2025 Senior Officials Meeting - Tallinn, Estonia

Summary of Day One, 12 November

Opening Remarks

Estonia opened the meeting with an overview of its digital governance background and its experience working across several countries. Lauri highlighted the importance of mutual learning between nations, sharing challenges and mistakes, and maintaining an open and informal forum where participants can speak freely. He also described recent structural changes in Estonia, where the role of the Government CIO was divided into two deputy director general positions. One is responsible for infrastructure and cyber, and the other, held by Lauri, is responsible for digital services, data, AI, and regulation. The digital directorate recently moved to the Ministry of Justice and Digital Affairs, creating a closer link between digital operations, regulation, and privacy. Estonia's national digital strategy remains unchanged.

Country Updates

Canada
Canada presented its centralized structure under the Treasury Board of Canada Secretariat and its multi-year Digital Ambition plan, which guides federal digital transformation. In 2025, two new ministerial portfolios were created: the Minister of Government Transformation and the Minister of AI and Digital Innovation. This year, Canada published its first ever AI Strategy for the Federal Public Service, launched a governmental AI hub, developed GC Translate, and is preparing a public registry of governmental AI use. Canada is also advancing commitments under the G7 Leaders' Statement on AI for Prosperity which includes "Rapid Solution Labs" and a G7 AI Network.

Israel
Israel presented the government's transition from slow and rigid IT systems to the AI era. There is a need to upgrade the government's core capabilities so that services can be delivered more quickly, decisions can be improved, and ministries can adopt smarter tools. There are three main layers of work: front line services, back-end infrastructures, and a data and AI layer. Israel is working with ministries on transformation plans, improving cross ministerial service flows, and using cloud technology as a strategic tool. Israel also noted the gap between the speed of innovation in the private sector and the government's need for long term partnerships.

New Zealand
New Zealand described the challenge of a government made up of 42 separate agencies, each operating differently and lacking unified governance. Two national priorities are digital identity and digital governance. New Zealand is developing a trust framework for digital identity together with a government app and a national digital wallet. The government is taking the lead because the private sector is not progressing fast enough in this area.

Korea
Korea focused on the combination of data, cloud, and AI as the foundation of digital government, with an emphasis on digital sovereignty and security. Korea shared lessons from past attempts to create a data sharing economy. Incentive models for citizens and paid access for companies did not succeed financially, leading to market failures. Korea is now working on resilient digital infrastructures, privacy protection, and AI enabled public services.

Portugal
Portugal highlighted its transition toward event-based government, national digital public infrastructure, and alignment of processes across many agencies. The country is advancing digital identity, data governance, and AI use cases while working within budget constraints.

United Kingdom
The UK described the role of the Government Digital Service (GDS) as the leader of national digital platforms, responsible for unified digital services, shared infrastructures, automation, and increased AI adoption. The UK emphasised the importance of international cooperation on digital standards.

Uruguay
Uruguay shared that its new government is defining digital priorities for the next five years and remains committed to active participation in the DN network. The main challenges are cross government services, data mobility, and responsible AI adoption.

Deep Dive: Data

Israel opened the session by presenting the main challenge in data sharing between ministries. Because ministries operate as silos and often see their data as a source of power, many hesitate to share information. This limits the government's ability to create cross-government insights and slows the development of data-based services and high-quality policy.

Israel described the current legal process for data sharing, which is formal, complex, and often takes more than a year. Many ministries avoid initiating data sharing altogether because the timelines do not match operational needs. The problem becomes more severe in emergencies, where there are no exceptions to the process, making it difficult to transfer essential information to local authorities in real time. Israel is now working to implement the recommendations of a national committee that proposed reforms, including fast track mechanisms for emergencies.

The technological direction Israel presented is to avoid building a single separate data catalogue, a model that failed in the past. Instead, Israel is developing a network-based connection layer, inspired by military systems, where data is accessed in real time through authorised APIs (Application Programming Interfaces). Metadata is created as a natural byproduct of this network rather than as an independent project.

<u>Discussion Among Countries</u>

Estonia presented the X Road system as a decentralized, secure, and encrypted mechanism that keeps ownership of data in each ministry. Only the minimum required data is exchanged. Citizens can see who accessed their information and for what purpose. Estonia is promoting a single shared tool for all governmental data exchanges instead of each agency developing its own.

Canada described how outdated privacy laws limit data sharing, even when it would serve the public interest. The main barrier today is legal, not technological. Canada is working on legislative reform to enable clearer and more consistent data sharing, including wider use of automated positive decisions.

New Zealand discussed challenges with automated decisions. While automated positive decisions work well, errors in negative automated decisions can create debt repayments for citizens and undermine trust. New Zealand applies a model where positive decisions are automated but negative ones require human review. They also described difficulties with inconsistent metadata across agencies, which prevents proper integration.

The UK highlighted the role of the Office for National Statistics, an independent body that aggregates and anonymizes data from multiple ministries. This enables simulations and policy analysis without transferring raw data between agencies.

Korea shared challenges with monetization-based models that attempted to reward citizens for sharing data while requiring companies to pay fees. This model led to financial collapse of participating companies. Korea is seeking a new balance between privacy, economic sustainability, and data access.

Deep Dive: Artificial Intelligence

The session, led by **Uruguay**, focused on responsible adoption of AI in government.

Uruguay presented a risk classification framework for AI use. Low risk services can be highly automated, while sensitive services require strong human oversight and robust validation.

The discussion emphasised that positive decisions, such as granting benefits, can be automated, while negative or complex decisions must remain under human review to avoid errors and maintain public trust.

A recurring challenge across countries is poor data quality and fragmented systems. High quality data is a prerequisite for the reliable use of AI. AI cannot compensate for structural problems in government data.

Participants discussed how to measure performance in AI based services. Countries are trying to decide whether to measure speed, decision quality, cost, or citizen trust. There is a need for a unified evaluation framework.

Privacy and trust were highlighted as essential foundations. Transparency about AI use, clarity about decision making processes, and proper documentation of models are needed to maintain citizen confidence.

Shared challenges include outdated privacy laws, shortages of skilled professionals, and difficulty integrating new models into legacy systems. Countries agreed there is a need for joint international work on test methods and evaluation practices.

Uruguay presented its regulatory sandbox for AI, which allows public and private entities to test AI solutions in a controlled environment. Its approach is to start small, validate results, and then scale. AI tools should be reusable and easily expandable.

Israel described the extensive legal advisory training conducted to support responsible AI adoption. The guidance includes ethical principles, transparency requirements, monitoring guidelines, and tools to distinguish real risks from perceived ones. The goal is to ensure legal advisors do not slow down projects unnecessarily.

Deep Dive: Cloud

Canada presented the evolution of its national cloud strategy and the lessons learned over eight years.

In 2016, Canada launched its first "Cloud Adoption Strategy" where departments had discretion to adopt cloud independently. This flexibility helped early adoption but led to uneven progress. Two years later, Canada moved to a "Cloud First" policy making public cloud the default for new or modernized systems. This resulted in accelerated adoption but also exposed significant legacy technology challenges. In 2023, Canada shifted towards a "Cloud Smart" approach, where cloud adoption was based on actual needs. A year later, Canada adopted the "Application Hosting Strategy" (AHS) which moved beyond a heavy cloud focus to a whole-of-government hosting framework. The AHS supports departments in selecting the most cost-effective and business-aligned hosting model – cloud, enterprise services, or modernized GC data centres – and reinforces modernization as the foundation for migration.

Canada stressed the importance of budget management. Cloud adoption changes budgeting from equipment-based spending to consumption-based spending. Strong cooperation with finance teams is essential, otherwise ministries face double costs and budgeting difficulties.

On digital sovereignty, Canada uses a layered model that combines international cloud providers with national infrastructures such as GC Cloud One and government data centres for sensitive workloads. Cloud contracts include sovereignty related clauses.

Canada emphasised that not all systems should be moved to the cloud. Each system must be assessed to decide whether it should remain on local infrastructure, move to public cloud or private cloud, or be rewritten entirely. These are architectural decisions, not purely technological ones.

Canada is investing in shared security layers, identity and authentication tools, and common foundational services to allow ministries to focus on service development.

Key conclusions were that cloud adoption is a long-term journey requiring alignment between technology, law, finance, and security. Success depends on governance and planning, not only on technical migration. Mistakes are part of the process and ongoing knowledge sharing is essential.

Summary of Day Two, 13 November

Opening Remarks

Estonia opened the day by emphasizing the importance of a clear work structure for the coming years, the need for continuity between presidencies, and the importance of strengthening professional cooperation across member states.

Presentation by New Zealand on Reducing Digital Costs and Building Cross-Government Infrastructure

New Zealand presented a national strategy for building a smarter state, focusing on reducing costs, creating shared digital public infrastructure, and preparing government systems for AI based services. The strategy reflects a shift from government as a direct service provider to government as an orchestrator of a broader digital ecosystem where the public and private sectors operate together.

Key principles:

Digital Public Infrastructure as a national foundation

New Zealand is developing a unified national infrastructure layer including a government app, decentralized digital identity, secure payments, and a data orchestration layer. This approach is intended to reduce duplication and improve development efficiency.

From data lakes to data orchestration

The focus is on accessing data at its source rather than duplicating datasets, enabling secure real time use and maintaining data sovereignty.

Integration of government services with private organizations

New Zealand presented a model in which citizens may receive some government services through banks, financial institutions, and community organizations. The implementation will be gradual and carefully managed.

AI based service interfaces

New Zealand anticipates a future where citizens interact with government through conversational AI interfaces instead of portals. Citizens ask a question, and an intelligent layer delivers the service. A national AI competition has already taken place, and such an interface is being developed.

Long term planning

Targets for 2028 include two million downloads of the government app, four million digital credentials, and infrastructure that supports full automation of financial processes such as loan approvals based on verified digital income information.

Discussion Among Countries

Internal organizational barriers
Countries reported similar challenges: slow processes, limited operational alignment, and difficulty coordinating between ministries. Many agreed that digital transformation is held back primarily by government structure rather than by technology.

Government procurement as a bottleneck
Countries described long, rigid procurement processes, lack of technological expertise, and restrictive regulations that limit experimentation. Some shared solutions such as flexible procurement, pilot routes, and regulatory sandboxes.

Legal complexities and data sovereignty
Countries described challenges in implementing AI and data projects due to overly cautious legal interpretations, regulatory ambiguity, and obstacles to data sharing. Several presented risk frameworks and updated legal guidelines to support responsible innovation.

Workforce and skills
Many states reported challenges in hiring and retaining skilled staff. The United Kingdom presented a national training program for civil servants focused on AI and digital skills. Other countries described similar efforts.

Follow up to New Zealand's presentation
Countries discussed government roles in a decentralised environment, public trust when services are offered via private platforms, the need for shared standards for AI and digital identity, and the feasibility of open architectures.

*See **Direction-Setting and Administration Table** for the meeting's Record of Decision.*