



Nortal

Government efficiency in the age of AI

Toward resilient and efficient digital democracies

AUTHORS:

Andres Raieste

SVP, Global Head of Public Sector, Nortal

Dr. Mihkel Solvak

Associate Professor of Technology Research, Tartu University

Dr. Ott Velsberg

Government Chief Data & AI Officer, Republic of Estonia Ministry of Justice and Digital Affairs

Dr. Keegan McBride

Senior Policy Advisor, Emerging Technology and Geopolitics, Tony Blair Institute for Global Change

This report may be cited as Raieste, A., Solvak, M., Velsberg, O., McBride, K. (2025) “Government Efficiency in the Age of AI: Toward Resilient and Efficient Digital Democracies”

REVIEWS AND CONTRIBUTIONS:

Dr. David Ronfeldt (retired from RAND Corporation)

EDITORIAL & DESIGN CREDITS:

Proofreading & copyediting – Kristi Kalmaru, Annabell Kuldmaa

Design & layout – Maarika Rosenstein, Annika Saar

Government efficiency in the age of AI

Toward resilient and efficient digital democracies



Table of contents

1.

Executive summary

[Page 7](#)

2.

Introduction

[Page 9](#)

3.

Government efficiency and
democratic principles

[Page 10](#)

- | | |
|--|----|
| 3.1. Whole-of-government system-level efficiency | 11 |
| 3.2. System-level efficiency of democracy | 14 |
| 3.3. Implications to digital government | 17 |

4.

Roadmap to efficient digital democracy Page 20

4.1.	Secure and trusted foundation to digital government	22
4.1.1.	<i>Base registries and the once-only principle</i>	22
4.1.2.	<i>National digital public infrastructure</i>	24
4.1.3.	<i>Transparency and public trust in personal data usage</i>	26
4.2.	Rise of intelligence in government systems and services	28
4.2.1.	<i>Government information systems and super-domains</i>	28
4.2.2.	<i>New public service delivery models and institutional reforms</i>	32
4.2.3.	<i>Automation in government: deterministic vs. AI systems</i>	36
4.3.	Future of democracy in the age of AI	39
4.3.1.	<i>Cyberocracy and the evolution of digital democracy</i>	40
4.3.2.	<i>Cyberocratic policymaking</i>	42
4.3.3.	<i>Impact on politics, elections and freedoms</i>	44

5.

Conclusion and key recommendations Page 46

6.

Bibliography Page 51

1.

Executive summary



Artificial intelligence and digital technologies are reshaping the foundations of government. While technology promises faster, more efficient and more adaptive public institutions, it also raises risks of over-centralization, weakened accountability and “digital authoritarianism.”

Government efficiency and democratic principles are not competing goals. Instead, when designed intentionally, digital government can and should embed democratic values, such as participation, transparency, competition, subsidiarity, accountability and inclusion, directly into its architecture, creating nations that are both more efficient and more democratic.

The paper proposes whole-of-government **system-level efficiency** as an important benchmark for public sector performance. System-level efficiency consists of **operational efficiency, state capacity** and **public trust**. These outcomes are constrained by four cross-cutting factors: **complexity, resilience, sustainability** and **digital sovereignty**. Short-term efficiency achieved by centralization may erode resilience and trust, while federated and modular systems, though more complex, foster adaptability and long-term performance.

Democracy itself is shown to be the most system-efficient governance model: its design principles – **representation, accountability, pluralism, subsidiarity, checks and balances** and **shared civic identity** – optimize outcomes and use of resources across multiple functions simultaneously against the maximum potential. Translated into digital government, these principles guide choices around open standards, federated data architectures, algorithmic transparency and citizen participation, in turn optimizing for long-term system-level efficiency.

The core thesis of this paper is thus: In pursuit of government efficiency through technology, the policy and technological decisions we make in designing the digital government are in fact steering us more toward a digital democracy or digital autocracy. In optimizing for long-term efficiency against maximum potential, we must in fact turn to democratic principles and implement them in digital government. In doing so, we not only increase government efficiency but also reinforce democracy.

The paper outlines a three-stage roadmap toward efficient digital democracy:

1. **Build a secure and trusted foundation** – with base registries, digital identity, federated data exchange and transparency tools to give citizens visibility and control over data use. If implemented right, it sets a strong democratic, equitable and efficient foundation for government.
2. **Increase intelligence in government systems and services** – horizontally and vertically integrating domains to move toward proactive and agentic service delivery while balancing deterministic automation with AI.
3. **Prepare for digital democracy and cyberocratic governance** – a model of “rule by information” that leverages real-time data and AI for policymaking while reinforcing, not eroding, democratic accountability, oversight and participation. Democratic processes must also evolve and adapt to these new capabilities.

Our conclusion is that governments can leverage technologies and become more efficient without compromising the fundamental values of democracy. In fact, as we have argued, those democratic principles are themselves drivers of long-term efficiency and performance. A digital government built on these foundations will not only achieve better outcomes – it will also strengthen the democratic fabric, ensuring that efficiency gains endure and benefit government and society as a whole.

2.

Introduction

As governments adopt increasingly capable **AI-based** systems, nations and the bureaucratic organizations that run them will be fundamentally transformed. The emerging era of AI-enabled governments will be defined by a growth in the creation and usage of data, increasing levels of automation, and run the risk of increasing the distance felt between governments and the governed. What this future looks like, and whether these governments will be more authoritarian or democratic, remains to be seen. But both futures are plausible. A decade from now, citizens will live inside the digital institutions we are designing and building today – the choices made today matter and will influence which future prevails.

We believe in the importance of a strong, digital and democratic future. That is why, in this paper, we argue and show that government efficiency and democratic principles are not in conflict. In fact, when democratic principles are properly operationalized, they lead to greater system-wide efficiency. Principles such as transparency, auditability, participation, collaboration, competition and decentralization are essential for delivering better services, strengthening state capacity and deepening public trust.

However, these aims are only achievable if architecture is treated as policy, and policy as architecture. The responsibility for building more robust, resilient and democratic digital systems, therefore, lies not only with ministers or rule-makers but also with CIOs, CTOs, CDOs, product owners and system architects. The code they approve, the standards they establish and the contracts they sign will influence institutions toward either openness or control, competition or monopoly, growth or stagnation. These are political choices, often disguised as purely technical decisions.

As these diverse groups of stakeholders collaborate to shape the future of AI-enabled governments, it is crucial to avoid shortcuts and the temptation of highly centralized systems that, outwardly, seem more efficient. Such an approach might produce quick results, but in the long run, these systems are likely to fail. Not only are centralized systems less robust, but they also erode the trust necessary for supporting continued legitimate democratic governance. Instead, governments should support systems that are distributed and self-organizing, governed by clear standards and shared values.

This involves adopting open standards instead of proprietary single-vendor solutions to foster market competition; integrating auditability and explainability into systems and algorithms to ensure accountability; facilitating open and inclusive participation channels; and federating data and services so that decisions occur at the lowest effective level. None of this suggests being naive about AI. Governments should automate deterministically where legal frameworks and data quality permit, applying AI thoughtfully in contexts where pattern recognition, scale or complexity surpass human capabilities. Human in the loop by default, well-documented models and data provenance, transparency of data processing, human control over their data, algorithmic transparency and independent oversight are not optional extras; they are essential for legitimacy at scale.

In the following sections of this report, we define government efficiency and provide an overview of how democratic principles drive excellence in digital architecture and service design. The report then provides a roadmap for building efficient digital democracies: (1) build a secure, trusted foundation (e.g., base registries, digital identity, once-only data exchange); (2) increase intelligence and responsiveness across information systems and services (from common standards to agentic, self-organizing models); and (3) prepare for cyberocratic governance – governance by information that remains firmly under the rule of law. Finally, the report offers key recommendations for putting these principles into practice.

3.

Government efficiency and democratic principles



3.1 Whole-of-government system-level efficiency

Across eras, governments turn to new tools to solve recurring problems: seeing society clearly, coordinating action, moving resources and securing borders. Each wave – from roads and censuses to the telegraph, electrification, digitalization and today’s AI – cuts transaction costs, speeds decisions and extends government’s reach and capacity, making services cheaper and more predictable at home while signaling reliability and competitiveness abroad. Adoption typically accelerates under crisis, fiscal pressure or strategic rivalry, when not adopting becomes costlier than change. Governments embrace technology chiefly to do more with less (operational efficiency), have more impact in doing so (state capacity) and to earn and sustain public trust:

Operational efficiency

Improving the internal performance of government operations and service delivery. This means achieving more output or higher quality services, with the same or fewer resources. Examples include faster processing times, reduced administrative costs, streamlined user journeys and less paperwork for citizens, companies and civil servants. Operational efficiency often represents the most visible early gain from digital transformation, but by itself it is insufficient.

State capacity (effectiveness)

Enhancing the government’s ability to design, implement and enforce policies and core functions. State capacity refers to the government’s ability to collect revenue, maintain rule of law, deliver public goods and respond to societal needs. Technology can strengthen state capacity by improving data quality for decision making, improving coordination among agencies, and enabling proactive and preventive interventions. Strong state capacity allows government to translate policy into tangible outcomes.

Public trust

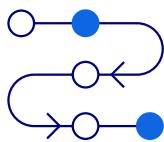
Strengthening citizens’ trust in government by improving transparency, integrity and user experience. Trust is both an outcome and a critical enabler of government efficiency: high-trust environments make policy implementation easier and encourages citizen cooperation, improves voluntary compliance and lowers transaction costs. Without trust, even the most technically efficient systems risk underperformance or public resistance.

Achieving progress in all these areas simultaneously – operational efficiency, state capacity and public trust – is what we refer to as **system-level efficiency of governance**, which must be evaluated against their maximum potential (e.g. is the system of governance maximizing use of resources and individuals and society to its maximum potential). Thus, we define the purpose of government system-level efficiency to maximize the use of resources and individuals for the benefit of the society as a whole. To achieve system-level efficiency, these three facets must be interrelated. For example, operational efficiencies can free resources that improve services (bolstering both effectiveness and

public satisfaction); meanwhile, maintaining public trust requires that efficiency gains are achieved without sacrificing accountability or equity. High-performing digital governments, such as those in some EU countries, often track a portfolio of KPIs across these dimensions.

Each project or policy should articulate which of these outcomes it advances and how that will be measured. For instance, a digital service project might primarily improve efficiency (faster responses) and potentially trust (better service experience), whereas a data-sharing initiative between law enforcement and courts might target effectiveness (higher conviction rates, quicker justice).

Importantly, pursuing the three above mentioned outcomes is not without challenges. Four strategic concerns often shape the success or failure of digital initiatives: complexity, resilience, sustainability and digital sovereignty. These concerns act as cross-cutting constraints or considerations:



Complexity

As government systems and processes grow complexity, complicatedness becomes the enemy of efficiency. Complexity itself is not the problem per se, but complicatedness. Highly complicated, fragmented processes and systems are harder to change or improve, and they increase the risk of failures. Simplifying processes, using modular architectures, and focusing on interoperability standards are strategies to tame complexity. If complexity is not (self-)managed, it reduces all outcomes – making efficiency gains harder, undermining reliability (effectiveness) and frustrating users (eroding trust). Thus, a successful digital government must continuously pursue reduction of complicatedness and introduce principles that enable self-organization into the system.



Resilience

This refers to the ability of government to withstand shocks and continue operating under adverse conditions – be it cyberattacks, natural disasters or sudden surges in demand (like a pandemic). Efficiency measures must not come at the expense of resilience. Centralizing infrastructure might be short-term efficient, but it can create single points of failure; conversely, distributed systems may be more resilient but harder to govern. A resilient digital government is adaptive to changing circumstances through strategically managing supply chain risks, technology options, policies and threats so that it can perform even under extraordinary circumstances. Resilience contributes to public trust (people know services will be there in a crisis) and to state capacity (the government can manage during emergencies).



Sustainability

Governments must balance short-term wins with long-term sustainability. This has two aspects: financial sustainability (avoiding projects that create unsustainable maintenance costs or technical debt) and policy sustainability (ensuring that digital reforms support long-term goals like inclusiveness and environmental sustainability). Launching a system that is not maintainable, lacks

staff with the right skills or is misaligned with a wider service strategy could yield a short-term boost but undermine capacity in the long run. Similarly, focusing only on near-term KPIs might neglect crucial long-term investments (like digital literacy or legacy system modernization). Policymakers should evaluate how each technology decision affects future flexibility and costs. Sustainable digital transformation often means incremental, user-centered improvements that can be built upon, rather than one-off “silver bullets.”



Digital sovereignty

Means having control over one’s own systems, policies and their outcomes – including control over data, third-party risk, technical infrastructure and the rules that govern them. For a nation, this translates to balancing external technological dependencies and cost, ensuring data is stored and processed in line with national laws, and retaining the ability to change and adapt systems without being “locked in”. Digital sovereignty is linked to state capacity (a sovereign digital state can implement policy without external interference) and resilience (less risk from supply chain disruptions or geopolitical tech restrictions). It can also influence trust, as citizens may trust digital services more if they know those services are governed by their own democratic laws rather than opaque global algorithms.

Any government digitalization policy or program should be justifiable in terms of system-level efficiency outcomes (operational efficiency, state capacity, public trust) – while explicitly addressing these strategic concerns (complexity, resilience, sustainability, sovereignty). A proposal that cannot articulate how it improves at least one key outcome is likely not a good use of public resources. Likewise, if a digital initiative undermines resilience (e.g., creating a single point of failure) or sovereignty (e.g., making critical systems dependent on an unaccountable external provider), it carries hidden costs and risks that must be weighed. By using these outcomes and concerns as evaluation criteria, policymakers can have more structured debates about digital investments. Notably, pursuing all outcomes and minimizing all risks simultaneously can be challenging – there will be trade-offs. For example, maximizing operational efficiency through extreme centralization might undermine resilience or public trust. Efficiency and resilience might conflict in highly complex systems (Artime 2024), governing complex systems itself prescribes more complex guidance, evaluation and coordination systems (Schünemann et al 2024, Yang et al 2024). Therefore, finding the right balance and looking for mechanisms that achieve this through self-organization is key.

The key questions then shift from what needs to be achieved to how it can be achieved. How can we move from striving for local efficiencies in a policy domain or core government function, to achieving global system-level efficiency across all government functions?

Next, we turn to this question by examining a system that delivers better performance across all functions, achieves higher system efficiency than others, and at the same time manages complexity, resilience, sustainability and sovereignty — democracy.

3.2 System-level efficiency of democracy

A (whole-of-government) system-level efficiency described earlier can result from many so-called functional forms, i.e., the institutions supporting the main functions of a society, which deliver health care, education, wellbeing and other key demands and rights citizens are entitled to. What truly makes a difference is, however, how all those functions are optimized simultaneously. We argue that this can only happen in a self-organizing system when there are key principles in place which interdependently ensure that the system optimizes over all of them. As defined above, we understand system-level efficiency as something that makes sure all the functions are performed either excellently or above average in conjunction.

Achieving this is certainly not easy as it should happen at the system-level. As governments modernize through information technology (including AI), they repeatedly encounter fundamental tensions in how subsystems are designed and governed.

These tensions, shown in Figure 1, represent opposing principles or approaches – each with its own advantages and risks.

Should we maximize control to ensure safety and force uptake of single pieces of technology, or should we rely on trust-driven exchanges and voluntary uptake of the best technology that emerges? Should we aim for full automation for efficiency or allow for human decision-making which allows for creativity and effectiveness? Do we value privacy so much that we are willing to trade it for the fairness that transparency enforces? Do we want centralized authorities for streamlined controlled processes, or do we want federated approaches which ensure this through checks and balances, mutual dependencies and market-based mechanisms?

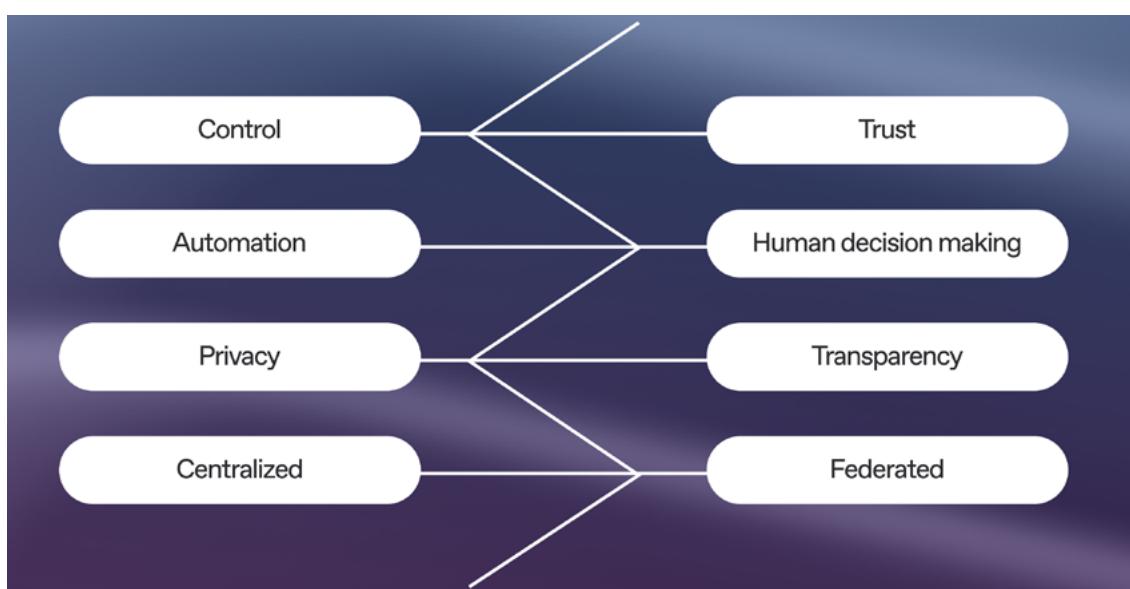


Figure 1: Example of typical socio-technical tensions that governments are navigating.

The technology choices made between the opposite poles of the dimensions profoundly influence policy outcomes and the risk of societal harm or benefit. We need to be aware that technology choices made today bring downstream consequences and path dependencies that can be overcome only at great cost. Conway's Law famously states that "any organization that designs a system will produce a design that mirrors the organization's communication structure" (Conway 1968). In other words, the way we organize governance (centralized vs decentralized, privacy vs transparency) will be reflected in how our IT systems are structured. This means that digital government architectures, intentionally or not, end up encoding the values and structure of the government that built them. This also works the other way around – technological choices influence organization and governance, e.g., if we design a centralized system, it has good likelihood to produce organization structures and forms of governance that will consolidate power. This puts tremendous responsibility for people designing digital government and related policies, as in fact, they are also designing our society and form of governance. It also drives home the point that we must have clear principles guiding technology choices, rather than fixating on the technologies themselves.

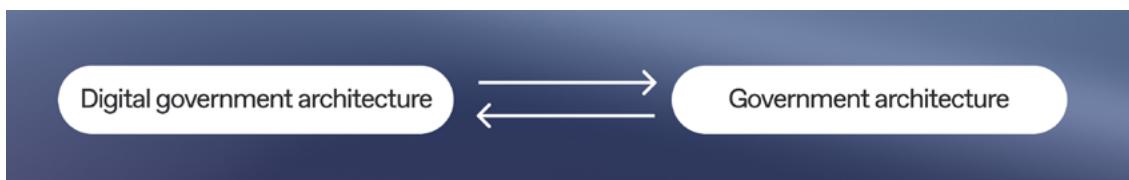


Figure 2: As per Conway's law, organizational structures and technological architectures mirror each other.

If we step back and look from a systems perspective, certain principles have stood the test of time in ensuring system-level efficiency by balancing these tensions. We need not look far – we are living in such a system through democratic political order. In principle almost 2,500 years old, and in its modern form a bit more than 200 years in the making, democratic systems clearly outperform other models in system-level efficiency, at least in delivering the functions people universally value.

There is plenty of empirical evidence backing this up with hard numbers. Though highly centralized (authoritarian) systems might outperform democracies at some functions under specific conditions, there is overwhelming evidence that when it comes to the most crucial dimensions, such as economic wellbeing, happiness, health and education in conjunction, democracies outperform other regimes. Democracies provide better health care and higher population health levels (Patterson & Veenstra 2016, Franco et al 2004, Besley & Kudamatsu 2006, Kudamatsu 2012), democracies ensure higher welfare and happiness and lower poverty levels (Flavin 2024, Paleologou 2022, Dörffel & Freytag 2023), democracies educate their populations better and more effectively (Dahlum & Knutsen 2017, Apergis 2018, Brown 1999), democracies excel at science (Whetsell 2021) and provide higher, more sustained economic growth (Acemoglu et al 2019, Di & Huang 2023).

In other words, **democracies are system-level efficient at higher rates than other political regimes**, optimizing the use of resources and collective outputs in relation to their maximum potential. This does not mean they outperform in providing every function, but they do certainly outperform when looking at all those functions jointly.

What are the core principles of a democratic system that lead to system-level efficiency? Let's examine them briefly. Volumes have been written on what constitutes democracy and the forms it can take, but there is a consensus on certain key principles that characterize such a system:

1. **Representation and participation.** A democracy allows citizens to participate in decision-making either directly or through regularly elected representatives. Free and autonomous individuals can decide what's best for themselves, and by engaging in joint direct decision-making or elections this becomes a collective will. This principle ensures that all interested parties have a say. It also reinforces the next principle, accountability.
2. **Transparency and accountability.** A democratic system must be transparent to ensure accountability of elected officials and appointed professionals. Accountability means there are mechanisms to hold those entrusted with power responsible for their actions. This principle ensures that those with power act in the interest of their ultimate principals: the citizens.
3. **Pluralism (competition).** No system is truly democratic without regular competition of ideas and actors. Competition ensures the best ideas thrive and are accepted based on merit. This principle allows innovation in the system and, through systematic trial and error, ensures that ideas with the potential to improve society are identified and adopted.
4. **Subsidiarity and self-organization.** A democratic system values subsidiarity, i.e., the rule that decisions should be made at the lowest possible level, allowing communities to self-organize. Self-organization allows communities and interest groups to act autonomously since they know what works best for them. It is also the ultimate efficiency rule: a self-organizing system needs low overhead (less central control) and tends to have the lowest transaction costs in interactions.
5. **Checks and balances.** There must be safeguards to ensure power is not concentrated unchecked, and that different institutions can limit each other's power. Such an equilibrium ensures that abuses of power are rare and can be corrected collectively when detected.
6. **Shared civic identity and social cohesion.** Despite each actor and individual in the system having their own interests, there is a shared common identity (civic or national) that ensures social cohesion. This shared identity means that while we differ as individuals and groups, we play by the same set of rules as citizens, and those joint rules are valued in themselves.

Together, implementing these principles ensures that the system self-optimizes at a higher level across all central government functions. The exact institutional setup might differ substantially between democracies (parliamentary vs. presidential systems, for example), but what matters is their functional equivalence. The specific electoral system matters less than whether it is free, fair and regular. Similarly, the particular accountability mechanisms a society chooses are secondary to the fact that functioning accountability exists in practice.

3.3 Implications to digital government

How are these principles relevant for digital government? The answer becomes clear by looking at them: If these principles have allowed us to build and govern complex societies while continuously improving living standards, then they must not only work well – they should be transferable and broadly applicable to yield the same effect in other contexts. In other words, **when applied to designing a digital government or state information system, these principles help optimize the efficiency of the system-as-a-whole**. Applying democratic principles to digital design makes the democratic system itself more resilient, effectively perpetuating democracy in the digital realm. This implies that **government digitalization ultimately makes democracy stronger, because good digitalization is essentially an emulation of democracy's core principles**.

Next, we argue how these democratic principles impact digital government architecture and highlight which efficiency outcome(s) each principle most strongly impacts.



Democratic principle	Implications for digital government architecture	Primary impact on
 <p>Representation and participation – Government reflects the will and diversity of the people.</p>	<p>Ensure digital accessibility for everyone regardless of their skills or impairments; design algorithms and interfaces to avoid bias and exclusion.</p>	Trust
 <p>Transparency and accountability – Officials are accountable for their actions.</p>	<p>Make systems and algorithms auditable and transparent. For example, provide public audit trails and open data on automated decisions. Clearly communicate what data the government collects, the legal basis for its use, and offer traceability and oversight for data sharing between agencies.</p>	Trust
 <p>Pluralism (competition) – No monopoly of power; ideas compete on merit.</p>	<p>Prefer open standards over monolithic proprietary solutions. Architectures should favor an ecosystem of interoperable modules with functional equivalence, avoiding any monopolistic technology structures that lock in one vendor or approach.</p>	State capacity and operational efficiency
 <p>Subsidiarity and self-organization – Decisions made at the lowest effective level.</p>	<p>Use a federated system architecture. Decentralize systems horizontally (across functions) and vertically (across levels of government), avoiding unnecessary concentration of power in a single authority. This distributed design mirrors democratic decentralization.</p>	State capacity and operational efficiency
 <p>Checks and balances – Power is limited and monitored by others.</p>	<p>Enforce segregation of duties in IT systems and data governance. Limit authorities' access to data and systems strictly to their defined mission to prevent mission creep. Implement oversight mechanisms for algorithms (e.g., requiring approval for any automated decision rules that affect rights).</p>	Trust and operational efficiency
 <p>Shared civic identity and cohesion – A unifying sense of equal citizenship.</p>	<p>Allow autonomous service delivery by different providers (including voluntary civic tech) but enforce universal interoperability standards. Provide universal access by giving every citizen equal access to digital services via a common secure digital identity and shared channels.</p>	Trust and state capacity

Table 1: Democratic principles, their implications for digital government architecture, and their highest-impact efficiency outcomes.

Adopting democratic principles in digital government is both necessary and feasible and through strategic technological choices these principles can improve government efficiency systematically across functions. These principles call for thoughtful alignment of governance values with system architecture – from ensuring representation through inclusive platforms, to baking in accountability through transparency features, to structuring systems in a decentralized way that mirrors distributed power. When done right, digital government will strengthen democracy, making institutions more responsive, inclusive and resilient.

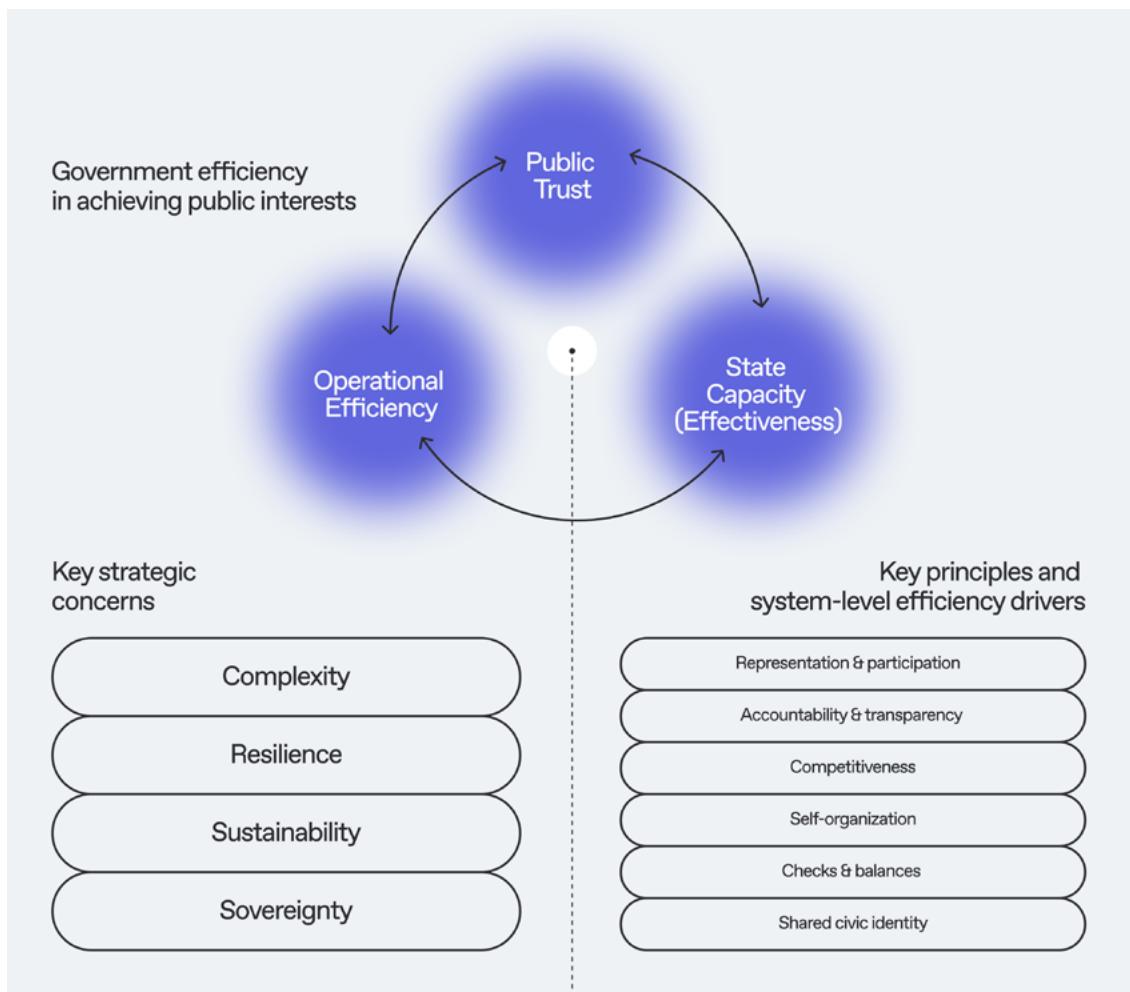


Figure 3: Framework to build efficient digital governments using democratic principles.

The next part of this paper translates these principles into an actionable roadmap, outlining how countries at various stages of digital maturity can progress toward **cyberocratic** governance (governance by information) in a controlled, value-preserving way.

4
+

Roadmap to efficient digital democracy

To translate these principles into practice, we can identify key stages of technology adoption in government and highlight fundamental phases and decision points that significantly affect the journey. The stages can be summarized as follows:

01.

Secure and trusted foundation for digital government

Establish the base digital infrastructure: core registries and databases, unique identifiers, digital identity for citizens, secure data exchange mechanisms and other digital public infrastructure (for example, digital payment systems). This stage focuses on getting the fundamentals right and offers opportunities to significantly increase efficiency. However, it also demands foundational choices that can either solidify democratic principles or erode them.

02.

Rise of intelligence in government systems and services

Once foundational systems are in place, governments turn to improving policy outcomes within specific sectors. In this stage, advanced digital governments gradually move toward citizen-centric, whole-of-government service delivery – breaking down silos between agencies so that services can be delivered seamlessly. The outcome is significantly increased effectiveness and citizen satisfaction in each major domain (health, justice, finance, etc.), as well as new policy insights from pooled data (Haug et al. 2023). In this stage, governments also encounter new choices about how to uphold democratic principles amid emerging technologies. Nations that execute this well develop a highly trusted and efficient digital government. They will prioritize data governance and have a highly developed data valuation culture, gaining new data-driven policy insights for better governance.

03.

Cyberocratic governance and the future of democracy in the age of AI

At the most advanced stage, government leverages high-quality data and AI to make governance more adaptive and predictive – essentially “rule by information,” or cyberocracy (Ronfeldt & Varda 2008). Policies can be adjusted in real time based on data (while preserving human oversight), and government incorporates more direct citizen input (potentially adopting elements of direct democracy through digital tools). This stage envisions governance that is not only efficient and personalized for the citizens but also continuously participatory – a blend of data-driven administration (OECD 2019) with active civic engagement, all under strong rule-of-law frameworks and technologically realized citizen control. Governments entering the cyberocratic era face a crucial fork: will their digital state evolve as a digital democracy or veer into digital autocracy?

In the following sections, we look at these stages in more detail, examining the choices and implications at each stage.

4.1 Secure and trusted foundation to digital government

4.1.1. Base registries and the once-only principle

Base registries are authoritative public databases that serve as the single source of truth for core information about persons, organizations, assets and locations. They underpin efficient governance and service delivery by providing legal legitimacy to records (acting as trust anchors for data on individuals, businesses, properties, etc.). Because many services rely on these foundational datasets, base registries must be high-quality and broadly accessible (European Commission 2018). This prevents each agency from keeping its own redundant records – such as parallel lists of citizens or companies – and ensures all parts of government use a shared, trusted source.

Crucially, base registries should be kept institutionally and legally separate to maintain proper checks and balances. Consolidating all vital data under one authority will inevitably lead to mission creep. Instead, different ministries or agencies each manage a different registry. Data sharing between them is permitted only when necessary and under clear legal rules. Many countries embed such rules in law (stipulating which authorities can access which data and for what purpose) and establish secure data-exchange systems accordingly. For example, Estonia designates certain registries as official sources and requires all agencies to use them rather than collect data anew. **This federated model prevents undue concentration of power and mission creep (even if unintentional).** Federation can occur both horizontally and vertically – systems can be federated across

functions (e.g., separate population and commercial registries) and across levels of government (local/municipal, regional/state, federal). This also reinforces the democratic principles of self-organization and subsidiarity.

Because base registries are widely used, data quality must be rigorously managed – any error can quickly spread across services. For this reason, base registries are often best operated by organizations that provide public services related to those registries, allowing data to be corrected as part of natural business operations. This approach also reduces complexity and improves sustainability. Federation of registries and systems further increases resilience – if executed well, failures or risks in one system do not necessarily propagate to others, improving the security and reliability of the entire digital government.

Another important design goal is to minimize the number of different identification numbers in use across government. Ideally, each person has one unique personal ID, and each company has one unique business ID, used for all interactions with public services. Wherever possible, governments aim to implement unified identifiers. Estonia, for example, uses one national ID number for nearly all services. If a single ID scheme is not feasible, interoperability strategies can cross-reference multiple IDs for the same person or entity. Notably, basic identifiers like a national ID code or business registration number

should be treated as non-secret public information to facilitate verification, whereas the personal data associated with those IDs remains protected. Simply knowing someone's ID number must not compromise their privacy, because any access to the actual personal records still requires proper authentication through the secure digital identity system.

Interconnecting base registries is a foundational step toward true digital government. They provide common identifiers and reference data that all other systems can rely on. This dramatically boosts efficiency and improves public satisfaction by reducing repetitive paperwork. Once information is recorded in a base registry, government services can retrieve and reuse it whenever needed, rather than repeatedly asking citizens to supply the same details. Reusing data in this way also builds trust, as people see that the government is not continually asking for information it already has. This practice of reusing information is known as the **once-only principle – citizens and businesses should have to provide standard information only once, after which government systems share it internally** (with necessary consent or legal authority) instead of asking again.

The once-only principle in practice hinges on the availability of comprehensive and trusted base registries. If those registries exist and are kept accurate, any government agency can query them to obtain needed information instead of bothering the citizen. For example, when someone applies for a pension, the system can automatically pull the person's birth date and identity details from the

national population register (instead of requiring a birth certificate), check employment history from tax or social security records, verify the current address from the address register and so forth. All of this happens behind the scenes without the individual having to resubmit data that the government already holds. When each component is interoperable, such end-to-end services become seamless and largely automatic, significantly improving the user experience.

Progress toward these foundational goals can be measured with clear success metrics. One key indicator is a reduction in duplicate data requests to citizens. For instance, Estonia tracks how many times data are shared between systems instead of asking a citizen to provide it; each such instance is counted as an application of the once-only principle, and a steadily rising count signals improvement. Another indicator is the adoption of common data standards and classifications across government (so that all agencies are “speaking the same language” when referring to countries, regions, businesses, medical terms and so on.). Investing early in shared code lists and taxonomies – such as a master list of government agencies with unique identifiers – pays off later by simplifying integrations and reducing errors.

Next, we look at **digital public infrastructure**, which enables the once-only principle and other efficiencies.

4.1.2. National digital public infrastructure

Practically implementing the once-only principle requires using data across government via secure infrastructure. Every interaction between systems must be trusted. It must be clear who is requesting or updating data, that the exchange is legally permitted, and that no unauthorized changes or leaks occur. Addressing these trust and security requirements

is the role of **digital public infrastructure (DPI)**. If implemented correctly, DPI also forms the first and most important layer of cyber defense (in effect implementing a nationwide zero-trust architecture), significantly lowering cybersecurity threats and costs across the public sector. Core components of a secure and trusted DPI include:

Digital identity and e-signatures

A high-assurance digital identity and e-signature system for all residents (as well as for legal entities and even government systems) is fundamental to providing government services online in a legally binding way. This must be backed by laws that recognize digital identity and signatures as equivalent to physical ones. Together, these enable the elimination of most paper documents and credentials, paving the way for significant efficiency gains across the entire economy. For example, Estonia's government calculates that digital identity and e-signatures save at least 2% of GDP annually. The design choices for digital identity have a paramount impact on society: with proper checks and balances (a design where the citizen controls the use of their identity), digital identity can enable significant efficiency gains that fuel further trust. However, if the system identifies citizens without giving them control (e.g., using pervasive biometrics without consent), it invites abuse; a system without strong safeguards will eventually erode effectiveness and outcomes.

Federated data exchange system

A federated, real-time data exchange network that links information systems in a secure way. Through this exchange layer, data remain in their original source systems and are provided to others on demand, transaction by transaction. All data requests and transfers should be end-to-end encrypted and authenticated, meaning only authorized systems and users can retrieve certain data (with full auditability for accountability and transparency). Domain-specific data exchange networks (e.g., for e-payments or e-invoicing) also fall in this category. A globally notable example is the X-Road platform for secure government interoperability – enabling data exchange horizontally (across agencies), vertically (across levels of government) and even across borders.

Data wallets and verifiable credentials

In addition to system-to-system real-time data exchanges, personal data wallets provide an alternative way for individuals to hold and selectively use their own verified credentials. For instance, instead of an employer having to verify an applicant's degree via a government database, the applicant could directly share a verifiable digital diploma from their personal data wallet. These wallets give users more control over their information and offer an alternative channel for data exchange – useful if automated interoperability between systems is unavailable or undesired. Personal data wallets embody principles of participation, subsidiarity and resilience by giving citizens more personal control over their data and reducing dependence on central systems.

Single digital gateways

One-stop-shop portals or applications that provide a unified front door to government services. A single digital gateway (often implemented as a government one-stop-shop or a mobile “super-app”) allows users to access a wide range of services from different agencies through one consistent interface. These gateways might operate at the national level or be specialized by sector or region, but in all cases, they simplify user interactions by aggregating services on one platform. Single digital gateways implement the principles of shared civic identity and participation. They do, however, need to balance choices between centralization and federation to provide the best service experience without concentrating too much control.

Sovereign clouds

These are cloud computing environments for government or public use that ensure government control over computing and data. Importantly, a sovereign cloud strategy should avoid concentrating risk in a single cloud provider. Instead, a system of clouds (potentially a mix of private and public clouds meeting sovereign requirements) can improve resilience, strengthen digital sovereignty and enhance cost-efficiency for digital government – especially if competitiveness principles are included (avoiding vendor lock-in and encouraging multiple solutions).

All these components work in concert toward the same goal: delivering efficient digital services in a secure and trusted manner. In effect, the digital infrastructure must serve as both an **enabler** and a **gatekeeper** for digital government. It enables seamless data flows and service automation, while simultaneously acting as a gatekeeper that enforces privacy, security and proper use of data. International initiatives such as the UN’s **DPI Safeguards** provide comprehensive guidance on built-in safeguards for such infrastructure.

It is also important how DPI itself is organized and provided. DPI should enable effective digital government functions while avoiding a new concentration of power and control. In other words,

DPI itself must not become a single, monolithic system – it should remain competitive and modular. DPI must allow incorporation and interoperability of different systems and technologies through common standards, rather than enforcing a single technology solution. For example, instead of mandating one specific digital identity solution or one “sovereign cloud” technical stack, government should provide interoperable standards and institutional mechanisms to procure and operate multiple competing solutions from public or private sectors. This approach upholds the principles of participation, competition and self-organization – fundamental drivers of both democracy and overall government efficiency.

4.1.3. Transparency and public trust in personal data usage

No matter how advanced the technology, a digital government can only function with the consent and confidence of its people. Thus, the trustworthiness of the digital public infrastructure itself must be beyond reproach. One way to bolster public trust is to build **transparency and personal control** into data practices by giving each citizen a clear view of, and control over, how their data are used by the government – a sort of accessible “*digital twin*” of the citizen’s government-held identity and records. This can be provided through a dedicated public service or portal. Through such a service, individuals can see which government agencies have accessed their personal data, what data were accessed and when. They can also review what information is on file about themselves and, in some cases, correct any inaccuracies. Estonia’s national e-portal and government mobile app, for instance, include a **Personal Data Tracker** tool that lets residents see every query made on their personal records. This level of transparency is now seen as vital to maintaining public trust in government data use.

Empowering citizens in this way creates a virtuous cycle linking transparency, trust and better outcomes. When people have real-time insight and control over their data, they are more likely to trust digital services. Greater trust leads to higher adoption and use of e-services, which in turn boosts administrative efficiency and compliance – since more interactions flow through streamlined digital channels and citizens are more likely to provide accurate information. Transparency breeds further trust: it drives uptake and cooperation, generates more data for improvements and thereby reinforces trust. This, in sum, is **the social contract of digital government** – citizens are willing to allow the use of personal data in return for efficient service outcomes, as long as they have visibility and agency in that exchange.

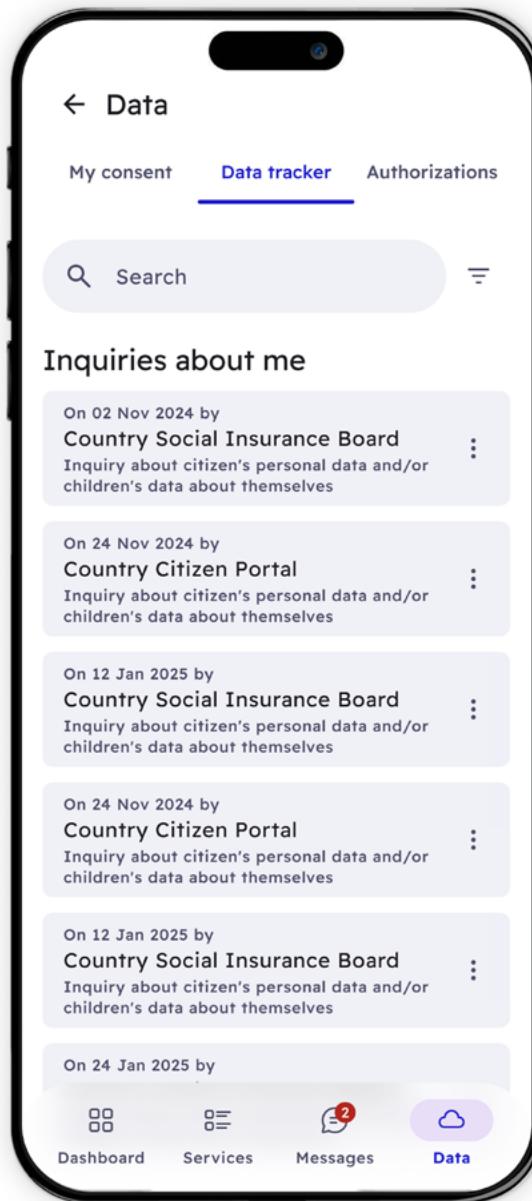


Figure 4: Personal data tracker in a government super app.

Case study:

Online voting as a benchmark for trust and resilience in digital public infrastructure

A telling measure of a nation's digital public infrastructure – and the trust it has built – is whether core democratic exercises, such as general elections, can be conducted online securely and with high public confidence. Secure internet-based voting for national elections remains rare globally, but Estonia has successfully provided it at scale.

Estonia first introduced nationwide online voting in 2005, leveraging its advanced digital identity and data exchange infrastructure to authenticate voters and protect the integrity of the ballot. Thanks to the robust design of its DPI, the system has never been compromised, even though Estonia has been a major target of nation-scale cyberattacks since 2007. The constant external threats have, in fact, been a key driver for building high resilience and security into the system. By 2023, the popularity of the online voting had grown to the point that more than 50% of all votes in Estonia's parliamentary elections were cast online – exceeding the number of paper ballots for the first time. This outcome reflects a remarkable level of public trust in the country's digital government systems.

Few other countries have ventured to implement internet voting on a large scale, precisely because the security and transparency requirements are

so stringent. To be viable, an e-voting system must ensure end-to-end integrity: every step from voter authentication and authorization to ballot submission, encryption, secure storage and accurate tallying of votes must be protected and verifiable. Strict oversight is essential – independent audits and verification mechanisms must ensure results are credible. Estonia's experience suggests that when a digital ecosystem is mature and citizens have seen its benefits over many years, they are more willing to accept even fundamental civic processes going online. The benefits of online voting include greater democratic accessibility and participation (citizens can cast their vote securely from anywhere) and potentially higher turnout. At the same time, a parallel paper voting option is maintained to ensure inclusivity and public confidence for those less comfortable with digital methods.

With strong online voting practice in place and with wide adoption, democratic processes can be conducted more cost-effectively and more frequently. This not only reinforces democratic practices but also enables new forms of civil participations, which we analyze further in later chapters.

By implementing these foundational elements, governments establish an efficient and trusted base for digital government while also reinforcing democracy. Even nations at an early digital stage can leapfrog by focusing on these fundamentals. With a secure foundation in place, governments can next turn to leveraging shared data and emerging technologies (such as AI) to further transform public service delivery and outcomes.

4.2 Rise of intelligence in government systems and services

With strong digital government foundations and safeguards in place, governments can shift focus to improving domain-specific outcomes. This next stage moves beyond digitalizing siloed services – agencies begin to collaborate across traditional boundaries to deliver integrated, citizen-centric services. In this stage, the information networks and data flows within government systems begin to rise in intelligence. We see both **vertical integration within sectors** (connecting all key actors in, for example, the healthcare or justice sector) and **horizontal integration across related sectors** (for example, linking social services with employment services, since outcomes in one affect the other). The **result is more proactive, personalized services in each domain, improved efficiency and outcome metrics** (e.g., faster case resolution in justice or better care coordination in health) and a **richer pool of information for policy insights within each domain**. This in turn leads to higher overall government efficiency. However, in this stage, governments also start to navigate difficult choices about how new data flows challenge old institutional structures, and they must balance short-term gains with long-term governance principles.

4.2.1. Government information systems and super-domains

National information ecosystems consist of the networks, standards and organizations that enable data and information to flow seamlessly across government, businesses and society. At this stage, each major policy domain (justice, health, public finance, education, social protection, transportation, land use, etc.) becomes a digitally coherent

environment where data, information, and knowledge flow seamlessly among relevant actors in real time. The primary purpose of these integrated ecosystems is to improve sector-specific outcomes. Below are some examples of domain-specific national information ecosystems, the key entities involved, and the benefits achieved:



Justice (criminal justice chain)

Integrates data across police, prosecutors, courts, prisons, probation services and even victim support organizations. This connectivity enables faster, fairer justice.



Healthcare

Links hospitals, primary care clinics, pharmacies, laboratories, emergency medical services and health insurers/national health funds. The outcome is better patient results and efficiency.



Public finance and real-time economy

Connects tax authorities, customs, the statistics office, social security administration, banks, business registries. This yields higher revenue collection and efficiency, and less administrative burden for entrepreneurs. Richer real-time economic data becomes available for better-informed policymaking.



Land and urban planning

Brings together local planning offices, cadastre and land registries, building regulators, environmental agencies and utilities. The result is quicker permits and smarter development. A unified digital permitting portal and shared land data make approval processes faster and decisions more informed and transparent. Speeding up permits accelerates housing construction and infrastructure projects, boosting economic activity.



Social services

Integrates social benefit agencies, public employment services, education/training providers, child protection agencies. This enables faster service delivery and improves social outcomes.



Public safety and emergency response

Links 911/112 emergency call centers with police, fire departments, ambulance services, disaster management agencies and even sensor networks (e.g., weather or earthquake sensors). The result is improved emergency response.



Security and intelligence (national security)

Connects intelligence agencies, law enforcement, border control, cybersecurity centers and international intelligence partners. With appropriate safeguards, this ecosystem leads to prevented threats and faster investigations and significantly improves a country's ability to anticipate and respond to security risks.

Each example shows how integrating data and processes within a domain translates into improved outcomes – faster justice, better health or greater safety. Each step up the maturity ladder brings greater efficiency and effectiveness, which in turn enables more advanced and citizen-focused service delivery in these domains.

Achieving a high-maturity information exchange requires progressing from basic, context-agnostic data sharing (basic interoperability that aims to achieve once-only data-sharing between registers) to rich, context-aware information sharing and ultimately knowledge exchange. At each stage, the **depth of interoperability increases – common semantic standards** (such as shared taxonomies and ontologies) ensure that data is not only transmitted but also understood in context. In essence, standards serve as a common language, allowing different systems and organizations to exchange data meaningfully rather than just technically.

As the ecosystem matures, stakeholders adopt common data standards and models so that information carries explicit meaning across systems. Here, **data exchange becomes true information exchange** – data are augmented with standard definitions and metadata that make their context understandable to any authorized receiver. This is achieved by implementing shared taxonomies or data dictionaries that define each data element consistently across the domain. Using standardized taxonomies makes data *self-describing*, enabling semantic interoperability within that domain (the data's meaning is preserved across systems). Many domain-specific standards emerge at this stage. For example, in healthcare the HL7/FHIR standards define common formats and codes for exchanging patient records, lab results, medications, etc., so all hospitals and clinics

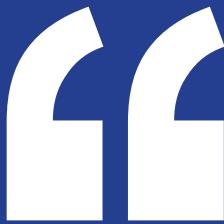
interpret the data the same way. In finance, the XBRL standard allows businesses and regulators to share financial reports with a common understanding. By using such standards and taxonomies, there is far less need for manual data mapping or guesswork – the meaning itself “travels” with the data.

The most advanced stage moves beyond **exchanging structured information into exchanging knowledge (semantic interoperability with ontologies)**. At this maturity level, government information systems don't just share data with agreed meanings; they integrate reasoning, relationships and insights derived from that information. Multiple taxonomies can be linked under a common ontology – effectively uniting various domain vocabularies into an interoperable whole. For example, an ontology might incorporate a healthcare taxonomy, a pharmaceuticals taxonomy and a geographic taxonomy, enabling knowledge to be shared meaningfully across medicine and location (such as tracking a disease outbreak by place). This enables parties to ask complex questions or discover insights that weren't possible at the basic information level. An ontology provides a shared context model that computers can use to infer new information and ensure unambiguous interpretation across domains. While a taxonomy might list and categorize, say, medical terms or legal concepts, an ontology describes how those concepts relate (e.g., understanding that *Diabetes* is a type of *Chronic Disease*, so if a patient has diabetes, the system can infer that the patient has a chronic condition even if not explicitly stated).

Knowledge exchange is enabled by technologies like knowledge graphs, reasoning engines and linked data standards. A well-known example is the Google Knowledge Graph, which aggregates facts about people, places and things from many sources and uses

ontologies to integrate multiple taxonomies and data feeds into a cohesive graph of knowledge. This allows, for instance, a query that spans domains or infers relationships across datasets. Generally, ontologies and knowledge graphs act as a “contract for meaning” so that all parties share the same understanding of concepts and relationships. Together, they enable a knowledge-driven information ecosystem or **super-domain** where machines can understand context, detect patterns and even draw basic inferences from shared data.

Crucially, each step up this maturity ladder brings greater efficiency and intelligence to the ecosystem. Higher semantic interoperability means less ambiguity, less manual intervention and more reuse of data and services across government. It also helps to reduce complexity and makes decisions more understandable and transparent, which invites more participation and oversight.



At each stage, the depth of interoperability increases – data is not only transmitted, but understood in context.

4.2.2. New public service delivery models and institutional reforms

Having richer information flows and stronger interoperability opens the door to fundamentally improved public service delivery models. As digital public infrastructure and standards mature, governments have been moving beyond basic transactional e-government portals toward services that are personalized, proactive and citizen-centric. Rather than forcing people to navigate complex bureaucratic structures, the idea is for government to assemble what each person needs, when they need it, across organizational boundaries. Service delivery is evolving to become anticipatory and seamlessly integrated into citizens' lives.

For many years, a flagship approach to this vision has been the “**life-event**” service model. Life-event services (for example, “Having a child,” “Starting a business” or “Retirement”) bundle multiple agencies’ services and requirements into one unified, end-to-end journey for the user. Done well, life-event services eliminate duplicate data requests (honoring the once-only principle so that citizens don’t have to provide the same information twice), reduce the time to achieve an outcome, and build public trust through a more user-friendly experience. In principle, a citizen entering a life-event portal provides their information once,

and the government handles the behind-the-scenes coordination across departments.

However, implementing real life-event services (not just describing how they work, but integrating all these digital services into a unified whole) has proven notoriously difficult. It requires intense cross-agency governance and cooperation: clarity on who “owns” the service or life-event process, agreements on shared funding and service-level agreements, harmonization of rules and processes across agencies, and often new legal bases for data sharing. Many ambitious life-event programs have stalled not due to technology, but because of institutional and policy frictions – agencies may struggle to agree on responsibilities, funding or data-sharing rules. The coordination overhead is high, and negotiating every detail of a complex life-event can take years. This opens the door to a key policy choice for mature digital governments: **now that we have data flows that do not neatly follow traditional institutional structures, should we rethink institutional boundaries and structures for efficiency?** Many institutional reforms, such as merging tax and customs administrations for better coordination on VAT and excise taxes, are linked to efficiency gains. However, proper checks



Now that we have data flows that do not neatly follow traditional institutional structures, should we rethink institutional boundaries and structures for efficiency?

and balances are crucial to ensure that in pursuing efficiency we do not unnecessarily consolidate power in ways that undermine democratic principles or public trust.

An alternative route – one better aligned with the democratic principles of subsidiarity and decentralization – is now emerging as **self-organizing services with agentic-driven AI**. In this model, instead of pre-defining every cross-agency service bundle and assigning a single agency “owner,” the government focuses on exposing secure, standardized capabilities as APIs (for example: verify identity, check eligibility, fetch a citizen’s civil status, validate a permit, issue a payment or schedule an appointment). This approach **shifts the burden of integration from the institutional layer to the service layer**. Instead of agencies needing to negotiate upfront who owns an entire life-event process, agencies simply agree to provide certain capabilities under common standards and governance. The agentic service layer – which could manifest as a government super-app, a digital assistant or third-party apps – stitches together the necessary steps in real time. The outcome for the citizen is the same or better level of personalization, proactivity and convenience that a life-event service would promise but achieved with fewer structural bottlenecks behind the scenes. Essentially, the user interacts with one smart interface that can handle many tasks proactively.

To enable self-organizing, agent-driven services at scale, governments must have robust digital infrastructure and standards in place. Key enablers

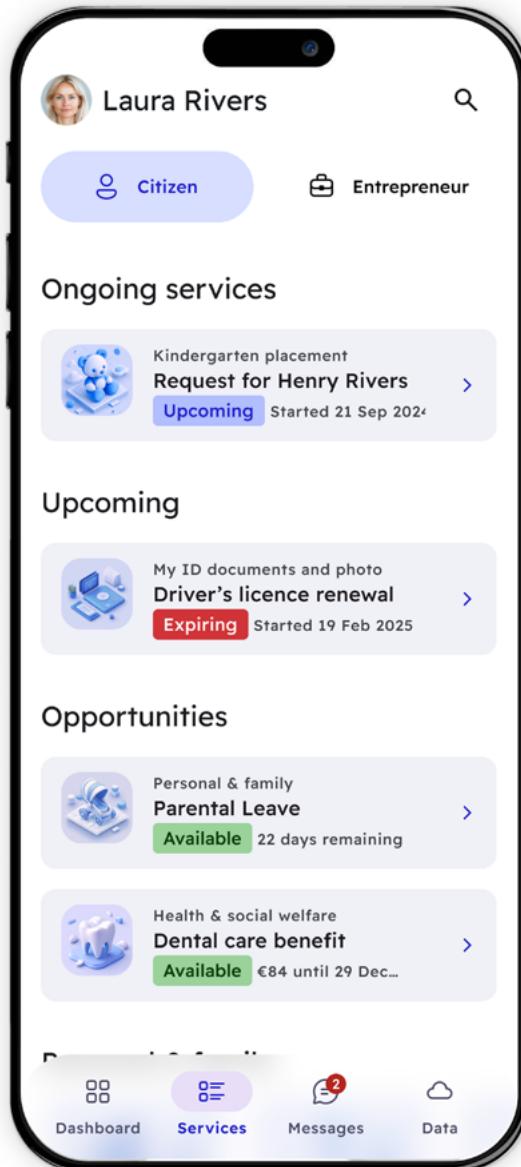


Figure 5: Self-organizing, agent-driven and proactive services in a government app.

include high-quality authoritative data, common data models, and semantic interoperability across agencies (so that an agent can understand and use information from multiple sources). Equally important are well-defined service APIs for core functions, available for trusted internal or external use and an event-driven architecture that allows systems to react to changes in real time (for example, a change in a citizen's status automatically triggers relevant updates or services).

With **self-organized services**, services become significantly more proactive and adaptive. Instead of reactive, one-size-fits-all processes, the government can deliver support that is tailored and timely for each individual's context. For government organizations, the focus shifts to owning and excelling in capabilities – ensuring high-quality data, reliable APIs and clear rules encoded as software – rather than trying to manage every possible end-to-end customer journey themselves. Cross-agency agreements and governance also evolve: the question is no longer “Who owns this entire life-event service?” but “Who ensures that each underlying capability is delivered reliably and securely?” Each agency or product team takes responsibility for the performance of the capabilities it provides, treating them as critical products. Oversight bodies and regulators, in turn, focus on the outcomes and ensure that when AI agents are involved, they operate transparently, safely and without bias. For instance, audits shift to examining how an AI agent used data and why it made certain decisions on a citizen's behalf, rather than evaluating only human case handling.

All this builds upon the concept of **government-as-a-platform**: the government provides foundational building blocks and various service providers or even intelligent agents can innovate on top of them. For example, a private-sector company might build a

more user-friendly mobile interface for a government service or personal digital assistants could interact with government APIs to get things done for users – all within the policy and security frameworks set by government.

Self-organizing, agentic public services are a prime example of using the right technology in the right way to deliver public value and improve efficiency. Next, we further analyze the use of AI in government and how it can enhance efficiency when applied responsibly.

Service model	Service logic	Citizen effort	Strengths	Limits
Traditional digital services	Citizen initiates separate applications per agency; point-to-point workflows.	Medium. The citizen must search, re-enter data and repeat submissions (still better than physical paperwork or phone calls).	Simple to build and manage; low coordination costs between agencies.	Fragmented experience; duplicate data entry; slower outcomes; risk of exclusion for some users.
Proactive services	Government initiates service based on known events/data (e.g., a benefit offer triggered by a life event).	Very low. Citizen only needs to confirm and consent, if anything.	Inclusive and fast; builds trust; once-only principle fully applied within scope.	Limited to well-defined events; requires solid legal bases and very accurate data.
Life-event service bundles	Pre-designed end-to-end journeys for major life events.	Low. A single entry point and bundled steps for the user.	Holistic, intuitive service; measures outcomes across agencies.	Hard to scale across all life events; high institutional coordination needed; disputes over ownership and funding.
Self-organizing agentic services	AI agents compose capabilities dynamically per context and can be conversational or event-driven.	Potentially lowest. Largely assistive (prefilled, guided interactions; the citizen can opt out if desired).	Highly personalized and adaptive; spans multiple domains; avoids many institutional bottlenecks.	Requires very mature DPI and standards; transparency, bias mitigation and safety must be engineered by design.

Table 2: Comparison of public service delivery models – traditional digital services, proactive services, life-event bundles and self-organizing agentic services.

4.2.3. Automation in government: deterministic vs. AI systems

Technology should always serve outcomes, not the other way around. As emphasized earlier, no tool – AI included – should be adopted for its own sake. The case for deploying any advanced automation must rest on clearly defined problems to be solved and measurable public value to be gained, balanced against well-understood risks (such as bias, opacity or erosion of privacy). In this context, government leaders

should view artificial intelligence as one part of a broad automation toolkit, to be used only where appropriate and effective.

Government agencies can draw on a spectrum of automation approaches ranging from deterministic, rule-based systems to non-deterministic AI systems. The difference lies in how each handles information and reaches decisions:

01.

Rule-based (deterministic) automation applies predefined logic to well-structured inputs and will, given the same conditions, always produce the same outcome. If the rules and data inputs are known and complete, the process is entirely predictable. This predictability makes rule-based systems transparent and straightforward to audit, because one can trace every decision to an explicit rule or law. In essence, these systems encode the application of policy or legislation into software. They excel at tasks that are repetitive, standardized and grounded in clear criteria.

02.

AI or machine learning (non-deterministic) automation involves systems that learn patterns from data (including unstructured or incomplete data like free-text documents, images or sensor feeds) and make probabilistic inferences or predictions. Rather than following fixed if-then rules, AI models recognize complex patterns and correlations to estimate outcomes (e.g., the likelihood of fraud, the classification of a document, a prediction of service demand). This is valuable when not all decision criteria can be exhaustively specified in advance, or when the volume of data to analyze is massive. AI systems can adapt and improve as they process more data, but their decision logic is implicit in the model and not a simple set of human-readable rules.

In government – which fundamentally operates based on laws and rules – deterministic automation should remain the first priority wherever possible.

Rule-based systems are the right choice wherever processes are well-understood, repetitive and clearly defined by legislation or policy. Examples include calculating eligibility for benefits using established formulas, performing routine financial reconciliations, processing standard permit applications or integrating records between systems. In these cases, data can be structured and decision logic explicitly defined and explained when needed. Rule-based automation delivers speed and accuracy at scale, ensures consistency (equal treatment under the same rules) and is inherently auditable. In effect, it allows government to execute laws and policies quickly and reliably through digital systems.

AI, on the other hand, is most useful in situations where tasks cannot be fully specified upfront or involve recognition of complex patterns beyond human capacity. This includes scenarios like detecting anomalies or fraud across millions of transactions, analyzing unstructured data (scanning vast numbers of documents, emails or images for relevant information), or providing predictive analytics and decision support. For example, AI might be used to triage cases in a social services or justice system to prioritize those needing urgent attention, or to forecast public health or social care needs. In such settings, AI's value is not just doing things faster – it can enable entirely new capabilities that were not feasible with manual or rules-based methods alone. For instance, an AI model might analyze thousands of benefit applications and automatically approve the simple, low-risk cases (with explanations logged), freeing up human caseworkers to focus on more complex ones. Or a machine learning system could monitor real-time data from city infrastructure to predict and prevent failures before

they happen. These are tasks where a static set of rules either cannot be written to cover all nuances or would be too rigid to adapt to new patterns.

Both rule-based and AI-driven approaches can significantly improve performance, but in different ways. Rule-based deterministic automation streamlines well-defined processes – for example, compressing a task that once took a clerk 30 minutes into a few seconds of automated processing, and doing so with near-zero error rate. Multiplied across thousands of transactions, the time and cost savings are enormous, and every decision can be traced back to a clear rule (maintaining transparency). AI, by contrast, removes analytical bottlenecks – it can review millions of records or continuous data streams far faster than any team of human analysts, surfacing risks or insights (fraud patterns, public health trends, etc.) that neither rules nor humans might catch in time. Used well, **AI augments human decision-making and enables earlier, better-targeted interventions**, whether it's preventing waste and abuse or delivering services to those who will benefit most.

However, efficiency and innovation must not come at the expense of legitimacy and public trust. If an AI system's decision process cannot be explained or audited, it should not be deployed at scale in government services without a human in the loop. This is not more than we ask from human public servants – freedom in action with transparency and adherence to regulations, or strict supervision. In areas where AI is necessary to achieve effectiveness (because no other solution can reasonably handle the complexity or volume), governments must secure transparency and accountability through other means. This includes adopting a human-in-the-loop design for important decisions – ensuring that human officials remain responsible for final judgments that affect individuals'

rights or entitlements, and that they can override or question the AI's suggestions. Clear boundaries should be established delineating where an AI may assist or prioritize cases and where only rule-based or human decision-making will apply (especially for decisions with legal or ethical consequences). Moreover, operational transparency is critical: government authorities must document their AI models, data sources and validation processes; log the AI's actions and recommendations; and be prepared to provide meaningful explanations to both citizens and auditors about how a decision was made. This might also mean providing an audit trail that shows which data influenced an AI recommendation or giving an individual a simplified explanation for why they were flagged by an algorithm.

Governments can capture the benefits of both traditional automation and AI while upholding democratic values by applying the right tool to the right problem. Deterministic, rule-based automation should be used to encode the transparent application of law

and policy wherever data is well-structured and rules are clear. This not only speeds up current services but also reinforces fairness and accountability. AI should be deployed judiciously – only where it genuinely adds value, such as making sense of patterns in large, unstructured datasets or adapting to new trends – and always within a framework of human oversight, auditability and privacy protection.

The success of this stage (enhanced intelligence in services) becomes visible to citizens in everyday life: quicker services, fewer forms to fill out and a sense that the government knows them and helps them without endless red tape. It also sets the stage for the next evolution: leveraging real-time data and AI not just to improve services, but to transform governance itself into a more adaptive, responsive system – the realm of cyberocratic governance.

4.3 Future of democracy in the age of AI

With data and information increasingly available and accessible for strategic policymaking and operational decision-making, we are approaching the limits of our current governance model. The vision of evidence-informed, adaptive governance is encapsulated in the idea of cyberocracy (Ronfeldt & Varda 2008) – a system where governance is deeply integrated with real-time data and algorithmic tools. The key distinction between democratic cyberocracy and digital authoritarianism lies in whether democratic values and public accountability to guide the use of these technologies. We must ask: can real-time data and AI improve public service delivery and citizen engagement, or will these tools concentrate power, reduce transparency and erode fundamental rights?



4.3.1. Cyberocracy and the evolution of digital democracy

In a cyberocratic government, the feedback loop between citizen needs, data and policy is significantly accelerated. Traditional governance often relies on periodic statistics, delayed reports and infrequent elections to adjust course. Cyberocracy implies real-time sensing of and reaction to events. For example, consider crisis management: if a natural disaster strikes, a fully integrated government can sense the impact (through sensors, social media signals, emergency calls) in real time and coordinate a response across agencies instantly, dynamically reallocating resources as data on needs comes in. We saw glimpses of this during the COVID-19 pandemic – some countries leveraged near-real-time data on cases, hospital capacity and mobility to inform their policies (for instance, adjusting lockdown measures or vaccine distribution on the fly). A cyberocratic future would generalize this capability: whether it is an economic shock, a public health issue or an environmental threat, governments could respond with agility unheard of in the past, using data-driven simulations and AI to weigh options quickly. Policies themselves could become more conditional and adaptive – for example, a tax policy might automatically adjust rates for certain sectors if indicators show those sectors are struggling, rather than waiting for the next year's budget law.

However, **real-time policymaking pushes against the limits of current democratic processes**. Democracies are built on deliberation and due process, which take time. If decisions become very rapid, how do we ensure accountability and public input? One possibility

is that as data empowers faster executive action, there must be commensurate strengthening of oversight, such as AI tools aiding legislators or requirements that any algorithmic decision rule be transparent and approved by elected officials beforehand. Another aspect is **direct citizen participation in real time** – perhaps through more frequent digital referenda or citizen votes on issues, enabled by secure e-voting technology. If policies can change week to week based on data, could citizen feedback be gathered as frequently? In Switzerland, referendums every few months are routine; with digital tech, one could theoretically consult citizens much more often. There are risks of decision fatigue or populism if such mechanisms are not designed carefully. Still, we may see democratic innovations like online citizen assemblies or crowdsourced policy proposals operating continuously alongside data-driven administration.

One intermediate approach is the concept of **liquid democracy** or delegated voting, where people can delegate their vote on specific issues to trusted experts and reclaim it at any time. Digital voting platforms (building on secure e-voting infrastructure) can enable such flexible representation. The “experts” in this scenario might even include specifically vetted AI models that can represent a citizen's interests in very specialized policy domains (**AI-augmented**) – potentially much more knowledgeably than another human could. This remains hypothetical, but it aligns with cyberocracy's need to combine expertise with broad participation.



We must ask: can real-time data and AI improve public service delivery and citizen engagement, or will these tools concentrate power, reduce transparency and erode fundamental rights?

Another dimension is the **information sphere for citizens**. In a cyberocratic era, highly available, high-quality information – and tools to make sense of it – will be crucial for meaningful citizen participation. If governance becomes very complex and data-heavy, average citizens could feel left behind without concerted efforts in civic education and user-friendly transparency tools. We can imagine AI-powered interfaces that help explain policies to people in personalized ways. For example, a citizen could ask, *“How will the proposed city budget affect me?”* and an AI assistant (drawing on government data) could produce a personalized, easy-to-understand answer. Presenting complex information in accessible forms (data visualizations, interactive simulators, personalized summaries) would improve citizen participation by making people better informed and able to see evidence behind the decisions. For instance, if a local government is considering a new traffic policy, a public online simulator might allow any resident to tweak parameters (like closing a street or changing bus frequency) and see the projected

impact on congestion or emissions. Engaging citizens in data-driven exploration makes public debates more fact-based. Empirically, when citizens are given unbiased information and tools to understand it, deliberations tend to yield more moderate, consensus-oriented solutions rather than polarized ones. Thus, investing in open data and explanatory tools becomes a democratic imperative in cyberocracy.

4.3.2. Cyberocratic policymaking

We must also address the role of AI in policymaking itself. As AI models become more prevalent, they will be used to generate policy options, predict outcomes or make certain administrative decisions automatically. This raises a provocative question: **if an AI system significantly influences policy, how do we ensure it aligns with human values and democratic choice?**

One approach is that if AI inherently involves judgments or biases (as any model trained on human data might), then perhaps citizens or their representatives should “vote” on which AI systems or which parameter settings to use for important decisions. For instance, if an algorithm is used to prioritize infrastructure projects, its criteria (e.g., economic return vs. helping disadvantaged areas) reflect value judgments – those should be democratically determined, not left to engineers or opaque algorithms. Governments or markets might present multiple AI-generated recommendations and have a public consultation or an expert citizens’ jury choose among them. The key point is that **algorithmic governance requires oversight**. Many jurisdictions are already moving toward this: the EU’s proposed AI Act would classify government AI systems that affect people’s rights as “high-risk,” subjecting them to audits and transparency requirements. Ultimately, maintaining human agency is vital. Cyberocracy should not mean abdicating decisions to black box AI without accountability; it means using AI smartly as a tool for human decision-makers and citizens.

In terms of policy co-creation, cyberocracy could enable more of a **wiki government approach**: policies posted online in draft form for continuous citizen input, with potentially thousands of contributions analyzed (by AI) to improve the proposals. This could become standard: before a government finalizes a

major regulation, it runs an online deliberation where any citizen or stakeholder can contribute. Arguments are mapped and rated, often with AI helping to find common ground or summarize themes, and the results inform the final decision. It’s slower than purely top-down decision-making, but perhaps faster than traditional committee processes, and it can produce legitimacy that top-down approaches cannot.

For a democratic cyberocracy, we might also see the emergence of **algorithmic jurisprudence** – where legal rules are at least partly encoded into automated systems. For example, tax formulas could be directly implemented so that taxes are calculated and adjusted in real time with economic changes (indeed, some aspects already are, such as inflation-indexed benefits). However, legal interpretation and value trade-offs will still require human judgment and democratic debate. We may find that parliaments need new technical advisory units to help them write laws that can be implemented in code without ambiguity.

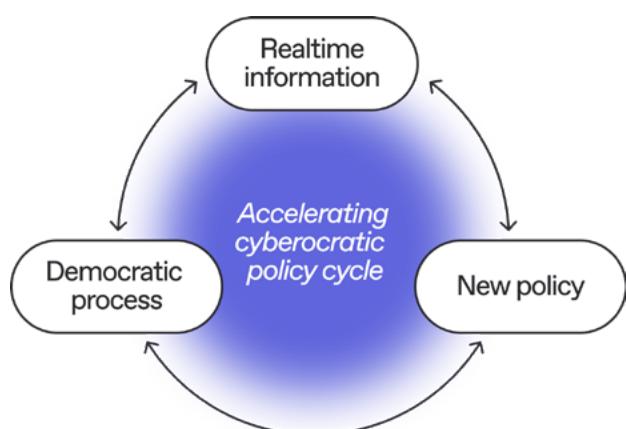
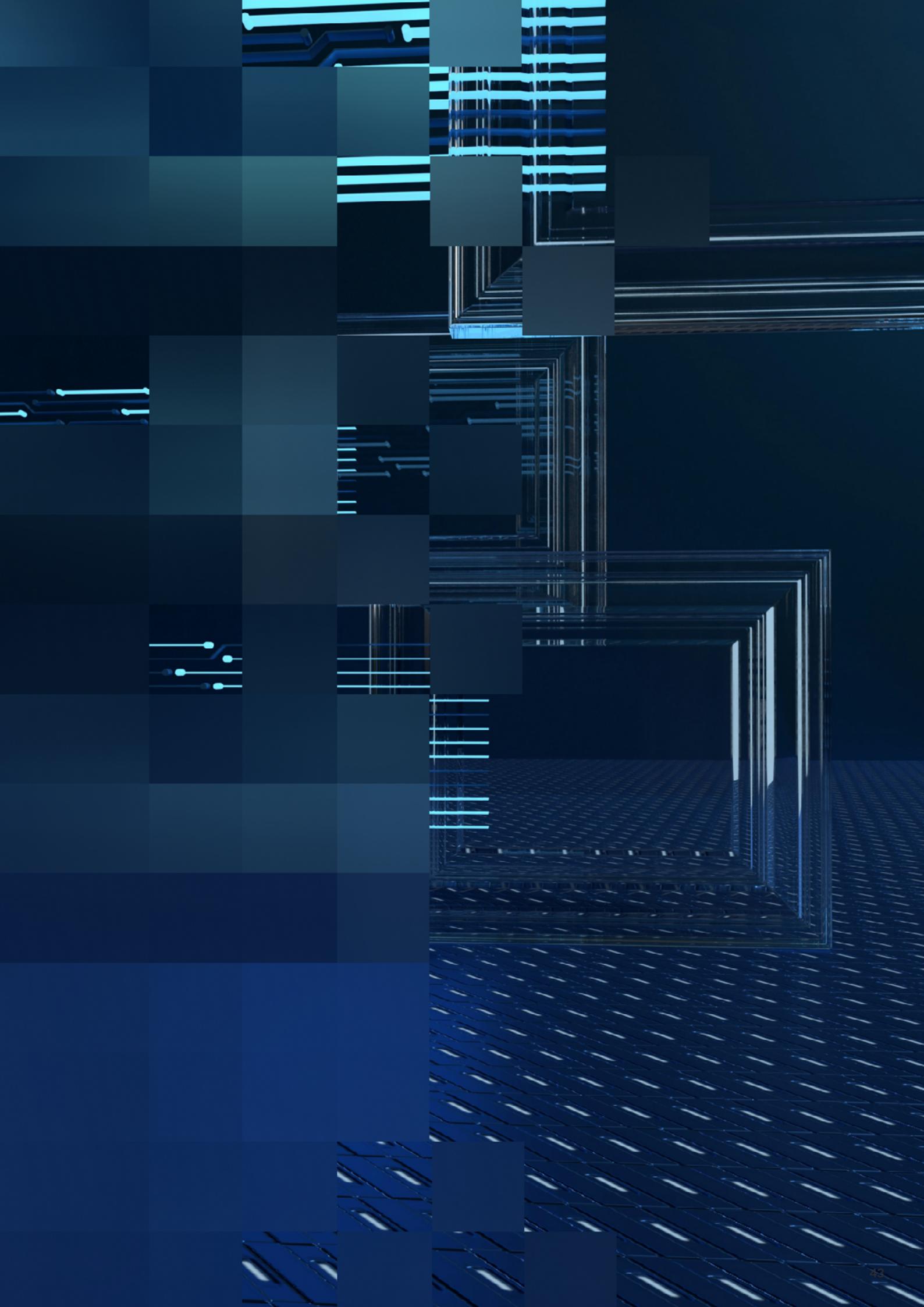


Figure 6: Realtime information and AI facilitated policymaking will require to accelerate democratic processes.



4.3.3. Impact on politics, elections and freedom

Another aspect to consider is the impact on politics and elections themselves. If governance becomes more continuous and based on performance data, political accountability is likely to shift. Voters may expect real-time results and become more impatient with leaders – or conversely, data transparency could help build trust if it shows genuine improvements. The availability of high-quality live data on government performance (e.g., dashboards for crime rates, school performance, hospital wait times) and on the projected impacts of proposed policies might influence public opinion and election outcomes – for better (more accountability and informed debate) or worse (data misinterpretation or hyper-fragmented messaging). In a best-case scenario, a well-informed electorate could base decisions more on track records and less on rhetoric. But there is also the danger of information overload or the misuse of big data for micro-targeted propaganda, as we have already seen in recent years. Ensuring that quality information is available to all, and not just to some, will be crucial. Efforts to combat disinformation will be even more important in a cyberocracy – without trust in information, the whole model collapses. As Freedom House and others have documented, the past decade has shown how digital tools can spread propaganda and erode democracy in many places. A democratic cyberocracy will need strong institutions to ensure truthful, evidence-based discourse – potentially including public broadcasters with mandates to explain data clearly, educational curricula emphasizing data literacy, and swift responses to false information online.

Cyberocratic governance holds great promise for democracies if done right. It could mean governments

that respond to citizen needs instantly, policies that continuously improve based on evidence, and citizens who are deeply informed and engaged in the governing process. Cyberocracy can be more efficient at monitoring and managing complexity than bureaucracy and technocracy have been. However, it also comes with serious risks that must be managed: surveillance creep, loss of privacy, algorithmic bias, erosion of deliberative processes and the specter of authoritarian abuse of these technologies. We may lose the very meaning and fabric of our society and culture if we get this wrong.

The difference between a digital democracy and a digital dictatorship will hinge on safeguards, transparency and empowerment. In a democracy, cyberocracy must empower citizens – giving them more information and voice – rather than merely surveilling or nudging them without consent. It must also preserve human dignity and agency, ensuring that behind all the data, individuals are treated fairly and that decisions can be appealed or corrected. The technologies involved are value-neutral; it is our implementation that determines the outcome. If we adhere to the principles discussed, the future can be one in which technology greatly enhances democracy. If we ignore those principles, we may slide into what some call “digital authoritarianism,” where the state uses technology to control and manipulate – a scenario already visible in some countries.

The future of democracy in the cyberocratic era will depend on a grand bargain: citizens trust government with a lot of data, and in return government becomes more transparent, accountable and responsive. The best outcome is a virtuous cycle where informed

citizens and data-informed officials co-create policy in near-real-time, leading to effective solutions to societal problems – all while upholding fundamental rights. Achieving this will require continuous vigilance: new institutions, such as data ethics councils,

algorithm auditors, participatory platforms, and possibly new rights, such as data ownership rights and rights to explanation for AI decisions, will need to be established. But if done well, cyberocracy could revitalize democracy for the 21st century.

Strategy

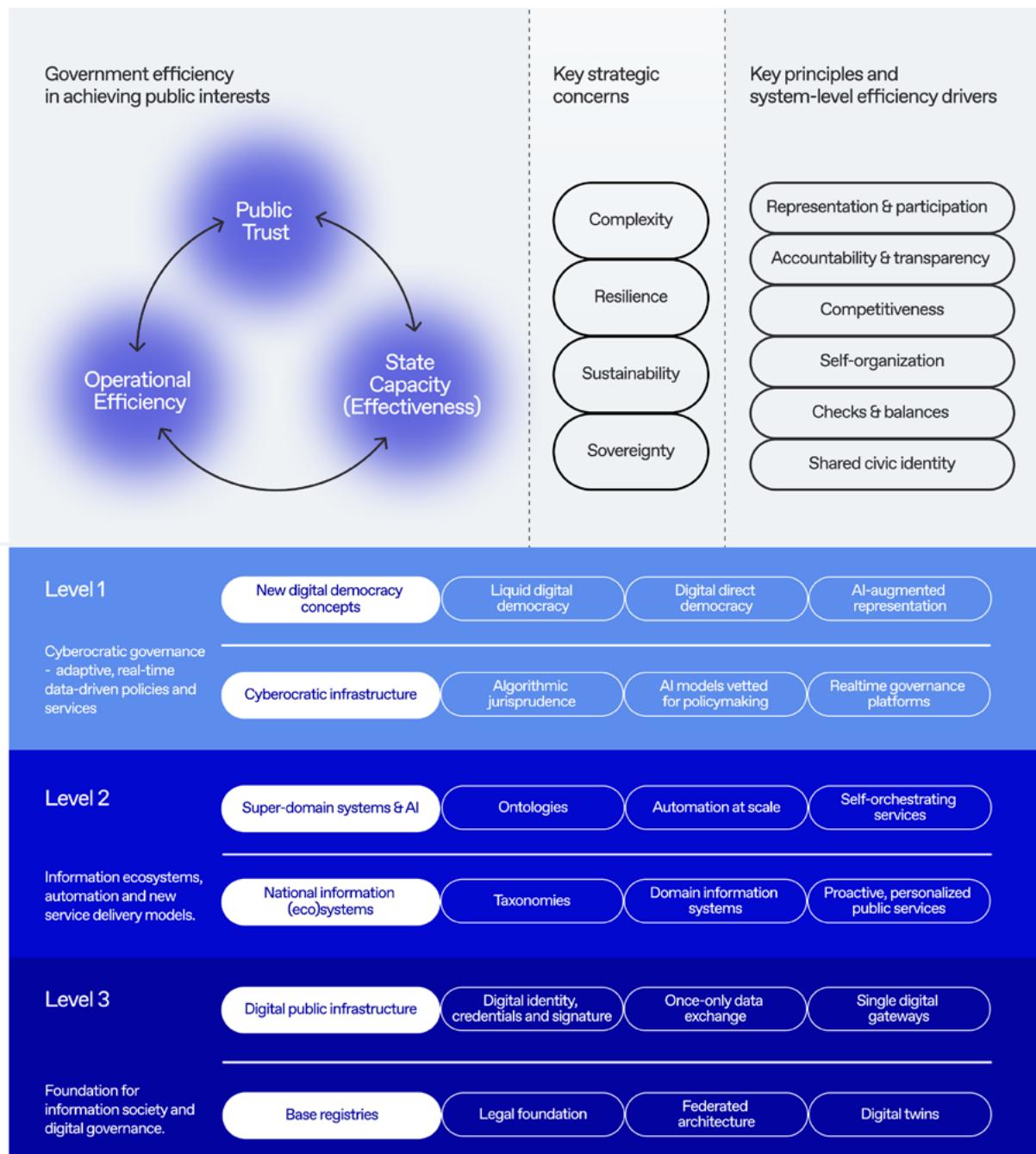


Figure 7: Whole-of-government system-level efficiency framework with a path to democratic cyberocracy.



5.

Conclusion and key recommendations

In earlier chapters, we outlined what constitutes system-level efficiency and what constrains its achievement. We looked at how one system – democracy – has achieved high levels of system efficiency and identified the core principles of democracy that contribute to that success by design. We also mapped these principles onto key information system design decisions. Then we showed how these design decisions can be implemented in practice through technology, and what implications this has for the governance of societies. Now we will sum up the macro-level implications.

One way to visualize the argument is with two triangles: one standing upright and one inverted. The choices made at the foundational layers (the base of the triangle) determine the freedoms and efficiencies at the top.

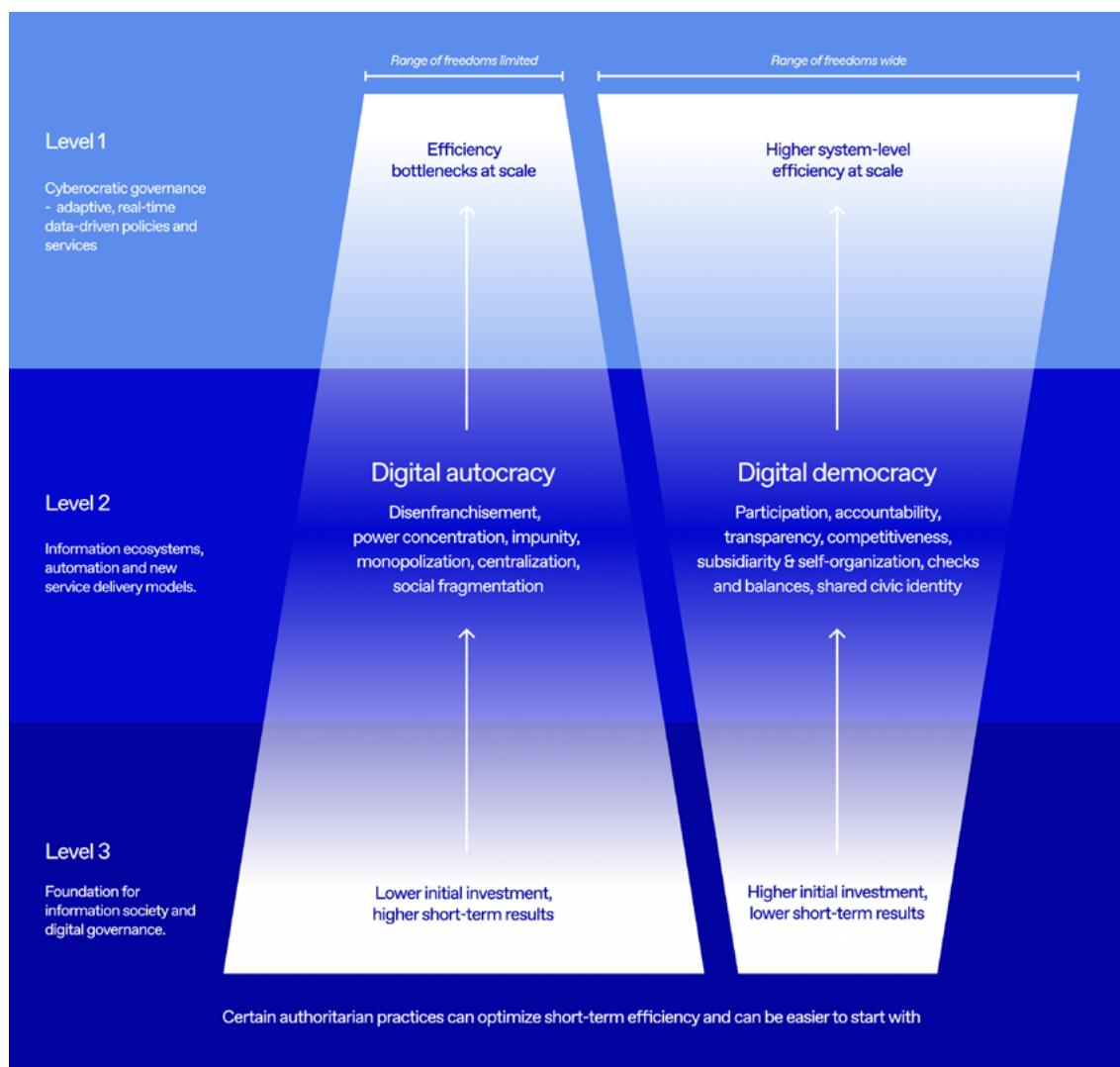


Figure 8: System design principles leading to different levels of efficiency and freedom.

In a democracy designed with bottom-up principles, freedoms widen toward the top because the system is set up to allow maximum choice and autonomy by design. In a digital dictatorship, by deliberate design, power is concentrated at the top – leading to fewer freedoms and less capacity for self-organization. The result is low system efficiency, even if such a regime may achieve strong operational efficiency in some isolated domains. In short, a choice to centralize may feel secure at first but it will reduce the room for action later and is never a basis for a self-organizing, resilient ecosystem. If you centralize your architecture and decision-making, you maximize control and dependency, stifling competition and innovation; eventually, at the very top – where policy choices and service designs are made – there will be far less freedom or flexibility. In an overly centralized model, the CTO effectively becomes the de facto CEO of government.

Modern democracies do not look like that. Their freedoms widen at the top rather than narrow, because the system is built to allow for maximum freedom and choice from the bottom up through the core principles that govern us. A digital dictatorship, however, narrows freedoms at the top: a deliberate decision to centralize will concentrate power and inevitably lead to fewer choices and less self-organization capacity.

What are the implications? The first is that our digital government leaders – and the technical and policy decisions they make – will shape how our government and society look in the future. Not immediately, but over time, as each layer of technology and policy is built on the last. Unfortunately, we will only fully know the consequences in hindsight. However, as discussed earlier, we can emulate systems that have stood the test of time – democracies – and aim for system efficiency that is complex yet still self-organizing. Or simply, we can copy what works.

Key recommendations

Governments must adopt technology to increase public-sector efficiency and deliver greater public value. In doing so, they will need to navigate policy choices that affect the design of digital government. Thesis of this paper is that these same design and policy choices determine (or strongly influence) the form of governance itself. In optimizing system-level (whole-of-government) efficiency, democratic principles drive government efficiency – because those principles fundamentally lead to better performance at scale.

The key recommendations are:

01.

Embed core democratic principles into digital transformation and initiatives

Treat the principles of participation, transparency, competition, subsidiarity, accountability, and civic inclusion as design criteria for digital initiatives. Ensure a variety of service delivery channels and use the ones people prefer (participation); mandate transparency of algorithms and decisions; prefer interoperable, competitive solutions over monolithic ones; push decision-making authority and data ownership to the local or individual level whenever effective (subsidiarity); enforce checks and balances in data governance and system access; and ensure every citizen can access digital services (through inclusive design and assistive measures). By aligning technology projects with these democratic principles, governments not only improve performance but also reinforce public trust and legitimacy.

02.

Build a secure, trusted digital foundation with democratic safeguards

Invest in high-quality base registries, unique identifiers for people and businesses, secure data exchange (interoperability) infrastructure, and universal digital identity with e-signatures. Ensure legal and institutional checks and balances in this foundational infrastructure so that no single authority can abuse concentrated data or power. This foundation should emphasize privacy, security and transparency by design to build public trust from the ground up.

03.

Manage complexity, resilience and sovereignty proactively

Embed organizational goals to simplify processes and legacy systems wherever possible to reduce complexity. Use modular architectures and open standards to make

systems adaptable and interoperable. Incorporate resilience strategies (redundancy, decentralization of critical systems, contingency planning) so that services withstand shocks and cyber threats. Prioritize digital sovereignty for critical systems – adopt open-source or multiple-vendor solutions to avoid lock-in, and ensure critical data and systems remain under national or democratic control. Build horizontal and vertical integration across domains using same principles.

04.

Deliver citizen-centric, integrated services (personalized and proactive)

Redesign services around life events or user needs, minimizing the burden on citizens. Implement the once-only principle so that citizens and businesses never have to provide the same information twice. Strive for single front-door access to services (one-stop portals or apps) and proactive service delivery (where the government initiates or pre-fills services when data indicates a need). Ensure that integration of services across agencies doesn't erode accountability: maintain clear ownership of data and functions and use legal frameworks to enable responsible data sharing and leverage emerging technologies such as self-organizing agentic services where applicable. Focus on user experience and inclusiveness across all channels (web, mobile and in person) to boost adoption and satisfaction.

05.

Apply automation and AI responsibly, with humans in the loop

Use rule-based automation as the default for well-defined, rule-based processes – this improves speed, consistency and transparency in service delivery. Deploy AI or machine learning tools only where they add clear value (e.g., detecting patterns in large datasets, providing predictive insights) that cannot be achieved with simpler and more transparent means. For all AI deployments, implement strong accountability measures: human oversight for critical decisions, explainability requirements, audit logs, and regular bias evaluations. In other words, treat AI as an assistant to human officials and citizens, not a replacement – maintaining the primacy of human judgment, especially in critical decisions affecting rights or entitlements.

By following these recommendations, governments can modernize and become more efficient **without** compromising the fundamental values of democracy. In fact, as we have argued, those democratic principles are themselves drivers of long-term efficiency and performance. A digital government built on these foundations will not only achieve better outcomes – it will also strengthen the democratic fabric, ensuring that efficiency gains endure and benefit government and society as a whole.

6.

Bibliography



- Acemoglu, D., Naidu, S., Restrepo, P., & Robinson, J. A. (2018). Democracy Does Cause Growth. *Journal of Political Economy*, 127(1), 47–100. <https://doi.org/10.1086/700936>
- Artimo, O., Grassia, M., & De Domenico, M. (2024). Robustness and resilience of complex networks. *Nature Reviews Physics*, 6, 114–131. <https://doi.org/10.1038/s42254-023-00676-y>
- Apergis, N. (2018). Education and democracy: New evidence from 161 countries. *Economic Modelling*, 71, 59–67. <https://doi.org/10.1016/j.econmod.2017.12.001>
- Besley, T., & Kudamatsu, M. (2006). Health and democracy. *American Economic Review*, 96(2), 313–318. <https://doi.org/10.1257/000282806777212053>
- Brown, D. S. (1999). Reading, writing, and regime type: Democracy's impact on primary school enrollment. *Political Research Quarterly*, 52(4), 681–707. <https://doi.org/10.1177/106591299905200401>
- Conway, M. (1968). How do committees invent? *Datamation*, April, 28–31.
- Dahlum, S., & Knutsen, C. H. (2017). Do democracies provide better education? Revisiting the democracy–human capital link. *World Development*, 94, 186–199. <https://doi.org/10.1016/j.worlddev.2017.01.001>
- Di, S., & Huang, F. (2023). Is democracy good for growth? Development at political transition time matters. *European Journal of Political Economy*, 78, 102355. <https://doi.org/10.1016/j.ejpol eco.2022.102355>
- Dörffel, C., & Freytag, A. (2023). The poverty effect of democratization. *World Development*, 165, 106186. <https://doi.org/10.1016/j.worlddev.2023.106186>
- European Commission (2018). Good Practices in Access to Base Registries (ISA² Programme Publication). Brussels: European Commission.
- Flavin, P. (2024). Democracy and life satisfaction: Evidence from updated global data. *Social Indicators Research*, 174, 409–419. <https://doi.org/10.1007/s11205-024-03392-x>
- Franco, A., Alvarez-Dardet, C., & Ruiz, M. T. (2004). Effect of democracy on health: Ecological study. *BMJ*, 329(7480), 1421–1423. <https://doi.org/10.1136/bmj.329.7480.1421>
- Haug, N., Dan, S., & Mergel, I. (2023). Digitally-induced change in the public sector: A systematic review and research agenda. *Public Management Review*, 26(7), 1963–1987. <https://doi.org/10.1080/14719037.2023.2234917>

- Kudamatsu, M. (2012). Has democratization reduced infant mortality in sub-Saharan Africa? Evidence from micro data. *Journal of the European Economic Association*, 10(6), 1294–1317. <https://doi.org/10.1111/j.1542-4774.2012.01092.x>
- OECD (2016). Advanced Analytics for Better Tax Administration: Putting Data to Work. OECD Publishing, Paris. <http://dx.doi.org/10.1787/9789264256453-en>
- OECD (2019). A Data-Driven Public Sector: Enabling the Strategic Use of Data for Public Value. OECD Working Papers on Public Governance No. 33.
- Paleologou, S.-M. (2022). Happiness, democracy and socio-economic conditions: Evidence from a difference GMM estimator. *Journal of Behavioral and Experimental Economics*, 101, 101945. <https://doi.org/10.1016/j.soec.2022.101945>
- Patterson, A. C., & Veenstra, G. (2016). Politics and population health: Testing the impact of electoral democracy. *Health & Place*, 40, 66–75. <https://doi.org/10.1016/j.healthplace.2016.04.011>
- Ronfeldt, D., & Varda, D. (2008). The Prospects for Cyberocracy (Revisited). Social Informatics Research Network Working Paper No. 29.
- Schünemann, C., Johanning, S., Reger, E., Herold, H., & Bruckner, T. (2024). Complex system policy modelling approaches for policy advice – comparing systems thinking, system dynamics and agent-based modelling. *Political Research Exchange*, 6(1). <https://doi.org/10.1080/2474736X.2024.2387438>
- Whetsell, T. A., Dimand, A.-M., Jonkers, K., Baas, J., & Wagner, C. S. (2021). Democracy, complexity, and science: Exploring structural sources of national scientific performance. *Science and Public Policy*, 48(5), 697–711. <https://doi.org/10.1093/scipol/scab036>
- World Bank (2021). Estevão, M. Why Tax Administrations are Embracing Digital Transformation. World Bank Blogs – Voices (Dec 1, 2021).
- Yang, C., Gu, M., & Albitar, K. (2024). Government in the digital age: Exploring the impact of digital transformation on governmental efficiency. *Technological Forecasting and Social Change*, 208, 123722. <https://doi.org/10.1016/j.techfore.2024.123722>

25 years of shaping
the future