PHILIPPINE DAILY INQUIRER

WEDNESDAY / MARCH 21, 2018
WWW.INQUIRER.NET

A10

Developing a cybersecure culture

DINDO MANHIT

The rise of digital technology has provided opportunities for growth but also created new threats and risks. Cybersecurity has become a critical concern in a modern world. With almost 60 percent of Filipinos with access to the internet, more people have become victims of cybercrime, data breach, and identity theft, among others. As the fastest growing economy in Asia, the Philippines needs to develop a "cybersecure culture" to prevent the economic consequences of cybercrimes, security threats such as cyberespionage, and other political consequences of cyberconflict in the region.

The list of reported cyberattacks that began with the embarrassing defacement of government webpages has grown to include potentially catastrophic data breaches that threaten to paralyze enterprise-scale operations. Though we have a long way to go, the accelerating shift to efficient and reliable cloud technologies has prompted stakeholders from the government, academe, and private sector to discuss the urgency of developing a cybersecure culture. The theme was timely for the roundtable organized recently by the Stratbase ADR Institute to examine the systems and mechanisms available to ensure an effective and viable cybersecurity strategy for the country.

All agreed on the need to make cybersecurity a policy priority of this administration. While there is a vision to build a "smart digital society built on trust," there were concerns about cyberespionage, data security and data-sharing for unscrupulous motives. If the government and private sector will not collaborate in this aspect, our strength in ICT will also be our greatest weakness. Reports show that the Philippines was the eighth most attacked country by mobile malware in 2016.

The 2017 Global Cybersecurity Index report classified the Philippines as one of the "maturing" countries in the area of cybersecurity strategy. It was 39th on a list of 193 countries, based on technical, legal, regulatory and cultural, as well as organizational aspects.

At the forum, Assistant Secretary Allan Cabanlong, executive director of the Department of Information and Communications Technology's Cybercrime Investigation and Coordination Center, said the DICT is focusing on the imminent danger brought about by rising threats of cybercrime in coordination with the Philippine National Police and other law enforcement authorities.

Cabanlong warned that criminals, illegal drug traders, the Islamic State, terrorists and other extremist groups are able to use websites and social media for their crimes and illegal activities. The DICT unveiled the National Cybersecurity Plan (NCSP) in May 2017 to ensure security of the country's constantly evolving ICT environment, he said.

The NCSP provides the foundation for policymaking efforts on cybersecurity, covering the details of the implementation plan. It includes a holistic and multilayered response system to better protect critical infostructure against any cyberthreat, as well as capacity-building efforts to support the development of cybersecurity professionals.

Prof. Francis Domingo of De La Salle University discussed the "cyberrevolution" and how it is slowly changing the way state and nonstate actors interact, as well as its potential use as a tool to resolve conflicts and as a leverage for weaker states to level the playing field in strategic affairs.

The promise of cyberrevolution, he said, has influenced numerous states to develop capabilities for military cyberoperations.

According to Domingo, the Philippines needs more resources and capacity to strongly move forward, especially in improving our cybercapabilities to cope with cyberthreats in the region and globally.

Commissioner Raymund Liboro of the National Privacy Commission said a cybersecure culture entails a risk management approach, and prevention and mitigation of data breach. He said the challenge now is to ensure the full enforcement of the trinity of laws that includes the Cybercrime Protection Act, Data Privacy Law, and the creation of the Cybercrime Investigation and Coordination Center.

The success of a cyberstrategy to promote national security and data integrity is anchored on the government's commitment to promote compliance with the laws and the private sector's cooperation and support.

Dindo Manhit is founder and managing director of Stratbase Group.

*CYBERSECURITY