From fragmentation to flexibility: Architecting European digital resilience

by Christian M. Bissinger and Hanna Zylowski

I. Introduction: From ‘wartime survival’ to ‘societal continuity’

When missiles struck Kyiv in 2022, the Ukrainian state didn’t collapse, it migrated. The Diia application, originally launched in 2020 as a comprehensive e-government tool (Sirtaine and Torre, 2024), transformed overnight into a ‘digital lifeline’ between the state and its citizens. However, while Diia’s reactive agility was a success, its rapid centralisation under pressure created technical vulnerabilities and potential single points of failure (European Union Agency for Cybersecurity, 2023). For the European Union (EU), the lesson is clear: it cannot wait for a crucible moment to weld systems together. It requires a digital foundation that ensures preparedness and societal continuity, utilising distributed models such as Estonia’s geographically distributed data embassies to safeguard core state functions even during territorial attacks (e-Estonia, n.d.).

This resilience model is no longer a purely civilian concern, but it could be utilised as a strategic foundation for transatlantic collective defence. Therefore, with the latter increasingly relying on civilian digital logistics, deeper EU-NATO collaboration is essential to align the Union’s regulatory power with operational security requirements, such as the transportation of military assets. For instance, in case of any future armed conflict on the Eastern Front, the mobility of the alliance’s military assets is key. This article assumes that resilience is not about securitising the state, but about ensuring the social contract remains intact through decentralised, interoperable, and rights-protective infrastructure.

Therefore, this article addresses the following research question: *‘How can the EU design digital infrastructure that ensures both security and civil rights for times of peace and crisis?’*. Furthermore, digital resilience is not considered a reactive patch but rather a property of the architecture itself, serving as a foundation that ensures the state remains capable even under extreme hybrid pressure.

II. Between adaptation and anticipation: Resilience by design as a prerequisite for a European capacity to defend itself

Digital infrastructure rarely attracts critical scrutiny under normal operating conditions. However, crises expose what routine functioning conceals: whether a system has been genuinely engineered for resilience or merely designed to appear so (Ferroli and Weich, 2026). The cases examined below illustrate this distinction. Ukraine’s Diia application is emblematic of what happens when a well-functioning digital governance platform meets a full crisis. Therefore, launched as an e-government tool offering digital IDs, tax services, and business registration, Diia was a success story of modern public administration (Ministry of Digital Transformation of Ukraine, 2020). However, when Russia’s full-scale invasion began in February 2022, the platform was rapidly expanded beyond its original scope. Features such as the eVorog chatbot, which enables citizens to report geolocated information on enemy troop movements, were integrated under acute pressure and within a very short timeframe (Interfax-Ukraine, 2022).

This reactive expansion produced two structural problems. Technically, the rapid centralisation of functions created new vulnerabilities. As more critical services were consolidated into a single platform, the system became increasingly exposed to the risk of cascading failure. A successful cyberattack, server outage, or connectivity disruption targeting Diia could simultaneously disable citizen identification, military reporting, and essential administrative services. If these functions had remained distributed across separate systems, they would have failed independently rather than all at once (ENISA, 2023). Legally, the boundary between citizen-as-users and citizen-as-participants in security-relevant activities became increasingly blurred, with consequences that were neither planned nor fully foreseeable at the time. To learn more about the legal implications of this shift, particularly regarding civilian protection under international humanitarian law, please refer to Benda and Stoian (2026). Ultimately, the architectural conclusion is clear: reactive design provides short-term resilience, but at a cost that cannot be assessed in advance. Hence, crisis-driven design is not a model for peacetime.

Estonia shows a different approach, not as a reaction to a crisis, but as a deliberate architectural choice in peacetime which was built on three pillars. First, a decentralised data architecture: X-Road connects public authorities without centralised data storage, meaning that if one node fails, the network continues to operate (Information System Authority of Estonia, 2022). Second, legally secure identity systems: the eID gives citizens control over their own identity, keeping them 'citizen-as-client' with rights built into the architecture, not added as an afterthought (e-Estonia, 2024). Third, geographically distributed data storage: data embassies safeguard core state functions even in the event of territorial attacks, ensuring the state cannot be digitally wiped out (e-Estonia, 2018).

What these three pillars share is that none of them required citizens to take on security roles, nor did their design presuppose a military emergency. Therefore, resilience by design works without militarisation and without drawing citizens into security functions. Robustness is embedded in the architecture before any crisis demands it. For instance, Estonia has a population of 1.4 million people and a unified system. On the other hand, the EU has 27 member states with different systems and different levels of appetite for the delegation of their digital sovereignty (Ferroli and Weich, 2025).

Consequently, one approach to alleviating this tension is to implement systems that perform purely administrative functions during peacetime through their architecture alone. This requires no restructuring or emergency upgrades when a crisis occurs. There are several possible attributes to this: a decentralised identity system held by the citizen continues to function even if ministry servers fail; geographically distributed data servers remain operational even when one node is attacked; and interoperable standards between member states to ensure continuity even when a national system is compromised. In this model, resilience is not an additional function layered onto existing infrastructure, but it is a property of the architecture itself.

Nevertheless, building this kind of architecture at the EU level requires three things: a shared identity infrastructure that resides with the citizens, standards that enable national systems to communicate without undermining sovereignty, and resilience requirements that public administration approaches on terms comparable to those governing critical infrastructure. Does the EU already have these building blocks? The following part shows that the answer is manifold.

III.I The European framework: Sovereignty through collective standards

Identity as a personal fortress: The EUDI wallet

The EU Digital Identity (EUDI) Wallet is legally mandated by Regulation (EU) 2024/1183, requiring all EU member states to provide at least one digital wallet to citizens by the end of 2026 and mandatory acceptance by private-sector entities by late 2027. This digital wallet would enable the transition from centralised state databases to decentralised citizen-led identity, where citizens can choose which verified attributes (e.g., diplomas, bank accounts, driving licenses) to disclose, without revealing unnecessary personal data. The technology behind, such as on-device storage, minimises risks and ensures that even in a cyber-conflict, a citizen's 'legal personhood' remains under their control (Podda et al., 2025; European Commission, 2024b). Therefore, in a theoretical scenario where a hostile actor executes a denial-of-service (DDoS) attack against a central ministry, citizens holding valid credentials in their EUDI Wallets could still prove their identity to access medical services, cross borders, or open bank accounts. Thus, the EUDI Wallet's 'Privacy as Security' design minimises data collection and maximises security, whilst aligning with the EU's General Data Protection Regulation (GDPR).

Mandating continuity: NIS2 and Critical Entities Resilience Directives; Interoperable Europe Act

Since October 2024, the EU's NIS2 Directive has expanded cybersecurity obligations to public administrations at different levels, classifying them as 'essential entities' alongside energy, healthcare and transport. Whilst public administration was historically viewed as a service provider distinct from critical infrastructure, the war in Ukraine shattered this distinction as digital government services have become the primary lifeline for displaced populations. Currently, NIS2 obliges public administrations to adhere to the same resilience requirements, including power grids and other types of critical infrastructure (European Commission, 2022). This profound shift in governance implies that the 'digital state' must maintain comparable uptime and recovery standards to a power grid. In this sense, a town hall's server going down is no longer an administrative annoyance, but it is a breach of critical infrastructure compliance (Pop and Centeno Casado, 2025).

The Critical Entities Resilience (CER) Directive complements NIS2 insofar as it requires EU member states to conduct risk assessments and identify critical operators by July 2026, with a focus on physical security and cross-border threats (European Commission, 2024a). Accordingly, the Interoperable Europe Act (IEA) mandates cross-border communication between EU member state public-sector digital services, such that a German passport must be readable by Swedish scanning systems. In this context, the failure of any single national system has direct and immediate consequences for the cross-border mobility of its citizens.

By mandating open standards and cross-border data flows, the IEA allows for overcoming national digital silos and establishing fail-safes. This governance architecture ensures that the collapse of a single node does not compromise the social contract across the bloc, building redundancy through the standardisation of inter-state communication frameworks rather than through data duplication, thereby sustaining service continuity even under conditions of localised infrastructure stress. While these new standards advance more harmonised approaches to incident reporting, risk management, and continuity planning, the European Cyber Security Organisation and the European Parliament have both identified EU-wide cybersecurity certification and real-time threat intelligence sharing as necessary complements to address remaining gaps in cross-border coordination.

Federated digital resilience: The Belgian Common Services for Access Management

Known for its complex, multi-layered federalism, Belgium has inadvertently built one of the most resilient digital architectures in Europe through its Federal Authentication Service, as part of the Common Services for Access Management (CSAM) system. Hence, Belgium's political fragmentation between federal, regional (Flanders, Wallonia, Brussels), and community levels forced it to adopt a federated identity model long before it was a security best practice. Indeed, the CSAM provides a federated identity and access management platform for all levels of government (CSAM, 2026). By using 'Single Sign-On' and decentralised authentication, it ensures that if one access point, such as services at the regional level, is compromised, the core federal authentication and the rest of the network can theoretically remain operational (Cybersecurity Coalition, 2024). Whilst relying on a network of trusted identity providers instead of a centralised system, the design of CSAM incorporates digital resilience as an overarching principle.

Belgium illustrates that political complexity, when architected correctly, can be a feature of a digital state that is modular, segmented, and more resilient. Its model can be seen as a potential blueprint for EU-wide digital resilience, as it aligns with the EU's regulatory framework for the digital sphere, such as the IEA's objectives for cross-border cooperation, and a decentralised and modular infrastructure. If one were to assume that the Belgian CSAM is a good blueprint for EU-wide harmonisation, the following challenge remains: how to ensure that singular EU member state systems, such as CSAM and Estonia's national digital infrastructure, remain interoperable?

Looking forward, it will be key for the EU to reduce reliance on foreign cloud providers, i.e. via supporting the creation of EU digital unicorns. In this sense, the Digital Networks Act adopted in January 2026 which aims to *'modernise the legal framework for connectivity to boost innovation and investment in an advanced and resilient digital infrastructure'* (European Commission, 2026) in the Union, is a good step towards the EU and member states becoming more independent, whilst improving overall digital resilience. Therefore, increasing the EU's digital resilience is a key component of a potential future EU preparedness policy.

III.II The strategic horizon

Digital resilience is no longer a matter of domestic policy, but it has become a question of geopolitical stability. An overwhelming part of modern state functions is now digitised. For instance, energy grids, transport networks, administrative registers, and identification systems form the backbone of governance, and they are increasingly the target of hybrid attacks that aim to destabilise societies without firing a single shot (NATO–EU Joint Declaration, 2023). Consequently, when civilian digital services collapse, it is not only citizens who are stranded, but it is the operational capacity of the entire alliance.

This is the structural paradox at the heart of Euro-Atlantic security. NATO holds the operational capabilities for collective defence, but it has no regulatory authority over the civilian infrastructure; it depends on ports, railways, and digital logistics systems (Bendiek and Kerttunen, 2023). Conversely, the EU holds the regulatory power to set binding standards across its member states, but it does not command troops. However, twenty-three of the twenty-seven EU member states are also NATO allies. This institutional overlap is not a complication. Hence, it is a strategic opportunity, provided the division of labour is properly coordinated. However, as Bendiek and Kerttunen (2023) note, the EU's central weakness remains the absence of focused and proactive joint assessment to respond to shared threats.

Nowhere is this gap more visible than in military mobility. Hence, modern defence capabilities depend not only on roads, bridges and air corridors; they depend increasingly on digital authorisation procedures, interoperable customs systems, and harmonised regulations for the transport of dangerous goods. Additionally, because of administrative fragmentation, moving military equipment across the EU can sometimes take over a month (European Parliament, 2025a).

From governance tools to strategic foundations

This is precisely what the concept of a 'digital military Schengen' addresses. In November 2025, the European Commission presented its Military Mobility Package, proposing a binding regulatory framework to remove procedural barriers, harmonise rules, and establish a digital platform for cross-border movement authorisations (European Commission, 2025a). The European Parliament stressed that military mobility is a priority for EU-NATO cooperation and essential to enable the movement of allied forces in times of peace and crisis. Critically, meeting these ambitions is not purely a logistical or political challenge, it is a digital one. Moreover, achieving the proposed rapid reaction force deployment timelines of three days under peacetime conditions and 24 hours during a crisis, benchmarked explicitly against NATO standards, is contingent on the resilience of the underlying digital infrastructure, including authorisation platforms, customs databases, and interoperability protocols. A cyberattack, a server outage, or a fragmented national system at the wrong moment could freeze troop movements just as effectively as a physical barrier. Therefore, digital resilience is not a background condition for military mobility, but it is a prerequisite for it.

This is not about militarising civilian infrastructure, but about removing bureaucratic friction. The same interoperability logic that underpins the Interoperable Europe Act, which was previously alluded to in Part III.I, is now applied to defence logistics. Indeed, as noted by co-rapporteur Auštrevičius, overcoming administrative burdens and developing dual-use infrastructure is not a luxury but a necessity (European Parliament, 2025a). It is precisely the civilian character of interoperability and administrative coherence that constitutes their strategic credibility. Therefore, the EU instruments examined in part III.I, such as the EUDI Wallet, NIS2, and the IEA, were designed as governance tools, but their strategic significance extends far beyond public administration. The mechanism is precise: EU regulatory standards produce stable and interoperable civilian infrastructure, which in turn ensures that NATO operational capacity remains intact. When the digital systems that underpin border crossings, logistics authorisations, and identity verification continue to function under pressure, allied forces retain the ability to move, coordinate, and act. In other words, the strength of collective defence rests not only on military readiness, but on the resilience of the civilian architecture beneath it (Riedenstein, Echikson & Landrum, 2025). Ultimately, what Estonia understood at the national level, so that the state functions must survive disruption through distributed architecture, the EU is now beginning to institutionalise at scale.

A promise to citizens, a challenge for institutions

Nevertheless, the most powerful argument is not military; it is civil. Therefore, a citizen who retains the ability to prove their identity during a cyberattack, access medical services, cross a border, and open a bank account is not merely protected; they are proof of a functioning state. This is itself a strategic signal: to its own population, that the social contract holds; to potential aggressors, that digital destabilisation will not achieve its goal.

Yet a structural gap remains. While NATO analyses threats, the EU translates them into regulatory standards. However, these two processes still run largely in parallel, which delays the conversion of threat intelligence into concrete protective measures (Lété and Pernik, 2017). Existing coordination mechanisms, such as the NATO Permanent Liaison Team at the EU Military Staff in Brussels, the EU Cell at SHAPE in Mons, seven structured dialogues covering areas such as cyber and military mobility, and three joint declarations (2016, 2018, 2023), provide a basis for information exchange. Yet these formats remain largely consultative: they facilitate mutual briefings, but do not systematically translate threat assessments into binding regulatory responses, leaving a structural gap between NATO's threat analysis and the EU's standard-setting processes (Lété and Pernik, 2017).

Nevertheless, greater coordination does not require new institutions. Indeed, it requires better use of existing formats: structured dialogue and voluntary platforms for digital resilience which are flexible enough to accommodate the different strategic preferences of member states (NATO–EU Joint Declaration, 2023).

IV. Conclusion: Resilience as the new social safety net

When Russia launched its full-scale offensive against Ukraine in 2022, the latter had no choice but to expand its digital resilience under acute pressure. On the other hand, Estonia had made that choice decades earlier, without a crisis forcing its hand. The difference was not necessarily technology; it was timing. Ukraine showed what happens when resilience is built reactively: it works, but at a cost that cannot be fully anticipated. Conversely, Estonia showed what happens when resilience is designed into the architecture from the start: it simply holds. Therefore, the EU's task is not to choose between these two models, but to learn from both and to start building what cannot be improvised in a genuine crisis context.

In relation to this, the instruments examined in this article, from the EUDI Wallet, NIS2, and IEA, to the Belgian CSAM model, are not emergency measures. They are the quiet infrastructure of a functioning social contract that shows that the EU's regulatory competence and NATO's operational capacity are not parallel attributes, but complementary ones. Together, they form an interdependent digital resilience architecture.

For countries such as Germany, adopting these European standards is the guarantee of peace through an architecture that does not break under pressure. Therefore, in an era of hybrid threats, digital resilience is not only a security project but also a civic right. Building it in peacetime is the most consequential political choice the EU and single member states can make.

Annexes

Definitions

- **Data Embassie**s: servers storing encrypted copies of central government registers abroad, which remain under the legal sovereignty of the originating state, ensuring the continuity of core state functions during territorial disruption or cyberattacks (e-Estonia, 2018);
- **Digital resilience:** capacity of an entity to 'anticipate, absorb, recover from and adapt to adverse events' that may affect its digital assets (EU Agency for Network and Information Security (ENISA), 2017);
- **Dual-Use infrastructure:** items that can be used for both civil and military applications. In a digital context, this includes software and technology that can 'functionalise' civilian infrastructure for military logistics or surveillance. For further details, refer to EU Regulation 2021/821, which aims to set up an EU regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items;
- **EU Digital sovereignty:** the EU's capability to decide how data is collected, stored, processed, and transferred, independent from foreign entities or external legal systems in its own jurisdiction;
- **Hybrid threats:** combine military and non-military as well as covert and overt means, including disinformation, cyber-attacks, and economic pressure. These aim to destabilise and undermine societies and the functioning of the state (Adapted from: Lee. Joe, 2025);
- **Interoperability:** the capacity of different (digital) systems to exchange and use information seamlessly across technical, institutional and geographical boundaries. In the EU context, this allows national infrastructures to function together without centralising data or control. (Adapted from: Regulation (EU) 2024/903, Interoperable Europe Act);
- **Self-Sovereign Identity** (SSI): a model of digital identity where the individual has full ownership and control over their data without relying on a central administrative authority to act as an intermediary for every transaction (Adapted from: Schardong and Custódio, 2022);
- **Single Sign-On:** an authentication method allowing users to log in once with a single set of credentials (i.e. one username/password) to access multiple independent applications, services, or websites;
- **Strategic capabilities**: refer to the entirety of the military, political, technological and infrastructural assets of a state or alliance that are necessary to ensure security, manage crises and credibly implement collective defence.

Bibliography

- Benda, Malte and Stoian, Iasmina (2026). *Dual-use GovTech and Civilian Protection: How digital public services evolve into security infrastructures, a story of Ukraine and Estonia*. EPIS Thinktank e.V. Magazine Article. Available at XYZ (Accessed: XYZ)
- Bendiek, A. and Kerttunen, M. (2023). *Enhancing EU-NATO Cooperation: Critical Infrastructure Protection*. SWP Working Paper. Berlin: Stiftung Wissenschaft und Politik. Available at: https://www.swp-berlin.org/publications/products/arbeitspapiere/SWP_WP_Enhancing_EU-NATO_Cooperation_Critical_Infrastructure_Protection_Bendiek_Kerttunen.pdf (Accessed: 24 April 2026)
- CSAM. (2026). *About CSAM*. Federal Public Service Policy and Support (BOSA). [online] 20 January. Available at: https://www.csam.be/en/about-csam.html (Accessed: 03 April 2026)

- Cybersecurity Coalition. (2024). *Report Focus Group Identity & Access Management: Decentralised Digital Identity*. [online] 2 October. Available at: https://cybersecuritycoalition.be/resource/report-focus-group-identity-access-management-decentralised-digital-identity/ (Accessed: 29 April 2026)
- e-Estonia. (2018). *Data Embassy – the digital continuity of a state*. [online] Available at: https://e-estonia.com/solutions/e-governance/data-embassy/ (Accessed: 05 April 2026)
- e-Estonia. (2024). *eID – Digital identity*. [online] Available at: https://e-estonia.com/solutions/e-identity/id-card/(Accessed: 29 April 2026)
- EU Agency for Network and Information Security (ENISA). (2017). *Overview of Cybersecurity and Related Technology*. Available at: https://www.enisa.europa.eu/sites/default/files/all_files/2017-09-07-ENISAoverviewOfCybersecurityAndRelatedTechnology.pdf (Accessed: 29 April 2026)
- EU Regulation 2021/821. *Setting up an EU regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items*. Available at: https://eur-lex.europa.eu/EN/legal-content/summary/dual-use-export-controls.html (Accessed: 09 April 2026)
- European Commission. (2022). *The NIS2 Directive*. [online] 27 December. Available at: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (Accessed: 29 April 2026)
- European Commission. (2024a). *The CER and NIS2 Directives enter into application*. [online] 26 March. Available at: https://ec.europa.eu/newsroom/cipr/items/859754/en (Accessed: 09 April 2026)
- European Commission. (2024b). *The security and privacy features of EU Digital Identity Wallets*. [online] 15 July. Available at: https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/712508927/Security+and+Privacy (Accessed: 29 April 2026)
- European Commission. (2025a). *Military Mobility Package: Joint Communication and Regulation Proposal*. COM(2025) 847. Available at: https://transport.ec.europa.eu/transport-themes/military-mobility_en (Accessed: 29 April 2026)
- European Commission. (2026). *The Digital Networks Act*. [online] 21 January. Available at: https://digital-strategy.ec.europa.eu/en/policies/digital-networks-act (Accessed: 20 April 2026)
- European Cyber Security Organisation (ECSO). (2025). *NIS2 White Paper*. [online] 15 January. Available at: https://ecs-org.eu/ecso-uploads/2025/01/ECSO-NIS2-White-Paper.pdf (Accessed: 29 April 2026)
- European Parliament. (2025a). *MEPs back "military Schengen" to help withstand potential Russian aggression* [Resolution on military mobility]. Strasbourg: European Parliament. Available at: https://www.europarl.europa.eu/news/en/press-room/20251211IPR32166 (Accessed: 29 April 2026)
- European Parliament. (2025b). *Report on European technological sovereignty and digital infrastructure*. [online] 11 June. Available at: https://www.europarl.europa.eu/doceo/document/A-10-2025-0107_EN.html (Accessed: 29 April 2026)
- European Union Agency for Cybersecurity (ENISA). (2023). *Report on the Resilience of e-Government Services*. Athens: ENISA.
- Ferroli, F. and Weich, S. (2026). *Europe's Digital House of Cards: The Race to Build Resilience*. dotmagazine, eco – Association of the Internet Industry. [online] March. Available at: https://www.dotmagazine.online/issues/data-centers-digital-infrastructure/europe-digital-resilience-federation (Accessed: 02 March 2026)
- Information System Authority of Estonia. (2022). *X-Road*. [online] Available at: https://www.ria.ee/en/state-information-system/x-tee.html (Accessed: 29 April 2026)
- Interfax-Ukraine. (2022). *Diia app gets eVorog chatbot for reporting enemy troops*. [online] Available at: https://en.interfax.com.ua (Accessed: 29 April 2026)
- Lee, J. (2025). *What is Digital Sovereignty?* Trendmicro. [online] 9 December. Available at: https://www.trendmicro.com/en_us/what-is/data-sovereignty/digital-sovereignty.html (Accessed: 29 April 2026)
- Lété, B. and Pernik, P. (2017). *EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions*. German Marshall Fund of the United States. Available at: https://www.gmfus.org/news/eu-nato-cybersecurity-and-defense-cooperation-common-threats-common-solutions (Accessed: 29 April 2026)
- Ministry of Digital Transformation of Ukraine. (2020). *Diia – State in a Smartphone*. [online] Available at: https://diia.gov.ua (Accessed: 12 March 2026)
- NATO–EU Joint Declaration. (2023). *Third Joint Declaration on EU-NATO Cooperation*, 10 January 2023. Available at: https://www.consilium.europa.eu/en/press/press-releases/2023/01/10/eu-nato-joint-declaration/ (Accessed: 14 April 2026)

- Podda, E., Hölzmer, P., Amard, A., Sedlmeir, J. and Fridgen, G. (2025). The impact of zero-knowledge proofs on data minimisation compliance of digital identity wallets. *Internet Policy Review*, 14(3). Available at: https://policyreview.info/articles/analysis/impact-zero-knowledge-proofs (Accessed: 29 April 2026)
- Pop, F. and Centeno Casado, L. (2025). *The NIS2 Directive: the road map to strengthen cybersecurity across the EU*. *EIPA*. [online] 11 February. Available at: https://www.eipa.eu/blog/the-nis2-directive-the-road-map-to-strengthen-cybersecurity-across-the-eu/ (Accessed: 11 April 2026)
- Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act). *OJ L*, 2024/903, 22.3.2024. Available at: https://eur-lex.europa.eu/eli/reg/2024/903/oj (Accessed: 29 April 2026)
- Riedenstein, C., Echikson, W. and Landrum, L. (2025). *Defend in the Cloud: Boost NATO Data Resilience*. Center for European Policy Analysis (CEPA). [online] 30 April. Available at: https://cepa.org/comprehensive-reports/defend-in-the-cloud-boost-nato-data-resilience/ (Accessed: 29 April 2026)
- Schardong, F. and Custódio, R. (2022). *Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy*. Sensors (Basel), 22(15), p.5641. doi: 10.3390/s22155641
- Sirtaine, S. and Torre, A. (2024). *Ukraine's Diia: A Digital Lifeline in Times of Crisis. CGAP*. [online] 24 October. Available at: https://www.cgap.org/blog/ukraines-diia-digital-lifeline-in-times-of-crisis (Accessed: 02 April 2026)