RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 213 – 28 December 2020

Global Health Security:
COVID-19 & Its Impacts

Small States and COVID-19: Estonia's Approach

By Deep Datta-Ray

SYNOPSIS

Estonia's digital infrastructure and IT savviness, developed since the mid-1990s, helped manage the COVID-19 pandemic. The Baltic state is cushioning the effects of post-globalisation and associated threats with increased international cooperation in digitalisation and cyber governance.

COMMENTARY

WITHIN A month of the first case of COVID-19 in March this year, Estonia had over a thousand cases. A state of emergency was declared and borders were closed, yet disruption was reduced because of Estonia's digital capacity and capability. Both helped stabilise infection rates which eventually led to the easing of the lockdown and creation of a Baltic "travel bubble" in May.

Despite a second wave of infections across the continent, measures to control COVID-19's spread in Estonia proved effective. This month Fitch, a major credit rating agency, revised downwards the contraction of the Estonian economy from 4.9 percent to 2.9 percent. Fitch forecasts robust recovery in 2021.

Navigating 'New Normal': First-Mover Advantage

The challenges of navigating the "new normal" are met by a strategy of increased digitalisation and more international cooperation, particularly with the other small states around the world. Tallinn, the capital of Estonia, remains entrenched in the

European Union while maintaining close ties with the United States. These decisions are helping to cushion the effects of post-globalisation.

Estonians believe their government has insulated them from the economic downturn brought on by COVID-19, and from potential threats arising from their powerful neighbour, Russia. At the same time, Estonians feel vulnerable to the intense geopolitical rivalry and competition between the US and China, and the EU still finding its footing.

Estonia's digital advantage is due to its early embrace of IT since the mid-1990s. By 2002 Internet access was deemed a human right, but digitalisation became extensive with the digital ID. Usable across the public and private sectors, the ID is for both public and private use. For instance, the ID could be a driver's licence and an access card for a private, paid, gym membership. The private sector is an active participant in making the digital ID of practical value to Estonians.

Estonia was also confident about digital security at COVID-19's onset. In last year's elections, 43.8 per cent of the vote was electronic. Training in online safety was widespread and 87 per cent of schools were using e-learning by 2020. Financial transactions too, were largely online.

Since 2009, pensions and social benefits have only been paid electronically and 96 per cent of income tax declarations are online. The security measures in place and the population's familiarity with them is why the incidence of online crime went up only marginally during the pandemic.

The lockdown was therefore transitioned into rather seamlessly. For example, Estonia's University of Tartu switched to online teaching overnight. Already-in-place online health records and e-prescriptions allowed doctor's quick redeployment to manage the pandemic. Infections were also reduced by the widespread availability of contactless options. This extends to border crossings.

Countering the Pandemic

The existing system facilitated quick implementation of new policies to counter the pandemic, such as minimal punitive actions on tax arrears. The tamper-proofing of IT systems enabled the labour laws to be updated despite their complexity arising from many more inputs required to make the system reliable in times of pandemic.

Even though this so-called digital inheritance dampened concerns about data security and permitted the rollout of the contact-tracing app HOIA, the government constantly assesses its technology and vulnerable points. Hence, the University of Tartu's funding was topped up with 880,000 euros in November to extend studies of the efficacy of the government's emergency measures with the goal of an orderly exit from the emergency situation.

That remains contingent on managing global infection rates, for the opening of borders is inevitable. Hence Estonia's conception of the "new normal" is to build on its first-mover advantage, with its acknowledged successes, and to promote more international cooperation on digitalisation. Reiterating the need is the rapid uptick in

infection cases and deaths since the onset of autumn, despite earlier successes in pandemic containment.

Estonia hosted an online ministerial conference on digitisation in July which was attended by more than 60 countries, and is currently co-sponsoring with Singapore, a global declaration arising from the meeting titled, “Close the Digital Divides: the Digital Response to COVID-19”.

The declaration prioritises international cooperation to re-focus resources for a digital transformation. This includes reinforcing digital capabilities for health care as well as e-commerce, implementing e-education and improving digital literacy, and ensuring secure digital spaces while broad-based connectivity and e-governance are embedded.

The co-chair of the Group of Friends on e-Governance and Cybersecurity at the United Nations (UN), Singapore’s Foreign Minister Vivian Balakrishnan, explained the declaration intends to empower people against COVID-19 by allowing safe access to services, and to reopen borders by, for instance, speeding up contact tracing. Moreover, the “digital future” rides on international cooperation to build resilient and trusted networks within the UN framework.

Cushioning Post-Globalisation Threats

Post-globalisation for Estonia sees a dangerous intensification of disagreements between its closest allies, the EU and US, as well as of threats from China and Russia to Tallinn’s sovereignty and strategic autonomy.

Estonia is managing these by committing to the “fundamental interest of small states to defend multilateral cooperation and a rules-based order”. Tallinn therefore is increasing trade and digital cooperation with more small states. For example, Estonia and the United Arab Emirates recently agreed to recognise each other’s driving licences, which are now issued digitally.

The EU is Estonia’s bedrock for negotiating the post-globalisation landscape. Tallinn demonstrated its commitment to the EU by doubling down on the EU’s climate change targets. The EU welcomed Tallinn’s pandemic management and cited it as an example for emulation to other EU countries.

The US remains a close ally and cooperation now extends to increasingly sensitive matters of online security. Prior to November’s US presidential election, US Cyber Command operatives visited Tallinn to observe Russian hackers attacking Estonian IT systems, and be trained to counter them.

Looking Ahead

The pandemic is buffeting EU-US relations, in particular, on resuming business and travel; working with the World Health Organisation (WHO) on vaccine development and distribution; and on blaming China for originating COVID-19. Estonia sought, in vain, to ameliorate disagreements between allies on combatting the infection. Tallinn

therefore seeks a closer alliance with the EU and US to help mitigate threats from China and Russia.

Apart from territorial disagreements between Estonia and Russia, Moscow is likely also responsible for several cyber-attacks and disinformation campaigns. The massive hacking of the Baltic state's parliamentary, government, and banking systems in 2007 left an indelible mark on Estonian psyche.

Tallinn was drawn into Sino-US rivalry, when it signed a memorandum with the US on strengthening digital cooperation and restricting products from the Chinese manufacturer Huawei. This year, the Estonian Foreign Intelligence Service observed, "it is important to understand in the eyes of the Communist Party of China (CPC), decision-makers in other countries are only useful pawns to help implement CPC strategies". Beijing's calls to have the report amended were met by Tallinn calling for more unity within the EU.

Estonia's digitalisation strategy enabled it to weather the pandemic. Nevertheless, the global milieu remains uncertain. Similarly, the cyber domain is fluid, as technologies constantly evolve, and international norms and regulations remain unsettled. In short, small states remain vulnerable.

Deep Datta-Ray is a Visiting Senior Fellow at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. He is author of The Making of Indian Diplomacy: a critique of Eurocentrism (New York, OUP: 2015). This is part of an RSIS Series.

Nanyang Technological University
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg