OSCE PA

BIRMINGHAM

29TH ANNUAL SESSION OF THE OSCE PARLIAMENTARY ASSEMBLY

2 - 6 JULY 2022

Special Representative on Digital Agenda Radu-Mihai MIHAIL

January - July 2022

Report of the Special Representative on the Digital Agenda to the OSCE PA Annual Session

Mandate

OSCE PA President Margareta Cederfelt (Sweden) appointed Radu-Mihai Mihail (Romania) as Special Representative on Digital Agenda in January 2022.

- Raise awareness within the OSCE Parliamentary Assembly regarding the benefits and the security implications of the digitalization process;

- Promote within the OSCE area an inclusive digital society which benefits from all research, technology and innovation initiatives that enable future technologies, software, networks and services, including in the areas of transport and urban mobility;

- Facilitate, in close consultation with the OSCE PA's General Committee on Political Affairs and Security, co-operation and discussions among OSCE PA delegations on how to increase information exchange and awareness in the field of cybersecurity in OSCE participating states;

- Monitor the developments on digital transformation in the OSCE region;

- Monitor the acceleration of the digital transformation during the Covid-19 crisis and post-pandemic implications;

- Communicate with relevant actors within the OSCE and work in close co-operation with the OSCE PA Second Committee.

Birmingham, July 2022

Focus

OSCE's mission is to enable security in Europe, security for all the member states. To reach a strong security environment, the strength of independent, sovereign democracies is paramount. And in modern days, a strong democratic state and its efficient administration are enabled by a strong and secure digital services environment.

01 Digitalisation in times of crisis

The implementation of digital solutions has accelerated during crises, such as the pandemic and the war in Ukraine – it is therefore important to analyse their impact and understand how they can enable even further the positive transformation of the societies in the OSCE member countries and beyond.

02 Digital public administrations

Attention should also be given to the digital transformation of the public administration, of the electoral processes and their impact in strengthening democracy and contributing to the OSCE area security by deterring corruption, and by assuring the transparency and resilience of the democratic processes in each country.

As a key challenge to the digitalisation of our societies that we need to tackle, it is obvious that **Cybersecurity** also requires our continuous attention.

Working sessions

Having as a milestone the Annual Session in Birmingham, the 6 months of mandate consisted of monitoring the developments on digital transformation in the OSCE region and facilitating co-operation and discussions among OSCE PA delegations on how to increase information exchange and awareness in this field. By exchanging with participating States that have made significant progress in specific areas, it is possible to bring to the table insights for members that have until now only marginally benefitted from the opportunities offered by digitalization.

Bucharest, Romania

throughout March

Director of the Romanian Digitalisation Autority, Dragoș-Cristian Vlady
Head of Ops, Cybercrime Programme Office for the Council of Europe, Virgil Spiridon
Technical Deputy Director of the Special Telecommunications Service, Mădălin Mihai

Copenhagen, Denmark

5th April

Vice-Chair of the Business Committee, Danish Parliament, Kasper Roug
Deputy Head of the Delegation of Denmark to the OSCE PA, Malte Larsen
Deputy Director General, Danish Agency for Digitisation, Mette Lindstrøm Lage
Danish Parliament MPs, Orla Hav and Lisbeth Bech-Nielsen

Nicosia, Cyprus

25th May

Deputy Ministry of Research, Innovation and Digital Policy, Kyriacos Kokkinos
Commissioner of Communication George Michaelides
Director of the Digital Security Authority, Antonis Antoniades
Chief Officer of the Digital Security Authority, Diamandis Zafeiriades
National Computer Security Incident Response Team (CSIRT)

London, United Kingdom

1st July

Chair of the Communications & Digital Select Committee, House of Lords, Baroness Stowell
Cyber Director at the Foreign, Commonwealth and Development Office, Will Middleton
Head of Research & Insights, Government Digital Office, Liz Lutgendorff

Preliminary take-aways

During the working sessions held in Bucharest, Copenhagen, Nicosia and London, the following key conclusions were preliminary drawn.

01 A long-term approach on digitalisation

Nowadays, to be considered successful and sustain funding, any technology initiative needs to demonstrate measurable return on investment and this is particularly relevant for governments' aim to reform and digitalise. A long-term approach is needed, one that delivers quantifiable results and builds up trust and reliability. One particular challenge identified during the discussions is the procurement of human resources. Cyprus is currently relying on hiring talents from outside the country. In the long-term this problem can only be overcome by reforming the educational system.

02 Building trust with the citizens

When adequate safeguards are in place, technology can play a vital role in strengthening the citizens' interaction with the state, thus improving the quality of government, meeting people's needs and expectations, and ultimately contributing to greater trust in public institutions. Nevertheless, prior to fostering the use of technology, governments need to dispose already of a certain level of trust in order to assure the adoption of the intended digital transformations. Skepticism in some technologies, such as the cloud infrastructure, is however present even within government and public structures.

03 Collaboration within and beyond borders

One significant similitude among the prospected countries was the existence of a dedicated body responsible for citizen-centric public digitalisation, through the form of governmental agencies. Their main role is to interact with all institutions and assure the coordination of the digitalisation efforts nationwide. In order to do so, they often learn from the experience of other countries and therefore, extensive collaborations in the form of MoUs exists between digitalised states and those in process of transformation (such as Cyprus and the UK).

04 Cyber security: an ongoing process

Cybersecurity is key in keeping data secure, digitalisation sustainable and citizens' trust intact. In order to do so, it must be equipped with: resilience through risk management and implementation of security measures, training and capability development, effective response through crisis management and creating a security culture. Building the cybersecurity infrastructure thus required is and will continue to be an ongoing process, given the constant technological progress states must adapt to.

Preliminary take-aways

The digital transformation of public services often comes as a response to ongoing crises. Most recently, the Romanian government in partnership with the NGO Code for Romania, developed an online platform, Dopomoha.ro, in order to assure a reliable source of information and organisation of resources for Ukrainian refugees coming to Romania. This was put in place in just a couple of days, which was only possible following the recent covid-19 crisis. The past two years paved the way for a digitalisation wave. The need to assure remote access to public services gave governments no choice, but to have targetted, mandatory services made digital fast. However, it has also been noted that the covid-19 pandemic in general also diverted many resources that could have been allocated to the execution of national digital strategies and wider long-term projects, such as, but not limited to, building a strong cloud infrastructure or developing further cybersecurity capabilities.

At the core of all national digital strategies the implementation approach of new, digital services must follow the fundaments of project management, similarly as in the private sphere because the use of new technologies demands an agile, highly adaptive environment. In this context, the responsible entities must benefit of autonomy and be ready to continuously develop its capabilities in terms of human resources, attracting talents and experts in the field.

Digitalisation through collaboration within as well as beyond borders

The co-operation among countries (also through parliamentarians) plays a crucial role in this regard. The discussions focused on the way the beneficiary, which is the state, the provider and usually, a supranational body are sharing competences and knowledge. Governments collaborate beyond borders to tackle the challenges of digitalisation, not only because such bodies offer the technical support required for the implementation phase of digital transformations, but also bring examples of good practices and lessons learnt from the past. For instance, the Cybercrime Programme Office for the Council of Europe provides on-hand support and technical knowledge, being ready to cooperate with any OSCE member state and help build the legislative framework required. This is particularly relevant for parliamentarians. And their role is not limited at legislative level, it also involves opening the debate at a larger scale, whilst gathering at the same table all stakeholders of digitalisation. This implies a continuous debate on the country's digital strategy and the development of a long-term vision in this regard.

Furthermore, countries engage bilaterally both in the interest of their digitalisation process, as well as to help other countries that are early into the process and can learn from them. Such is the example of Cyprus who has a memorandum of understanding with the United Kingdom on the development of their digital government services, but also is signing MoUs with third countries and pass on their experience further as well (most recently with Albania and Kazakhstan).

Building trust with the citizens: between digital adoption and security

Another highlighted topic during the discussions was the relationship between the state and its citizens. More specifically, digitalisation is both an opportunity and challenge in fostering a closer, more efficient relationship with the citizens. In Estonia for instance, people were reserved regarding the public sector's capacity to bring added-value and the way it intended to introduce digitalisation. This is why the government focused on building trust as part of its digitalisation strategy.

It has been highlighted that trust must not only be gained in order for citizens to start using the digital services, adapting to change, but it must also be maintained. In Denmark, multiple cases of IT issues and data security incidents made it to the headlines of the public opinion, generating mistrust in the system and hence damaging the citizens' confidence in the government's way of managing their data. This is where cybersecurity steps in as a continuous journey. A digital government service must be user-centered, but also agile and have the right capabilities to stay up-to-date to new threats and the technological progress.

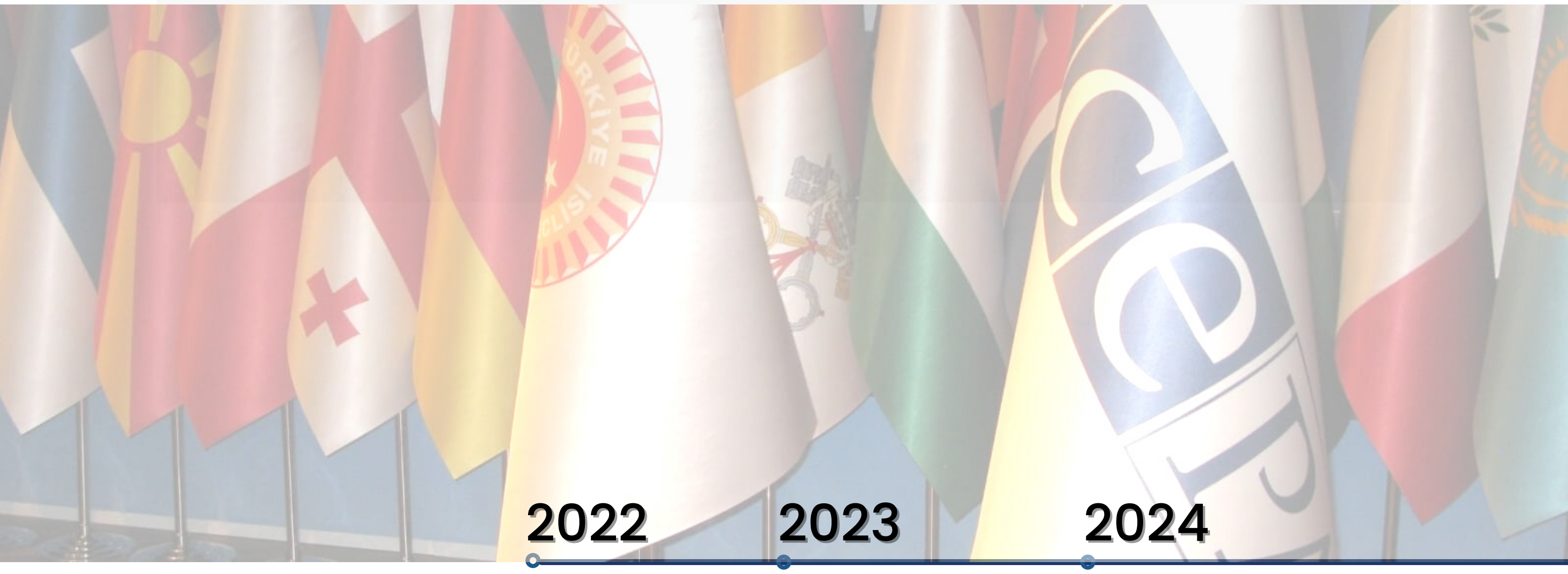
Next steps

The past months have consisted in a research phase through interactions held with various actors in the field of digitalisation in Romania, Denmark, Cyprus and United Kingdom. As next steps, we have identified further topics to be validated starting from the above presented preliminary take-aways:

- better understanding the way in which bilateral relationships are created in form of memorandums of understanding between two countries or a country and an international organisations in order to prospect and present the opportunity it may represent for other OSCE member states;
- further engage on the topic of digitalisation of the electoral systems and prospect the wide range of solutions, from machine voting or partial e-voting for those living abroad to a fully digitalised model;
- gathering additional insights and best practices on the budgeting, funding and performance measurement of digitalisation.

As part of these directions, the role of cybersecurity and of the cross-border co-operation in this field is also important and will be reviewed.

Moreover, on a long-term timeline, there is a potential of contributing to the digital agenda through information exchange sessions held in OSCE member countries with a particular interest. The participation of member states' parliamentarians from countries at an earlier stage in the digitalisation process can increase the awareness on the topic of digitalisation in the OSCE region. Lastly, the 2024 Annual Session to be held in Romania can represent an opportunity to organise a dedicated side-event on the Digital Agenda.



2022

Data-gathering interactions building upon the preliminary conclusions

2023

Information-exchange sessions with the participation of OSCE member states

2024

The prospect of organising a side-event on the digital agenda with the occasion of the 2024 Annual Session in Romania