NRD Companies
NEW CHAPTER. BETTER.

infobalt
L I E T U V A

NRD Cyber Security

DISCUSSION PAPER FOR

THE WSIS+20 FORUM HIGH-LEVEL EVENT 2024

Small States Towards Meaningful Connectivity: Lessons Learned & Future Perspective

27-31 MAY 2024
GENEVA, SWITZERLAND

Table of Contents

Introduction

In an era of rapid digital transformation, small states face unique challenges in navigating the complexities of modern governance. Limited resources, scarce talent pools, and policy intricacies often hinder their progress towards building robust digital infrastructures. However, through collaboration and knowledge exchange, these nations can leverage shared experiences to overcome these obstacles.

The emergence of GovTech offers promising solutions for citizen-centric governance, but success depends on robust cybersecurity measures. Collaboration between public and private sectors, both domestically and internationally, is crucial for driving innovation and fostering resilience in small states.

Lithuania's leadership in promoting collaboration in digital governance serves as a compelling example. By sharing expertise and best practices, Lithuania demonstrates the transformative power of collective action in the digital realm.

This paper explores the challenges faced by small states in their digital transformation journeys and highlights the importance of tailored solutions and holistic approaches to fostering effective collaboration. Through real-world examples and insights, we aim to guide small states towards a secure and resilient digital future.

Challenges and Collaborative Solutions for Small States

Emerging digital technologies are transforming how governments function and economies operate. Simultaneously, governments face the increasingly complex needs of the population, driven by such factors as rising expectations of citizens and businesses towards quality and efficiency of public services, the growing amounts of data in public domain, and high complexity of issues faced by the public sector. While this presents both challenges and vast opportunities for all nations, small states face multitude of unique obstacles in their digital transformation journeys. Limited financial resources often constrain investments in modern IT infrastructure, software, and cybersecurity. Finding and retaining skilled IT professionals and other specialists instrumental for digital initiatives can be difficult due to a shallow talent pool. Furthermore, physical limitations like unreliable internet or outdated government digital systems can further complicate adoption. Policy challenges are also notable, since governments need to develop a clear national digital strategy with well-placed priorities, as well as navigate the complexities of data privacy regulations and robust cybersecurity measures, all while handling limited resources impacted by the size of the state.

While small states exhibit a remarkable diversity - from island nations to landlocked states, and from developed economies to those striving for development, they all share the same challenges that come with their size and limitation of available resources. By sharing their experiences and lessons learned, states that were already able to achieve success in digital governance can provide valuable guidance to other small states embarking on their digital transformation journeys. This knowledge transfer can encompass best practices for overcoming resource constraints, navigating policy hurdles, and implementing effective GovTech solutions. Regional forums, joint workshops, and joint knowledge exchange and technical assistance projects can facilitate this collaboration, empowering all small states to learn from each other and collectively rise as digital leaders. This approach fosters a collaborative ecosystem where all small states act as active participants and partners in moving towards a more efficient and citizen-centric digital future.

Such collaboration between small states is well-suited for embracing the emerging concept of "GovTech", which advocates the principles of citizen-centricity, universally accessible, secure public services and a "whole-of-

government" approach to digital government transformation, and is based on effective use of advanced technologies and data, and close collaboration between public and private sector. Simultaneously, GovTech concept heavily relies on robust cybersecurity measures to ensure the confidentiality, integrity, and availability of sensitive data and critical infrastructure, as without clear cybersecurity protocols in place, GovTech initiatives would become vulnerable to various cyber threats, compromising public trust and hindering the effective delivery of government services.

Furthermore, it is important to acknowledge that such collaboration should occur not only between governments, but across public and private sectors, both locally and internationally, too. Innovative companies that are active both in national and international markets, which engage, work, and learn across different contexts, can apply their experiences with supporting digital transformation, utilize their global understanding about relevant trends in the field, and help different partners (whether public or private) from other small states get a better understanding about how to build strong and secure foundations for digital society and government.

Lithuania is a good example of a state that is becoming increasingly open to co-creation. The country with a modest population of less than 3 million has achieved significant developments in the fields of digital governance, cybersecurity and digital economy over the past couple of decades. Yet at the beginning, Lithuania was learning quite a lot from others, including other small states. Following this fresh experience, Lithuania exemplifies a small state actively embracing collaboration and co-creation for digital transformation.

Having overcome its own challenges with limited resources, Lithuania recognizes the value of shared experiences. The country is now a leader in promoting knowledge exchange and technical assistance programs in GovTech and public sector innovation, hosting various regional forums and workshops. This openness extends beyond government institutions.

By sharing expertise and best practices, Lithuanian companies can assist other small states in building secure digital foundations and implementing effective

GovTech solutions. Lithuania's commitment to collaboration positions it as a valuable partner for other small states seeking to navigate their digital transformation journeys. One particular example is the family of INVL Technology companies - **NRD Companies** and **NRD Cyber Security**, whose experts contributed to Lithuania's digital journey and now act as advisors and developers of digital solutions for other small states around the world, and are openly embracing the approach of co-creation for the solutions of the unique challenges faced by small states. The practical insight of these companies, with experience of working with small states across the entire globe, are presented below. They showcase Lithuania's experience in small state cooperation and numerous lessons learnt, that might be useful for any small states interested in embracing cooperation and co-creation in GovTech.

No "One Size Fits All" Approach

No matter how small, each state is unique in terms of its history, context, and experience of state modernization. Thus, if you are in the position of being a technical advisor or government representative that is supporting a small state with digital transformation, you need to dedicate time to fully understand to local context and work closely with local stakeholders in creating something that addresses their unique needs.

As a good example, **NRD Companies** supported the Ministry of Digital Transformation of Trinidad and Tobago with creating their unique GovTech open innovation framework, titled Developer's Hub (D'Hub). While this process utilized the experience of the GovTech Lab from Lithuania, D'Hub Challenge Series, a first of its kind in the Caribbean, was co-created by GovTech practitioners from **NRD Companies** and public institutions of both states, and expanded beyond the practices in Lithuania by focusing on not only creating robust GovTech solutions but also supporting the nascent local developer community of the country. This is a great example how innovative approaches can combine best practices from other states with local context and needs, as well as efficiently blend experiences from both public and private sectors.

Left to right: Andrius Petrauskas, Mrs. Mathabo Mokoko (The Revenue Services Lesotho Commissioner General), Michailas Traubas, Andrius Kaikaris, and Julius Zubė from NRD Companies

Another example of this lesson learnt comes from **NRD Cyber Security**'s experience – the Lithuania-based company supported Kingdom of Bhutan in its journey to more resilient digital transformation. Back in 2016, the NRD Cyber Security worked in Kingdom of Bhutan on setting up a fully operational BtCIRT within the Department of IT & Telecom (DITT) in the Ministry of Information and Communications in order to coordinate information flow, respond to and manage cyber threats, and enhance cyber security in the country.

In 2023-2024, **NRD Cyber Security**, in cooperation with The World Bank, had another opportunity to work in Bhutan – the company provided technical

NRD Cyber Security team (in the middle: A. Stanelytė and T. Jakštas) in Bhutan, GovTech, during onsite mission, 2024

assistance to the Government Technology Agency (the GovTech), which took over the functions of (Department of Information Technology and Telecom) DITT. During the implementation of the project, **NRD Cyber Security** worked with the BtCIRT specifically, in developing a final draft of proposed National Cyber Security Strategy and an action plan for its implementation as well in drafting a proposed Critical Information Infrastructure (CII) list and development

of an action plan for the Government's consideration to proceed with subsequent steps to develop a robust CII protection program.

The strong involvement of the local stakeholders helped to achieve results that were tailored to the specific ecosystem of the country. This project has been supported by the Cybersecurity Multi-Donor Trust Fund under the broader Digital Development Partnership (DDP).

Digital Transformation Is Not Just About Digital

Every country has its challenges in fast-tracing public sector modernization, which are often not about technology but about "soft" factors: institutions, processes, and mindsets. Are the institutions ready to open up, cooperate, and break out of their traditional silos, while placing the citizen at the center? Are they ready to embrace the wholistic transformation of the government, beyond the mere digitalization of the existing processes? Lithuania's experience in cooperation of Lesotho well-illustrates the importance of this approach. **NRD Companies** is currently implementing a project with the Revenue Services Lesotho (RSL), focused on developing an e-invoicing system that will help the RSL to make its revenue collection processes more

effective and ensure compliance among taxpayers. In this case of co-creation, the project not only aims to simply develop a dedicated e-invoicing system, but also aims to comprehend and address the unique challenges of revenue collection in the country, as the development of the technology is accompanied by implementation of the necessary legal changes, internal organizational changes, and awareness raising in the population. The experience of this project showcases, that only when such comprehensive approach and close cooperation of institution's and expert's teams is embraced, one can expect that the introduction of a dedicated digital systems will lead to efficient positive changes in the overall tax ecosystem.

The development of e-invoicing system in Lesotho was kicked-off by thorough discussions between Revenue Services Lesotho and NRD Companies about unique revenue collection needs in Lesotho

Another good example is **NRD Cyber Security**'s work in Rwanda. It is well-known that the Government of Rwanda has placed ICT as a central tool for its transformation and to facilitate its service delivery across all sectors. However, as mentioned before, cybersecurity is a foundation for digitalization, and it is essential to understand the starting point of the state. The Cybersecurity Capacity Maturity Model for Nations (CMM) developed by the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford, provides a framework that helps states to understand what does and does not work across all areas of cyber security and can compare cybersecurity capacity across different nations over time.

In partnership with the GCSCC, **NRD Cyber Security** conducted a cybersecurity capacity maturity review in the Republic of Rwanda in 2022 at the invitation of the National Cyber Security Authority. The aim of this review was to enable Government of Rwanda to understand how to strategically prioritize investments in cybersecurity capacity using the CMM. This activity was part of the Joint Integrated Cyber Analysis Project (JICAP), which brings together a range of proven cyber capacity building programs and projects under one integrated approach.

In addition to the implementation of CMM model, National Cyber Risk Assessment was performed by UK Home Office and development of National Cyber Strategy was done by International Telecommunications Union.

Ensuring Coherence of Interventions

In order to prevent duplication of efforts and to ensure that projects are designed to achieve relevant results for the states, it is vital to coordinate cyber capacity-building and digital transformation-related interventions among donor organizations as well as recipient states in the planning and implementation phases. For instance, during the design and implementation of OCWAR-C (West African Response on Cybersecurity and Fight against Cybercrime), considerable effort was made to foster synergies with existing projects at the regional and national levels. This was done to ensure that the project did not duplicate current or planned activities or solicit the same interlocutors for the same actions.

Building Trust Is Critical

True change, whether in the case of digital transformation or any other type of reform, only starts when sincere relationship is built between the government/institutions and external experts/advisors. For teams working in different states/setups it is critical to understand the motivations, needs, fears, and doubts of all parties involved. When entering a new state, institution, or team, we must demonstrate the value and experience that is being provided to the intended beneficiary while also being prepared to listen and understand.

The good example is close relationship established between the government of Belize and **NRD Companies** during the development of an online Business Registry System (OBRS). This digital solution marked a breakthrough for the country's e-government progress, providing the first digital government services in Belize and transforming the way businesses are registered in the country, improving transparency, and promoting accessibility to information in the country. As indicated by the government of Belize, this breakthrough was achieved largely due to close cooperation between the **NRD Companies** and Business Registry team, including a large focus on ensuring that **NRD Companies** team fully comprehends the unique institutional processes and challenges faced by the Business Registry in Belize, which led to the implementation and launch of the system twice as fast than other projects of similar nature.

Sustainability of Project Outcomes

Sustainability of project outcomes is a paramount element in the planning as well as implementation of digital transformation and cyber capacity-building interventions. While implementing various projects internationally, companies observe that sustainability-related activities are usually much appreciated. During their capacity building projects, both **NRD Companies** and **NRD Cyber Security** teams strongly focus on institutional capacity building, sensitization of the high-level government officials as well as knowledge transfer to local experts through train-the-trainer events, preparation and dissemination of awareness-raising materials, etc. It has been proven that these activities can help to ensure the sustainability after the project is implemented, and the recipient country received an actual positive impact.

Insights for the Future

With all these lessons learnt in mind, Lithuania's experience in small state co-creation provides the following insights for the future:

Secure Digital transformation requires mindset shift.

It's going beyond just implementing digital tools, as "soft" elements of any digital transformation – policies, regulations, processes, institutional setups, capacities of staff, awareness of users – are crucial for overall success. Such holistic approach ensures true transformation, not just digitalization.

Small states have unique digital transformation needs and require tailored solutions.

Collaboration between different actors further drive innovation and ensure application of relevant practices according to the actual context of a country. Cooperation among states that can relate to each other's situation can further ensure that everyone's needs are taken into account.

Successful collaboration requires a combination of trust and openness.

Complex government challenges often require expertise beyond traditional bureaucracies. Co-developing with private companies, combining international and

domestic expertise, unlocks a wider pool of talent and ideas, fosters solutions tailored to local needs while growing and empowering local talent.

In conclusion, navigating the dynamic landscape of secure digital transformation can be daunting, especially for resource-constrained small states. Therefore, it's recommended that countries begin with modest steps, focusing on essential measures to initiate progress towards establishing a secure digital ecosystem. As highlighted, co-creation and cooperation offer a powerful solution, fostering knowledge exchange and accelerating innovation journeys, especially within a region.

About the Contributors

NRD Companies is a global, Lithuania-based GovTech and Fintech focused group of companies providing out of the box solutions and bespoke development along with subject matter consultancy services for public and private organizations. With over 27 years of experience and a track record of successfully completing more than 350 projects spanning across 55 states.

More information: **https://www.nrdcompanies.com/**

NRD Cyber Security is a Lithuania-based company that offers cybersecurity solutions, consulting, and other services. The company creates a secure digital environment for countries, governments, and organisations and implements cybersecurity resilience enhancement projects around the world. NRD Cyber Security has more than 10 years of experience and has implemented more than 1000 projects in more than 50 states.

More information: **https://www.nrdcs.eu/**

Infobalt is a DigiTech Sector Association to create the best conditions for technology application, market development and export. The company is a locally and internationally recognized representative of the Lithuanian ICT industry. The association unites more than 160 strong members, including national and global businesses, universities, education and research institutions, with a network of 10,000 experienced ICT professionals.

More information: **https://infobalt.lt/**