Free trade negotiations with UAE expected to wrap up by October

THE PHILIPPINES hopes to conclude negotiations with the United Arab Emirates (UAE) on their proposed Comprehensive Economic Partnership Agreement (CEPA) as early as October, the Philippine Exporters Confederation (Philexport) said.

In a bulletin, the association quoted Trade Undersecretary Allan B. Gepty as saying that he hopes to finish talks with the UAE before the year ends.

"Our agreement with the UAE is to conclude the negotiations within the year. We're looking at October or November," Mr. Gepty said.

The Philippines and the UAE planned four full rounds of face-to-face negotiations aside from virtual meetings to move things along.

"The first round was held in May 2024, and they are now set to conduct the second round, focused on market access negotiations, from July 8 to July 10 in Manila," he added.

CEPA is a free trade agreement (FTA) aimed at expanding trade and investment opportunities with the UAE and the greater Gulf region.

In December, the Philippines and the UAE signed the terms of reference for the CEPA, setting guidelines for the conduct of the negotiations and the scope and coverage of the FTA.

The Departments of Agriculture, Labor and Employment, and Environment and Natural Resources, the Tariff Commission, Board of Investments, and the Bureau of Customs are joining the talks as negotiations progress.

"Working groups are being created to negotiate the relevant chapters of the ToR, which include trade in goods, rules of origin, trade in services, digital trade, customs procedures and trade facilitation, investment, intellectual property rights, and trade and sustainable development," it added.

The Department of Trade and Industry (DTI) said it sees opportunities to access the UAE market for halal-related products, tropical fruit, garments, and high-end finished consumer goods.

"Some of the Filipino food and other agri-based products with unrealized export potential in the UAE include banana, desiccated coconut, coconut oil, pineapple, and raw cane sugar. Also with much potential are personal care products, including perfumes and eye makeup," it added.

Tradeline Philippines reported that total trade between the Philippines and UAE grew 5% to $1.9 billion in 2023.

"If realized, the PH-UAE CEPA will be the first FTA of the Philippines with a member state of the GCC (Gulf Cooperation Council) and in the entire Middle East," Philexport said.

"It will also be the Philippines' fourth bilateral FTA after the Philippine-South Korea FTA signed in 2023, the Philippines-Japan Economic Partnership Agreement in 2006, and the Philippine-European Free Trade Association FTA in 2016," it added.
— **Justine Irish D. Tabile**

Rice EO signals greater PHL openness to trade — BCCP

By Chloe Mari A. Hufana

EXECUTIVE ORDER (EO) No. 62, which cut rice import tariffs to 15% from 35% signals that the Philippines is opening itself up to more trade, the British Chamber of Commerce of the Philippines (BCCP) said.

"When you reduce tariffs... that helps because your signal is that the Philippines is more and more open to trade and investment," BCCP Executive Director and Trustee Christopher James Nelson told *BusinessWorld* by phone.

"There's a lot of interest (from foreign investors) and clearly the signal that the President sent by reducing (rice tariffs) is very good," he added.

Mr. Nelson added that EO 62 benefits the Philippines because cheaper overseas products will be available in Philippine markets, keeping prices lower.

American Chamber of Commerce of the Philippines, Inc. Agribusiness Chair Christopher A. Ilagan told *BusinessWorld* via Viber that the Philippines is an important partner for American agricultural business. It is the ninth-largest export market for US agricultural goods.

"EO 62 offers more predictability as it ensures a clear and transparent tariff regime over the next few years, unlike the previous practice of annually renewing the tariff rates, keeping on edge those who are reliant on these trade flows," he added.

Mr. Ilagan added that improved predictability will keep prices and trade volumes steady instead of fluctuating, especially at the end of financial years.

"Better predictability and policy stability are basic characteristics foreign traders and investors rely on for longer-term commitments in the market," he added.

Mr. Marcos last month issued EO 62 as an inflation-containment measure.

Rice inflation in June eased to 22.5% from 23% in May for a third straight month of declines.

The Philippine Statistics Authority last week said the price of a kilo of well-milled rice fell to P55.96 in June from P56.06 in May.

Regular-milled rice prices increased to P51.07 in June from P51.03 in May, and special rice prices rose to P64.56 in June from P64.41 in May.

FULL STORY

Read the full story by scanning the QR code with your smartphone or by typing the link <tinyurl.com/25drudfh>

Doubts raised about Dalian train arbitration

DOUBTS have been expressed about the prospects of the Transportation department's plan to seek an arbitration ruling against Chinese train maker CRRC Dalian Co. Ltd.

"Arbitration on the Dalian trains will have a poor chance of success. The railcars have been with the DoTr for the last eight years, during which time they have plenty of time to return the cars or seek a refund. Arbitration (only means) more income to foreign consultants," Rene S. Santiago, former president of the Transportation Science Society of the Philippines, said via Viber.

The Department of Transportation (DoTr) is considering seeking an arbitration ruling against CRRC, Transportation Secretary Jaime J. Bautista said on the sidelines of an event last week.

"There will be liquidated damages because they were unable to meet our requirements. But of course, subject to agreement. We should be fair and reasonable in terms of what should be collected from Dalian," Mr. Bautista said.

"There's a possibility that this leads to arbitration. In fact, I am seeing that this leads there."

The possible pursuit of arbitration could go forward before the planned privatization of the operations and maintenance of Metro Rail Transit Line 3 (MRT-3), which is expected by 2025.

The government procured the Dalian trains in 2014, with deliveries taking place in 2016. The trains were expected to increase the capacity of the MRT-3 to 800,000 passengers daily.

Mr. Bautista said that the Dalian trains were too heavy to use the MRT-3 tracks.

Operating them "would result in higher maintenance costs and would also result in higher operating costs," he said.

For now, the DoTr is still working with the Chinese train maker to determine how to operate the trains for the MRT-3.

Earlier, the DoTr said it is hoping to auction the operations and maintenance contract for MRT-3 by 2025.

The private rail line concessionaire may still opt to use the rail cars once it takes over the operations and maintenance of MRT-3, Mr. Bautista said, adding that one of the proponents has submitted a proposal detailing how to operate the Dalian trains.

"A private concessionaire can find ways to combine the Czech & Dalian trains efficiently by exploring parts standardization," Mr. Santiago said.

Nigel Paul C. Villarete, senior adviser on public-private partnership at the technical advisory group Libra Konsult, Inc., said having the concession holder come up with a solution to operate the unused trains would be a better option, rather than seeking arbitration.

"If these trains can be used, I think we'd better use them rather than completely repudiate the purchase. They may want to do a full financial and economic comparative analysis on the options to take," Mr. Villarete said via Viber.

However, he said that operating the unused trains once the private concessionaire takes over would entail higher maintenance costs, which can be passed on to consumers if viable. — **Ashley Erika O. Jose**

OPINION

Key GenAI cybersecurity challenges and risk mitigation strategies

IN BRIEF:

- *While it holds extraordinary promise for the future, GenAI comes shrouded in various concerns, extending from ethical dilemmas to security susceptibilities.*
- *To mitigate attack vectors, organizations must establish comprehensive regulations and standards that can guide the responsible use and development of GenAI.*

SUITS THE *C*-SUITE
RAJIV KAKAR

While the potential of GenAI is undeniable, a cautious, forward-thinking approach is crucial to navigating its potential pitfalls.

Generative artificial intelligence (GenAI) has the capacity to understand, learn, adapt, and implement knowledge across a broad range of tasks at a level equal to or beyond human capability. Unlike Narrow AI, which is designed to perform a specific task such as voice recognition or recommendation algorithms, GenAI can apply intelligence to any problem, and be able to perform any intellectual task that a human being can do.

While it holds extraordinary promise for the future, GenAI comes shrouded in various concerns, extending from ethical dilemmas to security susceptibilities. This article will explore some of the key challenges of GenAI and risk mitigation strategies from a cybersecurity perspective.

KEY CHALLENGES OF GENAI

A persistent issue of AI is the lack of transparency, frequently referred to as the black box problem. It's difficult to understand how complex AI models make decisions, and this can create a security risk by allowing biased or malicious behavior to go unchecked.

Businesses are rapidly exploring GenAI solutions with little forethought on the security implications on the rest of the IT estate. There is currently no limit for the complexity of attack surfaces of AI systems or other security abuses enabled by AI systems. In addition, AI models heavily rely on third-party technologies, where the large language models (LLMs) like ChatGPT are outside the control of an enterprise. Consequently, the learning parameters where AI systems may be trained for decision-making outside an organization's security controls or trained in one domain and then "fine-tuned" for another raises concerns about intended and actual usage.

Datasets used to train AI systems may become detached from their original and intended context, or may become stale or outdated relative to deployment. This introduces the problem of decisions made on incorrect data. Moreover, changes during training of models may fundamentally alter AI system performance and outcomes.

LLMs typically capture more information than they process, and considering the privacy policy of ChatGPT, the platform may regularly collect user data such as IP address, browser info and browsing activity. These may be shared with third parties, competitors, and regulators. The use of pre-trained models that can advance research and improve performance can also increase levels of statistical uncertainty and cause issues with bias management, scientific validity, and reproducibility.

On top of the computational costs for developing AI systems and their impact on the environment and planet, it is very difficult to predict failure modes for the emergent properties of large-scale pre-trained models. AI systems may require more frequent maintenance and triggers for conducting corrective maintenance. Additionally, it is challenging to perform regular AI-based software testing, or determine what to test, since AI systems are not subject to the same controls as traditional code development.

"Artificial stupidity," the term used to describe situations where AI takes decisions that may seem illogical to humans due to its inadequate understanding of the real-world context, presents another challenge. Talk of AI singularity, a hypothetical scenario where AI outstrips human intelligence, have also started to gather momentum. Critics argue that a super-intelligent AI poses a real existential risk, as it might spin out of human control.

The dehumanizing effects of GenAI are another cause for concern. Over-reliance on AI risks devaluing human skills and minimizing human interactions. Moreover, the widespread application of GenAI may give rise to economic disparity, as the benefits of AI may not distribute evenly across society. Finally, the misuse of GenAI, particularly for harmful purposes like illegal surveillance, spreading propaganda, or weaponization, cannot be overstated.

The already dense and complex AI landscape is further complicated by substantial hype and a multitude of diverse solutions. The resulting application environment is scattered with multiple third-party technology solution components which require thorough vetting in enterprise contexts.

TYPES OF GENAI ATTACKS

There are various types of GenAI attacks manifesting across enterprises. Adversarial attacks involve manipulating an AI model's input data to make the model behave in a way that the attacker desires, without triggering an alarm. For example, an attacker could manipulate a facial recognition system to misidentify an individual, allowing unauthorized access.

A data poisoning attack involves maliciously manipulating the data used to train AI models. By introducing false or misleading data into the training dataset, attackers can compromise the accuracy and reliability of AI systems. This can lead to biased predictions or compromised decision-making. On the other hand, a model theft or model inversion attack may attempt to steal and/or reverse-engineer AI models to obtain sensitive information.

In a transfer learning attack, an attacker manipulates an AI model by transferring knowledge gained from one domain to another, resulting in the AI system producing incorrect or harmful outcomes when applied to new tasks. In input manipulation, interacting with a chatbot or an AI-driven system can lead to incorrect or harmful responses simply by changing words or asking tricky questions. For instance, a medical chatbot might misinterpret a health query, potentially providing inaccurate medical advice.

AI can also be used by malicious actors to automate and enhance their cyberattacks. This includes using AI to perform more sophisticated phishing attacks, automate the discovery of vulnerabilities, or conduct faster, more effective brute-force attacks.

GENAI SECURITY RISK MANAGEMENT

To mitigate attack vectors, organizations must establish comprehensive regulations and standards that can guide the responsible use and development of GenAI. A GenAI Risk and Control framework can be very helpful in highlighting areas of vulnerability and risk mitigation in some of the following areas:

Threat recognition. Identify possible threats GenAI might enable, such as autopilot system hacking, data privacy threats, decision-making distortion, or manipulation.

Vulnerability assessment. Evaluate weak spots in the system that might be exploited due to GenAI characteristics.

Risk impact analysis. Look into potential implications if any threats were actualized (financial implications, impact on company reputation, etc.)

Mitigation strategy development. Develop strategies to mitigate these risks, whether that means strengthening your network security system, creating backup systems, securing data privacy with improved encryption, or continuously auditing & updating the AI's programming against potential manipulation.

Contingency planning. Develop a plan for responding to any breaches or issues that occur, despite mitigation efforts. Include steps to fix the issue, mitigate the damage, and prevent future occurrences.

Constant monitoring & updating. GenAI systems should be regularly monitored and updated to patch vulnerabilities and keep up with the evolving threat landscape.

Training & awareness. Ensure that all users of GenAI systems are properly trained on security best practices and are aware of the potential threats.

External cooperation. Cooperate with other firms and institutions to share threat intelligence and promote a collective defense strategy.

Regulation compliance. Ensure compliance with all applicable laws and regulations surrounding data security and AI, such as general data protection regulation (GDPR).

Incident response plan. Prepare a clear and concise plan to follow when a breach occurs, which includes reporting breaches, managing and controlling the situation.

Organizations must consider upgrading cloud security and moving towards zero trust principles, whereby every access request is authenticated, authorized and validated every time. Antivirus systems should be upgraded from the current norm of using a pre-programmed list of known attack vectors (signature based) to systems that can observe unusual patterns and alert on deviations (anomaly based). Embracing GenAI monitoring by introducing the appropriate tools allows organizations to monitor AI prompts and see that they do not deviate from original scenarios.

Review and strengthen security around a GenAI application stack emphasizing on integration points between systems (API's) and identify AI systems and assets by drawing up a plan of usage. Organizations can assign a dedicated team to test AI models at base and application level, as well as introduce moderation and control on user developed applications, tools and products. Any experimental or uncontrolled work on GenAI within the enterprise must be monitored.

Applying these strategies can minimize the risks associated with GenAI and help efficiently manage cybersecurity.

NAVIGATING AI PITFALLS BY MITIGATING RISKS

While the potential of GenAI is undeniable, a cautious, forward-thinking approach is crucial to navigating its potential pitfalls. It is imperative to establish comprehensive risk mitigation, standards, and frameworks that can guide the responsible use and development of GenAI.

This article is for general information only and is not a substitute for professional advice where the facts and circumstances warrant. The views and opinions expressed above are those of the author and do not necessarily represent the views of SGV & Co.

RAJIV KAKAR is a technology consulting principal of SGV & Co.