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

RSIS COMMENTARY

www.rsis.edu.sg No. 121 – 29 August 2023

Digital Security's Place in Human Security

By Tamara Nair

SYNOPSIS

In today's world where digital technology plays a critical role in our daily lives, digital security has become a paramount concern. Since digital technology can be sabotaged or attacked to create various insecurities for people, digital security should be made a key element of human security.

COMMENTARY

When the concept of human security was introduced in the 1994 Human Development Report, the authors focused on the fundamental deprivations and hardships suffered by human beings. While there had been "unprecedented human progress", there was also "unspeakable human misery". The report dealt with the various dimensions related to the well-being of human societies: water, food, energy, health, the environment, the individual, and the community.

That the world would transit so rapidly into the digital age was not a development many foresaw at the time. The increasing reliance on digital platforms and the Internet has exposed individuals and societies to the threats related to each of the above dimensions, making it imperative to view digital security as an essential and integral component of human security.

As such, digital security protection should move beyond state-centric definitions such as cyberattacks on state operations or structures. In fact, digital security should be extended to the defence of human lives and critical infrastructure securing food, water and energy, making it vital not only to national security but to human security as well.

Digital Technology and Human Security

Human security, which relies heavily on sustainable development, is dependent on

digital transformation: the process of adopting and implementing digital technology to better access, manage and distribute the requirements needed for the well-being of societies.

The following examples illustrate how human beings have become dependent on digital technologies for their well-being, hence leading to the need for digital security.

Digital technology plays a crucial role in safeguarding environmental and energy infrastructure, such as power grids and oil refineries. Digital technology also plays a crucial role in monitoring and managing the impacts of climate change. From weather forecasting to climate modelling, digital systems provide valuable insights for climate adaptation and mitigation.

Digitalisation is increasingly used in agriculture, food production, and water management systems, helping in crop monitoring and irrigation management. These agricultural systems rely heavily on technologies, such as sensors, drones, and automated machinery.

Digital technology also plays a crucial role in protecting water infrastructure – including dams, reservoirs, and water treatment plants – through access control, staff training, and regular cybersecurity assessments.

Access to digital technology is now crucial for education, employment, and social participation. Digital tools and resources have revolutionised the way we learn, made learning more accessible and allowed us to learn at our own pace. They have also transformed the working life of millions, allowing many to work from their homes or wherever an internet connection is available – workplace changes that were a boon during the global COVID-19 pandemic lockdowns.

Social connections and interactions have also been greatly expanded following the advent of social media platforms made possible by digital technology. How people communicate has also been revolutionised, with news and information transmitted almost instantaneously as events unfold.

Threats to Digital Technology, Need for Digital Security

As important as digital technology is to human lives, any disruption to its systems, through cyberattacks for instance, can have catastrophic consequences. There is a perpetual threat posed by those that seek to sabotage them.

Critical infrastructure, such as power grids, transportation systems, and healthcare facilities, rely heavily on digital networks. As digital technologies are increasingly integrated into existing critical infrastructure, including the aforementioned, it is essential to give weight to digital security to ensure the protection and resilience of these sectors.

Without adequate digital security measures, individuals and communities become more vulnerable to cyber threats. The digital age has witnessed rapid growth in the collection and storage of personal data. From social media platforms to online banking,

individuals disclose personal information, which render them vulnerable to identity theft, fraud, and privacy breaches.

Such exposures may result in psychological harm or physical threats for those, such as ethnic minorities or the LGBTQ community, who receive hate speeches made online. In such cases, the protection of communities and individuals will depend on reporting mechanisms or even legal instruments, such as the Online Criminal Harms Act, a digital security tool.

Cyberattacks that result in data breaches can compound complex emergencies like humanitarian relief efforts, increasing the vulnerabilities and insecurities of people already under stress. In February 2022, the International Committee of the Red Cross (ICRC) suffered a data breach in which servers hosting personal data belonging to more than 515,000 people worldwide were hacked in a sophisticated cyberattack. Data lost included those on missing people and their family members, as well as others receiving support from the ICRC who were victims of armed conflicts, natural disasters, and migrations.

It should be noted that some states might have used the cover of COVID-19 surveillance to intrude into the everyday activities of their citizens, including e-commerce transactions, individual movements, and social travel. In using digital means for the purpose of protecting health security, the state must also be cognisant that it can overstep into other areas of human security. Digitalisation used for human security, even when wielded by legitimate authorities, can also be a source of insecurity.

But digital technology is not a threat. It becomes one when it is used by malevolent people to attack national security. The potential threats outlined above signal the need to be vigilant and to emphasise digital security in human security concerns.

We must also anticipate and be prepared for attacks on critical infrastructure that supports and sustains human lives and activities. It can even be argued that digital security concerns should now focus more on attacks against individuals given the increasing incidents of data and privacy breaches, online hate speeches and online violence against women and girls. Failing to do so would have devastating consequences for human societies.

Expanding Human Security

The concept of human security, as introduced in the 1994 Human Development Report, must be expanded to include digital security if we are to fulfil its aim of providing for stable and secure human lives. The increasing reliance on digital platforms exposes individuals and societies to various threats, making it imperative to prioritise digital security for the protection and resilience of critical infrastructure and human well-being.

By expanding the concept of human security beyond its theoretical meaning – of providing for stable and secure lives – to include digital security, we are better able to detect blind spots in security strategies or policies. This will help in creating holistic

and targeted policies for the protection of institutions and citizens, safeguarding human security in the digital age.

Tamara Nair is Research Fellow in the Centre for Non-Traditional Security Studies, at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
T: +65 6790 6982 | E: rsispublications@ntu.edu.sg | W: www.rsis.edu.sg