Digital Governance in Practice 2026

Lead the Digital Future. Learn from the Best.

Study visits and training programmes on-site

Strategic study visits and training programmes for executives and experts driving digital transformation.

- Practical and tailored to your needs and goals.
- Delivered by Estonia's digital governance experts.
- From executive sessions to week-long programmes on-site and online.

Digital Learning for Public Sector Transformation

e-Governance Academy's Digital Learning Hub empowers public institutions in building digital capacities at every level – from leadership to frontline staff

Equip your team with a shared understanding of digital governance

Flexible	Learn anytime, at your own pace
Accessible	Available wherever your team is
Customisable	Tailored to your strategic goals and local context. Perfect for onboarding, capacity-building, and change management

Training for Trainers (ToT) – Expert-led ToT covers all aspects of digital learning

How it works

- Secure access with individual user logins
- Engaging content: videos, multimedia, quizzes, real-life case studies
- Multilingual options and technical support available

Get started

Visit our digital learning environment

A free sample course is available for everyone
Just register to get started

CERTIFIED ISO 9001

eGA e-governance academy

Digital Governance in Practice 2026

Chief editor and project manager:	Anu Vahtra-Hellat
Editor:	Liis Linn
Authors:	Hannes Astok, Oleg Burba, Mark Erlich, Piret Hirv, Kristiin Jets, Kadi Kanarbik, Kristi Kivilo, Oleksandr Kozlov, Marit Lani, Liis Linn, Merle Maigre, Tõnis Mäe, Elsa Neeme, Katrin Nyman-Metcalf, Marge Oldermann-Neeme, Mari Pedak, Taimar Peterkop, Federico Plantera, Piret Saartee, Priit Vinkel, Carlos Vargas, Ene Višnev, Rica Williams, Anto Yermakov
Proofreading:	Refiner
Design:	Dada AD
Photos:	Adobe Stock, eGA, Jake Farra, Stas Kartashov, Rasmus Kooskora, Raul Mee, Jakob Meier, Edmond Mäll, Raigo Pajula
Cover photo:	Sedge (carex cespitosa) by Argo Argel

Contents

eGA at a glance **6**

Entering the age of artificial intelligence **8**
/Hannes Astok

Highlights of 2025 **10**

Publications **13**

The e-Governance Conference: A mirror, a map and a springboard **14**

Trends of Digital Transformation **15**

AI in society: Treasure chest or Pandora's box? / Dr Katrin Nyman Metcalf 16

From pilots to practice: What it takes to make AI work in government / Piret Hirv 20

Scaling AI skills through global cooperation / Kristi Kivilo 23

From aid dependency to data sovereignty / Piret Hirv 27

Redesigning digital evidencehandling / Piret Saartee, Kadi Kanarbik 30

Stopping corruption in construction through digitalisation / Anton Yermakov 33

LAC countries' approach to digital transformation and cross-border collaboration / Carlos Vargas 36

EUDI Wallets beyond the app: What Europe is really building / Oleksandr Kozlov 39

Ukraine's case: Moving towards the EU's single digital market / Oleg Burba 42

From networks to norms: Critical infrastructure and trust in digital democracies / Elsa Neeme 45

Lessons from Ukraine on protecting critical infrastructure / Taimar Peterkop 48

Building cyber defence through NATO cooperation / Liis Linn 52

Building cyber resilience: Global insights into government preparedness / Marit Lani 54

Strengthening cyber defence through practice / Merle Maigre 55

Keeping people at the centre of cybersecurity / Rica Williams 58

Western Balkans: Building cybersecurity awareness through local action / Kristiin Jets 61

Enhancing capacity and cooperation through cyber diplomacy education / Ene Višnev 64

What makes digital identity work / Mark Erlich 66

Key considerations for planning a national digital architecture / Tõnis Mäe 68

The power of digital learning / Marge Oldermann-Neeme 70

From startup to system: Ukraine enters a new phase of digital transformation / Mari Pedak 72

What 2025 taught us about elections, technology and trust / Priit Vinkel 75

"Big Brother" under control: Estonia and Ukraine are letting citizens check who's watching / Federico Plantera 79

Organisation at a glance **83**

We are the e-Governance Academy! 84

eGA outstanding colleagues in 2025 85

Kristina Reinsalu: Engagement is not an add-on. It runs through everything we do / Liis Linn 86

eGA's activities in figures 2003–2025 **89**

Organisation chart **92**

Increasing the prosperity and openness of societies

Driven by our mission, eGA experts have, since 2002, worked with 308 organisations and 147 countries around the world to build successful digital societies that improve citizens' lives, strengthen their economies and deliver transparent, democratic and effective public administrations.

The e-Governance Academy (eGA) is a centre of excellence to increase the prosperity and openness of societies through digital transformation.

CERTIFIED ISO 9001

High-quality services

eGA's management system for project implementation, study visits and consulting services has been independently certified to the ISO 9001:2015 standard.

Trusted partner

eGA completed the the European Commission's pillar assessment and can implement large-scale digital projects supported by the European Union. Moreover, eGA has successfully collaborated with donors such as USAID, the World Bank, UNDP, SIDA, EBRD, ESTDEV and many others. eGA also works with ENISA, GFCE and NATO to enhance countries' cybersecurity.

eGA at a glance

DT4UA & DT4UA Phase II
the largest project by activities and funding, totalling €27.4 M

Tonga
eGA's most geographically distant engagement

Ukraine
the most supported country, with six ongoing projects

37,600
downloads of Digital Government Podcast episodes since 2020

11,500
government leaders participated in our training programmes, 2002–2025

2,000+
participants trained via digital learning courses

380+
projects implemented since 2003

308
partner organisations collaborated with since 2004

140+
countries featured in the National Cyber Security Index 3.0

2025 at a glance

€26.5 million
in annual turnover

2,488
days spent on onsite consultations across 206 missions

903
participants from 54 countries attended 36 training events

655
participants from 85 countries joined the 11th e-Governance Conference in Tallinn

103
procurements conducted totalling **€9.3 million**

40
projects implemented with 70 countries

Entering the age of artificial intelligence

Hannes Astok
Executive Director

Photo: Hannes Astok promoting collaboration with Ukraine at the DT4UA project event.

At the end of 2024, it seemed like the world could not possibly get any worse – that all the madnesses had already happened. But then 2025 began, and we realised that the situation can always get worse. As of the beginning of 2026, things have deteriorated even further.

Global politics is shifting from a values- and agreement-based order toward transaction-based policy. Eighty years of effort to make agreements matter is fading into history.

The United States Agency for International Development (USAID) was dismantled in a single month, leaving behind a significant gap, including in digital development cooperation.

Global development cooperation is changing as well. Here too, values are being replaced by transactions, and transactions are not necessarily value-based.

The war in Ukraine shows no signs of ending. The more fragmented the common front against Russia becomes, the more emboldened Russia is. But the war in Ukraine is not a transaction. It is the fight of a free Ukrainian people for their country, their nation and their independence. And only Ukrainians can decide Ukraine's future, not superpowers negotiating behind Ukraine's back.

> Supporting Ukraine is part of the e-Governance Academy team's daily work.
>
> Hannes Astok

Supporting Ukraine is part of the e-Governance Academy team's daily work. Our 35-member team in Kyiv, together with experts and back-office staff in Estonia, continues to support Ukraine by building digital solutions, preparing for EU accession and strengthening cyber resilience.

We are also witnessing a shift in buzzwords. Blockchain is giving way to artificial intelligence. But unlike blockchain, AI is not just a buzzword. In 2026, the question is no longer whether AI will be used in governance but how, and on whose terms. As these questions are answered, the coming decade will be shaped by the adoption of AI in governance and in our everyday lives.

Photo: The President of Estonia Alar Karis and Hannes Astok at the e-Governance Conference.

One thing, however, must be clear from the start: AI does not change responsibility. When public authorities use AI, they remain fully accountable for the decisions they make. Responsibility cannot be delegated to algorithms, models or systems.

Alongside this, the issue of transparency in decision-making becomes even more critical. Transparency is not a technical feature; it is a fundamental democratic requirement. Without it, trust disappears. And without trust, democratic governance and democratic societies cannot function.

As we at eGA have seen through successive technological waves, the weakest link in adoption is people. Public institutions must understand the tools they use – their limits and their risks. Civil servants need the skills and confidence to ask the right questions, to recognise when AI helps and when it does not, and to assess whether the necessary enablers for AI adoption are even in place. The choices governments make today will determine what AI becomes tomorrow.

> If we invest in responsibility, openness and people, AI can strengthen institutions rather than erode them.
>
> Hannes Astok

If we prioritise speed over accountability, efficiency over transparency, and innovation over people, AI will weaken governance – even if it appears to make it faster. If we invest in responsibility, openness and people, AI can strengthen institutions rather than erode them. This path might be slower.

Our experience in Estonia shows that AI must be made accessible to everyone and that schoolchildren and university students in particular must learn how to use it. In the next decades, they will be the engineers, teachers and politicians who shape our lives.

To explore how these principles can be put into practice, I invite you to read this publication, Digital Governance in Practice 2026, and engage with the insights and guidance of e-Governance Academy experts, drawn from real-world experience across diverse countries and contexts.

Unfortunately, there is no indication that the world in 2026 will be any more peaceful or predictable. But here at the e-Governance Academy, we still believe – perhaps even naively – that together with you, our partners and readers, we can make the world a better place to live.

> Here at the e-Governance Academy, we still believe that together with you, our partners and readers, we can make the world a better place to live.
>
> Hannes Astok

Highlights of 2025

Partner of the Year 2025 is the Ministry of Public Administration of Montenegro

The e-Governance Academy (eGA) recognised the Ministry of Public Administration of Montenegro as its Partner of the Year 2025 for outstanding cooperation in strengthening national cybersecurity and interagency coordination. With support from eGA and the European Union, the partnership enhanced election-related cybersecurity, deployed key cybersecurity tools, delivered extensive CSIRT (Computer Security Incident Response Team) trainings and launched a 24/7 Security Operations Centre. Together, these efforts significantly strengthen national cybersecurity, public service resilience and the protection of citizens' rights.

eGA supports Ukraine's European digital integration

Within the DT4UA projects framework, eGA supports Ukraine in aligning its legislation with key European Union digital acts, including eIDAS 2.0, the AI Act, the Data Governance Act, the Data Act, the Interoperable Europe Act and the Critical Entities Resilience (CER) Directive. This work lays the legal and technical foundation for Ukraine's future digital services, supports Ukraine's EU accession path and strengthens its role as an integral part of digital Europe. Harmonisation enables cross-border digital services and trust services and Ukraine's participation in EU pilot projects and expert groups as an equal partner. The goal is to ensure full compatibility between Ukrainian and European systems, allowing citizens and businesses to use digital services seamlessly at home and across the EU. Read more on pages 42-44.

Technical support and policy advice for Belgium, Germany and Spain

In 2025, eGA supported **Belgium**, **Germany** and **Spain** in accelerating digital transformation in public administration. In Belgium, cooperation with the courts improved digital evidence management and streamlined case handling, strengthening the efficiency and accessibility of the justice system. In Germany and Spain, eGA supported the modernisation of public services for regional entrepreneurship through a Technology Adoption Roadmap and targeted training, enabling authorities to deploy innovative digital tech, including AI, more effectively. Funded by the **European Union via SG Reform**, these projects delivered practical reforms, strengthened institutional capacity and advanced digital governance in support of economic growth and societal resilience.

Tallinn Cyber Diplomacy Summer School brought together cyber experts from 54 countries

The sixth edition of the Tallinn Cyber Diplomacy Summer School convened 60 diplomats and experts from 54 countries for a high-level programme on international cyber cooperation. Over one week, participants explored international law, responsible state behaviour and the governance of emerging technologies such as AI. This global event was organised by Estonia's Ministry of Foreign Affairs, the e-Governance Academy (eGA) and the Estonian Centre for International Development (ESTDEV) and supported by the European Commission Directorate-General for International Partnerships (DG INTPA). Read more on pages 64-65.

Tallinn Cyber Capacity-Building Fellowship Programme launched

The Tallinn Cyber Capacity-Building Fellowship Programme brought together 20 cybersecurity professionals from around the world for two weeks of online and in-person collaboration in Estonia. The fellowship focused on action-oriented outcomes, with participants developing policy briefs, project proposals and roadmaps based on real national needs. Co-organised by the e-Governance Academy and the Estonian Ministry of Foreign Affairs and funded by the European Commission (Directorate-General for International Partnerships – DG INTPA), the programme strengthens global cyber capacity and fosters a more cooperative and resilient cyberspace. Explore more at cyberdiplomacy.ee.

Strengthening cyber resilience in the Western Balkans: three-year impact

With EU support, the e-Governance Academy (eGA) worked closely with national authorities, CSIRTs (Computer Security Incident Response Teams) and security institutions in Albania, Montenegro and North Macedonia to address growing cyber threats. Through Cybersecurity Rapid Response projects (2022–2025), partner countries strengthened their technical and operational capacity to manage large-scale cyber crises, with a strong focus on risk mitigation and incident response. The projects delivered tangible improvements in cyber preparedness across the region.

Explore the case study

574 Ukrainian cyber experts strengthened their skills through advanced training

Under the exercise "UA–EE Cyber Shield via Tallinn Mechanism", 574 Ukrainian cyber experts from law enforcement, critical infrastructure and academia enhanced their cyber skills through advanced hands-on training. The training strengthened participants' practical skills to address real-world cybersecurity threats. The trainings were delivered jointly by eGA, CybExer Technologies and Ukraine's National Cybersecurity Coordination Centre. Funded by ESTDEV (the Estonian Centre for International Development), the project is part of Estonia's contribution to strengthening Ukraine's cybersecurity and resilience.

eGA main office moved to Golden Gate in Tallinn

The e-Governance Academy's main office relocated to the Golden Gate building in Tallinn. The new premises provide a modern, more functional working environment, offering improved space and comfort for staff and visitors. The office includes a dedicated guest area – eGA Events Hub – available for external meetings and events. We look forward to welcoming partners and guests to our new location!

Book a room for your event

Publications

Strengthening Critical Infrastructure Protection: Strategic Insights and International Best Practices

This publication brings together leading experts and senior officials to share international best practices in critical infrastructure protection and cyber resilience. It offers practical insights into developing national systems, covering NIS2 implementation in Czechia, Albania and Moldova; Poland's integrated crisis management model; Estonia's Situation Centre; Finland's comprehensive defence approach; and Estonia's national resilience and defence framework.

The Cybersecurity Baseline Study sheds light on cyber resilience in Central Asia

The study provides a comprehensive overview of cybersecurity capabilities and challenges in Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan. Compiled by eGA experts, it highlights the region's evolving cybersecurity landscape, with each country at a different stage of digital transformation and cyber maturity.

North Macedonia Elections Cybersecurity Report

The report shares insights on cybersecurity risks related to North Macedonia's electoral processes and offers detailed recommendations to strengthen the resilience of democratic institutions against growing digital threats. The report focuses on the cyber preparedness of election-related IT systems and infrastructure, based on consultations with national stakeholders and research conducted around the 2024 elections. The report is part of the European Union-funded project "Cybersecurity Rapid Response for Albania, Montenegro and North Macedonia 2.0", implemented by the e-Governance Academy.

The e-Governance Conference: A mirror, a map and a springboard

For 11 years, the e-Governance Conference has fostered meaningful connections among digital transformation leaders, experts and donors while addressing the key challenges in digital governance. It has served as a mirror, a map and a springboard, helping participants understand where they stand, envision what is possible, and turn ideas into action.

Throughout its 11-year journey, the conference has focused on sharing knowledge about how technology can empower economies and societies. Hosted in Estonia, one of the world's most advanced digital societies, the conference has offered participants a unique opportunity to explore cutting-edge digital government solutions where they are developed and implemented.

Technology holds immense potential. The real challenge is using it responsibly to deliver meaningful, transparent and measurable outcomes for people, businesses and governments. Digital transformation is not about doing more. It is about doing better, guided by strategic thinking beyond trends and buzzwords.

With this in mind, eGA experts look forward to meeting you around the world or welcoming you again in Tallinn, Estonia, to turn ideas into reality. Digital transformation must continue – meaningfully and with impact.

Highlights from 11 years

- 655 participants on-site (2025)
- 1150 participants online (2020)
- 144 countries represented (2021)

e-Governance Conference 2025 at a glance

- 655 participants from 85 countries in Tallinn
- 100+ speakers from 25 countries across three continents

Rewatch the keynotes, discussions and showcases of #egov2025

Trends of Digital Transformation

AI in society: Treasure chest or Pandora's box?

Dr Katrin Nyman Metcalf
eGA Partner

That AI is part of society is a fact. It would be presumptuous to suggest whether it will prove to be more beneficial than dangerous. Although technology scepticism has existed for as long as technology itself, quite often it was based on a lack of understanding of the innovation, and this lack of understanding could be mitigated by explaining the new tools.

However, for AI, warnings about potential unforeseeable and perhaps unstoppable negative effects are also coming from real experts. Geoffrey Hinton, who won the Nobel Prize in physics in 2024, is one such person. He states: "There is also a longer term existential threat that will arise when we create digital beings that are more intelligent than ourselves. We have no idea whether we can stay in control. But we now have evidence that if they are created by companies motivated by short-term profits, our safety will not be the top priority. We urgently need research on how to prevent these new beings from wanting to take control. They are no longer science fiction."[1]

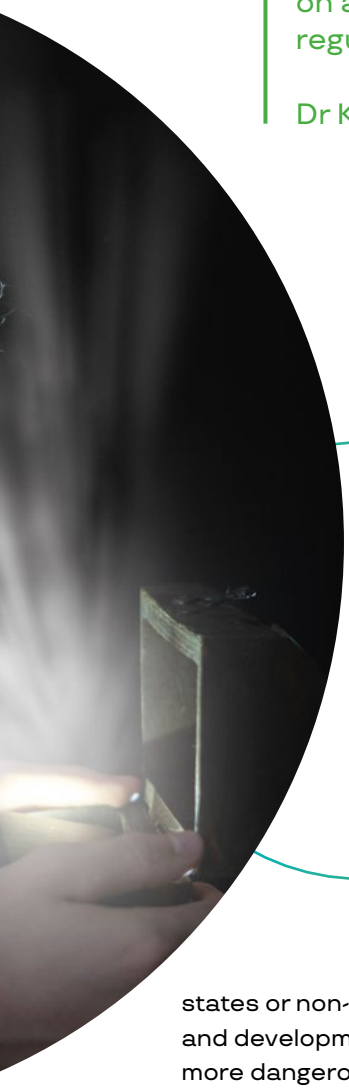
> AI has the potential to make our lives easier, but as with most technologies, it will not do so by itself.
>
> Dr Katrin Nyman Metcalf

Should we de-invent AI?

With such an uncertain outlook, some feel it would be better if AI had not been invented at all and that ideally, it should be de-invented. This is not the first time in history that there have been calls to de-invent a particular technology; similar statements were made about cars and nuclear weapons. Those debates showed the futility of the idea. If something has been invented, it exists, and pretending it does not is unlikely to be effective. Even if some states would agree not to use a technology, other

1 https://www.nobelprize.org/prizes/physics/2024/hinton/speech/

> The right to issue automated decisions, whether using AI or earlier technologies, is based on authorisation norms in acts regulating various fields.
>
> Dr Katrin Nyman Metcalf



states or non-state actors could continue, and developments in the dark would be even more dangerous. Furthermore, the geopolitical landscape of 2026 is hardly conducive to even imagining a global consensus on countering the potential negative effects of new technologies. Not only are states highly likely to come together at this moment, but in addition, private firms (which tend to be more interested in short-term profits) have unprecedented power in the AI field.

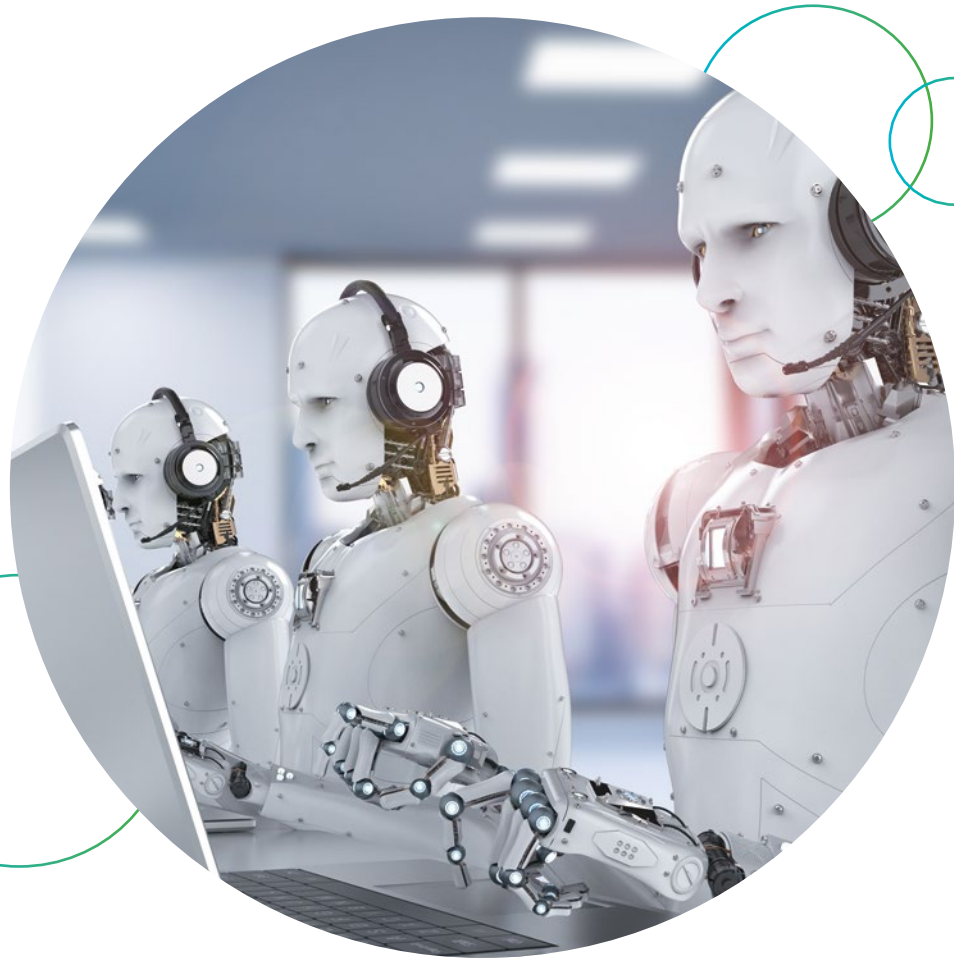
Consequently, we are destined to share our future with AI – at least for as long as AI agrees to share its future with us! Doomsday scenarios with machines taking over make for exciting discussions, but extreme debates may deflect attention from more mundane and immediate concerns. The rapid spread of the technology to users in the private and public sector poses problems and questions that may not threaten humanity with extinction but that nevertheless challenge the rule of law and protection of fundamental rights – or simply make the daily lives of ordinary people less comfortable. AI has the potential to make our lives easier, but as with most technologies, it will not do so by itself. Technologies are generally neither good nor bad – everything depends on how they are used. The same is true for AI, albeit with the important difference that the technology's autonomy may mean that it is not a human who decides how it will be used. This creates an extremely challenging situation for regulation.

Regulations for innovation

In Estonia, people are generally favourable toward the use of technologies for governance. We have used digital tools for more than a quarter-century, and people are familiar with digital data and e-services. Digital solutions are integrated into legislation on many different issues to ensure that digital governance is not separate from "regular" governance but that digitalisation is integrated throughout society. The right to issue automated decisions, whether using AI or earlier technologies, is based on authorisation norms in acts regulating various fields. In a highly digital society, it is easier to move to the most modern technologies. In 2018, the Estonian government established a cross-sectoral expert group to analyse and prepare for the introduction of AI, including the development of a test environment and a study commissioned from the Tallinn University of Technology to determine the legal changes required.

> Regulation does not mean stopping innovation – it means creating an environment in which potential risks must be evaluated.
>
> Dr Katrin Nyman Metcalf

> Perhaps in certain cases, we still need simply to decide not to use a technology, even when it is available.
>
> Dr Katrin Nyman Metcalf



The study (issued in 2019) advised against a single, comprehensive AI law, as the issues were too disparate and the technology was not developed enough to be meaningfully regulated.[2] Estonia participated in the AI regulatory work of the EU, leading to the AI Act in 2024. The fact that this act is already subject to change illustrates just how difficult it is to regulate a technology that is still disparate and rapidly developing, even if it is so widespread that regulation is nevertheless meaningful. Regulation does not mean stopping innovation – it means doing what is possible to prevent negative consequences or at least to create an environment in which potential risks must be evaluated. The AI Act (as well as AI laws in other countries) has an important role in creating systems and institutions that can make risk assessments.

Automation without discretion

Authorities (just like private firms) may be overly eager to automate everything just because it is possible. In the private sector, consumer demands and competition can keep the developments reasonable. For the public sector, policy decisions must be made. If effective digital administration is used wisely, it will free up resources to deal with non-routine queries and human contacts.

Take Estonia as an example. In line with its general technology-friendliness, the government has embraced AI, but the initial uses have been for what may loosely be likened to back-room activities. Even before AI, most queries in the X-Road data interoperability platform were automated, with databases being updated by the machines themselves If technology permits more comprehensive data management, it is unlikely to lead to problems or protests.

2 T. Kerikmäe et al., 1st Report on legal framework and analysis related to Autonomous Intelligent Technologies, Riigikantselei/Estonian Government Office, 2019.

To promote AI use and at the same time make it more transparent, access to open-source AI components is provided for interested parties, whether in the public or private sector, to reuse free of charge.[3] However, delegating discretion to AI is another thing. It is possible that the technology would make fewer mistakes and be less biased than humans, but whether this is the case is largely unknowable, which is the main problem with AI from a legal and human rights viewpoint. Perhaps in certain cases, we still need simply to decide not to use a technology, even when it is available.

Ensuring human-centred administration

In comparison with end-of-the-world scenarios, the concern that AI prevents reasoning for administrative decisions appears insignificant. However, this is one of the seemingly small matters that help to ensure a human-centred administration with the rule of law. If a person knows why a certain decision was made, there is more opportunity to challenge it, for which there should be an independent court process. It is easier to identify discrimination, corruption and nepotism if the decision-maker must explain themselves and ordinary observers can see on what basis something was decided. Access to information is an essential tool in a democratic state: we have to share information about ourselves, and we have to fulfil various obligations in order to live in a society, but we do so in the knowledge that we have a right to know, for instance, how our data is used and what our taxes are paying for. An algorithmic decision presented as a fait accompli deprives us of this key part of the social contract.

So far, there is limited case law on the use of AI, but cases are starting to appear in courts around the world. Complaints in Estonia and elsewhere claim that AI has made wrongful decisions in administrative cases. Still, in many such cases, the outcome of the court deliberations shows that the final decision – the one for which there is discretion, the need to choose between possible outcomes – was made by humans. Even if an AI autonomous decision was made, courts have focused on how humans used the AI and what prompts and what data were given. Thus, the key outcome is that the administration is responsible for its decisions regardless of what technology it uses to reach them.

Trying to stay in control

This is a reasonable principle, but whether it is future-proof is another question. Furthermore, even if courts retain such reasoning, it might not be adequate at a time when administrations might have less and less knowledge about how a certain decision was reached and might not even know the basis on which it was made. We may come to a point where the administration either feels it cannot be responsible or finds itself responsible for something it cannot affect in any way. Today we may say this illustrates why discretionary decisions cannot be made by AI – but can AI be blocked from exercising such powers indefinitely? In the debate, it has been suggested that AI should be given a legal personality, but it is difficult to see how this would provide a solution unless the AI itself can answer in court and rectify any damage.

I am fully aware that this article contains several question marks. As Dr Hinton said, we have no idea whether we can stay in control – but for now, we should at least try. Even just accepting that human rights and the rule of law shall continue to apply under new technological circumstances means something. It is possible to create environments and institutions that ensure that in the development and application of AI, there is a legal (and moral) obligation to consider the technology's potential for good – or bad.

3 The open-source AI components are available in the eGovernment code repository and/or GitHub https://www.kratid.ee/en/kratijupid; https://koodivaramu.eesti.ee/users/sign_in

From pilots to practice: What it takes to make AI work in government

Piret Hirv
Head of Data Management Competence Centre

The conversation around artificial intelligence in government is evolving. Not long ago, the focus was on speed, automation and efficiency – if something could be automated, it should be. Today, that focus has shifted.

Before talking about models or tools, the real question is what problem needs solving and whether AI is the right answer. Experience has shown that many AI pilots fail not because the technology is inadequate, but because governance frameworks, processes and capacities are not yet in place to support their integration into everyday public administration. What is missing is not innovation, but coherence.

The core enablers are missing

In practice, the shortcomings are frequently the same. Data is scattered across institutions and governed unevenly, while issues with data quality often surface only after systems are already in place. Processes are poorly documented, making them difficult to translate into algorithmic logic. Responsibility for AI-supported decisions is blurred and divided among policy units, IT teams and external suppliers. Skills are concentrated in small expert groups rather than embedded across organisations. Under these conditions, scaling AI becomes primarily an organisational challenge rather than a technical one.

This has shaped the way people in the governments and beyond now think about AI projects. They are no longer seen as single interventions, but as journeys that unfold in distinct phases, each requiring different questions and disciplines. Early on, it is essential to assess whether AI is appropriate at all and whether affected users are involved from the start.

During the development of any AI project, data quality, privacy and cybersecurity are not side issues, but core factors that must be addressed by design. AI piloting is not a demonstration exercise, but a moment to surface risks, user concerns and governance gaps. Scaling, when it happens, demands transparency, explainability and clear accountability for outcomes.

Trust as the foundation

Trust runs through all of this. AI in government operates within existing power balances. People accept automation only when decisions remain understandable and contestable. Safeguards, impact assessments and oversight mechanisms are often perceived as slowing innovation, yet they are what enable it. Systems designed to be explainable from the start are easier to govern, audit and trust over time.

Context also matters more than we often admit. Administrative traditions, legal concepts and language shape how public services function. When AI systems fail to reflect this context, services risk becoming less accessible and less fair. This is not an abstract concern: it affects whether citizens understand the decisions made, whether officials trust the tools they use and whether public institutions retain legitimacy in an increasingly automated environment.
Value behind the scenes

There is a strong temptation to focus AI efforts on visible interfaces, especially conversational tools. These can improve access, but the most durable value often emerges behind the scenes. Decision-support systems for caseworkers, analytical tools that improve resource allocation and early warning mechanisms that help governments act proactively often deliver quieter but deeper impact. However, they also require stronger governance and higher-quality data.

> Experience has shown that many AI pilots fail not because the technology is inadequate, but because governance frameworks, processes and capacities are not yet in place.
>
> Piret Hirv

Listen to the episode on AI learning curve feat. Piret Hirv.

AI literacy and risk management are the cornerstones

One of the most important lessons has been about capacity. Sustainable AI cannot be fully outsourced. Governments that invest in digital and AI literacy across the civil service are better equipped to govern technology responsibly. This includes not only technical skills, but the ability to define problems, evaluate outcomes and reflect on unintended effects. Community practices, shared standards and internal learning structures matter more than individual success stories.

5 policy takeaways

1. **Start with the problem, not the technology.** AI delivers value only when it addresses a clearly defined (public service) problem. Automation without purpose rarely scales.
2. **Data quality and data governance matter more than models.** Fragmented, poorly governed data limits impact. Treat data as core public infrastructure, not a technical afterthought.
3. **If the process is unclear, AI will amplify the confusion.** Understanding and simplifying administrative processes must come before automation.
4. **Trust is a prerequisite, not a bonus.** Explainability, accountability, and privacy by design determine whether citizens accept AI in sensitive public services.
5. **Build capacity before scaling solutions.** Lasting impact comes from skilled public servants and institutional learning, not from isolated pilots or outsourced expertise.

Photo: Workshop with Spanish and German beneficiaries on developing AI-enabled public services within SG REFORM supported project.

> AI is a test of how coherent and resilient our digital governance really is.
>
> Piret Hirv

Our understanding of risk has evolved as well. Responsible use of AI is not about avoiding uncertainty or embracing technology blindly, but about managing risk deliberately throughout the lifecycle of a system: setting expectations early, monitoring impacts continuously and being willing to adapt or stop when public value is not delivered.

AI as a governance test

What is most valued over time is sustainability and continuity: not of specific technologies, but of principles, institutions and ways of governing digital change. Trust is not built through constant reinvention. It grows when people recognise stable responsibilities, predictable safeguards and familiar rules, even as tools evolve. In this sense, AI is not a rupture with the past, but a test of how coherent and resilient our digital governance really is.

Seen this way, AI is neither a destination nor a shortcut to modernity. AI is simply the next chapter in a longer transformation shaped less by technology than by choices about responsibility, transparency and how people are treated in their everyday interactions with the state. When those choices are made well, AI becomes almost invisible. Not because AI is insignificant, but because it works quietly in the background, supporting institutions that remain stable, humane and worthy of trust over time.

> Safeguards, impact assessments and oversight mechanisms are often perceived as slowing innovation, yet they enable it.
>
> Piret Hirv

Explore the report

Scaling AI skills through global cooperation

Kristi Kivilo
Senior Expert

In the era of the "Fourth Industrial Revolution", Artificial Intelligence (AI) has become more than a visionary idea associated with science fiction. Now, it is a basic utility, much like electricity or the internet. Yet, the true potential of AI lies not in its algorithms, but in people's ability to use them. For governments, the challenge has shifted from simply building digital infrastructure to encouraging digital intelligence at scale.

Who owns AI literacy?

While the government serves as the essential architect who provides the roadmap and legal certainty, the private sector drives innovation through new tools, academia supplies crucial research, and civil society organisations ensure ethical oversight and human rights protection. Together, these stakeholders build a social contract in which the state lays the foundation, while the journey of learning and implementation unfolds across all levels of society.

> For governments, the challenge has shifted from simply building digital infrastructure to encouraging digital intelligence at scale
>
> Kristi Kivilo

Photo: Participant of the training of trainers held in Moldova.

The government's role is fundamental for several reasons, all of which are systemic. Firstly, equity and inclusion are at risk. If left to the market, AI skills are likely to cluster around tech hubs, thereby creating a new "AI divide". Governments must ensure that marginalised groups and the elderly are not left behind.

Secondly, national competitiveness is now tied to the workforce's ability to automate routine tasks and focus on high-value, creative problem-solving.

Finally, the government is the ultimate guardian of safety and ethics. A literate populace with the right knowledge and awareness is the best defence against deepfakes, misinformation and the unethical use of data.

Three Golden Rules for building a culture of informed scepticism

To move beyond theory, governments must provide citizens with a practical "mental toolkit" to navigate the AI-driven landscape. This isn't just about the technical skills to use the software; it is about building a culture of informed scepticism. This framework can be summarised through three "Golden Rules":

- **Rule 1: Cultivate "informed curiosity".** Explore AI to boost productivity, but never mistake fluency for accuracy. Public messaging must reinforce that AI is an "hallucination-prone" architect of language. The citizen's role is to be the final editor.
- **Rule 2: Prioritise data sovereignty and personal security.** Cyber hygiene is often overlooked. Citizens must be taught that interacting with a public AI model is akin to speaking in a public forum. Sensitive information – such as passwords or banking details – must remain strictly offline.
- **Rule 3: The verification mandate.** As AI makes it easier to generate convincing content, the responsibility to double-check facts becomes a civic duty. Governments must promote the habit of cross-referencing AI-generated information with trusted, primary sources.

> A literate populace with the right knowledge and awareness is the best defence against deepfakes, misinformation and the unethical use of data.
>
> Kristi Kivilo

The need for rapid upskilling mechanisms

While integrating AI into formal education is essential, traditional education systems change slowly, often taking years to update curricula, textbooks and teacher training.

Meanwhile, AI is evolving at an exponential pace that will not allow governments to wait 10 to 15 years for a new AI-competent generation to enter the workforce. To remain competitive and secure, governments must act now to enable citizens to upskill in real time by prioritising adult learning and placing non-formal education at the heart of national strategy.

From mystery to mastery in public understanding of AI

To build a resilient society, the state must first manage public expectations and cultivate the correct mindset and a realistic understanding of AI. The rapid rise of generative AI tools such as ChatGPT, Gemini and Perplexity has created a paradox: they are incredibly accessible yet widely misunderstood. When a citizen interacts with a tool that communicates in flawless natural language, the mental inclination is to anthropomorphise it.

To prevent "AI-dependency", education initiatives must focus on a key truth: AI is a tool, not a teammate. Strategic communication should emphasise that, while these chatbots generate impressive text and ideas, they operate on mathematical probability rather than consciousness. Framing AI as a "smart helper" will help ensure that citizens remain in charge through oversight, fact-checking and ethical judgment.

Furthermore, the emergence of advanced visual AI requires greater awareness. As realistic images and videos become easier to produce, governments must teach citizens that, in the digital age, visual confirmation can no longer be trusted and critical evaluation is essential.

The way forward

Digital transformation shows that the greatest barrier to innovation is not a lack of technology but gaps in skills and mindset. Experiences from European Union-supported initiatives, including the CyberAcademy and Sigurantadigitala.md in Moldova, KnowCyber.eu in the Western Balkans, and Rural Empowerment through Digital Inclusion in Georgia, demonstrate that while national contexts vary, the core principles of educator empowerment and inclusive design remain consistent.

Going forward, the government's role will increasingly be one of enabling, convening and empowering. Through strategic communication, awareness-raising and accessible lifelong learning, governments can ensure that citizens are not only prepared for an AI-enabled future, but also active, informed and critical participants in shaping it. In the global race for AI capability, the most resilient societies will be those that treat their citizens as more than just users of technology but, instead, as its capable and confident stewards.

Key takeaways for governments seeking to build AI skills at scale

Based on international trends in digital transformation, several universal truths emerge for any government seeking to build AI competence:

1. **Build strong digital foundations.** AI skills cannot be developed in isolation. Basic digital literacy, reliable access to connectivity and familiarity with digital public services lay the groundwork for AI competence.
2. **Institutionalise lifelong learning systems.** Digital and AI skills are not a "one-and-done" achievement. Governments must move toward lifelong learning ecosystems that combine formal education, micro-credentials and continuous reskilling. Modular learning pathways allow citizens to adapt as technologies evolve.
3. **Scale through "Training of Trainers" (ToT).** To achieve a multiplier effect, priority should be given to training youth and adult educators, librarians, and community members. Non-formal education through ToT models enables knowledge to cascade efficiently into local and underserved areas.
4. **Leverage public-private and civil society cooperation.** The fastest innovations occur in the private sector, while governments provide reach and legitimacy. However, the role of civil society organisations is critical; they often serve as a bridge to vulnerable communities, which is necessary to ensure that AI training is inclusive and human-centric. Cooperation with these groups allows for more agile, community-based learning.
5. **Embed ethics, inclusion and public value.** AI skills development must go hand in hand with moral awareness. Governments have a responsibility to frame AI as a means to strengthen transparency, trust and public value.

Photo: Participants of the cyber exercise.

Key projects

Moldova Cybersecurity Rapid Assistance 1.0 & 2.0

2022–2025

The Rapid Assistance Project 1.0 & 2.0 focused on increasing the cyber resilience of public sector organisations and critical infrastructure sectors of Moldova. The projects supported the alignment of national frameworks with EU requirements, strengthened institutional capacities and enhanced the protection of critical information systems through targeted capacity-building and international cooperation.

Funded by the European Union

REDI (Rural Empowerment through Digital Inclusion) in Georgia

2023–2027

This project aims to bridge Georgia's digital divide by enhancing access to affordable digital infrastructure and boosting digital literacy in rural regions like Imereti, Guria, Racha-Lechkhumi, Kvemo Svaneti and Kakheti.

Funded by the European Union

Cyber Balkans

2023–2026

This project aims to strengthen cyber resilience in the Western Balkans by enhancing cybersecurity prevention, preparedness and response, in alignment with EU standards and best practices, among public and private stakeholders in Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, and Serbia.

Funded by the European Union

Photo: Participants of the training of trainers held in Moldova.

> Governments must teach citizens that, in the digital age, visual realism no longer equals authenticity, and critical evaluation is essential.
>
> Kristi Kivilo

From aid dependency to data sovereignty

Piret Hirv
Head of the Data Management Competence Centre

As digital systems become integral to how states design and deliver public services, questions of data sovereignty and privacy are no longer abstract policy debates. They increasingly shape how citizens experience health care, education and social protection.

At their core, these discussions are about trust: trust in institutions, trust in partnerships and trust that personal information will be handled with care.

In late 2025, Kenya entered into a new health cooperation framework with the United States aimed at strengthening disease surveillance and improving access to essential health services. Local media expressed concerns that the government may have sold Kenyan health data.[1] As part of the public discussion that followed, questions were raised about how health data would be governed, protected and overseen. Kenya's High Court temporarily paused elements of the framework while these questions were examined, prompting a broader national conversation about data protection, public participation and institutional safeguards.[2]

> Strong data governance helps ensure that digital transformation remains people-centred, partnerships remain equitable and public services remain worthy of trust.
>
> Piret Hirv

Shared rules create trust

Rather than being an isolated case, this episode reflects a challenge faced by many countries as they navigate rapid digitalisation alongside international cooperation. Governments are increasingly relying on data-driven solutions and cross-border partnerships to deliver services and address complex societal needs. At the same time, citizens expect clarity about how their personal information is used, shared and protected. These expectations are not contradictory. They highlight the growing importance of robust data governance as a key enabler of sustainable cooperation.

Data governance is often misunderstood as a technical or legal exercise. In practice, it is a framework that helps governments manage data responsibly throughout its lifecycle, from collection and use to storage and deletion. When governance frameworks are clearly defined and operationalised, they create shared rules of the game. They help ensure that data is used for agreed purposes, that responsibilities are transparent and that safeguards are in place before data is exchanged across institutional or national boundaries.

1 https://www.ictworks.org/kenya-just-sold-citizen-health-data/

2 https://www.reuters.com/business/healthcare-pharmaceuticals/kenyan-court-suspends-health-pact-with-us-hear-data-privacy-case-2025-12-11

Kenya Just Sold Citizen Health Data for $5.66 Per Person. Expect More & Worse.

By Wayan Vota on December 9, 2025

The Saturday Standard

Data agreement

Suspect health deal

The development community may be asking the wrong question about Kenya's controversial new health agreement with the United States. While digital rights advocates express outrage over data sovereignty violations, they're missing an economic reality that forced this deal in the first place.

Photo: Screenshot of the newsletter The Saturday Standard.

In contexts where governance arrangements are still evolving, even agreements entered into with good intentions may raise questions about how personal information is handled. This does not indicate ill intent but rather highlights the importance of aligning digital cooperation with governance capacity. Strong governance provides that alignment. It ensures that personal data is shared not simply because it is technically possible but because there is a clear legal basis, appropriate safeguards and mechanisms for accountability.

From principles to practice

One of the key contributions of data governance is the limitation of purpose. By clearly defining why data is used and under what conditions, data governance frameworks prevent information from being repurposed in ways that were not originally intended or communicated. This clarity protects individuals while also providing certainty to institutions and partners involved in service delivery.

> These expectations highlight the growing importance of robust data governance as a key enabler of sustainable cooperation.
>
> Piret Hirv

Equally important is the role of governance in embedding consent and individual rights into data-driven systems. When consent management, access rights and redress mechanisms are part of everyday operations, citizens remain active participants rather than passive data subjects. This strengthens trust and supports the legitimacy of digital public services.

Governance also translates values into practice through technical safeguards. Access controls, encryption and classification of sensitive data ensure that information remains protected even when systems become interconnected or data is shared across borders.

These measures are prerequisites for responsible collaboration. Transparency and auditability further reinforce this trust. When decisions about data use are documented, auditable and subject to independent oversight, both citizens and partners gain confidence that commitments are being honoured. Such transparency helps prevent misunderstandings and supports long-term institutional learning.

Finally, data governance brings attention to the full lifecycle of data. Clear retention and deletion rules minimise long-term risks and ensure that personal information is not stored or reused indefinitely without a valid justification. This lifecycle perspective is especially important for sensitive data, such as health records, where long-term exposure can have significant consequences.

Strong governance prevents data colonialism

Taken together, these elements show how data governance acts as a protective and enabling framework. It helps countries engage in international cooperation without losing control over their data, avoiding extractive or asymmetric arrangements sometimes described as data colonialism. Instead, governance supports balanced partnerships in which data serves public value while respecting individual rights.

For public services, the benefits are tangible. When citizens trust that their information is protected, they are more willing to engage with digital services and share accurate data. This, in turn, improves policy design, service quality and outcomes across sectors. Good data governance allows data to function as a shared public asset rather than a transactional resource.

The discussion sparked by the Kenyan example underscores a broader lesson: data sovereignty and privacy protection are not obstacles to cooperation but foundations for it. Investing in governance capacity, legal clarity, institutional roles and technical safeguards enables countries to participate confidently in the digital ecosystem.

Ensuring data sovereignty: Key measures

- **Clear purpose limitation** – define why data is collected and used and prevent reuse beyond agreed objectives
- **Strong legal and institutional frameworks** – ensure a clear legal basis, defined responsibilities and accountability before data is shared
- **Embedded consent and individual rights** – integrate consent management, access rights and redress mechanisms into everyday operations
- **Robust technical safeguards** – apply access controls, encryption and data classification to protect sensitive information
- **Transparency and accountability** – document data use, enable auditability and ensure independent oversights to build trust
- **Data lifecycle management** – establish clear data retention and deletion rules to minimise long-term risks

In an increasingly interconnected world, strong data governance helps ensure that digital transformation remains people-centred, partnerships remain equitable and public services remain worthy of trust. This is not a destination but an ongoing process that benefits from shared experiences, dialogue and sustained capacity-building.

> When citizens trust that their information is protected, they are more willing to engage with digital services and share accurate data.
>
> Piret Hirv

Redesigning digital evidence-handling

Piret Saartee
Head of the Digital Services Competence Centre

Kadi Kanarbik
Senior Expert

The digital transformation of justice systems is no longer a matter of innovation alone. As the volume and complexity of digital evidence continue to grow, traditional approaches to evidence management are increasingly unable to meet today's operational, legal and technical demands. The digital transformation has therefore become a necessity for sustaining efficiency, trust and legal certainty in modern societies.

Digital evidence has become an essential part of modern criminal cases, yet it is often still handled through physical data carriers such as CD-ROMs, USB drives and external hard disks. These practices introduce vulnerabilities – from data loss and deterioration to unauthorised access and broken chains of custody – undermining both efficiency and legal reliability.

To respond to these challenges, the entire digital evidence-handling process – together with criminal case management – must be redesigned. This shift requires moving away from fragmented and manual workflows towards integrated, secure and centralised systems that ensure the highest levels of availability, integrity and confidentiality.

This shift requires moving away from fragmented and manual workflows towards integrated, secure and centralised systems.

In practice, this means storing digital evidence and criminal case data in central components that significantly streamline workflows, enable controlled access for authorised institutions, strengthen traceability and support reliable chain-of-custody management. Such systems also facilitate the efficient reuse of evidence across proceedings and provide a scalable, future-proof foundation capable of handling rapidly increasing data volumes and future EU-level integrations.

An approach to process redesign

Redesigning digital evidence management is not a purely technical exercise – it is a systemic transformation that affects the entire justice ecosystem. Such a change requires engaging stakeholders from day one and ensuring that their needs, constraints and expectations are understood and addressed throughout the process.

The first step is to develop a comprehensive understanding of stakeholder and end-user needs, existing evidence management processes, information systems and architecture, as well as the broader legislative and strategic context. Mapping current practices helps identify key challenges, opportunities and areas for improvement, creating a shared understanding of why change is necessary.

Based on this analysis, a future vision can be developed using an interactive and collaborative approach. This ensures that the proposed solution is aligned with operational realities, user needs and legal requirements while remaining technically feasible. Throughout the project, business, technical and legal perspectives must be integrated to avoid siloed solutions.

As agreed by stakeholders, digital evidence management should function as a seamless and efficient ecosystem, based on a unified governance model and designed to support the entire digital evidence lifecycle – from collection and storage to use, reuse and archiving.

> Throughout the project, business, technical and legal perspectives must be integrated to avoid siloed solutions.

Critical enablers for avoiding failure

Successful digital transformation is as much about people and organisations as it is about technology. Even the most advanced technical solutions will fail without clear governance, defined ownership and sustained change management that supports institutions and individuals through the transition.

A strong regulatory framework must be complemented by agreed data management and information security principles, a coherent system architecture and standardised business processes. However, these elements alone are not sufficient. Continuous communication, stakeholder engagement and capacity-building are essential to ensure that new ways of working are understood, accepted and adopted across institutions.

Strong leadership and central governance play a critical role in driving change. Clear ownership must be established early, and cooperation between evidence providers and justice institutions must be maintained. Change leaders at both managerial and operational levels are needed to translate strategic objectives into day-to-day practices and to address resistance, uncertainty and concerns as they arise. Success also depends on a realistic roadmap and trust across institutions.

Organisational adaptation matters the most

Implementation requires significant investment – not only in infrastructure, security, integration and operations but also in training, support and organisational adaptation. While costs can be estimated, the risks of inaction, such as evidence loss, compromised integrity, failed prosecutions or inadmissibility in court, are difficult to calculate but can potentially be severe, with a lasting impact on justice and public trust. For this reason, the transformation must be delivered in a phased and coordinated manner, involving all key stakeholders to ensure legal compliance and operational suitability.

Digital evidence management should be treated as a national priority, supported by stable long-term funding that also covers ongoing change management activities. It is not merely an IT upgrade but a foundational capability for the justice system. Without sustained political and organisational commitment, fragmentation and inefficiencies risk undermining the shared vision.

Principles that guide

Clear organisational and technical principles must guide both implementation and change. Ownership of central components must be clearly defined, along with roles and responsibilities for data controllers and processors. Criminal case data and digital evidence should be stored centrally and accessed securely by authorised stakeholders only.

High standards of availability, integrity and confidentiality are essential, but so is usability. All processes should follow the "once-only" principle, ensuring that information and evidence are stored and accessed from a single trusted source, reducing duplication and user burden. A dedicated support structure, including a helpdesk, training programmes and a shared knowledge hub, is critical to support users during and after the transition.

Change built to last

After implementation, change management does not end. Governance must evolve into a sustainable operating model that supports continuous improvement. Clear ownership and oversight must be maintained, supported by a coordinating body bringing together justice institutions and law enforcement. Ongoing training, user support and feedback mechanisms help ensure that systems evolve alongside legal, technological and operational developments. Together, these elements ensure that digital evidence management remains resilient, interoperable and fit for future demands.

Effective change requires structured inter-institutional cooperation at three levels:

- **Ministerial level**, providing strategic direction, political backing and resource allocation while resolving major cross-institutional issues.
- **Senior management level**, coordinating implementation, aligning organisational practices, monitoring progress and managing risks.
- **Specialist level**, delivering operational, legal and technical work through joint working groups.

Key project

Digital Evidence for the Belgium Justice

2024–2025

The project contributed to modernising evidence management processes in Belgium and strengthening the digital administration of justice. Engaging a broad range of beneficiaries and key stakeholders across the justice and law enforcement ecosystem, the project developed a robust blueprint for an optimised digital evidence management system aligned with the evolving needs of law enforcement and judicial authorities and designed the digital court clerk system as a new access point to judicial services. While the project's immediate focus was on criminal proceedings, the proposed solutions and vision are designed to be extensible and can be applied to other types of cases in the future.

Funded by the European Union

Stopping corruption in construction through digitalisation

Anton Yermakov
Communication Expert

Digitalising construction is an important step in strengthening transparency, safety and trust in public administration. By replacing the human factor with transparent, rule-based digital processes, Ukraine is setting a new standard for the construction sector, with the e-Governance Academy supporting this transformation.

Few sectors test the integrity of public administration as severely as the construction industry. Large budgets, complex regulations and high discretion at the final stages of decision-making have traditionally made construction one of the most corruption-prone areas of governance worldwide. Ukraine is no exception. According to the National Agency on Corruption Prevention, construction and real estate have ranked among the sectors with the highest perceived corruption risks for years. Yet over the past five years, Ukraine has quietly rewritten the rules of the game – not through increased control alone but through systemic digitalisation.

At the core of this change is a principle that has long guided Estonia's digital state and now shapes Ukraine's reform path: minimising the human factor through digital means. Standardised, traceable and transparent processes reduce the chance for misuse – not because people become perfect but because the system prevents arbitrary decisions.

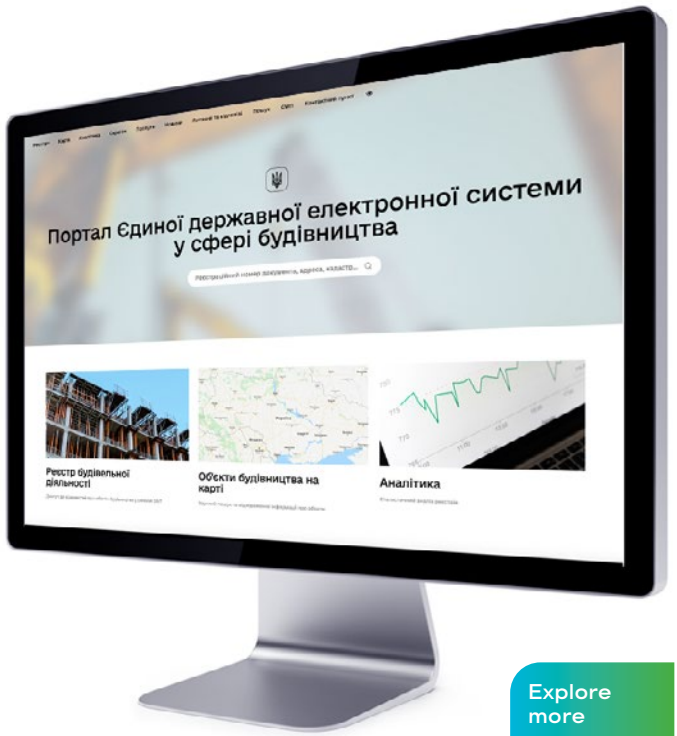


Photo: Ukraine's state electronic system in the conctruction sector.

Explore more

From fragmented procedures to a single digital standard

The launch of Ukraine's Unified State Electronic System in the Construction Sector marked a structural shift in how construction-related services are delivered. For the first time, interactions among developers, inspectors, registries and public authorities were brought together in a single digital environment. The system streamlined document submission, synchronised data with key state registers and significantly reduced processing times for administrative services. Most importantly, it replaced fragmented regional practices with a nationwide digital standard, ensuring equal rules for all market participants.

Yet one critical vulnerability remained. The final stage – the commissioning of completed buildings – continued to rely on physical inspections conducted by individual officials. This moment of direct contact between inspector and developer represented the last major corruption risk in an otherwise increasingly digital process.

Turning inspections into a digitally governed process

To address this challenge, the Ukrainian authorities introduced the Transparent Construction application. Rather than merely digitising paperwork, the solution re-engineers the inspection process itself. Later, it was supported by the e-Governance Academy team within the EU-funded DT4UA project and enhanced into Transparent Construction 2.0.

Each inspection is now conducted through a step-by-step digital workflow that leaves no room for improvisation. Inspectors authenticate securely, follow a mandatory electronic checklist, document compliance through geotagged photographs and upload all materials directly into the central construction system. The application enforces completeness: inspections cannot be finalised unless every required element has been verified and documented. Metadata embedded in photos prevents substitution, manipulation or retroactive changes.

In practice, this means that the system guides the inspector, not the other way around. What once depended on subjective judgment is now governed by predefined rules, digital evidence and automated validation.

> The broader digitalisation of construction services in Ukraine may generate economic benefits exceeding approximately €60 million annually.
>
> Anton Yermakov

Closing loopholes by design

The evolution from the first version of the application to Transparent Construction 2.0 illustrates a core lesson of digital governance: meaningful reform is an iterative process. Early implementation revealed technical and procedural gaps, which were closed in the updated version with the support of the e-Governance Academy's experts. Transparent Construction 2.0 introduced stricter validation logic, mandatory minimum documentation thresholds and the automatic generation of inspection reports, which are transmitted directly to the digital construction register.

As a result, practices that once enabled abuse, such as partial inspections, selective documentation or informal agreements, are no longer technically feasible. The system does not simply record actions; it prevents non-compliant behaviour from occurring.

Economic and anti-corruption impact

Quantifying the full anti-corruption effect of such reforms is inherently difficult. However, a study by Civitta suggests that the broader digitalisation of construction services in Ukraine may generate economic benefits exceeding €60 million annually, driven by faster procedures, reduced administrative costs and the elimination of informal payments. For developers, transparent processes mean predictability and fairness. For citizens, they translate into safer buildings and access to publicly verifiable inspection results. For the state, they strengthen institutional credibility and oversight capacity.

Crucially, all inspection data is set to become publicly accessible through the construction system's portal, enabling civic oversight. Investors, homeowners and journalists can verify whether buildings were commissioned lawfully, when inspections took place and whether all requirements were met. Transparency thus extends beyond internal control; it becomes a shared public safeguard.

A model with global relevance

While developed in response to Ukraine's specific challenges, the Transparent Construction solution addresses a universal governance dilemma: how to regulate high-risk sectors without overburdening them with bureaucracy or relying solely on punitive controls. The answer lies in process-level digitalisation, where integrity is embedded into workflows rather than enforced.

> All inspection data is set to become publicly accessible through the construction system's portal, enabling civic oversight.
>
> Anton Yermakov

Ukraine's experience builds on decades of Estonian practice but adapts it to a vastly different scale and context. In doing so, it demonstrates that digital governance is not about copying solutions but about translating principles into locally effective systems. As many countries continue to grapple with corruption risks in construction and infrastructure development, Ukraine's approach provides a practical and scalable reference point.

The lesson is clear: when rules are embedded in systems, transparency becomes a default condition rather than an effort. And when computers, not people, enforce compliance, the most common forms of corruption simply lose their operating space.

Transparent Construction in practice

The Transparent Construction application transforms building commissioning into a fully digital, rule-based process where every action is predefined, documented and traceable.

1. **Secure authorisation**
   The inspector logs into the application using Diia.Signature. Access is granted only to a specific inspection, ensuring personal accountability and preventing unauthorised actions.
2. **Mandatory digital checklist**
   The application guides the inspector through a standardised checklist covering all required elements of the building, including engineering systems, fire safety, accessibility, utilities and surrounding infrastructure. The sequence is fixed and cannot be altered.
3. **Evidence-based inspection**
   Each checklist item must be confirmed with photographic evidence. Photos are taken directly in the application and automatically linked to the relevant checklist section.
4. **Automatic verification**
   Every image includes metadata such as time and geolocation. This prevents the use of archived photos, manipulation of inspection dates or substitution of objects.
5. **Built-in completeness control**
   The inspection cannot be completed unless all checklist items are filled and the minimum required evidence is provided. Skipping steps or partial inspections is technically impossible.
6. **Instant data transfer**
   All inspection data is automatically transmitted to the Unified State Electronic System in the Construction Sector, where it is stored as part of the official digital record.
7. **Transparency and public oversight**
   Inspection results become available through the public construction portal, enabling citizens, investors and oversight bodies to verify compliance and monitor decisions.

LAC countries' approach to digital transformation and cross-border collaboration

Carlos Vargas
Expert

Digital transformation in Latin America and the Caribbean (LAC) rarely unfolds evenly. Through our work with the EU–LAC Digital Alliance, we have seen real progress alongside persistent challenges. Much of this is shaped by politics, institutions and a growing realisation that digital transformation is less about technology and more about governance.

One lesson stands out from eGA's work in the region: digital tools alone do not change public administration. What matters is how they are governed, coordinated and embedded in daily practice. Encouragingly, many governments are now moving beyond isolated solutions and focusing on interoperability, trust, legal frameworks and institutional roles. This is an important shift, even if it is not always the most visible one.

Structural challenges remain

Observations from the past year's projects from across the LAC countries confirm that structural challenges remain deeply embedded. Different approaches within governments continue to limit impact, with digital identity systems, electronic signatures, registries and platforms often evolving in parallel. Capacity constraints, staff turnover and limited budgets are realities for many administrations. In several cases, ambitious national strategies coexist with weak implementation mechanisms, reminding us that vision alone is not enough.

> There has been growing recognition that cross-border collaboration depends on strong internal coordination, which involves breaking down silos at home before attempting to connect across borders.
>
> Carlos Vargas

However, governments' willingness to cooperate, together with eGA's engagement in the region, has focused on strengthening foundations rather than promoting magical solutions. Through policy dialogues, technical consultations, peer exchange and capacity-building activities, we have collaborated with public institutions to address the core conditions of digital transformation, including governance models, interoperability frameworks, trust services and citizen-centric design. Our role has been less about providing answers and more about helping governments ask the right questions at the right moment.

Focus on cross-border interoperability and digital identity

One of the most notable changes over the past year has been the way governments increasingly frame their challenges in regional terms. Cross-border interoperability, digital identity and mutual recognition of trust services are now discussed as practical requirements rather than distant aspirations. These conversations have helped create alignment around shared principles and approaches, even in contexts where national differences exist.

Several developments were clearly accelerated through these exchanges. We have seen governments move from exploratory discussions toward more concrete roadmaps on interoperability governance, clarify institutional responsibilities around digital identity and electronic signatures, and begin to position trust services as part of broader digital ecosystems rather than standalone tools. Just as importantly, there has been growing recognition that cross-border collaboration depends on strong internal coordination, which involves breaking down silos at home before attempting to connect across borders.

From regional dialogue to local solution

The work in the region has also generated meaningful spinoffs. In Ecuador, recent engagements have built directly on regional experience to support national discussions on digital governance and interoperability. In Guatemala, consultations have helped translate regional dialogue into concrete discussions on public sector modernisation and service delivery. Collaboration with Cuba has also shown that, even in complex contexts, technical cooperation and sustained dialogue on digital public infrastructure can foster trust and transparency in governance. Together, these experiences also highlight how Uruguay, alongside Brazil, has emerged as a regional leader in advancing cross-border digital signature recognition with the European Union.

What emerges from these experiences is not a model to be replicated but a shared understanding that is gradually taking shape. LAC countries increasingly recognise that digital transformation is a long-term institutional reform, requiring continuity, coordination and political commitment. Regional cooperation is therefore seen as a strategic accelerator, particularly for countries that benefit from shared standards, peer learning and collective problem-solving.

Finally, as LAC countries continue their digital journeys, the past year has reinforced a simple but important insight: meaningful digital transformation is built over time, through trust, learning, patience and cooperation, combined with hard work. The challenge ahead is not only to digitalise more but to do so with clarity of purpose, ensuring that digital transformation ultimately serves citizens, institutions and regional collaboration alike.

> LAC countries increasingly recognise that digital transformation is a long-term institutional reform that requires continuity, coordination and political commitment.
>
> Carlos Vargas

Cross-country cooperation in LAC countries

The EU–LAC project focuses on developing a cross-border framework, primarily through testing concepts in international exercises and events.

- In 2025, activities included two-day international tabletop exercises on cross-border service development between:
  - **Uruguay and Chile**
  - **Costa Rica and Guatemala**
  - **Trinidad and Tobago, Belize, Dominican Republic, Barbados and Jamaica**
- In 2024, EU–LAC activities involved collaboration on ICT governance with Guatemala.
- A two-day digital inclusion seminar was organised for the Central American region, with participation from government officials and civil society representatives from:
  - **Dominican Republic**
  - **Guatemala**
  - **Costa Rica**
  - **Panama**
  - **Honduras**

Cross border solutions

Lessons learned from LAC experience

- Governance must come before technology.
- Interoperability should be treated as both a policy issue and a technical one.
- Investment in people, institutions and communities of practice is essential.
- Meaningful digital transformation is built over time, through trust, learning, patience and cooperation.
- Digitisation should involve a clear purpose.

Photo:
Interoperability workshop in Costa Rica.

Key projects

EU-LAC High-Level Policy Dialogue on Digital Policy and Regulations

2023–2025

This action supports faster digital transformation in Latin America and the Caribbean by strengthening regulatory harmonisation, governance frameworks and EU–LAC cooperation in areas such as data protection and sharing, cybersecurity, e-governance, interoperability, AI and connectivity. The e-Governance Academy team contributes through e-governance consultations. The project forms part of the EU–LAC Digital Alliance under the Regional Team Europe Initiative, cofinanced by the German Federal Ministry for Economic Cooperation and Development.

Funded by the European Union and the German Federal Ministry for Economic Cooperation and Development

Digital governance enhancement in Guatemala

2023–2029

The project aims to build a more advanced, efficient and inclusive digital governance system in Guatemala by strengthening governance, building institutional capacity and implementing interoperability solutions. Through pilot programmes, co-creation and training, it supports Guatemalan institutions in leading a coordinated and sustainable digital transformation aligned with European and global best practices.

Funded by the European Union

Cuba Digital

2024–2028

The project supports digital transformation in Cuba by improving access to digital public and private services and strengthening digital interaction between citizens, businesses and authorities. It has been implemented by the e-Governance Academy and FIAP (the International and Ibero-American Foundation for Administration and Public Policies). The activities led by eGA focus on building capacity and infrastructure for digital public services, including secure service portals and telecare systems.

Funded by the European Union

EUDI Wallets beyond the app: What Europe is really building

Oleksandr Kozlov
Senior Expert

Anyone who has followed the EU digital identity over the past decade will feel a strong sense of déjà vu when looking at the European Digital Identity Wallet (EUDI Wallet or "wallet"). Ambition is high. Deadlines are tight. Standards are still evolving, and many people in the trust services ecosystem quietly admit that parts of the system are not yet ready.

These concerns are understandable. The interoperability of eID schemes under eIDAS 1 has been fragile. The cross-border use of qualified electronic signatures (QES) has improved, but remains uneven. In many countries, high-assurance eID remains limited, and meaningful public services for foreign eID users are still scarce. From this perspective, scepticism towards yet another "big wallet initiative" is understandable.

Some critics go further, arguing that the EUDI Wallet risks becoming a distraction that will draw attention away from the unresolved fundamental concern: a shared European understanding of identity, representation and trust. Without this common foundation, they argue, no wallet can truly work across borders.

All of this is worth taking seriously. And yet, I remain more optimistic than many of the critics. This optimism does not come from technology hype, but from structure and obligation.

The EUDI Wallet is more than an app

When people discuss EUDI Wallet, they typically envision a smartphone app. But the wallet is not just an app; it's an ecosystem.

The wallet requires collaboration between wallet providers, PID Providers, Authentic Sources, Qualified Trust Service Providers (QTSPs) and Relying Parties to function effectively. Each has different obligations and bottlenecks. Without full participation across the entire ecosystem, including banks, mobile network operators, police administrations and online platforms, even the most polished app will deliver little value.

For this reason, piloting matters greatly. Customer authentication requirements vary not only between industries but also among individual players within each industry. The wallet ecosystem must remain flexible enough to accommodate these variations while maintaining security and interoperability.

Why this time is different

For the first time, EU law does not merely encourage digital identity interoperability – it requires every Member State to provide an EUDI Wallet and the supporting ecosystem. Under eIDAS 2.0, the wallet becomes a default public instrument available to everyone, not an optional add-on.

Both public and private services must accept the wallet. This changes incentives fundamentally. When acceptance is mandatory, the infrastructure question shifts from "Will anyone use this?" to "How do we make it work at scale?"

What will wallets actually do?

The wallets will serve as high assurance eID means for storing user credentials that will enable them to be securely shared with trusted Relying Parties, as well as supporting qualified electronic signatures and ensuring the security and portability of personal data.

This will not magically solve digital identity interoperability overnight. However, it changes incentives, particularly in countries where eID and qualified electronic signatures were not widely adopted previously. Public services must accept the wallet, private services can rely on it, and citizens will increasingly encounter it as a core feature of digital infrastructure rather than an experiment.

The messy reality

EUDI Wallet standards and specifications are evolving in parallel with testing, which creates problems. Sometimes specifications that look

> Public services must accept the wallet, private services can rely on it, and citizens will increasingly encounter it.
>
> Oleksandr Kozlov

fine on paper don't work in practice. But if we wait for every standard to be finalised before building anything, wallets will arrive in decades, not years.

There's another uncomfortable truth: the EU-only restriction remains a major flaw. Wallet and PID Providers, as well as Relying Parties, must all be established in the EU, with the exception of actors such as British car rental companies, Swiss banks or Ukrainian public procurement systems. This limits the wallet's usefulness for cross-border scenarios beyond the EU – exactly where digital identity infrastructure could have the most impact.

Ukraine has already shown what this future looks like. Citizens value mobile-based solutions that solve their authentication, signing and document management requirements. For most, when ID, driver's license, vehicle registration, credit card and insurance live securely in your smartphone, physical wallets are no longer essential.

From frameworks to functioning wallets

In 2025, collaboration around the EUDI Wallet intensified, with countries working together to move from frameworks to implementation. Regulators, standardisation bodies and private actors are all contributing to delivering wallets to citizens.

The European Commission is often criticised for moving forward while specifications and legal acts remain in flux. Yet without firm deadlines, Europe risks endlessly refining frameworks. Someone must start the clock, or the digital identity wallets will remain technically perfect but relevant only to future historians.

Ukraine's participation in the EUDI Wallet pilot demonstrates that this might become more than an internal EU project. This points to a framework with the potential to extend beyond current borders and support both accession candidates and broader digital trade partnerships.

The EUDI Wallet will not solve everything. Rather, it represents a shift from aspiration to requirement, from fragmentation to convergence and from optional experimentation to mandatory infrastructure. That shift matters.

EUDI Wallet in brief

- The European Digital Identity Framework entered into force in May 2024.
- The EU Digital Identity Wallet improves current eID systems by offering personal digital wallets that can be used across the EU to identify yourself online and securely share electronic documents.
- Each EU Member State will offer at least one version of the EU Digital Identity Wallet, built to the same common specifications, by 2026.
- 360 private companies and public authorities across 26 Member States, as well as Norway, Iceland and Ukraine, are participating in the pilots.
- Within the DT4UA phase 2 project, eGA experts are supporting Ukraine in the EUDI Wallet pilots.

> The EUDI Wallet represents a shift from aspiration to requirement, from fragmentation to convergence and from optional experimentation to mandatory infrastructure.
>
> Oleksandr Kozlov

Ukraine's case: Moving towards the EU's single digital market

Oleg Burba
Senior Expert
Coordinator of the Cross-Border Interaction and Trust Services Direction of the European Union

Digital integration with the EU's Digital Single Market is a strategic priority for Ukraine's development, competitiveness and future within a unified digital Europe. The e-Governance Academy's team is supporting Ukraine on this path.

Through EU-funded projects such as DT4UA and EU4DigitalUA, the e-Governance Academy works directly with Ukrainian partners to bring national legislation, digital infrastructure and public services closer to EU standards, ensuring compatibility, security and interoperability with European systems.

Ukraine has already delivered substantial results in digital European integration and, in several areas, is moving faster than many peers. For example, Ukraine has aligned legislation in the field of trust services with the eIDAS regulation; its trust services system is built according to European standards and has undergone multiple audits by EU experts; and it has successfully tested the compatibility of electronic documents with prototypes of the EU's digital wallets.

This progress is also recognised in the European Commission's latest enlargement report, which highlights Ukraine's strong results in implementing European standards on electronic identification and trust services.

Progress in three key areas

Ukraine has already made significant strides in digital integration with the EU. The most visible progress falls into three key areas:

1) Electronic identification and the digital wallet

Ukraine is actively developing its electronic identification system, which now enables citizens to access public and private online services securely. For instance, Ukrainians can now use eID to access digital public services such as business registration and tax services, cutting processes that once took weeks down to just a few hours.

Ukraine is also taking an active role in EU-level pilot initiatives through European consortia. The first of these was POTENTIAL, which brought together EU Member States and Ukraine to contribute to the development of the European Digital Identity Wallet (EUDI Wallet) (read more on page 39–41). Today, the Ministry of Digital Transformation and the State Enterprise Diia, with expert support from the e-Governance Academy (eGA), are continuing this work within the APTITUDE consortium. Notably, among the participating countries in these consortia, Ukraine is the only non-EU country.

2) Trust services and electronic signatures

Ukraine's trust services already meet European legal requirements, allowing citizens, businesses and public authorities to use EU-compatible solutions. As a result, Ukraine became the first non-EU country whose trust services system has been formally recognised by the EU. The framework is now considered to represent an advanced level of trust. To achieve Qualified

Photo:
Ukraine's expo booth at the e-Governance Conference.

Trust Service status, the final step will be full mutual recognition and the signing of the relevant agreement between Ukraine and the EU.

3) Alignment of national legislation with eIDAS 2.0

Ukraine is systematically aligning its national legislation with eIDAS 2.0, the updated EU regulation that sets the rules for electronic identification and trust services. Building on earlier work — where legislation was adapted, the national eID system deployed and the eIDAS node tested within the EU infrastructure — the focus now shifts to full alignment with the updated eIDAS 2.0 standards.

The biggest challenge: Legislation

Although Ukraine has already achieved significant progress, there are still many challenges to address and tasks to complete. The biggest challenge is legislation: Ukraine has not yet adopted the key law on personal data protection that would align it with the GDPR, and it has only partially implemented the security requirements for digital services under NIS2. Adopting these laws and ensuring their full implementation is a necessary condition for Ukraine's integration into the EU Digital Single Market. At the moment, the GDPR-aligned draft law has passed its first reading in the Verkhovna Rada, while around 80% of the NIS2 requirements have been implemented.

Beyond legislation, there are also ongoing challenges related to coordination and synchronisation among institutions. Harmonising standards across government bodies and international platforms takes time, sustained effort and resources. Still, our strategy is to work systematically with European partners, achieve alignment step by step and continue clearing the obstacles along the way.

Next steps and priorities

Ukraine's and the eGA team's shared top priority is integrating Ukraine into the Single Digital Gateway (SDG), the EU's single online portal for accessing public services. This step is essential to ensure that Ukrainian services are visible and accessible to Europeans and that Ukrainian citizens can fully benefit from the opportunities available across EU countries.

Imagine, for example, a Belgian citizen who wants to study in Ukraine or use a Ukrainian public service. Through the SDG, they would simply open the Ukraine section of the portal and choose from a list of available services. For the user, it's just a few clicks, but behind that simplicity lies a significant amount of preparatory work to make cross-border access seamless, reliable and compliant.

In parallel, together with the Government of Ukraine, we are modernising the guide of public services development to bring its classification system in alignment with European standards. The EU uses a clear service structure, categorised, regulated and standardised, and Ukraine's portal needs to match these requirements to ensure consistency and interoperability.

> The final step will be full mutual recognition and the signing of the relevant agreement between Ukraine and the EU.
>
> Oleg Burba

eGA is supporting the Government of Ukraine in advancing along other European integration tracks. In November 2025, the second phase of the EU-supported project DT4UA began, marking Ukraine's move into a deeper stage of integration with the European digital space.

This work will include building sustained operational cooperation with the European Commission and EU Member States; conducting business analysis and launching cross-border services; providing advisory support to Ukraine on implementing key European acts; testing the EUDI Wallet; and updating Diia.Signature, among other priorities.

From preparation to integration

2026 is set to be a turning point in Ukraine's digital integration with the EU that will bring a shift from preparation to practical alignment and cross-border services.

The European Commission has indicated its readiness to begin assessing Ukraine's legislation and infrastructure with a view to the full recognition of qualified trust services under eIDAS 2.0. In parallel, work will continue on integrating Ukrainian services into the Single Digital Gateway and advancing practical cooperation under the Once-Only Technical System.

In the following years, as accession negotiations progress, digital integration is expected to move from preparatory and pilot phases towards broader deployment, including the gradual launch of cross-border digital services, deeper interoperability between Ukrainian and EU public sector systems, and sustained participation in EU digital governance structures. Together, these steps will anchor digital integration as a permanent and practical component of Ukraine's EU accession path.

> 2026 is set to be a turning point in Ukraine's digital integration with the EU
>
> Oleg Burba

Impact of digital European integration on Ukraine

- Reduced administrative barriers for citizens and businesses
- Trusted cross-border electronic transactions
- Equal digital access to public services with EU citizens
- Faster, simpler services for Ukrainians living in the EU
- Reliable verification of personal and business data
- Lower compliance costs for cross-border companies
- Greater predictability for businesses and investors
- Gradual integration into the EU Single Market
- Stronger institutional capacity, transparency and resilience – factors that are critical both in the context of wartime governance and future recovery

Key project

DT4UA Phase 2

2025–2026

The second phase of DT4UA marks a new stage in EU–Ukraine digital integration that, with many Ukrainians now living in EU Member States, will support access to public services across borders. As Ukraine begins EU accession negotiations, digital transformation has become a core part of preparation for membership, linked to Chapter 10 of the EU acquis. DT4UA Phase II therefore focuses on legislative harmonisation, cross-border digital services and modernising the infrastructure underpinning the digital state.

Funded by the European Union

From networks to norms: Critical infrastructure and trust in digital democracies

Elsa Neeme
Senior Expert

Across Europe, cybersecurity has moved decisively from the realm of technical networks into the sphere of legal norms. In recent years, organisations have had to navigate an increasingly dense regulatory landscape as the European Union introduced a series of new instruments aimed at protecting its digital ecosystem.

These measures extend obligations across a wide range of actors, from manufacturers of digital products to financial institutions, health care, food production and other service providers vital for societies. This shift reflects a growing recognition that cybersecurity is no longer merely an IT concern.

As public administration, energy, transport, health care and communications become digitally interconnected, cyber incidents increasingly translate into societal disruption and national security risks. Failures in cyberspace can interrupt essential services, undermine public confidence and weaken a state's ability to function during crises. In this context, cybersecurity legislation is best understood as part of a broader resilience strategy rather than as isolated compliance rules.

A European legal baseline for critical infrastructure protection

The EU's response has been to construct a layered legal baseline linking resilience, accountability and the internal market. The NIS2 Directive significantly expands risk-management and incident-reporting obligations while strengthening supervision and cross-border cooperation. The Cyber Resilience Act complements this by embedding security requirements into products with digital elements, shifting responsibility earlier into design and supply chains. The Cyber Solidarity Act adds a collective dimension, focusing on shared detection capabilities and coordinated response when incidents scale beyond national borders.

> Cybersecurity legislation is best understood as part of a broader resilience strategy rather than as isolated compliance rules.
>
> Elsa Neeme

Together, these instruments mark a clear regulatory shift: cybersecurity is treated less as a technical function and more as a governance responsibility, tied to leadership accountability and institutional preparedness. For operators of critical information infrastructure (CII), this means that resilience is no longer discretionary – it is a matter of public interest and, increasingly, national security.

Trust is the point

Cybersecurity law can be sometimes treated as a sign of mistrust towards technology or organisations. In practice, it works more like traffic rules: it is there not because we assume bad faith but because complex systems only function when risks are managed predictably.

For market actors, the promise of frameworks such as NIS2, the Digital Operational Resilience Act, eIDAS2 and the Cyber Resilience Act is not merely "more compliance". The better argument is that predictable rules can reduce uncertainty, guide investments and make cybersecurity a precondition of competitiveness and market confidence. Standardisation and clearer expectations are expected to reinforce trust among citizens, businesses and international partners, provided the rules are coherent and enforceable in practice.

That said, the trust dimension runs both ways. If the legal foundation is perceived as unstable, overly complex or constantly shifting, trust in lawmakers and in the law itself can erode. In digital democracies, confidence in regulation is part of societal resilience: market actors must believe that public institutions can set rules that are comprehensible, fair and oriented towards real risk reduction rather than a symbolic gesture or a struggle for control.

Avoiding classic failures

Despite its ambitions, cyber law remains vulnerable to structural failure. One risk is the creation of a "paper shield" – rules that appear robust on paper but are too vague or abstract to change real behaviour. In such cases, compliance becomes performative, reporting is inconsistent, and lessons from incidents are not effectively shared.

The opposite risk is a "compliance cage": overly prescriptive frameworks that prioritise box-ticking and blame-avoidance over genuine risk reduction. When organisations focus primarily on avoiding sanctions, they invest in paperwork rather than resilience and may hesitate to report incidents that could otherwise strengthen collective defence.

Avoiding these extremes requires a principled approach. Proportionality and risk-based obligations are essential, particularly for CII operators whose failure has systemic consequences. Rules should remain technologically neutral, focusing on outcomes rather than mandating specific tools. Equally important is fostering a learning culture around incident reporting.

For non-EU countries seeking to align with EU cybersecurity frameworks, harmonisation should not be reduced to copying legislative text. The real challenge lies in operationalisation: defining competent authorities, building incident-reporting workflows, coordinating sectors, testing crisis response and investing in institutional capacity. Successful reform treats cybersecurity law as governance reform rather than an elegant drafting exercise.

> Successful reform treats cybersecurity law as governance reform rather than an elegant drafting exercise.
>
> Elsa Neeme

Cyber law as an infrastructure of trust

Ultimately, cybersecurity legislation should be judged by whether it shapes behaviour in practice. More norms do not automatically mean more security; excessive density can obscure priorities, dilute responsibility and create a false sense of safety. Security emerges from clarity, proportionality and shared understanding – especially because language in law is not decoration. Terms such as "risk management", "appropriate measures" or "significant incident" only strengthen resilience if they are understood in the same way by lawmakers, regulators, operators and technical staff.

When cyber law is clear, foreseeable and usable, it helps markets invest sensibly and helps states coordinate during crises. When it is not, it becomes part of the risk landscape. In an era where digital networks underpin both prosperity and national security, building a legal framework that secures critical infrastructure while sustaining trust is no longer optional – it is a defining condition of resilience in digital democracies.

Photo: Elsa Neeme speaking on cybersecurity legislation.

Key projects

Improving Cyber Resilience in Eastern Partnership Countries 2.0

2024–2027

16 PEACE, JUSTICE AND STRONG INSTITUTIONS 17 PARTNERSHIPS FOR THE GOALS

The EU's Eastern Partnership Cybersecurity Initiative boosts cyber resilience in Azerbaijan and Moldova (via the e-Governance Academy) and in Ukraine and Armenia (via GIZ) through cooperation, legal alignment and capacity-building.

Funded by the European Union

Team Europe Initiative on Digital Connectivity in Central Asia: Cybersecurity component

2025–2028

16 PEACE, JUSTICE AND STRONG INSTITUTIONS 17 PARTNERSHIPS FOR THE GOALS

The cybersecurity component of the project focuses on supporting Central Asian countries in strengthening their cybersecurity capacities and enhancing their responsiveness to cyber threats. This will be achieved by establishing resilient cybersecurity governance mechanisms and improving national cybersecurity capabilities.

Funded by the European Union

> In digital democracies, confidence in regulation is part of societal resilience.
>
> Elsa Neeme

Lessons from Ukraine on protecting critical infrastructure

Taimar Peterkop
Senior Expert

After more than ten years of sustained, multi-vector Russian attacks, Ukraine offers hard-earned lessons on critical infrastructure protection. For Europe and its partners, learning from Ukraine is no longer optional. It should be seen as essential.

Since the start of Russia's war of aggression in 2022, Ukraine has endured sustained attacks on its power grid, telecommunications networks, water systems, transport infrastructure and digital services. These attacks have combined missiles, drones, cyber operations and information warfare in an attempt to break the functioning of the state and the resilience of society. Yet despite unprecedented pressure, Ukraine has continued to operate as a state, provide essential services and adapt its systems in real time.

And not only that, Ukraine has continued to develop its digital society, which has only become more effective during the war, proving that digital society can effectively function during full-scale conventional military conflict. This is not accidental. Ukraine's resilience is the result of deliberate governance choices, institutional reforms, international cooperation and the mobilisation of society.

Photo: Oleksandr Potii, Head of Ukraine's Special Communications Service.

Critical infrastructure is a primary target

One of the most important lessons that the conflict in Ukraine has reminded us of is that, in conflict, critical infrastructure is not solely a secondary or incidental target. It is a strategic objective. The Russian warfighting doctrine is not just about how to fight the state militarily. These attacks not only aim to degrade military capability but also undermine economic activity and erode civilian morale.

The Ukrainian energy sector illustrates this clearly. Large-scale missile and drone strikes against power plants and substations have caused widespread blackouts, particularly during the winter months. Unlike traditional warfare, where infrastructure damage is often localised or temporary, Ukraine has faced repeated, coordinated waves of attacks designed to overwhelm repair capacity and exhaust resources. As a result, authorities and operators have had to rethink how infrastructure is designed, protected and restored.

> Russian warfighting doctrine is not only about how to fight the state militarily.
>
> Taimar Peterkop

Ukraine as a testing ground for cyberattacks

Cyber operations have played a complementary role. Ukraine has been a testing ground for cyberattacks on industrial control systems, government networks and telecommunications providers. The 2015 and 2016 cyberattacks on the Ukrainian power grid were early warnings of what cyber-physical attacks could look like. Since 2022, cyber operations have been integrated into broader military campaigns, targeting situational awareness, coordination and trust.

Importantly, Ukraine's experience demonstrates that cyber and physical domains cannot be treated separately. Physical damage to infrastructure increases reliance on digital systems for coordination and recovery, while cyber disruptions can amplify the impact of physical attacks. This interconnectedness of cyber and physical domains is a defining feature of modern critical infrastructure risk.

Another key aspect of the threat landscape is uncertainty. Attacks do not follow predictable patterns. Targets change, tactics evolve and defenders must adapt continuously. This has profound implications for how critical infrastructure protection should be organised: static compliance-based models are insufficient; adaptive, learning-oriented systems are required.

> The interconnectedness of cyber and physical domains is a defining feature of modern critical infrastructure risk.
>
> Taimar Peterkop

Key elements of Ukraine's response

Governance is central to effective critical infrastructure protection. Ukraine's experience shows that institutional clarity, coordination and leadership matter as much as technical capability. In wartime, fragmented responsibilities and unclear mandates can be fatal.

Ukraine has progressively strengthened its governance framework by clarifying roles and responsibilities, improving coordination between civilian and security institutions, and integrating cyber and physical protection under a coherent policy, legal and institutional framework. Central authorities set priorities, maintain situational awareness and coordinate response across sectors. A key lesson is the value of a central coordinating body with real authority.

Legal and regulatory frameworks have also evolved. Ukraine has aligned its cybersecurity and critical infrastructure legislation with European standards, even while under attack. This demonstrates that crises can accelerate reform rather than halt it. Clear legal obligations for operators, incident reporting requirements, and defined standards for protection and resilience provide a foundation for coordinated action.

Photo:
Ukraine is offering valuable insights into crisis preparedness based on lessons learned from the war.

A fundamental shift in thinking

Ukraine's experience underscores a fundamental shift in thinking: the goal of critical infrastructure protection is not to prevent all disruption, but to ensure continuity and rapid recovery. Perfect protection is impossible under sustained attack. Resilience is the ability to absorb shocks, adapt to changing conditions and continue functioning at an acceptable level.

Redundancy and decentralisation have proven vital. Ukraine has increasingly relied on distributed energy solutions, backup generators, and modular systems that can be repaired or replaced quickly. Centralised, monolithic systems are more vulnerable to targeted attacks. Decentralised systems may be less efficient in normal conditions, but they are far more resilient under stress. The ability to restore functionality quickly can be more important than preventing damage in the first place.

Digital infrastructure under attack

A distinctive feature of Ukraine's resilience is the role of digital government and information infrastructure. Digital services have enabled continuity of governance, service delivery and communication even when physical infrastructure is damaged. Platforms for public services, identity and communication have reduced dependence on physical presence and enabled rapid adaptation.

> Ukraine's experience demonstrates that cyber and physical domains cannot be treated separately.
>
> Taimar Peterkop

Five lessons for global critical infrastructure protection

1. **Critical infrastructure protection must be** treated as a **national security priority**, not merely a regulatory or technical issue. This requires political leadership, strategic planning, and sustained investment.
2. **Governance matters.** Clear roles, strong coordination and trust-based public-private cooperation are essential. Fragmentation undermines resilience.
3. **Resilience should be prioritised over perfection.** Systems must be designed to fail gracefully and recover quickly, not to be invulnerable.
4. **Society is part of infrastructure.** Citizen preparedness, trust and adaptive behaviour are force multipliers.
5. **International cooperation is indispensable.** No country can address modern infrastructure threats alone.

Photo: Oleksandr Potii, Head of the Special Communications Service of Ukraine, and Annely Kolk, Ambassador of Estonia to Ukraine.

However, digital infrastructure is itself critical infrastructure and a prime target. Ukraine's experience shows that protecting digital government systems requires the same level of attention as energy or transport. Cybersecurity, redundancy and trust are essential. The failure of digital services during a crisis can undermine confidence and coordination.

A vital role for strategic communication

Information integrity is another crucial dimension. Disinformation campaigns aimed at undermining trust in infrastructure providers or government response can magnify the impact of physical disruptions. Ukraine has had to invest in strategic communication and public information as part of its infrastructure protection strategy. Keeping citizens informed reduces panic and enables adaptive behaviour.

Perhaps the most powerful lesson from Ukraine is that critical infrastructure protection is not solely a state challenge; it is a societal one. Infrastructure ultimately exists to serve people, and people play an active role in its resilience.

Public awareness and preparedness have been essential. Ukrainian citizens have learned how to cope with blackouts, conserve energy and adapt daily routines. This adaptive capacity reduces the impact of disruptions and buys time for repair. In contrast, societies unprepared for infrastructure failure may experience disproportionate social and economic damage even from short-term outages.

Trust between citizens, operators and the state is a critical asset. Transparent communication about risks, outages and recovery efforts builds credibility. Ukraine's experience shows that honesty about limitations can strengthen, rather than weaken, public confidence.

Lessons beyond Ukraine

These lessons extend far beyond Ukraine. Climate-driven disasters, cyberattacks and geopolitical tensions are increasing threats to critical infrastructure everywhere. Ukraine shows what resilience looks like under the most extreme conditions.

Its experience proves that resilience is practical, not abstract, built through governance, technology and society. Countries should learn these lessons now, not after crisis strikes. Investing in resilience before disaster strikes is far less costly than rebuilding after failure.

Ukraine's experience reminds us that critical infrastructure is not just about systems and assets, but about people, trust and the capacity to adapt under pressure.

As threats continue to evolve, the central question is how societies will respond. Ukraine offers a powerful answer: through coordination, resilience and collective resolve, even the most severe challenges can be endured.

Slava Ukraini!

Key project

Cybersecurity Readiness for Critical Infrastructure in Ukraine

2024–2025

The project supported Ukraine's State Service of Special Communications and Information Protection (SSSCIP) in strengthening Ukraine's capacity to protect critical infrastructure against cyber and hybrid threats and to support compliance with new legislation.

Funded by the US Government and ESTDEV

Building cyber resilience: Global insights into government preparedness

Marit Lani
Head of the Governance and Engagement Competence Centre

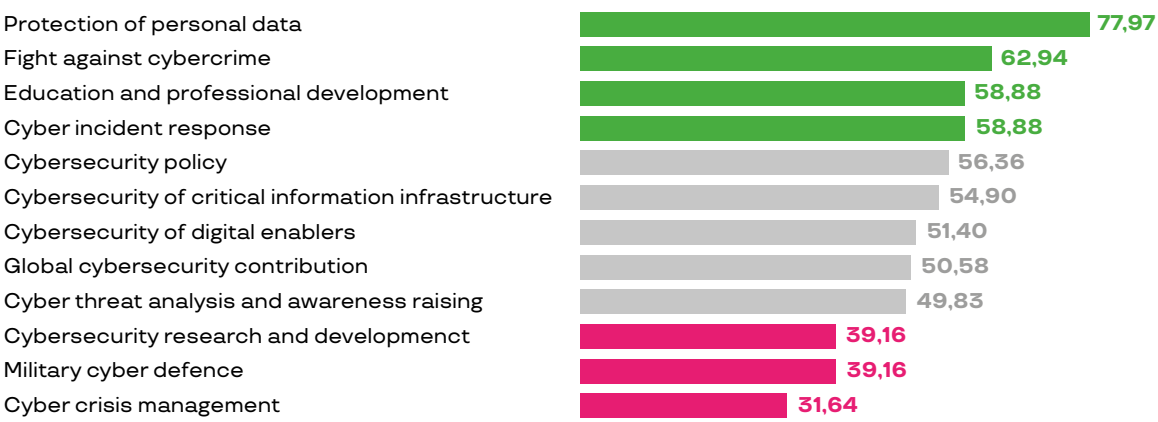
Over recent years, cybersecurity has become a core concern for governments worldwide. Governments are expected to prevent cyber threats, manage incidents, protect citizens' data and cooperate internationally. Against this backdrop, the National Cyber Security Index (NCSI) provides a structured way to assess how well countries are prepared to address these challenges.

First piloted in 2016, the NCSI has evolved into a widely used global benchmark. Today, it covers 140 countries and is developed through the contributions of more than 100 data providers worldwide, together with a dedicated team of NCSI experts at eGA, who ensure methodological consistency, quality control and the continuous development of the index.

At its core, the NCSI functions as a global database of national cybersecurity capacities. It assesses countries based on 49 indicators, each supported by publicly available evidence. This enables policymakers, practitioners and researchers not only to compare countries but also to consult real-world examples of laws, institutions, cooperation frameworks and practices.

By showing where cybersecurity capacities exist – and where gaps remain – the index turns global data into actionable insights for strengthening government preparedness. To further improve its output, the NCSI team looks forward to expanding the network of countries that contribute data, which will increase coverage and ensure the index remains up to date. Read more on page 63.

Cybersecurity capacity landscape: global strengths and gaps



Source: NCSI

NCSI
national cyber security index

The National Cyber Security Index (NCSI) is a live global index that measures countries' preparedness to prevent cyber threats and manage cyber incidents. The NCSI also serves as a database with publicly available evidence materials and as a tool for national cybersecurity capacity-building.

Explore more at

Four reasons why your country should participate in the NCSI

1. Facilitate better policy-making

NCSI insights guide the development of effective cybersecurity policies and legislation, ensuring alignment with international best practices and a forward-looking national framework.

2. Benchmark against global standards

The NCSI allows countries to compare their cybersecurity measures with global standards and best practices, helping to identify areas for improvement and maintain competitiveness in the digital economy.

3. Promote national cybersecurity maturity

Participation in the NCSI encourages regular updates to cybersecurity policies, strategies and practices, ensuring the nation is prepared to face evolving threats and enhance its overall maturity.

4. Gain access to comparative data and insights

The NCSI provides valuable data on member countries' cybersecurity readiness, aiding policymakers in making informed decisions based on comparative analysis and global trends.

Contact the NCSI team

For consultations on how to participate, contribute data and maximise the index's benefits, contact us at ncsi@ega.ee.

Building cyber defence through NATO cooperation

Liis Linn
Senior Communication Expert

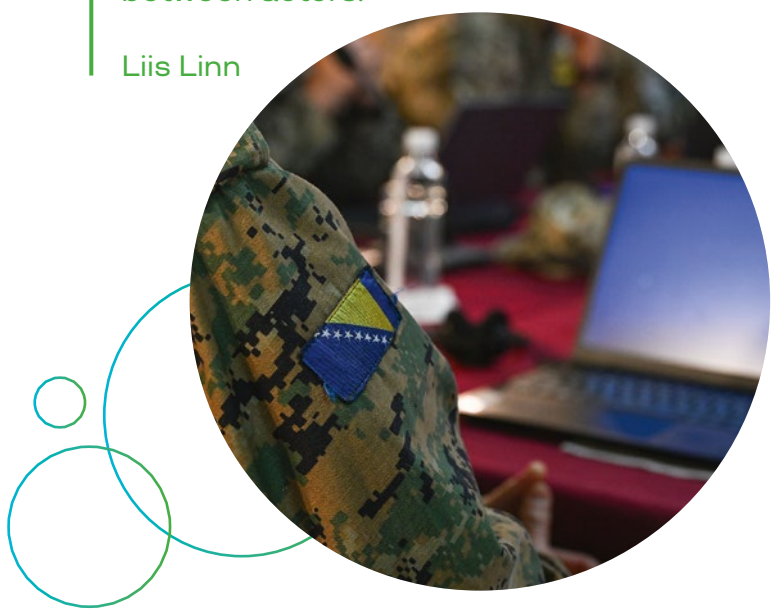
Cybersecurity cooperation rarely follows a single institutional line. For governments navigating an increasingly complex threat landscape, the real value lies in cooperation that is practical, trusted and responsive to national needs.

In 2025, NATO and the e-Governance Academy (eGA) worked together to deliver exactly that for Bosnia and Herzegovina and the Republic of Moldova: usable skills, clearer procedures and better operational readiness.

A key milestone in 2025 was the launch of activities in Bosnia and Herzegovina, where eGA implemented the first training under the NATO Defence and Related Security Capacity Building (DCB) Trust Fund project "Enhancing Cyber Defence in Bosnia and Herzegovina". Held in Sarajevo in October, the two-day training focused on cyber threat intelligence (CTI) and open-source intelligence (OSINT). Specialists from the Ministry of Defence and the Bosnian armed forces strengthened their ability to identify, analyse and mitigate cyber threats, supporting institutional readiness and interoperability with NATO standards. The training also laid a solid foundation for strengthening the country's cyber defence capabilities through a direct NATO framework.

In Moldova, as part of NATO's enhanced Defence and Related Security Capacity Building package, eGA collaborated with a government institution to enhance the institution's ability to defend against cyberattacks. The approach focused on two practical levers: augmenting technical tools and enhancing the skills of cybersecurity professionals. The training focused on the cyber threat landscape, available automated tools and practical experience with real security tools and techniques.

> The exercises created space for shared learning, more coordinated responses and increased trust between actors.
>
> Liis Linn



In addition, Moldova hosted national and regional tabletop exercises implemented by eGA through an EU-funded activity and supported by NATO expertise, with contributions from the NATO–Republic of Moldova Professional Development Programme and the NATO CCDCOE, strengthening coordination and cyber resilience in practice.

This work shows that cyber defence is strongest when cooperation is well aligned. Bringing together NATO expertise, EU support, and national needs helps turn international cooperation into real cyber capability.

Explore the project

Strengthening cyber defence through practice

Merle Maigre
Head of the Cybersecurity Competence Centre

Cyberattacks have become an inevitable part of our digital lives. Therefore, it is wise to expand the community of professional cybersecurity specialists and well-trained teams via practical cyber exercises.

"For Ukraine, cyber resilience is a frontline need in wartime. As Russia continues its full-scale aggression, cyberattacks increasingly target government systems and critical infrastructure to disrupt daily life. This year, CERT-UA (the Computer Emergency Response Team of Ukraine) has already registered more than 5,600 cyberattacks. Over the past two years, the number of attacks has doubled, and they often coincide with missile strikes," said Nataliia Tkachuk, head of the Cybersecurity and Informational Security Service of the Office of National Security and Defence Council of Ukraine and secretary of the National Cybersecurity Coordination Centre. "Building hands-on skills and trusted coordination across sectors helps keep essential services running and strengthens readiness to protect Ukraine's cyberspace. I'm convinced that hundreds of attacks are being thwarted because of the new knowledge participants take away from exercises like this."

The same applies for Moldova, Albania, Montenegro and North Macedonia and the whole Western Balkans as a region, where eGA has carried out cyber exercises in 2025.

Translating technical effects

During exercises, participants learn how to translate the potential effects of technical processes into language that management can understand. Why? Experience shows that cyberattacks often escalate into something much bigger, demanding the attention of high-level decision-makers. Tech experts learn to summarise their knowledge in a way that non-tech experts can understand. We have repeatedly seen that this skill is a weak spot in the cybersecurity community.

The cyber exercises that eGA offers its project partners go beyond textbook learning, providing hands-on experience and real-time feedback on participants' performance.

Photo:
A dynamic visualisation tool supporting real-time exercise monitoring.

Visualisation matters

An effective exercise requires a proper visualisation and scoring system to provide an objective evaluation of participants' performance and offer guidance on how they can improve. Visual tools also help observers quickly grasp results and overall progress.

Dynamic visualisation is especially important when reporting cyber incidents to senior management. Presenting complex technical information in a clear way supports timely decision-making and helps organisations prepare for the broader impact of cyberattacks. This contributes to enhancing public trust.

Investing in training and education is arguably the most worthwhile investment one can make. This is particularly pertinent in the context of technological advances, which create new opportunities but also make skills obsolete more quickly. Practical, hands-on learning is what truly builds human capital and prepares organisations and individuals for the future.

> "I'm convinced that hundreds of attacks are being thwarted because of the new knowledge participants take away from exercises like this."

Nataliia Tkachuk
Head of the Cybersecurity and Informational Security Service of the Office of National Security and Defence Council of Ukraine

Three types of exercises

Capture the Flag (CTF) exercises use Jeopardy-style tasks to test a range of cybersecurity skills, with participants working individually or in teams and receiving guided hints.

Threat-hunting exercises focus on developing advanced threat detection and mitigation skills based on real-world scenarios.

Live-fire exercises simulate cyber incidents to strengthen technical incident response, offensive security skills and leadership decision-making.

These exercises emphasise collaboration over competition, using benchmarks and feedback to improve performance rather than declare winners.

Cyber exercises in 2025

Cyber exercises organised by the e-Governance Academy (eGA) and CybExer in 2025 engaged:

- 187 Ukrainian government cyber specialists and students under the Tallinn Mechanism, supported by ESTDEV (Estonian Centre for International Development)
- 62 representatives from Moldovan critical infrastructure providers
- 32 technical experts during the EU-supported project "Cybersecurity Rapid Response for Albania, Montenegro and North Macedonia 2.0"
- 60 cyber specialists from the Western Balkan countries under the EU-supported project "Cyber Balkans"

"The exercise felt realistic and engaging, especially the variety of challenges like log analysis, network forensics and decoding tasks. It offered enough freedom to approach problems creatively, which made it feel closer to real-world incident response."

Participant in the cyber exercise

"The interactive format made it possible to put my new knowledge into practice, which was extremely useful. What I liked most was seeing how everyone's individual efforts came together to make us stronger as a team by sharing information and working together."

Andrii Fedorov

Specialist in the Analytics and Cyber Security Department of the State Emergency Service of Ukraine

"Overall, I really liked the event. Because we immediately see our own weaknesses and strengths."

Participant in the cyber exercise

Photo: Participants of the UA–EE Cyber Shield exercise share their feedback with Nataliia Tkachuk and other Ukrainian officials.

"The cyber range and format of the challenges differed from anything encountered in prior CTFs. This, in turn, increased our interest and motivation to complete the tasks."

Participant in the cyber exercise

Keeping people at the centre of cybersecurity

Rica Williams
Senior Expert

Imagine what would happen if a country's defence was only as strong as the password of its least-trained official. While this is an exaggeration, it contains a sobering pinch of truth.

As we look back at the cyber threat landscape of 2024 and 2025, a clear trend has emerged: while software grows more sophisticated, the human factor remains the most targeted vulnerability. In fact, according to the Estonian Information System Authority (RIA) 2025 yearbook, the vast majority of cyber incidents are still rooted in human error.

Cyber hygiene has moved beyond the remit of IT departments and dedicated cyber organisations such as CSIRTs (computer security incident response teams) and CERTs (computer emergency response teams). It is now a critical pillar of national resilience and social well-being. With the rise of AI-driven phishing and automated social engineering, a single compromised account can lead to large-scale data breaches or service interruptions. Governments must prioritise the "human firewall" because technical solutions alone cannot keep pace with the number of intrusions that start with a simple phishing link or scam scheme message.

> Governments must prioritise the "human firewall" because technical solutions alone cannot keep pace with the number of intrusions.
>
> Rica Williams

Recommendations for governments

To educate a population effectively, governments should consider:

- **Data-driven decisions:** Clear governance models that coordinate awareness-raising efforts.
- **Contextual learning:** Moving beyond generic advice to industry-specific training.
- **Addressing AI:** Training users to identify deepfakes and AI-generated phishing.
- **Large-scale campaigns:** Treating cyber hygiene with the same urgency as public health.
- **Multiple partners:** Engaging CSOs, NGOs and universities through grant schemes.

Local context is key in awareness activities

While trends in "human-driven" incidents are largely the same across the globe, there are nuances that require local knowledge to inform communication or capacity-building activities. This is where local intelligence and data-driven decision-making truly come into play.

If a country has a reliable system for incident reporting and data collection across institutions and sectors – rather than focusing solely on critical infrastructure –awareness-raising activities become far more effective.

> While 32.7% have used generative AI, far fewer understand its associated risks.
>
> Rica Williams

For example, while promoting strong passwords and the use of multi-factor authentication (MFA) is a basic principle of cyber hygiene, campaigns that address specific, emerging scams or phishing attacks tend to gain more attention. These attract more interest and are therefore more likely to achieve the end goal: changing user behaviour. In these cases, individuals are more likely to enable two-factor authentication or carefully check the URL of links sent to them.

A great example comes from Moldova, through the Moldova Cybersecurity Rapid Assistance 2.0 project. The cyber crime unit of the national police identified a rapidly growing investment scam, with both the number of incidents and financial losses increasing at an alarming pace.

A wide-angle view on digital safety

Taking a broad view of cybersecurity awareness is key to resilience. The definition of "online safety" has expanded beyond technical threats to include wider societal risks such as:

- Human trafficking: Many cases of human trafficking begin online, with digital malpractice contributing to the recruitment and exploitation of victims, as analysed by ASTRA Anti Trafficking Action (Serbia).
- Information integrity: Awareness activities in Moldova have included identifying mis- and disinformation, as well as AI-generated deepfakes. Supporting journalism that uncovers misinformation is now a vital part of cyber hygiene.

All these initiatives address the "why," openly pointing out the consequences of poor online hygiene. The European Digital Competence Framework (DigiComp 2.2) highlights that online safety is no longer just a technical skill but a blend of knowledge, skills and attitudes. In an AI-shaped world, citizens must develop a sense of healthy scepticism.

According to the report State of the Digital Decade 2025, online safety (cybersecurity) remains one of the weakest digital competence areas, with only around two-thirds of the European population possessing basic safety skills. While 32.7% have already used generative AI, far fewer understand its associated risks.

Cybersecurity awareness is as much a social challenge as a technical field. Our goal is to ensure that as technology evolves, people remain the strongest link in the chain.

"Stop Fake Investments!" campaign in Moldova

In Moldova, the urgent need for a "human firewall" was underscored by a sharp rise in sophisticated online fraud. Banking crimes increased from 73 million lei (about €3.5 million) in 2024 to over 211 million lei (about €10.1 million) in the first nine months of 2025 alone.

This alarming triple-digit increase in damages prompted the national police to launch the "Stop Fake Investments!" (Stop Investițiilor False!) campaign in October 2025 together with eGA. By issuing public warnings (featuring local influencers) and exposing scammers' tactics, the four-week social media campaign delivered significant impact:

- Reach: 513,725 people connected
- Engagement: Over 1.1 million impressions
- Media coverage: Nine TV channels and 35 articles in local media

Through the campaign, the cyber crime unit shifted from reactive policing to a proactive digital hygiene, engaging the public through leaflets, press conferences and direct outreach.

Listen to the episode on cyber hygiene awareness initiatives in Moldova

Targeted actions in the Western Balkans via KnowCyber grants

Similar examples of targeted awareness activities can be found among KnowCyber grantees in the Western Balkans (Albania, Bosnia and Herzegovina, Kosovo, Montenegro and North Macedonia). Here, NGOs designed activities relevant to specific audiences, ranging from students and teachers to SMEs and media organisations.

Low levels of cybersecurity knowledge among SMEs require urgent attention, as SMEs constitute the majority of many economies. As part of the Cyber Balkans project (funded by the EU and implemented by eGA), several insights emerged:

- **Albania:** A survey by the Independent Forum for the Albanian Woman found that over 70% of SMEs lacked formal cybersecurity policies and 80% had no training.
- **Montenegro:** A survey by the NGO Secure revealed that 76.5% of SME respondents were unfamiliar with the concept of cyber hygiene. Read more on pages 61-63.

Key projects

Moldova Cybersecurity Rapid Assistance 2.0

2024–2025

Building on the successes of Cybersecurity Rapid Assistance 1.0, version 2.0 of the project strengthened Moldova's cybersecurity by increasing the cyber-resilience of public sector organisations and critical infrastructure sectors.

Funded by the European Union

Cyber Balkans

2023–2026

This project aims to strengthen cyber resilience in the Western Balkans by enhancing cybersecurity prevention, preparedness and response among public and private stakeholders in Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia and Serbia, aligned with EU standards and best practices.

Funded by the European Union

> The low levels of cybersecurity knowledge among SMEs require urgent attention, as SMEs constitute the majority of many economies.
>
> Rica Williams

Photo: Rica Williams promoting online safety awareness.

Western Balkans: Building cybersecurity awareness through local action

Kristiin Jets
Communication Expert

Cybersecurity awareness cannot develop through policy alone. While strategies and legal frameworks give the necessary direction, real cyber resilience is built where digital risks are encountered every day – in classrooms, small businesses, communities and online spaces.

Through the EU-funded KnowCyber Grants for the Western Balkans, implemented by the e-Governance Academy (eGA), the European Union has focused on this practical layer of cybersecurity. Working with local civil society organisations across the region, the initiative promoted cyber hygiene, responsible online behaviour and a deeper understanding of digital risks, with a strong focus on awareness, education and hands-on skills.

A defining feature of the approach was its local delivery. Six local civil society organisations worked directly with small and medium-sized enterprises (SMEs), young people, educators, journalists and vulnerable groups, tailoring their activities to national contexts and community needs. By engaging audiences that are often hardest to reach through formal policy channels, these local projects helped embed cybersecurity awareness into everyday practices.

Photo: KnowCyber grantees' best practices workshop.

The KnowCyber grantees show that cybersecurity awareness is most effective when it is practical, locally grounded and closely connected to everyday realities. While local contexts vary, the core principle remains. Cyber resilience is built through knowledge, habits and informed decision-making. All told, it contributes to a more inclusive and sustainable cybersecurity ecosystem across the Western Balkans.

Montenegro: Strengthening SMEs' cyber resilience

Focus: Strengthening cybersecurity practices and incident-response mechanisms among SMEs. They are the backbone of the national economy, but particularly exposed to cyber risks.

Action: NGO Secure conducted quantitative research, revealing widespread unfamiliarity with cyber hygiene, limited access to cybersecurity training and weak internal policies and reporting procedures among SMEs. Based on these findings, the project provided targeted training for SMEs together with a national awareness campaign.

Result: Participants reported clear improvements in their ability to recognise phishing attempts, manage passwords securely and understand incident-reporting processes. At the same time, the training was rated as highly useful by SME representatives. By strengthening cyber hygiene at the organisational level, the project showed that cybersecurity resilience directly supports businesses' economic stability.

"By strengthening SMEs, we are strengthening the entire Montenegrin economy. Without awareness at the management level, employees are left without guidance, procedures or protection. Our goal was for every business to understand that cyber hygiene is clearly an economic necessity, not a luxury."

Ivona Dabetic,
president of NGO Secure

North Macedonia: Reimagining cybersecurity education

Focus: Making cybersecurity education meaningful and engaging for young people by connecting it to their everyday digital lives. Traditional approaches often struggle to achieve a lasting impact, particularly when cybersecurity is presented as abstract rules detached from students' everyday digital lives.

Action: Through the SHIELD project, the Center for Innovations and Digital Education Dig-Ed combined digital storytelling, gamification and AI-supported tools. Teachers were trained to use the EduGame AI framework to deliver interactive, age-appropriate lessons based on real-life online situations.

Results:

- 40+ teachers trained
- 2,300+ students tought
- Improved knowledge retention, motivation and confidence in handling online risks
- Reusable gamified learning materials shared among educators

"Cybersecurity is usually taught as a set of rules, and for students, those rules can feel distant and abstract. When learners don't see themselves in the content, they disengage. Teachers don't need to become AI experts or game developers. They need confidence, adaptable tools and a framework that supports them. And this is how the SHIELD project can support them."

Maja Videnovik,
co-founder of Dig-Ed Centre

Kosovo: Strengthening cybersecurity for media and civil society

Focus: Reducing cybersecurity risks for independent media and civil society organisations which play a critical role in democratic governance. These organisations depend heavily on digital systems but often lack sufficient resources and become more exposed to cyber threats.

Action: Open Data Kosovo, with Arcus Security, conducted cybersecurity assessments across 11 key areas, followed by tailored technical support, staff training and practical improvement plans aligned with each organisation's circumstances.

Results:

- Organisations received tailored improvement plans designed to fit their operational realities. Over the course of the project, organisations strengthened their data protection practices, improved incident-response preparedness and increased staff awareness of cybersecurity risks.
- Beyond individual organisations, the project also published a sector-wide report that highlighted systemic cybersecurity challenges faced by the media and civil society in Kosovo, helping to guide future support activities and policy discussions.

"We noticed that when leadership is involved, change happens much faster. Training creates quick wins, but management commitment is what makes those wins sustainable."

Blerta Thaçi,
executive director of Open Data Kosovo

KnowCyber.eu

This Cybersecurity knowledge hub brings together best practices, expert insights and key trends shaping the cybersecurity landscape in the Western Balkans. Developed in close cooperation with regional experts, the platform gives an overview of evolving cyber risks, policy developments and practical approaches to strengthen cyber resilience in the region.

Find out more:

Enhancing capacity and cooperation through cyber diplomacy education

Ene Višnev
Senior Expert

A solid understanding of cyber diplomacy and its core principles is vital for building capacity, equipping professionals with the knowledge, practical skills and networks needed to operate effectively in a complex and rapidly evolving domain.

As states, societies and economies grow increasingly dependent on digital technologies, engaging government experts in dedicated training programmes becomes essential. Such programmes enable participants to develop relevant expertise and contribute meaningfully to international dialogue and cooperation. The e-Governance Academy has been supporting this effort through specialised cyber diplomacy initiatives, including its flagship project, the Tallinn Cyber Diplomacy Summer School.

Participants in cyber diplomacy programmes benefit in several ways. They gain a solid understanding of how cyberspace relates to foreign policy, security, economic development and human rights. Through workshops, panels, scenario-based exercises and case studies, participants learn about diplomatic responses to cyber incidents, international norms of responsible state behaviour and best practices for multi-stakeholder engagement. The programmes also foster strong professional networks, enabling cooperation and exchange across regions and institutions beyond the training itself.

> Cyber diplomacy provides tools for confidence-building, crisis management and international cooperation, helping to reduce misunderstandings and prevent escalation.
>
> Ene Višnev

Not only for diplomats

Crucially, cyber diplomacy is not only the domain of diplomats but relies on the entire cyber ecosystem, including policymakers, technical experts, cybersecurity practitioners, the private sector, academia and civil society. At the national level, recognising this shared responsibility is essential, as coherent cyber positions and credible international engagement depend on strong coordination between ministries, agencies and non-governmental stakeholders. Cyber diplomacy training programmes increasingly reflect this reality by bringing together participants from diverse professional backgrounds and encouraging cross-sectoral cooperation.

States rely on cyberspace to operate critical infrastructure, deliver public services and protect democratic processes, while facing cyber threats that cross borders and escalate rapidly. Cyber diplomacy provides tools for confidence-building, crisis management and international cooperation, helping to reduce misunderstandings and prevent escalation.

Explore more at

Photo: Participants of the Tallinn Cyber Capacity-Building Fellowship 2025.

Photo: Participants of the Tallinn Cyber Diplomacy Summer School.

Expansion of topics

In a geopolitical environment marked by growing tensions, sustained dialogue in the cyber domain is more important than ever. While international law in cyberspace, cyber norms and confidence-building measures remain central topics, new issues have gained prominence. These include the security implications of artificial intelligence, emerging and dual-use technologies, supply chain security, cyber capacity-building and the protection of democratic institutions online.

The rapid development and deployment of AI in particular raise complex questions related to responsibility, transparency and governance, making AI an increasingly important topic in cyber diplomacy discussions.

Practice-oriented approach

By regularly updating its curriculum to reflect emerging developments in this field, the Tallinn Cyber Diplomacy Summer School remains relevant and continues to offer valuable opportunities for in-person learning and cooperation. Complementary initiatives, such as the Tallinn Cyber Capacity-Building Fellowship, take a practice-oriented and inclusive approach, enabling participants to apply new knowledge directly within their national and organisational contexts.

By strengthening capacity across the entire cyber ecosystem and promoting cooperation, cyber diplomacy training programmes make a lasting contribution to building a free, open, safe and secure cyberspace.

What makes digital identity work

Mark Erlich
Senior Expert

Electronic identification and digital identity underpin the modern digital economy, yet countries approach them with very different results. While some have built systems that work seamlessly for citizens and foreign residents alike, others continue to struggle. What explains the gap – technology, economics, governance or something more fundamental?

Before we get into potential issues in implementing electronic identification, we need to define identity. Identity is a set of data that uniquely describes a person, allowing them to be distinguished from others. The set of data that uniquely identifies a person should be as small as possible to minimise the risk of fraud and ensure robust security.

When identity is established (enrolled), personal data is collected to create a person's account in an identity registry. At that point, a unique identifier is created – a single data field that is unique and linked to the person, helping connect the person's identity to data related to him or her.

The purpose of a unique identifier

A unique identifier can differ depending on the context in which it is used and who has issued it. It may be an e-mail address, a loyalty card number, a national identity number, a social security number or the like. What is most important about a unique identifier is that it links a person's identity to personal data and other business data related to that person.

Since a unique identifier links data, it exists across different databases and services as a relational key element. If any registry, service or database leaks or exposes data, the unique identifier and related data will be exposed as well – but not the core identity data stored in the registry where the identity was originally enrolled.

For this reason, a unique identifier should not be used as a secret for identity verification. Instead, verification should rely on other methods, such as secure document elements and multi-factor authentication.

Self-declared vs. issued identity

There are different types of identity we use daily, but for simplicity, identity can be divided into two categories: self-declared and issued. With self-declared identity, a person claims an identity by registering data. This data is usually not checked or validated; it is trusted as is. This type of identity is commonly used in social media, e-mail services and communication platforms.

An issued identity, on the other hand, is issued by an organisation or a government. In this case, the issuer is responsible for the trustworthiness of the identity, and identity data is checked and validated during issuance. National identity issued by the government is an obvious example, but so are third-party identities based on national identity – such as those issued by banks, telecom companies or membership programmes – where identity data verification places them firmly in the category of issued identities.

Because issued identities are considered trustworthy, it is essential to maintain high trust throughout the enrolment and verification processes. One of the most dangerous approaches is when an issued identity relies fully or substantially on self-declared identity. This does not mean that self-declared identities (such as Google or Apple accounts) cannot be part of the data collected during enrolment,

but such information should not play a substantial role, as there is little or no guarantee that the identity data actually belongs to the person.

From physical to digital

When it comes to proving one's identity, traditional methods rely on presenting identity documents. An identity document contains basic identity data and a unique identifier (for example, a membership number or national identification number). To verify this data, the document usually includes physical security features such as holograms or microtext, as well as a photograph of the person. By examining these elements, it is possible to verify whether the document is real and authentic and belongs to the person presenting it. In addition, document issuers can provide information about invalidated (revoked) documents.

When identity-proofing moves online, we are talking about electronic identification (eID), where digital identity – identity data presented in digital form – must be verified by a third party. Because the risks of manipulation and forgery are much higher in the digital environment, digital identity data cannot be trusted on its own.

As a result, eID systems perform more complex functions and use secure systems to mitigate risks as much as possible. Encryption is typically one of the core security measures, ensuring that data and verification information are strongly protected. Multi-factor authentication (MFA) is also widely used to verify the identity of the given person.

Why eID projects fail

1. **Lack of knowledge.** Decision-makers want quick results and believe that technology is a miracle solution to existing problems. By demanding fast delivery of digital identity, they miss a fundamental point: without properly functioning identity management, there cannot be a trusted digital identity.
2. **Lack of a solid identity foundation.** First, a functioning core identity and its management system must be in place. If a country does not have a trusted and secure identity system, this needs to be fixed first. Only after that can identity proofing and verification systems be built, such as identity documents and an eID system (including eID means).
3. **Semantic confusion.** Problems often begin with an unclear understanding of what terms such as eID, digital identity and identity management actually mean and how they relate to one another. This frequently leads to the following situation: the buyer believes they know what they want but describes it using the wrong terms. The bidder delivers what they believe the procurer has asked for. In the end, something is delivered, but it barely works – if at all – and no one is satisfied.

Learning from experience

The e-Governance Academy (eGA) brings nearly three decades of expertise in identity management, rooted in Estonia – one of the world's earliest and most successful eID implementations. Working with governments across diverse contexts, eGA experts understand how different identity models function in different societies.

Learn more

Most commonly, this involves at least two factors (two-factor authentication, or 2FA): a knowledge-based factor (such as a password or PIN) and a possession-based factor (such as a smartcard, mobile phone or secure account). The possession-based factor must be under the given person's full control and must ensure (as much as possible) that it cannot be used by a third party without the knowledge of the given person. In many contexts, the solution for the possession-based factor is also called the eID means.

Key considerations for planning a national digital architecture

Tõnis Mäe
Senior Expert

True "digital government" represents a fundamental shift in how a country serves its people. In this model, all information generated through the daily activities of government, businesses and citizens is treated as a vital national asset – one that enables better decisions, more efficient services and greater public value. To achieve this, public sector leaders must look beyond fragmented IT projects and embrace a holistic government digital architecture.

Government digital architecture is more than a technical map; it is a social contract. It defines how the state respects its citizens' time, protects their data and utilises national assets to make better decisions. Success lies not in the complexity of the code but in the simplicity of the services. When the architecture remains invisible and the services feel seamless, the digital transformation has truly succeeded.

The need for a holistic blueprint

Building a national digital architecture is comparable to planning a modern city. It requires a solid foundation, clear construction rules and shared utilities such as water and electricity that are accessible to everyone.

Advancing this digital shift requires a high-level master plan that addresses three fundamental questions: what exists today, what do we want to achieve, and what is currently missing? In this sense, digital architecture focuses on the entire state's goals, business processes and organisational structures to answer a fundamental question: "How do we organise ourselves to deliver value?"

Photo:
Heiko Vainsalu (eGA)
speaking at the interoperability workshop.

5 reasons for failure

Even with a well-defined architecture, many digital government projects fail. While technology is often blamed, the reality is that governance, politics and culture are the most common causes of collapse. Common reasons for failure include:

- **Lack of clear authority:** Failure is rarely the result of insufficient funding; more often, it stems from unclear leadership. Effective digital architecture requires a designated lead agency with a clear mandate and empowered architects to guide implementation.

- **Mirroring inefficiency:** Architecture fails when it replicates the messy and siloed internal government structures instead of being designed around citizens' needs and service delivery.
- **The design-reality gap:** Architectural blueprints are often developed in isolation by external consultants or IT experts who lack a deep understanding of how governments function in practice.
- **Lack of internal ownership:** Governments often lack the internal skills to manage these projects and rely heavily on external organisations. While these experts may deliver high-quality content, insufficient ownership within government often results in the documents remaining unused.
- **Outdated legal frameworks:** In many countries, legal requirements still need physical signatures or "wet stamps". If legislation is not updated alongside digital architecture, new systems risk becoming an additional administrative step rather than an enabler of transformation.

Critical success factors

To avoid pitfalls and ensure that the digital architecture becomes a living, breathing foundation for the state, it is crucial that the lead agency responsible for the architecture is formally appointed and recognised by the wider community.

When developing a national digital architecture, the following factors are essential for success:

1. **Establish a mandate with teeth:** Digital architecture must function as an enforceable standard, not just a suggestion. The lead agency requires political authority to reject projects that do not align with the national blueprint, often by linking architectural compliance directly to the budgeting process.
2. **Implement the "once-only" principle:** To overcome institutional silos, architecture must be built on the principle that data belongs to the citizen, not individual agencies. Using a secure data-exchange layer allows different agencies to communicate and share information seamlessly, ensuring the government acts as a single, coordinated entity.
3. **Build in-house ownership:** While external experts and consultants provide technical expertise, the core vision must remain within the government. A successful digital state invests in its own architects, who understand the "ground reality" and use the architecture as a practical tool for daily decision-making.
4. **Practice "agile architecture":** Big-bang approaches that try to plan five years in advance should be avoided. Instead, governments should build small, reusable building blocks – such as national logins or digital signature services – that can be deployed incrementally, deliver value quickly and build public trust.
5. **Align law with technology:** Digital architecture and legal frameworks must evolve together. Every technical requirement, such as a digital ID or electronic signatures, must be supported by law that grants it equal legal standing to physical documents and processes. Without digital-first legislation, architecture risks becoming a parallel system with limited impact.

Key project

E-ffective e-governance: Accelerating e-government and digital public services in Bangladesh

2024–2028

This project aims to modernise Bangladesh's public administration by integrating digital processes, building a skilled workforce and enhancing public service accessibility and quality. eGA's focus is on improving digital interaction and coordination among government, promoting interoperability and building the capacity of public sector employees. The British Council, as a partner, will focus on enhancing public services provision.

Funded by the European Union

The power of digital learning

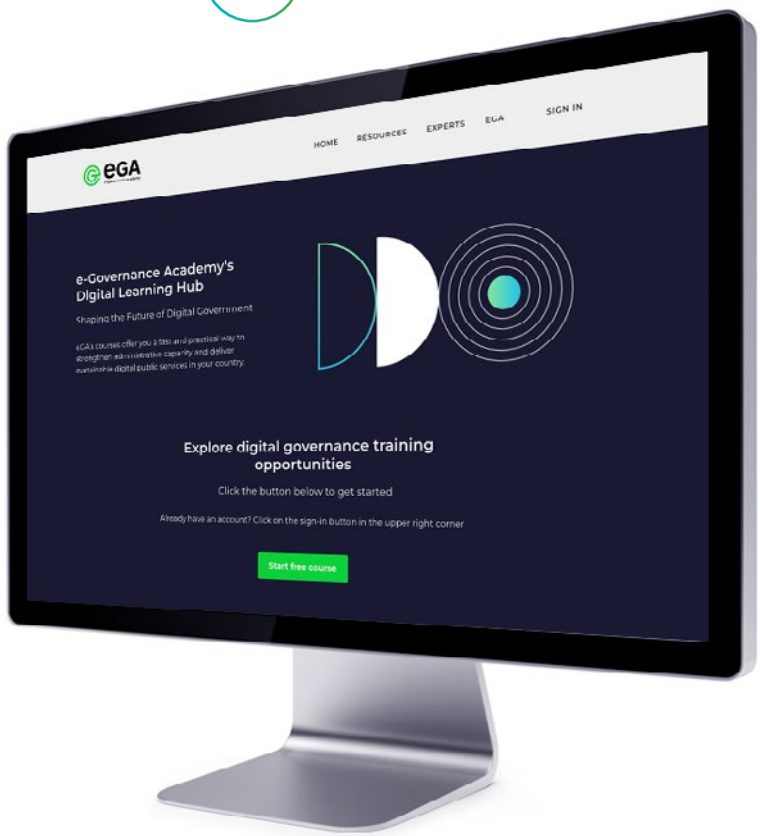
Marge Oldermann-Neeme
Digital Learning Expert

For over 20 years, the e-Governance Academy has worked with public officials through study visits and on-site programmes to demonstrate that digital government is both a viable and effective system. But lasting change requires more than a few convinced leaders. Digital learning scales this knowledge across organisations, making digital innovation a shared responsibility rather than the task of a small group.

Today, information is everywhere. Tools like ChatGPT can give quick answers in minutes, but information alone doesn't build competence. Public officials need a shared understanding of what digital government really means in their context, a common language around data, cybersecurity, interoperability and AI, and the confidence to make decisions and lead change. That confidence comes from structured learning that connects directly to the daily work.

Creating a shared language

Digital transformation is, above all, a form of change management. Technology can be bought and built. Changing mindsets, routines and processes takes longer. Digital learning helps because it creates a shared starting point for learning. When everyone, from policy officers to IT teams and senior managers, has gone through the same core e-course, they start from a similar understanding of key principles. Conversations become faster and more concrete because less time is spent aligning on basics, and more time is spent deciding what to do.



It also builds a common vocabulary. Terms like interoperability, the once-only principle, digital identity and artificial intelligence in public services become tools that can be actively used in discussions and planning. People across institutions begin to discuss the same issues in the same way, which is essential to ensure that digital projects connect to a bigger picture, rather than remain isolated systems.

> Digital learning enables the extension of the same knowledge and mindset across a wider organisation.
>
> Marge Oldermann-Neeme

Another important aspect is coping with the resistance to change. People might be unsure what exactly is changing, why it matters or how it will affect their daily work. The e-Governance Academy's digital learning e-courses explain the why and the how, not just the what. Once people feel they understand the basics, engagement grows.

Learning that fits the reality of public service

For busy public servants, flexibility is a necessity. Self-paced digital learning fits around everyday work, allowing participants to learn anytime in short and focused segments and return whenever needed. If a part of the course feels especially relevant or complex, it can be replayed as many times as needed.

Our e-courses at the e-Governance Academy's digital learning hub combine video, text, infographics, quizzes and practical reflections to keep learners engaged without overwhelming them. The key is to keep moving, step by step, towards greater digital confidence.

This is how big shifts often start – quietly, with a single decision to learn. Together.

Are we ready for digital transformation?

- ☑ Do our officials understand digital government beyond strategies and slogans?
- ☑ Do we share a common vision and language around digitalisation?
- ☑ Are practical learning opportunities available to staff today?

If any answer is "not yet", start with digital learning.
Even one course on a priority topic can be the first step toward lasting change.

eGA's Digital Learning Hub

At the e-Governance Academy, our e-courses are built on real experience and focus on the key areas of modern public administration, ranging from digital governance and public-sector transformation to artificial intelligence, enabling technologies and cybersecurity. You don't need perfect conditions to start, just the first step.

Explore our digital learning e-courses

Need something more tailored?
Request a custom e-course, digital learning consultation or content development that integrates seamlessly into your environment.

From startup to system: Ukraine enters a new phase of digital transformation

Mari Pedak
DT4UA Projects Team Lead

Photo: Mari Pedak, Hannes Astok (eGA) and Asier Santillán (EU Delegation to Ukraine).

Ukraine's digital transformation began not with digital passports or high-visibility online services but with foundational work behind the scenes.

This included modernising state registers, enabling secure data exchange, strengthening cybersecurity and building digital capacity in public institutions. These early efforts demonstrated that successful digitalisation depends not only on technology but also on standardised processes, institutional expertise and cooperation across government.

The e-Governance Academy (eGA) has been a reliable partner at every stage of Ukraine's digitalisation. For over 12 years, eGA has been working closely with Ukraine, supporting reforms, launching new e-services, building digital infrastructure and contributing international expertise through EU-funded projects such as EU4DigitalUA and DT4UA. This cooperation has helped ensure that Ukraine's rapid digital progress is built on sustainable and interoperable foundations rather than isolated technological solutions.

Learning from Estonia and building Ukrainian innovation

Estonia's experience has played a formative role in Ukraine's digital transformation journey. One of the earliest milestones was the introduction of Trembita, Ukraine's secure data exchange system based on Estonia's interoperability model and Cybernetica's UXP solution. Trembita became a cornerstone of Ukraine's digital state, enabling data to run between institutions so that citizens no longer had to.

Building on this foundation, Ukraine adapted international best practices to its own context. Drawing lessons from Estonia's electronic identity framework, the country developed its own innovations, including the world's first legally binding digital passport and the Diia.Signature mobile solution. Together with eGA and partners, Ukraine also introduced platforms such as Vulyk, which automated the work of municipalities' administrative service centres and brought digital standards to the local level.

Key facts

23+ million Ukrainians use the Diia application

65+ services available via mobile

160+ services available through the portal

A mobile-first state at scale

At the same time, Ukraine pursued its own user-centred path. Adopting a mobile-first approach, the state built services around how people actually interact with government. Today, Ukrainians use the Diia application, accessing over 65 services via mobile and more than 160 services through the portal. Many of these, ranging from educational documents to the integrated e-Entrepreneur service, were developed with eGA support and reflect a deliberate focus on simplicity, security and scalability.

As digital services multiplied, differences in institutional readiness became more visible, particularly at the regional and local levels. Projects aimed at strengthening the digital capacity of administrative service centres, including initiatives in Zhytomyr, revealed uneven levels of digital maturity, skill gaps among staff and varying readiness to adopt new systems. These disparities affected not only the speed of implementation but also the quality and consistency of services delivered to citizens.

From rapid growth to systemic maturity

As digitalisation accelerated, systemic bottlenecks became harder to ignore. The absence of unified standards, shared templates and common methodological approaches meant that government teams, international technical assistance projects and developers often had to repeatedly align identical documents and processes. Over time, this fragmentation became a limiting factor, slowing progress and increasing complexity.

After several years of fast-paced service launches, it became clear that the next stage of digital transformation would require more than innovation. Institutional capacity, standardisation and continuity had to move to the forefront. This shift is particularly important for Ukraine's digital integration with the European Digital Single Market and for the future rollout of cross-border services aligned with EU frameworks.

The Digital Competence Centre: institutionalising transformation

The need for a more structured approach became even more evident after the start of Russia's full-scale invasion. The pre-war "revolutionary" model of rapid experimentation was no longer sufficient. Knowledge, expertise and lessons accumulated between 2014 and 2022 had to be preserved, systematised and made accessible to a growing community of digital reformers.

In response, at the beginning of 2025, with the support of the eGA, Ukraine established the Digital Competence Centre, a consultative and advisory body under the State Enterprise Diia. Its role is to collect and structure methodologies, standards, analytical tools and best national and international practices, making them available to all actors involved in digital reforms.

The goal set by the Ministry of Digital Transformation in 2019 – to bring 100% of public services online – remains unchanged. However, behind the apparent simplicity of digital services lies the coordinated work of hundreds of professionals: lawyers, analysts, designers, developers and communicators. As demand for digitalisation continues to grow, with many institutions aspiring to bring their services into Diia, the Centre is designed to act as a force multiplier, accelerating service development without compromising quality.

> Successful digitalisation depends not only on technology but also on standardised processes, institutional expertise and cooperation across government.
>
> Mari Pedak

Early results and practical impact

One of the first tangible outcomes of the Digital Competence Centre was its role in revising the Cabinet of Ministers' resolution that regulates the lifecycle of information systems in public authorities. Acting as a coordination platform, the Centre brought together representatives of public authorities, international partners and Ukrainian businesses. This collaborative process resulted in amendments that aligned regulatory requirements with real-world practices and international standards, creating a regulatory framework that works for all stakeholders.

A system designed to evolve

The Digital Competence Centre is not a static institution. Its mandate allows it to support sector-specific digital reforms, assist chief digital transformation officers (CDTOs) and civil servants, test new solutions and accelerate policy implementation.

By enabling the reuse of knowledge accumulated over more than a decade of reform, Ukraine is improving services for its citizens today and laying the groundwork for a resilient digital state in the future.

Digital Competence Centre at a glance

The Digital Competence Centre (DCC) is a consultative and advisory body under the State Enterprise Diia, established in early 2025.

The DCC aims to institutionalise Ukraine's digital transformation and accelerate the development of high-quality digital services at scale.

The DCC systematises methodologies, standards, tools and best practices, making them accessible to public institutions and digital reformers.

Key projects

DT4UA

2022–2025

The project continues to support Ukraine's digital transformation and integration into the EU's Digital Single Market. Its activities focus on enhancing the efficiency and security of public service delivery, ensuring accessible services for citizens and businesses in alignment with EU standards, and providing rapid responses to war-related needs. Additionally, developing the e-case management system, SMEREKA, will strengthen governance and streamline the processing of criminal cases.

Funded by the European Union

DT4UA Phase 2

2025–2026

The second phase of DT4UA marks a new stage in EU–Ukraine digital integration, supporting access to public services across borders, as many Ukrainians live in EU member states. As Ukraine begins EU accession negotiations, digital transformation has become a core part of preparation for membership, linked to Chapter 10 of the EU acquis. DT4UA Phase II therefore focuses on legislative harmonisation, cross-border digital services and modernising the infrastructure underpinning the digital state.

Funded by the European Union

Explore the full story of Ukraine's digital transformation

What 2025 taught us about elections, technology and trust

Priit Vinkel
Senior Expert at eGA, former Head of the Estonian State Electoral Office

The year 2025 was a significant one for elections. Around the world, there were more than 60 national contests, pointing up the relationship between technology, security and public confidence.

As digital tools become more embedded in electoral processes, a central question emerges: how does the way we use election technology influence trust in the results themselves? Let us take a closer look at the recent elections in Albania, Kyrgyzstan, Germany, Canada, Moldova and Estonia.

Technology delivers when transparency is built in

Countries expanded their use of election technology, but outcomes varied.

- **Albania:** Electronic voter ID and biometric de-duplication were used for a second time in general elections. Ninety-five per cent of polling stations were positively assessed, yet limited public disclosure of system testing put pressure on overall confidence. (OSCE/ODIHR EOM Final Report)
- **Kyrgyzstan:** The new biometric and ballot-printing systems functioned well in technical terms. However, awarding the contract to supply the systems without a public tender process eroded the overall integrity of the technology. (OSCE/ODIHR EOM SPFC Report)

These cases illustrate that, when it comes to overall trust, transparent and auditable processes before, during and after elections often matter more than the technology itself.

Low-tech methods continue to deliver

Some countries are continuing with analogue systems, and this is working well for them:

- **Germany:** Paper ballots were used and counted by hand, a process that was quick and seamless. Turnout reached 82.5%. This was the highest in decades. Broad acceptance of the results followed. (OSCE/ODIHR EAM Final Report)
- **Canada:** Paper ballots and post-election audits continued at the federal level. Registration and the transmission of results were digitised. Digital solutions are common at the local level. (OSCE/ODIHR NAM Report)

Hence, digitalisation is not essential for successful elections if a country's voters prefer clarity and verifiability over faster processes and technological advancements.

> As elections become more digital, trust depends less on innovation itself and more on visibility, governance, accountability and public understanding.
>
> Priit Vinkel

AI shifts election risk from systems to perception

While voting machines and IT systems were one facet of election trust, 2025 also confronted a more insidious challenge: the information sphere around elections, supercharged by artificial intelligence (AI). As these digital tools evolved, so did the threats: AI-powered disinformation mushroomed in 2025. Generative AI enabled malicious actors to produce deepfake videos, synthetic voice messages and countless automated social media posts at minimal cost.

Canada's 2025 election offers a telling example that also echoed across many other electoral contexts in 2025. A dispute between the government and a tech company led to a ban on news links ahead of the elections, creating information vacuums often filled by AI-generated videos and synthetic audio. Disinformation, frequently linked to foreign interference, has become a significant operational risk. Authorities responded with rapid communication teams and cybersecurity units. (Digital Forensics Research Lab Case Study)

These national experiences reflect a broader international pattern. The OSCE Parliamentary Assembly's 2025 report highlighted digital threats, disinformation and online manipulation as growing dangers to democratic elections. Reviewing elections in Romania, Albania, Moldova and Kyrgyzstan, the report warned that voters are increasingly struggling to distinguish reliable information from fabricated content. In such conditions, genuine political debate risks being overwhelmed by manufactured noise. Taken together, these developments underscore a critical shift: technical security measures are insufficient if voters distrust what they see or hear during campaigns.

Estonia: Building trust over decades

Estonia's two decades of experience with internet voting illustrate that trust in digital elections cannot be created overnight. It is the result of long-term investment and institutional continuity rather than a single technological breakthrough.

Estonia's digital voting system has evolved steadily alongside its broader digital identity ecosystem. For years, the ID card and Mobile ID were used as digital identity measures. In 2025, a third eID variant, the SmartID, was introduced, and 54% of all voters used this method in these elections. Additionally, the new mobile voting feature was successfully piloted in May 2025.

What is particularly striking is how familiar internet voting has become for citizens. Close to half of voters continue to use internet voting, including in local elections, with minimal controversy. That confidence rests on a clear set of principles that have remained consistent over time: mandatory digital ID, voter-verifiable voting, independent audit opportunities, clear fallback rules and continuous open public communication. Together, these elements create predictability, a key ingredient of trust.

Importantly, the Estonian Information System Authority (RIA) now considers the primary risk to be not hacking but disinformation and the gradual erosion of public trust, as Alo Heinla, Head of the RIA's Election Technology Department, noted. This assessment mirrors broader international trends observed in the 2025 elections.

Estonia's experience points to a more general lesson: secure digital voting cannot be deployed quickly. It depends on sustained national commitment, a mature digital ecosystem and institutions capable of maintaining trust as technologies evolve.

Moldova: Resilience amid hybrid attacks

Moldova's 2025 parliamentary elections were held amid unprecedented cyber threats. Over 1,000 cyberattacks on government digital infrastructure were recorded ahead of the vote, and a large-scale assault on election day forced authorities to block a central hosting platform, knocking some 4,000 websites offline. Election authorities introduced a new risk-based cybersecurity framework, which helped strengthen the country's digital resilience. As a result, key election systems withstood the foreign hacking attempts and the coordinated disinformation campaigns aimed at undermining public confidence. (OSCE/ODIHR EOM SPFC Report 2025)

Moldova's experience also highlights the importance of sustained investment in cybersecurity beyond the election period itself. Over several years, EU-funded programmes have supported the development of national cyber resilience through institutional strengthening, capacity-building and close cooperation with Moldovan authorities. Within this broader ecosystem of support, the e-Governance Academy has contributed to strengthening cybersecurity frameworks and operational readiness alongside national institutions and other international partners. Together, these long-term efforts have helped create the conditions in which critical election systems were better prepared to withstand cyber threats.

Quantum computing risk: From theory to awareness

Quantum computing did not disrupt elections in 2025, but it changed how we perceive future planning. Experts increasingly warn that many of today's encryption methods may not withstand future quantum capabilities. Digital identity systems and internet voting, both of which rely on cryptographic integrity, must now be designed with a far longer horizon in mind.
In response, post-quantum cryptography standards are already under development, with direct relevance for election technologies. (Cyber Security in Estonia 2025)

As a result, election security planning is no longer confined to electoral cycles, forcing governments to prepare today for risks that may only fully materialise tomorrow.

Takeaways for 2026 and beyond regarding trust in elections

Below are five key takeaways in the context of electoral management on how to maintain trust in elections in 2026 and beyond.

1. **Design transparency into election technology.** As election-management solutions grow more complex and digitally integrated, transparency mechanisms need to advance accordingly to facilitate public oversight. This means not only making technical documentation and audit reports public but also involving citizens and observers in understanding system operations and how their integrity is preserved.

2. **Treat disinformation response as core election infrastructure.** In an age where AI-produced content can quickly mislead the public, it is essential to have mechanisms to identify, counter and address false information, much like safeguarding ballot boxes or voter data. Election management bodies must prioritise information integrity as a vital operational area, establishing dedicated teams, protocols and collaborations before, during and after elections.
3. **Prioritise cybersecurity in election planning.** As elections become more digital, the surge of cyberattacks seen in 2025 shows that protecting election IT systems is as crucial as safeguarding ballot boxes. Cybersecurity should be treated as core infrastructure (e.g. implementing rigorous threat monitoring, defence mechanisms and rapid-response protocols) to secure the vote and uphold public trust.
4. **Invest today in future-proofing election security.** As quantum computing and advanced AI develop, the security assumptions supporting current election technologies might become outdated. Governments need to invest now in research, standards and upgrades to safeguard the integrity of democratic participation against future threats.
5. **Strengthen citizens' digital skills and awareness.** Trust in digital components in elections also depends on people's ability to understand and confidently use public digital services. Governments should invest in digital literacy, public communication and user support to ensure inclusive and informed participation.

Altogether, as elections become more digital, trust depends less on innovation itself and more on visibility, governance, accountability and public understanding. Technology can support democratic processes, but only when it is governed in ways that people can see, question and ultimately trust.

Success factors of tech in elections

Secure and Verifiable Technology
Digital election systems rely on trusted digital identity, strong cybersecurity and practical verifiability so that results can be independently checked. Systems must be resilient, auditable and designed with long-term risks in mind, including cryptographic evolution.

Institutional governance
A clear legal basis is needed that defines responsibilities, oversight and accountability across institutions and vendors. Governance structures must enable lawful decision-making before, during and after the election.

Transparency and observation
A public source code, observable procedures, access for independent observers across all election phases and transparent disclosure during incidents support confidence and informed scrutiny.

Information integrity and crisis response
Disinformation and technical incidents affect voter trust in similar ways and must be addressed through coordinated response mechanisms. Clear, timely public communication reduces uncertainty and limits manipulation.

Cybersecurity frameworks and operational readiness

Voter capability, inclusion and agency
Voters need digital skill support, accessible interfaces and clear communication to participate confidently. Digital options must expand choice while preserving non-digital alternatives and voter autonomy.

“Big Brother” under control: Estonia and Ukraine are letting citizens check who’s watching

Federico Plantera
Researcher in Tech Policy and AI

Fewer than half of people in the European Union – 44% – feel well-protected in the digital space (Eurobarometer, 2024). This is despite the General Data Protection Regulation (GDPR): the EU’s landmark framework that grants citizens formal rights over their personal data, including access, rectification, erasure and the right to know.

Awareness of these rights remains relatively high. Yet as the 2024 Special Eurobarometer survey confirms, knowing your rights and feeling protected are not the same thing. Rights on paper do not always, or easily, translate into confidence in practice.

The GDPR establishes that personal data shall be processed “lawfully, fairly and in a transparent manner”. But what does a transparent manner actually mean? For most people, it means a privacy policy – a document that, by law, should be “easy, readable and accessible.” In practice, almost no one reads them. Research consistently shows this gap: a Pew Research Center survey in the US context found that 56% of Americans always or often agree to privacy policies without reading them, and 61% believe these policies are ineffective at explaining how companies actually use their data (Pew Research Center, 2023). This is transparency as formality, not as function.

The gap between legal frameworks and lived experience persists globally. Research on Privacy by Design implementation confirms persistent difficulties translating legal principles into engineering requirements: “The widespread adoption of Privacy by Design faces obstacles due to a lack of knowledge, insufficient awareness of benefits, and the absence of specific implementation guidelines” (Abomhara et al., 2024). Law says one thing – systems do another.

Between legislation and architecture

This is the gap that some governments are now attempting to close. They are doing so through tools and architecture, rather than regulation alone. Law sets boundaries, but infrastructure makes those boundaries visible.

As Yurii Kopytin, Senior Expert at the e-Governance Academy and deputy team leader in Ukraine, puts it bluntly, "Law cannot solve the issue of trust." Legislation can prohibit certain forms of data access, but prohibition alone does not demonstrate accountability. Citizens cannot verify what they cannot see. Trust in digital services must be a continuous practice based on systems that allow citizens to verify, rather than simply believe.

The data tracker – a mechanism that logs every government query to personal data and makes those logs accessible to the data subject – operationalises transparency in precisely this way. Rather than asking citizens to trust that rules are being followed, it shows them the record. When citizens can see who accessed their data and why, the relationship between government and governed shifts to a matter of evidence.

This also reframes data protection from a centralised enforcement problem to a principle requiring distributed monitoring capacity. As Hannes Astok, Executive Director of the e-Governance Academy, observes: "Instead of having 20 or 200 eyes in a Data Protection Agency, you have 1.3 million people in Estonia monitoring who is using their data. In Ukraine, you have 40 million." The logic here lies in incentive, while

> When citizens can see who accessed their data and why, the relationship between government and governed shifts to a matter of evidence.
>
> Federico Plantera

> 56% of Americans always or often agree to privacy policies without reading them.
>
> Federico Plantera

scale is only an additional advantage. Citizens have an intrinsic motivation to scrutinise how their data can be accessed, and bureaucracy cannot replace this. When technology is designed to respect this, it contributes to the growth of a data protection culture – embedding transparency and accountability into the entire architecture of digital government rather than treating them as afterthoughts.

Estonia pioneered this approach with its X-Road interoperability framework. The e-Governance Academy's team is now supporting Ukraine to implement a similar system with Trembita, its national data exchange platform. Both cases show what happens when visibility becomes infrastructure.

In Estonia, visibility feeds behavioural discipline

Estonia's Data Tracker allows any resident to log into the national portal and review which government databases have accessed their personal data, when, and for what stated purpose. Every query through X-Road gets logged, and those logs are surfaced to the citizen.

The effects extend beyond individual oversight. Maarja Kirss, Head of Cooperation at the Estonian Data Protection Inspectorate, describes a notable shift over fifteen years: "I remember that 15 years ago we had lots of cases where state officials, even policemen, had access to personal data to fulfil their job responsibilities – but they also looked at other data for their own interest. Just for curiosity." Today, such cases have become rare. The Data Tracker functions not only as a factual record but as a preventive mechanism. Fines for unauthorised access may be modest, typically around €100, but the deterrent lies in exposure.

Estonia's experience also reveals a shift in how citizens engage with data protection. Since GDPR came into force in 2018, the Inspectorate has seen queries triple – but questions far outnumber complaints. Citizens increasingly ask whether a certain instance of data processing is permitted before problems occur, rather than only filing complaints after violations. Estonia's inquiry rate per capita, according to the Inspectorate's calculations, exceeds most European counterparts.

In Ukraine, forty million monitors

Ukraine's Personal Data Access Monitoring Subsystem, which is embedded in Trembita, follows Estonia's logic but operates in a different context – one marked by ongoing war, rapid digital transformation and the pressures of EU integration. The subsystem logs transaction ID, date and time, the organisations requesting or providing access, the specific registry accessed, the stated purpose, and in many cases, the individual employee who made the request.

The architectural choice to embed this within Trembita reflects the practical realities of where data exchange happens. "Our data is stored in different government registers, and it is used by various authorities and companies to provide services to citizens," Kopytin explains. "When they need access, they go through Trembita. That's why we implemented the monitoring system there – because it is the main place where data is processed."

Connection to the system is mandatory. Any public institution processing personal data through Trembita must use the subsystem, while exceptions exist only for specific security and investigation – a 1:1 representation of how transparency by design becomes the default.

The system distinguishes between automated and human-initiated access. Approximately half of all transactions are fully automatic – routine background processes that citizens need not be notified about individually. But for critical services affecting property, finances or legal status, Ukraine plans to push notifications through the Diia app, alerting citizens in real time when their data is accessed in a significant manner.

Hannes Astok draws on Estonian experience to forecast what Ukraine might expect by 2030: illegal queries diminishing markedly, public cases where citizens catch unauthorised access and officials face consequences, and rising awareness on both sides of the equation. As Kopytin puts it, "In the case of misuse of the data, government should take steps – either improve the procedures or fire someone who was misusing his or her right to access the data."

> Ukraine's Personal Data Access Monitoring Subsystem, which is embedded in Trembita, follows Estonia's logic.
>
> Federico Plantera

> Trust is not a byproduct of good technology, but a pillar that makes digital government viable at all.
>
> Federico Plantera

Transparency and trust as reinforcing mechanisms

The data tracker is not a panacea. Its value depends on whether citizens know it exists, whether complaints are taken seriously, and whether violations carry consequences. But the core insight transfers: trust is not a byproduct of good technology, but a pillar that makes digital government viable at all. Without it, citizens stop using services, and infrastructure becomes irrelevant regardless of its sophistication.

Beyond deploying the tool, building a data protection culture also demands the institutional willingness to act on what citizens find – to investigate complaints, to impose consequences, to treat visibility as an ongoing practice rather than a one-time implementation. It requires public communication so that citizens actually know the mechanism exists and how to use it. And it requires accepting that transparency is not a threat to efficient government, but a precondition for legitimate government. The cases of Estonia and Ukraine suggest that when these conditions are met, the relationship between state and citizen can shift from one of blind trust to one of informed confidence.

For governments considering similar approaches, the question is not whether to regulate data protection – that ship has sailed – but how to make regulation visible, tangible and real. As Astok says, "The government doesn't have a monopoly on using your data. It's your data. You own it." Reversing the equation: what happens when citizens gain the capacity to watch back?

Organisation at a glance

We are the e-Governance Academy!

101 employees working at eGA

(as of 31 December 2025)

Education

- 11 PhDs
- 11 Bachelor's degrees
- 2 Other
- 68 Master's degrees
- 9 Applied science's degree

Division by gender

42

59

Time spent working at eGA

- 7 < 1 year
- 20 3–5 years
- 9 10–15 years or more
- 38 1–3 years
- 23 5–10 years or more
- 4 15 years or more

6 Competence Centres

created to assist governments with digital transformation:

- Cybersecurity
- Data Management
- Digital Services
- Digital Architecture
- Infrastructure & Solutions
- Governance & Engagement

eGA outstanding colleagues in 2025

Employee of the Year – Kristina Reinsalu, Senior Expert

Kristina has contributed significantly and purposefully to eGA's goals throughout the year. No mountain is insurmountable for her – there are no problems, only exciting challenges. Everything that is planned will be done! As a dedicated professional and a great storyteller, Kristina has a unique talent for showing how engagement can enrich any topic.

Colleague of the Year – Ingrid Toonekurg, Member of the Management Board

Ingrid passionately coordinates competence centres, supervises projects and is always available to support and inspire all eGA staff. She is a truly helpful, organised and intelligent team member, known for her friendliness and openness. She has strengthened the organisational culture, bringing a compassionate and empathetic perspective to the workplace.

Newcomer of the Year – Mari Sarapuu, Project Administrator

Mari is a highly professional, friendly and approachable team member who quickly became an essential part of eGA. From day one, Mari has proven to be a true team player – calm, constructive and always ready to offer support, provide advice or lend a hand. Her cheerful personality, operational efficiency and "let's get it done" attitude make her someone whom colleagues can always rely on.

Team of the Year – Legal and Compliance Unit

The unit brings together 13 dedicated team members working from Estonia (8), Ukraine (3), Kyrgyzstan (1) and Slovenia (1). They are eGA's safety net. They work quietly and precisely, ensuring that complex regulations, contracts and funding requirements are turned into practical solutions for the rest of the organisation.

Kristina Reinsalu: Engagement is not an add-on. It runs through everything we do

Liis Linn
Senior Communication Expert

For nearly two decades, Kristina Reinsalu has been a driving force at eGA, known for her belief that meaningful change always starts from understanding, engaging and trusting people. This people-first mindset, combined with her dedication and resilience, earned her the title of Employee of the Year.

Kristina and eGA: "I'm proud partners believe in us"

You've worked at eGA for 18 years. What keeps you motivated?

Variety is built into eGA's work. Every project brings a new country, new partners and a new context for digital transformation. When people say, "Let eGA do it! They're the ones who can deliver on time and to the quality we need", that's an enormous responsibility, but also huge recognition and motivation.

> Managing expectations has become a key part of engagement.
>
> Kristina Reinsalu

Your focus is on engagement – has it improved over time?

Years ago, engagement was often seen as a no-added-value thing. Today, local governments increasingly understand that involving people leads to better decisions. What has changed is not only awareness but also how expectations are managed: people don't always expect immediate results as long as the purpose and limits of the process are clear. Managing expectations has become a key part of engagement.

What do decision-makers most often overlook when it comes to engagement and change?

People are not opponents by default; what they fear is the unknown. Too often, those being engaged have far less background information than those making decisions. You can't always share everything, but you can reduce the information gap by explaining possible outcomes and impacts.

This is especially important in digital transformation. Technology alone doesn't drive transformation; people do. Without understanding fears, motivations and context, even the best digital solutions will fail.

Another common mistake is trying to change everything through one large engagement process. Engagement works better in smaller, concrete steps. People need to feel personally connected and see how their input matters. For example, with the PHOENIX project in Tartu, citizen discussions on food waste fed directly into the city's roadmap to a circular economy. Engagement worked because it was tied to something tangible and locally relevant.

When thinking about engagement, what is the one thing we tend to underestimate most?

We often underestimate how much common ground actually exists. Many challenges are universal, even if perspectives differ. When shared concerns are identified, it becomes possible to work towards solutions that serve common interests. Even between groups with very different priorities, there are almost always points of contact. Engagement is about recognising those points and building from there.

Running plays an important role in your life. How does the "marathon mindset" translate into your work?

Very directly. In both marathons and projects, you need preparation, checkpoints, flexibility and endurance. The hardest part often comes near the end, but that's also where the reward is greatest. I don't believe much in excuses, whether in training or at work. If you set a goal and make the process meaningful, or even enjoyable, you will find a way forward. That mindset carries me through both marathons and complex projects.

Looking ahead, what legacy would you like your work to leave?

That engagement doesn't remain a document on a shelf, but becomes real practice. Especially in difficult political contexts, I hope our work helps people resist disinformation, strengthen democracy and believe that change is possible. Engagement is not an add-on. It runs through everything we do.

About Kristina Reinsalu

Kristina Reinsalu has been part of the e-Governance Academy since 2007, where she works as a Senior Expert on digital engagement and open governance.

She supports governments and civil society in understanding how ICT shapes democratic life, how institutions can work with citizens as true partners and how transparent, participatory decision-making adds real value.

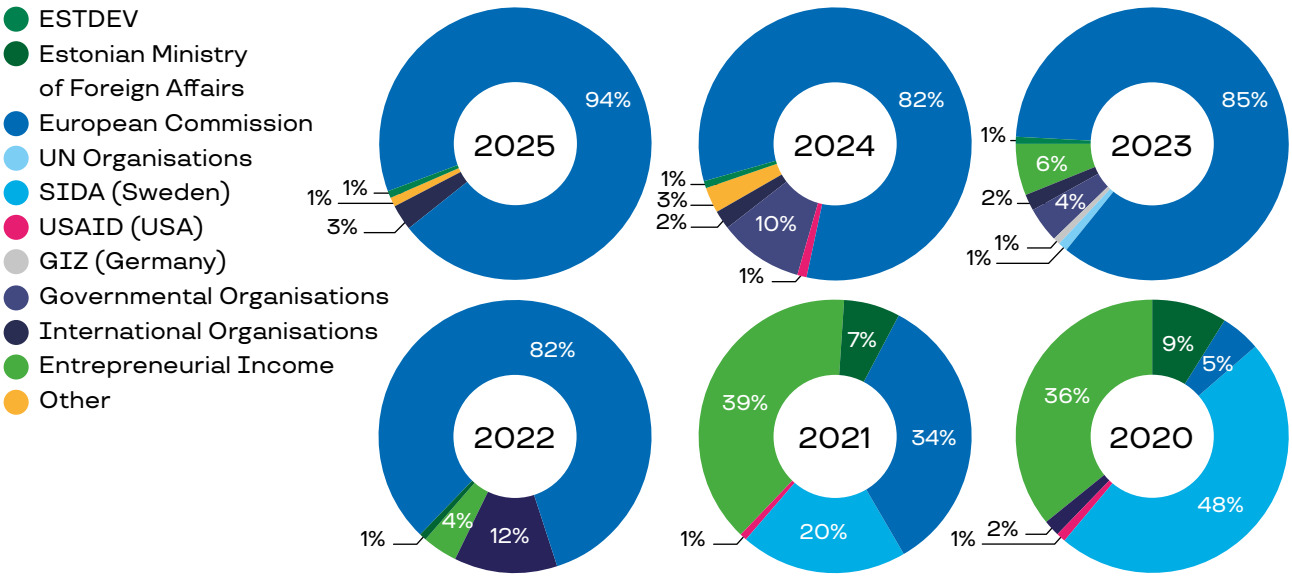
Local democracy is at the heart of Kristina's work. She has led open governance and e-democracy projects in countries such as Georgia and Moldova, as well as advised municipalities in Estonia, Latvia and beyond.

Kristina holds an MA in Public Relations and a PhD in Media and Communications. She has completed six marathons.

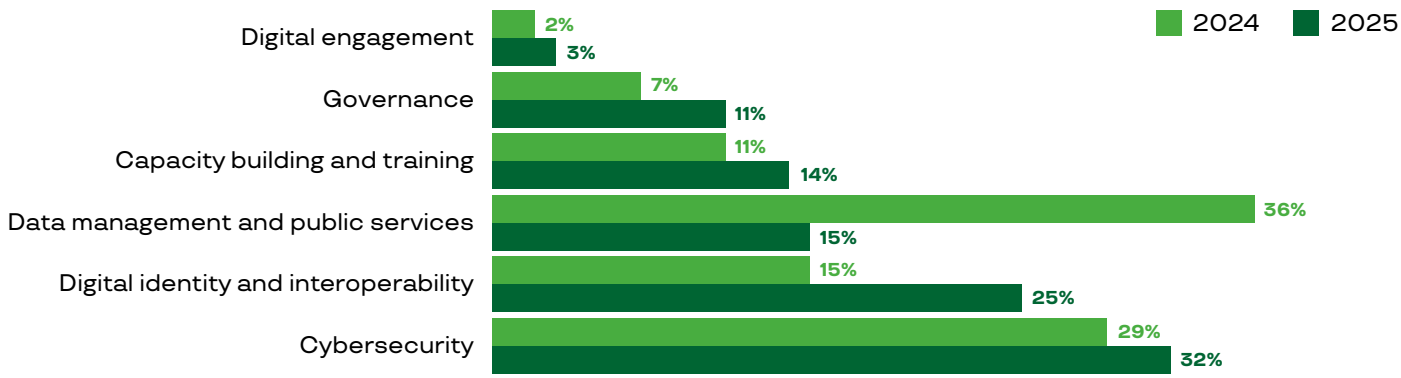
> I don't believe much in excuses, whether in training or at work.
>
> Kristina Reinsalu

eGA's activities in figures 2003–2025

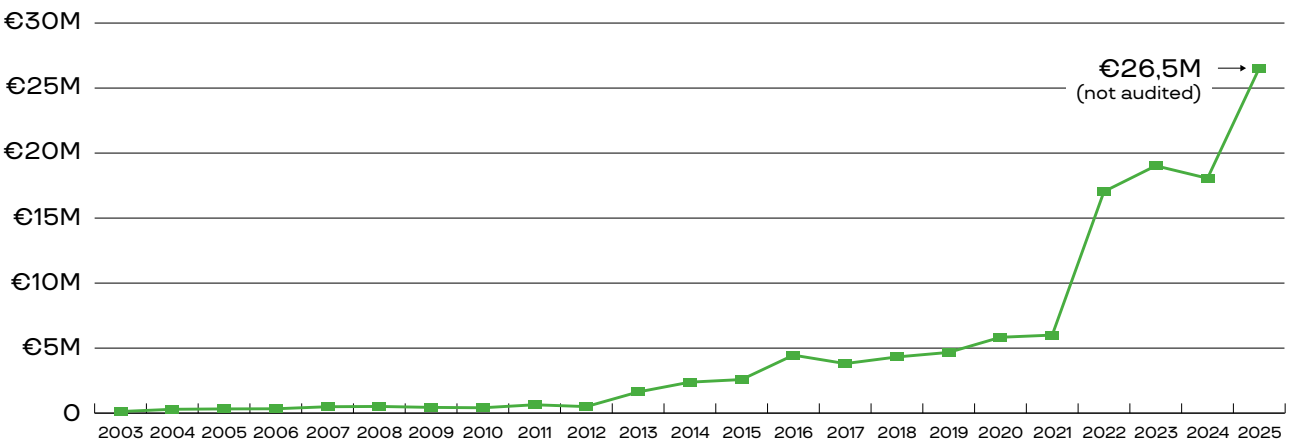
Income by source in 2020–2025*



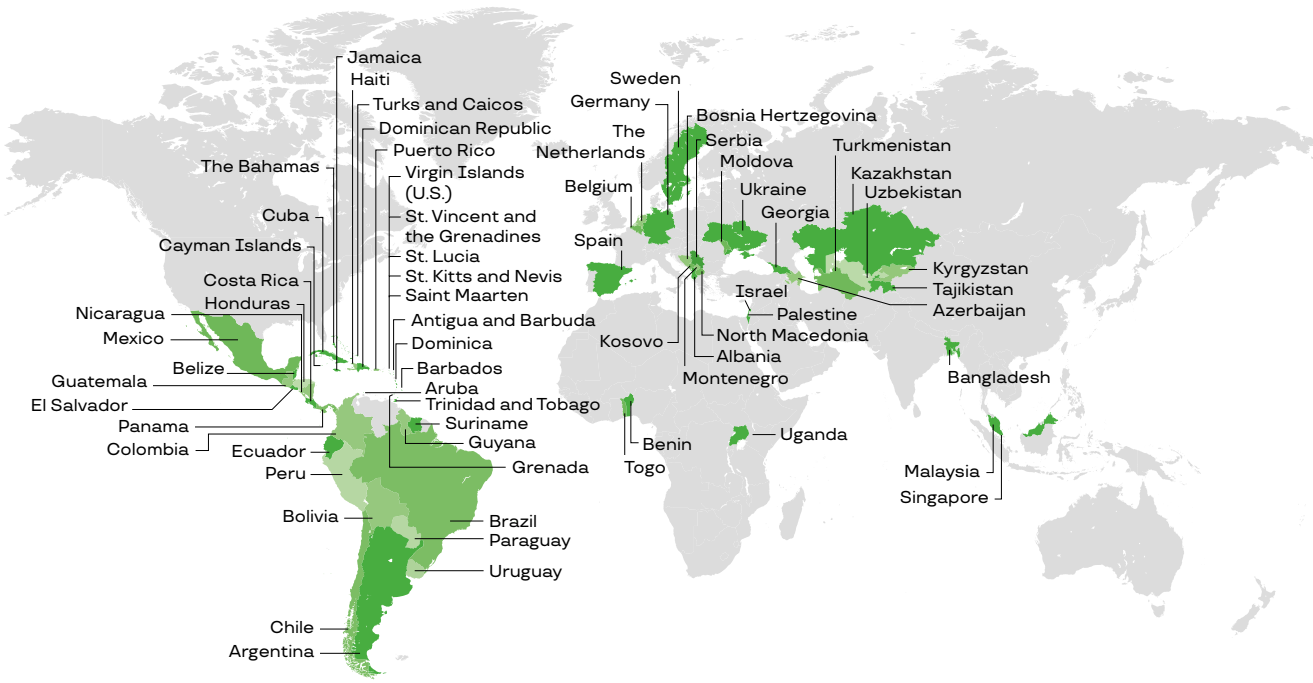
The most popular services in 2024 and 2025



Income in 2003–2025*



Partner countries/regions in 2025



Top 15 collaboration countries by funding (€) in 2020–2025

Supervisory Board


Anna-Greta Tsahkna
Chairman


Toomas Hendrik Ilves
Member


Märt Kivine
Member


Ines Mergel
Member


Jenik Radon
Member

Management Board


Ingrid Toonekurg
MB member
Operations
Competence Centres


Hannes Astok
Chairman
Development
Communication
Client Relations
Project Development
Training & Events


Aile Kullerkupp
MB member
Support
Finance
Legal & Compliance
ICT Services
People & Culture

Competence Centres


Marit Lani
Governance & Engagement


Arvo Ott
Digital Architecture


Heiko Vainsalu
Infrastructure & Solutions


Piret Saartee
Digital Services


Merle Maigre
Cybersecurity


Piret Hirv
Data Management

Development Division


Margareta Telliskivi
Project Development and Partnerships Unit


Annela Kiirats
Training & Events Unit


Anu Vahtra-Hellat
Communication Unit

Support Division


Liis Saat
Finance Unit


Britt Marie Jürman
Legal & Compliance Unit


Riini Saluri
People & Culture Unit

Digital Government Podcast

Stories that shape digital societies

Discover how digital technology can benefit every society – through real experiences, bold ideas, and lessons learned from digital transformation.

140+ episodes

Available on all podcast platforms

Did you know?

Every episode comes with a blog. Host **Federico Plantera** breaks down the key insights. Perfect for a quick catch-up!

Listen now

Search "Digital Government Podcast" or scan to start listening.

Notes for my next conversation with eGA experts

Unlock the potential of open digital societies with eGA's expertise!

Explore more

Take your country's digital transformation to new heights. From crafting strategic plans and capacity building to developing services and implementation of solutions, eGA provides the support you need to reshape your digital landscape effectively and efficiently.

Governance and Institutions Building

Rely on eGA for insightful guidance in shaping digital strategies and crafting future-proof legal frameworks.

- Digital Governance Analysis
- Digital Governance Strategies
- Digital Governance Coordination
- Legal Framework

Digital Engagement

Collaborate with eGA to design and implement innovative digital engagement strategies for citizens and stakeholders.

Data Management, AI and Public Services

Tap into eGA's expertise to develop public services that align with the evolving needs of citizens in the digital age.

- Public Service Management Frameworks
- Data Management Frameworks
- Public Service Digitalisation
- Digital Data Quality Management
- Digitalisation of Registers

Capacity Building and Training

Boost digital skills in your country with eGA's training and consultancy.

- Digital Skills and Capacity Building
- Study Visits and e-Courses
- e-Learning Platform Development

Digital Identity and Interoperability

Leverage eGA's expertise to create an ecosystem and find best-fit solutions to support your digital transformation plans.

- Interoperability Architecture Frameworks
- Government Infrastructure Planning
- Data Exchange Platform Implementation
- Digital Solutions for Identity Management
- Digital Signature and PKI

Cybersecurity

Strengthen your cyber defences and ensure digital safety with eGA's cybersecurity approaches.

- Cybersecurity Framework
- Cyber Risk Management and Capacity Building

e-Governance Academy
Ahtri 6, 10151, Tallinn, Estonia
+372 663 1500 | info@ega.ee | ega.ee
Facebook, LinkedIn, X: egovacademy

Digital Government Podcast

Follow us!