in Telegram.” Interfax-Ukraine, 10 Mar. 2022,

en.interfax.com.ua/news/telecom/810765.html. Accessed 8 Feb. 2026.

•Cabinet of Ministers of Ukraine. “Government Expands EVidnovlennia Programme.” Kmu.gov.ua, 2023, www.kmu.gov.ua/en/news/uriad-rozshyryv- prohramu-ievidnovlennia-iuliia-svyrydenko. Accessed 8 Feb. 2026.

•Ministry of Finance Ukraine. Bonds.gov.ua, 2022, bonds.gov.ua/en. Accessed 8 Feb. 2026.

• OECD. (2023). Digitalisation for recovery in Ukraine.

https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/07/digitalisation-for-recovery-in-ukraine_40746fbe/c5477864-en.pdf

•ENISA. “ENISA Threat Landscape 2023.” ENISA, 19 Oct. 2023, www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

•Information System Authority of Estonia. “Data Exchange Layer X-Tee | RIA.” Www.ria.ee, 2022, www.ria.ee/en/state-information-system/data-exchange-platforms/data-exchange-layer-x-tee. Accessed 8 Feb. 2026.

•e-Estonia. “Mobile ID - E-Estonia.” E-Estonia, 9 June 2024, e-estonia.com/solutions/estonian-e-identity/mobile-id/. Accessed 8 Feb. 2026.

•Republic of Estonia. “Data Embassy.” E-Estonia, 2018, e-estonia.com/solutions/e-governance/data-embassy/. Accessed 8 Feb. 2026.

•Ottis, Rain. Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective. 2008.

•NATO. “Strategic Concepts.” NATO.int, 2022, www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts. Accessed 8 Feb. 2026.

•Maurer, Tim. Cyber Mercenaries : The State, Hackers, and Power. Cambridge, United Kingdom ; New York, Ny ; Australia, Cambridge University Press, 2018.

•European Commission. “The EU’s Cybersecurity Strategy for the Digital Decade | Shaping Europe’s Digital Future.” Digital-Strategy.ec.europa.eu, 2020, digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0. Accessed 8 Feb. 2026.

•European Union. “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).” Europa.eu, 27 Apr. 2016, eur-lex.europa.eu/eli/reg/2016/679/oj. Accessed 8 Feb. 2026.