EAST-WEST CENTER

ASIA PACIFIC BULLETIN

Number 737 | March 26, 2025

EastWestCenter.org/APB

Cybersecurity in the Philippines: Advancing a Cyber Defense Posture

By Dr. Sherwin E. Ona

The Philippines, like many small countries, is often left to defend its own digital ecosystems. The Philippines has experienced major cyber-attacks targeting government agencies, public schools, and even the private sector. The country's reactive and technology-centric approach to cybersecurity is often a product of fragmented policies, inadequate resources, and traditional bureaucratic practices. To address these challenges, it must adopt a cyber defense posture to enhance its cybersecurity to ensure a safer environment to pursue its national interests.

Dr. Sherwin E. Ona, an associate professor at De La Salle University, examines the Philippines' efforts to combat recent increases in cybersecurity threats.

Malicious cyber incidents in the Philippines against law enforcement, public health, and national statistics agencies, among others, often coincide with developments in the West Philippine Sea. For instance, attacks against the Philippine National Police, the National Bureau of Investigation, and PhilHealth coincided with the Balikatan joint military exercises between the United States and the Philippines.

According to US cybersecurity firm Resecurity, there has been a 325 percent increase in hacking incidents in the first quarter of 2024 compared to 2023. Government agencies that manage public health, demographic, and public safety data are primary targets. Furthermore, a news article revealed that alleged Chinese cyber operators conducted a yearlong hacking operation against the Philippines from early 2023 to June 2024. These attacks specifically targeted critical government agencies such as the Office of the President and the Armed Forces of the Philippines (AFP).

To address this situation at the policy level, the Philippine government released the National Cybersecurity Plan (NCSP, 2023-2028). The NCSP emphasizes the need for a "whole of government" approach by revitalizing the National Cybersecurity Inter-Agency Committee. To further underscore its urgency, Executive Order (E.O.) 58 was issued for the NCSP's immediate implementation. E.O. 54 also added a deputy director general for cyber and emerging threats at the National Intelligence Coordinating Agency. Furthermore, the inclusion of the cyberspace domain in the Comprehensive Archipelagic Defense Concept is also noteworthy.

Although these are significant steps, the Philippines cannot afford to remain reactive. Its current cyber initiatives continue to suffer from inadequate resources and expertise as well as competing priorities in government agencies. Moreover, siloed implementation of digital transformation and cyber programs dampens collaboration and frustrates sharing of best practices. This underscores the need to adopt a cyber defense posture (CDP).

CDP goes beyond the traditional "castle principle" of protecting an organization through firewalls, software, and cyber hygiene practices. Cyber defense is defined as a collective concept that focuses on the protection of complex and critical systems and adopts a mosaic of deterrence strategies with the intent of imposing a higher cost on malicious actors. Aside from the technical requirements and data-centric focus of cybersecurity, CDP includes the ideas of continuity, resilience, and norms focusing on the protection of the

following: military systems, critical infrastructure, intellectual property, and information environment and democratic space. Furthermore, CDP must provide a space that requires stakeholders to synergize their strengths and address vulnerabilities. It also underscores the importance of a 'whole of society' approach.

Standards, leadership, and literacy are also important facets of a CDP. These components help encourage policymakers, organizations, and citizens to be part of an effort to defend the country's digital ecosystem. Moreover, policymakers and security planners must realize that adopting a CDP requires more than just investments in software, equipment, and human resources. It also highlights the importance of strategic foresight and underscores the need to understand an adversary's playbook.

The idea of "whole of society" and collective defense can never be emphasized enough. This concept usually involves all levels of government and requires collaboration with the private sector and international partners combined with a cyber-literate citizenry. In addition to a government systems focus, CDP proponents underscore the importance of defending critical infrastructure and its digital ecosystem against offensive cyber operations. This holistic approach also includes the ability to counter disinformation operations and recognize the potential of emerging technologies such as artificial intelligence (AI) and quantum computing.

"By using collective defense practices, a [cyber defense posture] will enable the Philippines to be more resilient in defending its digital ecosystems."

The United States and the United Kingdom are good examples on how national cyber strategies and practices reflect a collective defense approach by emphasizing the need to mobilize the various stakeholders to secure their digital ecosystems. Furthermore, these countries recognize cyberspace's transnational nature and the importance of international cooperation to achieve common goals.

Cyber defense posture advocates also underscore the importance of "connecting the dots" – a proactive approach that requires extensive situational awareness about potential threats and current incidents. To achieve this, collaboration and sharing agreements with stakeholders must be present. For instance, uncovering the attack morphology of a hack and sharing it with others can contribute to effective preparation and assistance in similar incidents. In addition, communicating threat information and vulnerabilities can be useful in mitigating cybercrimes, hacktivism, and cyberterrorism as well as advanced persistent threats.

Resilience is a key attribute of a CDP. Organizations, especially those who are part of in the country's critical sectors, must be able to revert to normal operations once a cyber-attack becomes successful. This means entities must have their business continuity protocols in place. On the technical aspect, disaster recovery mechanisms are crucial in restoring operations.

For large-scale attacks, the creation of sectoral computer emergency response teams (CERTs) is a cost-effective approach. This will allow critical sectors to combine their resources and share threat information. Furthermore, these sectoral teams must also be integrated into a national CERT structure to facilitate common strategies, competencies, and intelligence collection.

Another aspect of cyber defense is the ability to conduct offensive cyber operations (OCO). Seen as part of a proactive approach, OCO is based on the idea that states have the right to disrupt or halt malicious activities at their source. Similar to the "defend forward" concept and the idea of active cyber defense, this approach includes the development of hacking capabilities that can be used against malign actors. Once attribution is established, states can pursue diplomatic and legal actions to call out and expose alleged perpetrators.

To enhance defensive and offensive cyber capabilities, the Philippines' ability to harness international partnerships is paramount. Information sharing, capacity building, and collaboration with like-minded

nations like the United States, United Kingdom, Canada, and Australia will enable the Philippines to be more resilient against emerging cyber threats.

In conclusion, the alarming increase in malicious cyber incidents in the Philippines have placed the country at a crossroads. It can choose to remain reactive and techno-centric or adopt a more proactive stance through a CDP. By using collective defense practices, a CDP will enable the Philippines to be more resilient in defending its digital ecosystems. It will also encourage policymakers and security planners to develop strategies that can strengthen the commitment of critical stakeholders and provide spaces for collaboration among partners.

Dr. Sherwin Ona can be contacted at sherwin.ona@delasalle.ph

APB Series Founding Editor: Dr. Satu Limaye | APB Series Coordinator: Lance D. Jackson