CYBERSECURITY CONCERNS

Contributing to the cyber ecosystem is the next step

FARLINA MD SAID

IT seems a little too late to ask if Malaysia might be ready for digitisation. After all, Malaysia's first National Cyber Security Policy was announced in 2008 and Malaysia's pursuit of technology and K-economy dates back to the 1990s. In addition, the spread of Covid-19 drove many to adopt digital lifestyles and rely on cyber-enabled solutions such as contact-tracing to cope with the pandemic.

However, as the cyber lifestyle proliferates, so too will vulnerabilities stemming from and through the domain. Being fully digital should not forsake cybersecurity concerns. For example, the business sector may be concerned with malware, data leakage or employee cyber hygiene.

For observers of content and democracy, misinformation and disinformation, privacy and freedom of expression could be thought of disruptive factors.

Meanwhile, national security discussions would thread between known strategic issues, such as terrorism, to fears of foreign interference in one's systems.

The United Nations Group of Governmental Experts (UNGGE) and the United Nations Open-Ended Working Group (OEWG) are two international bodies pushing forward the agenda of Information and Communications Technology (ICT) security and stability. Expected to conclude next year, the iterations of UNGGE and OEWG could present views on how international law applies to ICTs as well as address the gaps in technical and political confidence-building measures.

However, while facing a myriad of cyber threats, what would these processes mean for the average Malaysian?

FIRST, is by ensuring the obligations and outcomes one would expect of governments, particularly in ensuring responsible state behaviour, investments in better mechanisms to protect critical infrastructure and ensuring networks are not misused. This could result in increased cybersecurity standards, the encouragement of security-by-design in industries as well as improvements in digital forensics.

As cyber is interconnected, its stability, security and peace would require international cooperation. Thus, in performing well to increase the standards of cyber domestically, Malaysia plays a role in ensuring a secure cyberspace beyond national borders.

SECOND, is by expanding discussions on transparency and accountability processes that could minimise risk and conflict via establishing communication or trust-building channels. These could mean sharing national cyber security capabilities and policies.

Malaysia currently has no specific policy on holding nations accountable for activities in Malaysian systems, perhaps due to the unfolding nature of international law and the developing landscape of Malaysia's own abilities. However, the lack of transparency and policy means that activities go undetected and the effect lacks precise measurements.

THIRD, is the capacity building that would improve national cyber resilience for users to enjoy the benefits of digital technologies and sustainable development. As capacity building in cyber can be anything from building infrastructure, improving national legislation and introducing new technologies, relevant projects could also aid in raising the expertise of ICT professionals. This would build confidence in and contribute to the development of Malaysian digital systems.

However, a practical implementation of any OEWG and UNGGE outcome can be challenging. Malaysia's varied views on cyber threats can create competing priorities in threat perception. In addition, threats far removed from the visible and at a low threshold of harm would not yield the impact that insists on urgency.

Compounding these circumstances and due to the wide area of vulnerabilities, the responsibility to address the threats fall across the purview of various ministries. This means information-sharing, coordination and trust between ministries is necessary to ensure the security of a cyber domain. This could also indicate the need for ministries and agencies less versed in cyber matters to pick up the portfolio.

The Malaysia Cyber Security Strategy (MCSS) which was recently launched could ensure an open, secure and stable cyberspace process. The document addresses effective governance, increases Malaysia's readiness and speaks of Malaysia's commitment to uphold international security in cyberspace.

The MCSS would not be the first in recent policies to highlight these concerns. The Defence Ministry's Defence White Paper, which was launched last year, highlighted non-traditional threats such as cyber attacks which could disrupt internal stability, cause loss of life and paralyse critical national information infrastructures.

While it seems as if Malaysia has been on this road to technological adoption for a while, the process to build a domestically and internationally secure cyberspace is still unfolding. As technological adoption increases, so must Malaysia's role to positively contribute to the cyber ecosystem.

The writer is an analyst, Foreign Policy & Security Studies, Institute of Strategic & International Studies (ISIS) Malaysia