Moderna rules out vaccine production in PHL for now

MODERNA, Inc. said its establishment of a presence in the Philippines does not signal near-term plans to manufacture vaccines domestically.

Patrick Bergstedt, Moderna senior vice-president and general manager, told reporters in a virtual briefing on Wednesday that the company is still at the "crawling phase" of its Philippine operations, which currently consist of an upcoming shared services facility, which will handle some back-office and testing tasks for the company in the region.

Mr. Bergstedt had been asked whether the facility being established in the Philippines is a prelude to local manufacturing.

"It is premature to talk beyond that at this point in time. I think we want to also be realistic to say that we need to crawl before we can (expand). And we're still in the crawling phase," Mr. Bergstedt said.

"The Philippine environment promotes innovation. You have many examples in the Philippines where businesses have innovated their sectors and really advanced the thinking, practices, processes, skills and technology. And we want to be part of that. Now that's going to be the first phase," he added.

However, Mr. Bergstedt noted the Philippines' strategic location that might suit an expansion later on.

"Maybe a couple of years and then beyond that. The Philippines is also very well located from a distribution and logistics perspective. So, you can imagine strengthening and bringing some of the people in the facility that also provide that capability," Mr. Bergstedt said.

"The message for the Philippines is that this is a large country of over a hundred million people. We went through a robust process to select the Philippines and we are here for a long-term commitment. We hope to continue to build upon that for the future," he added.

Mr. Bergstedt said the shared service facility in the Philippines is expected to be completed by the end of this year and will result in the creation of 40 to 50 jobs.

The facility will house finance, pharmacovigilance, medical, human resources, and commercial offices. It will provide business services across the Asia-Pacific region.

Mr. Bergstedt said that Moderna is currently in the process of seeking the Philippine government's approval for a bivalent coronavirus disease 2019 (COVID-19) vaccine, as well as other vaccines for respiratory syncytial virus infections, and combination vaccines that provides protection across various respiratory diseases.

"The Philippines is well-located regionally. It's relatively easy to get from Manila to a number of Asian countries where we are committed. Our expansion in the Philippines is an extension of a decision that we took in the beginning of 2022 to establish a presence in the ASEAN region," Mr. Bergstedt said. — **Revin Mikhael D. Ochave**

PNOC-EC confident in continued viability of drilling in SC 38

THE Philippine National Oil Co.-Exploration Corp. (PNOC-EC) said the Malampaya field remains a viable resource for natural gas following the expiry and 15-year renewal of the field's original service contract.

Candido M. Magsombol, a PNOC-EC vice-president with the company's Management Services Division, told a Senate joint hearing that the company will continue its "active participation in SC (Service Contract) 38 Malampaya," where the SC extension enables further well drilling to find and produce more gas.

"We believe that there is still gas there that we can still continue to produce," Mr. Magsombol said.

PNOC-EC is a partner in SC 38, which has generated $12.4 billion for the government and $828 million for the company.

President Ferdinand R. Marcos, Jr. on Monday signed an agreement to renew the SC for Malampaya gas field in offshore Palawan running until 2039.

SC 38 was scheduled to expire on Feb. 22, 2024. Under the new agreement, the contract was extended to Feb. 22, 2039.

The Department of Energy (DoE) said on Tuesday that the Malampaya Consortium is expected to spend around $600 million on new drilling within SC 38.

The Malampaya Consortium is composed of Prime Energy Resources Development B.V., a subsidiary of Prime Infrastructure Capital, Inc. (Prime Infra), which has a 45% stake; UC38 LLC; and PNOC-EC, which own 45% and 10%, respectively.

The Malampaya gas field's current well sites are expected to be commercially depleted by 2027. Mr. Magsombol said the PNOC-EC will "further explore other prospects outside the Malampaya prospect itself."

Mr. Magsombol said PNOC-EC will work on the "drilling of Chico-1 Well and Workover of Mangosteen-1 Well in SC 37 in Cagayancillo, and the seismic data acquisition and processing in SC 57 in Calamian."

"We (will) also coordinate with the Department of Energy on the award of new SCs," he said.

It is also seeking to continue with its Mine 3 Coal Project, covered by COC (coal operating contract) 41, which is expected to produce coal in the second half of 2023. PNOC-EC will open another mine, Mine 4, within COC 41, which is expected to produce coal by the fourth quarter of 2024.

PNOC-EC has produced 757,000 metric tons from small scale coal mines within COC 41 since 2002, Mr. Magsombol said.

He added that PNOC-EC is looking at further exploration in COC 204 in Malangas, Zamboanga Sibugay.

"We just bored a hole there... we can call these explorator, just to check if there's resources there."

Mr. Magsombol told senators that PNOC-EC "is encountering challenges in pursuing exploration activities in the West Philippine Sea due to territorial issues."

China claims more than 80% of the South China Sea, which is believed to contain substantial oil and gas deposits and through which billions of dollars in trade passes each year. A United Nations-backed arbitration court in July 2016 voided China's claim to more than 80% of the sea based on a 1940s map.

China has ignored the ruling, which has failed to stop its island-building activities in areas also claimed by the Philippines, Vietnam, Brunei, Malaysia and Taiwan. — **Beatriz Marie D. Cruz**

Ocean seen playing key role in carbon capture

THE potential for carbon capture in the ocean can protect Southeast Asia's coastlines and mitigate environmental damage, the Asian Development Bank (ADB) said.

"As countries and companies become more conscious of their carbon footprints while striving to achieve net-zero, some have started to look to the ocean — particularly its coastal areas," the ADB said in a blog.

"These areas are seen as an untapped source of 'blue carbon,' which refers to the carbon captured and stored in coastal and marine ecosystems, such as mangroves and seagrass meadows," it added.

The ocean has absorbed about 30% of human-produced planet-warming emissions since the 1980s, according to the ADB.

The ADB said that Asia could benefit from the "rush for blue carbon."

Southeast Asia is among the most financially viable regions for mangrove blue carbon projects, it said, citing a study.

"Research has shown that the carbon stored in mangroves or seagrass meadows can be up to three times more than in tropical rainforests, allowing for more credits to be sold per unit area. Blue carbon credits can also command higher prices due to their positive impact on coastal fisheries and job creation for local communities," it added.

"Wetlands are among the world's most endangered habitats due to land clearance, rising sea levels, and pollution," it said.

However, it also cited the challenges to blue carbon, such as lack of quantifiable data.

"A significant obstacle is the difficulty in quantifying the carbon that some blue carbon habitats can keep out of the atmosphere. For example, it is unclear how underwater carbon capture from seaweed or seagrass can reduce atmospheric carbon dioxide," the ADB said.

"The absence of a mechanism to accurately quantify carbon in an ecosystem means developers do not receive reliable estimates of their financial returns. Coupled with other political and technical concerns, such as overlapping land tenure rights and the transboundary nature of some blue carbon ecosystems, these projects are challenging to scale up," it added. — **Luisa Maria Jacinta C. Jocson**

Scams, potential privacy violations plague SIM registration process

THE registration process for Subscriber Identity Module (SIM) cards has been beset by scams, potential violations of phone subscriber privacy, and technical issues, the non-profit Foundation for Media Alternatives (FMA) said.

"All the glitches, setbacks, and failures documented throughout the ongoing registration period demonstrate how unprepared, ill-equipped, and weak-willed the Philippine government is in establishing and maintaining another massive database of personal information," the FMA, which advocates for information and communications technology users, said in a report.

FMA said the SIM card registration process, which was required under the Subscriber Identity Module Registration Act, also featured low turnout, function creep, surveillance, and the exclusion of some users.

The National Telecommunications Commission (NTC) estimated that as of May 15, only around 95.99 million subscribers or 57.13% of the total have registered.

"This problem is hardly surprising. Even before the system's implementing rules took effect, one telco official acknowledged the 'big challenge' the industry was bracing for was how to encourage people to actually register," FMA said.

It added that the NTC encountered many technical snags during the rollout, including unsuccessful registration, inaccessible registration portals, and the failure to send registrants their one-time PINs to proceed with registration.

"At any rate, the NTC became so concerned that it issued a memorandum directing telcos to report the problems encountered by their respective subscribers during registration. For its part, the Department of Information and Communications Technology launched a 24/7 complaint center meant to address SIM card registration issues and concerns," FMA said.

Once the registration began, reports surfaced about scammers offering to assist would-be registrants and asking for their personal details, according to FMA, in the face of warnings from telcos, the NTC, and the National Privacy Commission.

FMA said that the SIM registration could also be used by telcos for their own purposes such as for advertising and promotional offers.

"Controversy arose almost immediately after people complained of tick boxes put up by some telcos asking for their consent to the use of their personal data for marketing and profiling purposes, as well as the sharing of their personal data with third parties," FMA said.

"It is not inconceivable that the SIM card registration system will be weaponized and used as a tool of mass surveillance and authoritarianism," FMA said.

FMA said the Philippine National Police has not given assurances that the data collected from the registration will solely be used to investigate SIM card-aided crimes.

"Like any ID mechanism, a SIM card registration system has that inherent potential to exclude, and, more often than not, impacts people that are already disadvantaged," FMA said.

FMA said such disenfranchisement happened in Nigeria and Kenya after registration was required.

"Today, telcos appear to have made peace with that outcome given their full support for the system. They seem content with just ramping up their assisted registration initiatives," it said.

"Despite these efforts, however, there remains no credible solution to the problem that a significant portion of the population do not have IDs or even civil registration papers needed for registration," it added.

FMA said that the databases that will be created as a result of SIM registration will become security liabilities.

"Centralized databases are widely known to be honeypots that attract a lot of unwanted attention from bad actors," it said.

"In the meantime, the responsibility of the NTC, the NPC, and other regulators to protect the people and their personal data, as well as to holding telcos and other stakeholders (including fellow government agencies) to account is going to be critical," it added. — **Justine Irish D. Tabile**

OPINION

Adopting AI for cybersecurity

TAXWISE OR OTHERWISE
RAQUEL MARASIGAN

As hybrid work setups, digital transformation, and AI (artificial intelligence) continue in 2023, the risk of cyberattacks remains high. And while these technological trends keep pushing forward, the amount of data created also soars exponentially. Cyber attackers see this transitory period as an opportunity to wreak havoc on computer networks, particularly targeting small- and medium-sized organizations.

Cyberattacks are getting more advanced and sophisticated. To improve an organization's cybersecurity posture, we need more than human intervention. Organizations now need to leverage technologies that learn and improve, like AI, by analyzing historical data to identify new and future attacks. It can also help keep up with cybercriminals, automate threat detection, and respond more effectively and in a timely manner — better than conventional software or human intervention.

AI-BASED CYBERSECURITY SYSTEMS

According to International Standards Organization ISO/IEC 27032:2012, cyberspace is a complex environment that results from the interaction between emerging technologies such as AI, people, and internet services, which are supported by physical and information communication technology (ICT) and connected networks that are distributed worldwide.

Today, a significant portion of internet traffic consists of dangerous bots, causing anything from account takeovers using stolen credentials to phone account creation and data fraud. Automated threats cannot be countered solely through manual responses, though. But with the aid of AI and machine learning, it is possible to differentiate between good bots (such as search engine crawlers) and bad bots, as well as between humans and website visitors.

Sophisticated algorithms are designed to detect malware, run pattern recognition, scan behavior analytics, and detect the lateral movements of malware before it enters a computer system. AI amplifies predictive analytics with natural language processing, which organizes data by scraping cyber threats from the internet. This provides intelligence on new anomalies, cyberattacks, and prevention strategies for combating cyberattacks.

Artificial intelligence-based cybersecurity systems offer the most updated information on regional and sector-specific threats, helping prioritize important decisions based not only on what can be used to attack systems, but also on what are most likely to do so. They can monitor network traffic and user activity in real time to detect malicious activity and act quickly. They also assist in compiling an IT asset inventory, which is a precise and thorough list of all the devices, users, and applications with various levels of access to different systems.

The algorithm is also able to forecast how and where you are most likely to be compromised, so resources can be directed to areas with the greatest vulnerabilities. Processes and controls can be set up and enhanced to strengthen cyber resilience, with the help of prescriptive analytics from an AI-based analysis. There are essential instruments for information and cyber security available on the market. One illustration is a system powered by artificial intelligence that reveals hidden data, normalized data volume, eliminates segregated visibility of security issues, and enhances analytics efficacy. When we look at AI-driven endpoint protection, it significantly adopts a different strategy by establishing the baseline behavior through a repeated training process.

And this is where AI comes in: anytime something strange happens, the AI systems notify users and take the necessary action, such as sending a warning to security operation analysts or even wiping the device clean after a malware attack.

HOW AI CAN HELP SECURE YOUR BUSINESS

These are four ways how AI operates in cybersecurity to secure your business:

1. **Improved network security.** Traditional network security has two time-intensive aspects: creating security policies and understanding the network topography of an organization. AI improves network security by learning network traffic patterns and recommending functional groupings for workloads and security policies.

2. **Detection of cyberattacks.** While traditional vulnerability databases are critical for managing and containing known vulnerabilities, AI and machine learning techniques such as User and Event Behavioral Analytics (UEBA) can analyze the baseline behavior of user accounts, endpoints and servers, and identify anomalous behavior that might signal a zero-day unknown attack. These can help protect organizations even before vulnerabilities are officially reported and patched.

3. **Detection of low-level attack vectors.** AI can be used to detect low-level attack vectors, inspect for domain and application configuration or logic errors, provide best practices for secure system operation, and monitor networks once the code has been developed. Because AI is widely used by commercial and government organizations, open-source software development gives a unique and high-impact opportunity for AI-based security improvements.

4. **Identity management and access control.** AI-based systems can learn from previous interactions and expected behavior of customers, and in turn decrease threats to biometric authentication systems. Of course, monitoring behavioral patterns may result in privacy violations so more research is required to develop techniques that consider the ethical and technical aspects of AI-assisted identity management.

ENABLING TRUST THROUGH AI

In order to promote confidence and trust in artificial intelligence systems, always be honest about how the system arrived at a prognosis. It is important to be reminded that the usage of AI-based reasoning in human-loop systems can become more trustworthy. As an example, AI can be used to combat harmful internet bots. This can result in the deployment of more reliable AI-based cybersecurity solutions that can help with risk prioritization, incident response coordination, threat hunting, and early malware detection.

The views or opinions expressed in this article are solely those of the author and do not necessarily represent those of Isla Lipana & Co. The content is for general information purposes only, and should not be used as a substitute for specific advice.

RAQUEL MARASIGAN is a manager at the PricewaterhouseCoopers Consulting Services Philippines Co. Ltd., a member firm of the PwC network.
+63 (2) 8845-2728
raquel.marasigan@pwc.com