International Review of the Red Cross (2020), **102** (913), e1–e6.
Digital technologies and war
doi:10.1017/S181638312000034X

IRRC_

Interview with Prime Minister Jüri Ratas of Estonia*

Jüri Ratas has been Estonia's Prime Minister since 2016 and is currently serving his second term in office. From 2007 to 2016, Ratas was Vice-President of the 11th, 12th and 13th Estonian Parliament. He was elected to the Tallinn City Council in 2005, 2009 and 2013, and served as the city's Mayor from 2005 to 2007, and as its Deputy Mayor from 2003 to 2004 and during 2005. His service in the Tallinn administration started when he was elected Economic Adviser to the Tallinn City Office, a position he served in from 2002 to 2003. Prior to holding this post, he served on the board of OÜ Värvilised from 1999 to 2002. During his time in office, Prime Minister Ratas has supported Estonia's various State-led digital transformation processes. In this interview, he reflects on how the "digital State" of Estonia has relied on digitally rooted solutions to tackle the COVID-19 pandemic. He also provides insights for the humanitarian sector on digital transformation processes, private–public sector collaborations and preventive digital approaches, such as investing in digital literacy and education, that can help mitigate the potentially adverse effects of digital advancements.

:::::::

Can you give us an overview of some of the key State initiatives that have positioned Estonia as the world's leading "digital State"?

Estonia's success comes down to the combination of education and key technological advancements that have shaped the mindset. This means we have been open to taking steps towards an electronic way of life and a digital State.

The interview was conducted on 7 July 2020 by Saman Rejali, Thematic Editor for the *International Review of the Red Cross.*

* Since this interview first published, Juri Ratas is no longer in office and his views should not be regarded as reflective of the current Estonian government.

Underlying all of this is trust within society. Transparency and ease of use of systems need to go hand in hand with cultural changes, particularly educating the users and civil servants on good and bad practices on an everyday basis. Building a digital State is a never-ending process; there is always room for improvement, and Estonia is constantly mapping and building on new opportunities.

The fundamental pillars for this success have been the adoption of secure digital government-issued identity cards for every Estonian resident and a secure distributed data exchange layer, which we call X-Road, in 2001. Identity cards and the data transfer system are building blocks that enable us – both the government and the private sector – to build any kind of service and serve the Estonian people hassle-free.

Can you tell us about how Estonia has adapted its use of digital technologies during the COVID-19 pandemic to ensure continuity in its government processes and functions?

Prior to COVID-19, I was often asked, "But what happens when the Internet goes down?" Nobody asked, "What if the physical infrastructure fails?"

For the past twenty-five years of building a digital society, Estonians have been preparing their systems to function in any situation. While the global pandemic and its economic circumstances have had an impact on Estonia, I would argue that we are one of the best-prepared societies to tackle these types of situations. We are the only country that can do almost everything online. We are accustomed to voting, paying taxes, making decisions and signing contracts electronically. Of course, we had to make some adjustments to our processes, and yes, people were staying home on a voluntary basis where possible, but to a great degree it was business as usual.

People worked and studied from their homes and often from their remote country cottages, where social distancing was easier for families. With access to electronic tools, they could continue to sign documents and do their work in this extraordinary situation.

I am grateful to all the doctors, nurses and other medical staff who consulted as many patients as possible remotely using a mix of digital technologies. During the public health emergency, patients were able to avoid visiting doctors for prescriptions because 99% of medical prescriptions are issued online in Estonia.

And while school buildings were closed, children, like my own kids, continued studying over e-school platforms, with all classes running smoothly during the last few months.

Given the success of Estonia's e-governance mechanisms, what can other countries and sectors, particularly the humanitarian sector, learn from and emulate in this regard?

The humanitarian sector has been built on multilateral willingness to help others. Helping others in the global context is based on trust. We are optimistic that the humanitarian sector and the multilateral network of international organizations can learn from the Estonian example of community-building, using modern tools to create a sense of belonging. Most importantly, our model allows us to preserve privacy and offer efficient service delivery without trading one for the other. In order to preserve the privacy of individuals, we need to have a secure digital identity. In order to build mechanisms that work, the humanitarian sector needs to learn about distributed governance, because a centralized system will not be able to adapt as easily to all of the potential changes of the future. This is mainly a governance issue rather than a technological problem.

What steps has Estonia taken to protect the data of its "e-residents"? Why does the country focus on personal data protection? Why has this been pivotal to ensuring that the positive effects of using digital technologies outweigh the negative effects?

In 2014 we started issuing digital identity documents to people from all over the world, under the e-Residency programme. This opened the lively digital ecosystem up to new global users who have been carefully vetted. The same rules that apply to our citizens' data also apply to the data of our approximately 70,000 e-residents. The owners of all information systems are responsible for data protection and rule compliance, and the X-Road system is based on the principles of distributed architecture: there is no one large database or institution that would have access to all of the data.

Data protection, information security and sustainability are very important for Estonia given our high levels of digitization. People are owners of their own data and can review who has viewed their data.

Can you tell us a little bit about the Estonian government's efforts to ensure there is widespread digital literacy among the country's citizens, especially in light of the COVID-19 pandemic? Why is this important for the country and for other actors that are undergoing digital transformations?

Looking back, it feels like we were reasonably well prepared for the pandemic. Of course, when we prioritized people's digital skills in our education and digital strategies, we were not thinking about the necessity of making everything work remotely, but rather bearing in mind the idea of promoting equality and competitive advantages for our people, which prove useful in digitally transforming economies.

Addressing students' digital skills has been a norm of our education system for some time already – it is obligatory for general education schools to develop the digital competencies of students, and for vocational education and universities to address digital skills. We have many different initiatives for every possible target group available to support the development of digital skills. In addition to promoting these skill sets through formal education, there is mid-career retraining, local initiatives by regional authorities, tailor-made programmes by different organizations, cooperation programmes with employers and libraries etc.

Additionally, the Information System Authority, the agency responsible for the backbone of digital identity and cyber security, focuses on both public awareness-raising and making sure the services developed are secure.

Of course, one thing that we have learned from the COVID period is that we need to pay even more attention to skills and knowledge related to cyber security at all levels, from the average user's point of view to the core experts, in order to ensure that our e-services are functioning safely in the future as well. Additionally, as the digital traffic patterns changed dramatically in this transition to remote work, digital service providers had to assess and sometimes reallocate bandwidth to ensure connectivity where and when needed.

What are some of key areas of investment and lessons learned that have been pivotal for the implementation of Estonia's digital ambitions? How do you think the humanitarian sector can draw from these experiences?

The fundamental investment for building a new model for a society is education and access. Estonia started a vast educational programme called Tiger Leap in 1997. This has been key to getting people to use and trust digital services. Investments in education went hand in hand with investments in technical infrastructure. As a first step, this has meant connectivity for schools, libraries, municipal service centres and other public buildings.

One of the lessons learned from that period was that it is not necessary for everyone to have the Internet at their fingertips to start building a digital society. Therefore, Estonia has to a great degree used digital services to enhance the offering, not to replace paper-based options. This way, the users are offered choice and convenience and are also allowed to build trust and habits slowly. It has been well documented that such habits – often regular electronic banking – build trust in the whole ecosystem and facilitate the growth of less-often-used digital services such as elections.

Many actors around the world are now following Estonia's lead in putting together and implementing institutional "digital strategies". What advice would you have for these actors, based on your government's experiences with creating a digital future?

Start small, and don't be afraid to test different ideas – finding ways to digitalize specific services that have many users, like medical prescriptions, is already a big step forward. Also, the Estonian digital State relies on strong partnerships between the public and private sectors, which is a great model for other countries as well. However, it is not about copying what works for Estonia, but about finding a way to achieve digital transformation that works within the existing system.

Estonia has led the way in terms of State-driven public–private partnerships used to advance digital transformation. For example, Estonia has worked with

Microsoft on information technology principles and "digital continuity". Can you tell us about some roadblocks and positive outcomes that the country has faced in cementing these partnerships? In your opinion, what lessons learned are there for other public sector actors and States?

Estonia has been fortunate to have a community of skilful technical experts constantly advising the government. Most of these experts work in the private sector but form a community we often refer to as the "collective brain" that works together on developing the digital ecosystem. This means constant discussion and debate.

Estonia has unique knowledge of digital transformation that we are open to sharing with other countries. For example, we have worked with countries like Finland, Iceland, Germany, Japan, Cambodia and many others to implement the secure data exchange layer X-Road in these countries. In the current COVID-19 situation, we have been working with humanitarian organizations and countries needing assistance to support their fight against the pandemic with digital solutions. For example, the Estonian company Cognuse is working with the Kenyan Red Cross to implement the competence support tool CoNurse, which will help field nurses who lack experience in their work and help them make better decisions quickly. And speaking of working on digital transformation with international organizations and the wider International Red Cross and Red Crescent Movement, we are also working with the International Committee of the Red Cross on data protection; with the Office of the UN High Commissioner for Refugees on electronic ID; and with the World Health Organization on interoperability matters. During our May 2020 presidency of the UN Security Council, we also used a lot of different digital solutions.

The main lesson learned in Estonia is that the technical expertise usually lies in the private sector. If the public sector learns to trust and cooperate with the private sector, the transformation can truly bear fruit.

Estonia has carried out laudable work on cyber security. How big a threat to international security is instability in cyberspace? How has this been impacted by the COVID-19 crisis? And what are existing or desirable mechanisms to address this threat?

In 2007, Estonia experienced coordinated cyber attacks – government institutions, media, banks and e-services were targeted. This highlighted how cyber security is a matter of national security. As a result, we were the first or one of the first countries to have a national cyber security strategy. Now most countries have one.

In 2017, a flaw was discovered in the chips of our national ID cards – a building block of our digital society. We handled it very openly and publicly, in order to maintain trust in our e-government. A fix was implemented before the flaw could be taken advantage of, and that same autumn more people used internet voting during elections than ever before.

The COVID-19 crisis has put extra pressure on critical services in terms of cyber security. Many everyday functions and operations have moved online. Therefore, the need for a secure and functioning cyberspace is more pressing than ever.

We join those strongly condemning cyber attacks targeting hospitals, medical research facilities and other essential infrastructure, particularly during this global pandemic.

UN member States as well as our NATO allies have agreed long ago that existing international law also applies in cyberspace. We hold the strong view that existing international law provides comprehensive guidance for State behaviour regardless of the domain. By following this simple principle, the behaviour of States in cyberspace can become more transparent and predictable.