ACICE Issue 04/23 (April)

ACICE Monthly Digest

A monthly roundup of significant news around the world

ADMM Cybersecurity and Information Centre of Excellence

Cybersecurity

Learning Lessons from Latitude Financial's Data Breach

- On 16 Mar 2023, Latitude Financial, a leader in consumer finance in Australia and New Zealand, issued a statement reporting that it had detected suspicious activity that was indicative of a "sophisticated and malicious cyberattack". While initial reports indicated about 103,000 identification documents and 225,000 customer records stolen by the perpetrators, it was subsequently found that the losses totalled to over 14 million records, including eight million driver licence numbers and 53,000 passport numbers.

- The perpetrators of the breach had demanded a ransom, which Latitude Financial refused to accede, claiming that it did not want to "reward criminal behaviour" and encourage future cybercrimes.

- Latitude Financial's data breach incident is a timely reminder of the ongoing challenges that businesses and other entities face in safeguarding consumer data. In the light of the crisis, Latitude Financial wasted little time to reach out to the impacted individuals to offer support and provide updates on the the investigations, demonstrating quick service recovery.

- Government agencies such as the Australian Financial Complaints Authority and Australian Securities & Investments Commission also stepped in, releasing and circulating media reports to facilitate awareness, and informing consumers of ways to reach Latitude Financial for consumer support.

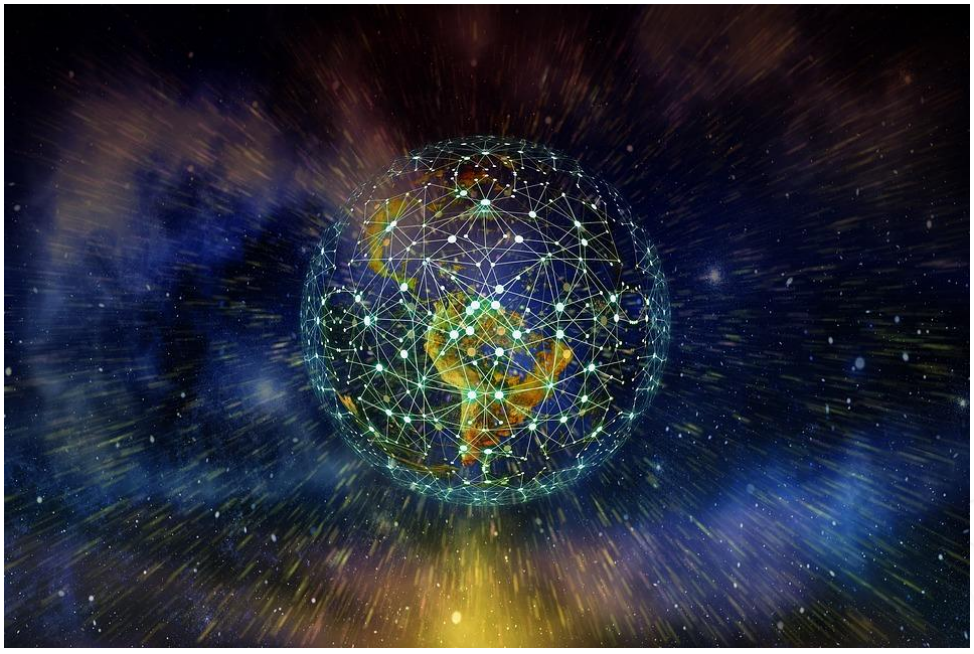
- To mitigate the risks of cyberattacks and data breaches, governments can provide a framework and formulate standards to guide industries in enhancing cybersecurity, as well as collaborate with critical information infrastructures (CIIs) to plug the vulnerabilities in their systems. Latitude Financial's data breach incident showed that the cost of not securing systems against breaches could be highly damaging and costly for companies. Despite the high cost, it is in the interest of companies to invest in their own cybersecurity systems as the consequences of not doing so could be worse. Companies could also seek an independent audit of their own cybersecurity processes and systems to identify shortfalls and gaps with the aim of addressing these vulnerabilities and minimising their risk profile.

Internet Governance

Mitigating the Risks of the Splinternet

- The splinternet, a portmanteau of the words “splinter” and “internet”, is a term that describes the scenario where the Internet is segmented into different ‘online regions’, and connectivity and accessibility between these regions are disrupted due to efforts to ring-fence and limit connections across networks and access to applications. Put simply, “a splinternet” happens when there is a number of national or regional networks that are unable to “speak” because they are using different platforms, incompatible protocols or technologies.

- Fears of the splinternet becoming reality are not new, and have surfaced over a decade ago amid rapid digitalisation. A September 2010 article by *The Economist* had warned that the free Internet might “splinter along geographical and commercial boundaries”, due to the combined pressures placed by states, large corporations, and network providers. These fears grew as inter-state geopolitical tensions triggered the move towards a splintering Internet.



- A free and open Internet allows for continuous and seamless flow of information across countries. This freedom means that people can access the internet using their devices across borders without difficulty, except in cases

where specific websites and applications are blocked in some national jurisdictions for reasons such as safety and national security. Institutions such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the International Telecommunication Union (ITU) help to develop standards and make decisions that are vital in enabling the interconnectedness and interoperability of devices, as well as supporting and maintaining a free, open, stable, secure, and unified global Internet.

- Over the last four decades, the open, decentralised and transparent nature of Internet allows it to be seen as legitimate and widely accepted. For instance, ICANN's decision to reject requests made by Ukraine, which would essentially cut Russia off from the global Internet, demonstrates critical need for such institutions to be seen as independent and neutral. Moreover, the Internet's openness allows mass participation, encourages innovation and facilitates the smooth functioning of business and public services. In the everyday, people can conveniently and seamlessly connect, interact and transact with each other via the devices.

- However, there is a risk that countries may seek to form rivalry bodies or alternative networks, with the aim of insulating their societies from external influence or minimising national security risks. For instance, Russia has been reportedly seeking to mitigate risks to its own security by requiring its companies and entities to repatriate their data us.ru domains and minimise the use of overseas service providers. The ongoing Russia-Ukraine conflict has also led to the establishment of digital walls in the midst of the crisis. According to the March 2022 article by the *Massachusetts Institute of Technology (MIT) Technology Review*, Russia had moved to block access to websites such as Facebook and Twitter. Multinational companies had withdrawn from and suspended their services in Russia, and some Russian media outlets were blocked from operating in several countries. This erecting of digital walls between Russian cyberspace and the rest of the world might be irreversible, as the article cautioned.

- Others such as Iran and China have sought to establish their own forms of a national-functional Internet. Meanwhile, countries or groups such as the EU have sought to contain the global nature of the Internet by imposing limits on the processing and movement of personal data.

- We will be worse off if the splinternet truly comes to pass. The limited access to information and online services could create challenges for international communication, endanger our prosperity and also present risks to personal data and national security.

- Hence, it is imperative for governments to work towards preserving one global Internet and guard against any fragmentation. Countries should continue to support existing institutions such as ICANN and ITU. In addition, members of the UN should come together to develop and implement common rules, norms and principles to guide responsible state behaviour and preserve the integrity of the Internet.

Artificial Intelligence

Threats and Benefits Posed by Generative Artificial Intelligence

- Generative artificial intelligence (AI) tools have surged in popularity among users and is a hot topic for discussion in recent months. In particular, ChatGPT by OpenAI, a US company, had broken grounds as an application that could generate ready and increasingly convincing answers to any questions, based on online big data collected and synthesised over time. With ChatGPT now having an estimate of 100 million monthly active users, generative AI could drastically shift the way we work and play, whereby machines could potentially replace human labour and even human relationships.

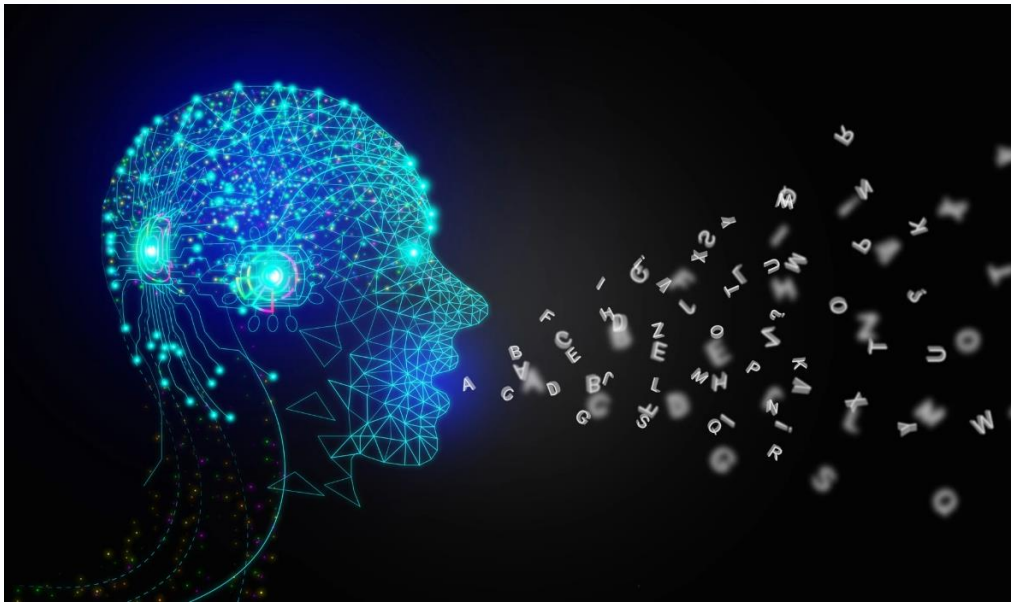
- Although ChatGPT is one of the most commonly known generative AI tools, other tech companies around the world have jumped onto the bandwagon and created similar tools of comparable technologies. ChatGPT and Baidu's Ernie are chatbots that can perform a whole range of tasks, from creating programming codes to explaining theoretical concepts. Other applications such as Midjourney, started by an independent US-based research lab of the same name, can be used to generate realistic images and art based on prompts. Some of the AIs developed are doing better than others, owing to more computing power and a larger database to reference from. For instance, a *TechCrunch* article in March concluded that GPT-4 was "unambiguously ahead of the others" when it was pitted against Anthropic's Claude and Google's Bard. In one of the tests, only GPT-4 was able to give an accurate book summary without using proper names.

- With generative AI being a relatively new technology, early adopters have been enjoying its benefits alike having a virtual assistant to generate ideas and content, including speech drafts or even holiday itineraries. When put to good use, generative AI can increase the efficiency and effectiveness of our work processes.

- However, generative AI has also vastly facilitated the creation of content that could aid nefarious actors in rapid production and viral spread of disinformation and misinformation to achieve their agenda. For instance, AI tools such as OpenAI's DALL-E have been used to generate realistic images and videos, from former US President Donald Trump being tackled by police officers to Russian President Vladimir Putin behind bars. These images and

videos may be used to promote false narratives that could "add noise during crisis events" or undermine trust in governments.

- Separately, with ChatGPT, even cybercriminals who may not be sufficiently proficient in coding can generate codes to be used in a malware attack. Such AI tools can also craft templates for scam and phishing emails, making it easier for malicious actors to cyberattacks.



- There is an increasing need to put in place suitable regulations to prevent the misuse of generative AI for malicious intent, which might disrupt social cohesion, national security, and harmony. However, regulating the use of generative AI is not necessarily a straightforward task, and has to be carefully managed by governmental authorities. There is a need to balance between safeguarding against the evils associated with technological advancements, and impeding the growth of technology that might contribute to betterment of lives. This debate is not new, as seen from the past century where we benefited from an interconnected world through the internet, while managing the exposure to the evils of dark web.

- To safeguard against the perils of generative AI, the Cyberspace Administration of China, for instance, has proposed regulations to address the development and implementation of generative AI. According to China Daily, among other objectives, the measures seek to ensure that AI-generated content is "true and accurate", and does not inflict harm to people's health or promote extremism and discrimination. Taking a consultative approach, the Chinese government had published a draft of the regulations, and invited the public to submit ideas and comments until till 10

May 2023. In contrast, the UK government currently prefers not to adopt blanket legislation to regulate the use of AI, believing that coherence and clarity can be similarly ensured through less rigid and more flexible approaches that can be adapted over time.

- Two researchers from the United Kingdom explored dilemmas in AI regulation in an April 2022 paper, on how the "imperative of facilitating technological discovery and enterprise conflicts with the governmental responsibility to ensure the safe and trustworthy development and use of AI technologies". They also highlighted a dilemma in how AI regulation could be approached, as horizontal and vertical regulations have their respective advantages and drawbacks. Horizontal regulation, which is uniformly applied across all sectors, may have comparatively less loopholes and better stability, while vertical regulation that focuses on specific industries or is entrusted to industry bodies to handle may allow for greater specificity and optimisation.

- Governments will have to tread cautiously when exploring options to regulate AI in their own countries. By studying how others have implemented and enforced their own policies, along with understanding their own contexts, authorities can stand to introduce the most effective set of measures to meet their needs in ensuring the responsible use of AI.

Terrorism

Continued Interest in Transnational Activity Among Terror Elements

- Terror groups continued to recruit followers from Southeast Asian states. In February 2023, an al-Qaeda supporter in Indonesia, who claimed to have gone to Yemen to study, was seen offering assistance and funding to interested parties to travel to Yemen to join al-Qaeda. More recently in April 2023, an Indonesian al-Qaeda supporter claimed that he was prepared to join Al-Qaeda in the Arabian Peninsula (AQAP) in Yemen, and actively promoted the group to local jihadists.

- In March 2023, a pro-ISIS supporter claiming to be a "brother" from Khorasan used Telegram to incite people to migrate to Khorasan. Khorasan is a general area coined by Islamic State militants that includes the areas of Afghanistan and Pakistan. In April 2023, an AQAP militant who claimed to be in Afghanistan also advised aspiring jihadists on how to avoid detection by global counter-terrorism agencies while joining the group.

- These recruitment efforts appeared to have inspired some individuals towards the terrorists' cause. In March 2023, an ISIS supporter shared videos of militants operating in the Philippines and expressed his willingness to become a martyr, while asking for tips to join the militants in the Lanao del Sur province.

- On 4 April 2023, Indonesian news agency Antara reported that four Uzbek nationals were arrested by Indonesian police on suspicion of spreading terror propaganda on social media. Preliminary investigations showed that the four were connected with an international terrorist organisation known as Katiba Tawhid Wal Jihad. They had apparently travelled to Indonesia from Türkiye, via the United Arab Emirates and Malaysia. Three of the suspects subsequently attempted to escape custody on 10 April 2023, through a knife attack that led to the death of an immigration officer. The Indonesian police hunted two of them down within 24 hours, while the last suspect was found drowned in a river.

- As international travel opens up following the easing of COVID-19-related restrictions, there may be a resurgence in terrorist movements in and out of

Southeast Asia. Hence, states need to remain vigilant and cooperate with one another to contain these terror threats effectively.

Annex

Sources

Cybersecurity

- Drawing Lessons from Latitude Financial's Data Breach
  - https://assets.latitudefinancial.com/media-release/latitude-cyber-incident.pdf
  - https://www.theguardian.com/australia-news/2023/mar/27/latitude-financial-cyber-data-breach-hack-14m-customer-records-stolen
  - https://www.afr.com/companies/financial-services/latitude-rules-out-ransom-restores-operations-20230411-p5czgy
  - https://www.afca.org.au/news/current-matters/latitude-financial-cyber-attack
  - https://asic.gov.au/about-asic/news-centre/news-items/guidance-for-consumers-impacted-by-the-latitude-financial-services-data-breach/

Internet Governance

- Mitigating the Risks of the Splinternet
  - https://www.economist.com/briefing/2010/09/02/a-virtual-counter-revolution
  - https://www.internetsociety.org/resources/2022/impact-of-ukraines-requests-to-block-russias-access-to-the-internet/
  - https://www.technologyreview.com/2022/03/17/1047352/russia-splinternet-risk/
  - https://www.internetsociety.org/resources/doc/2022/how-to-protect-the-internet-from-becoming-the-splinternet/
  - https://pixabay.com/images/id-3537401/

Artificial Intelligence

- Threats and Benefits Posed by Artificial Intelligence
  - https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/

- https://techcrunch.com/2023/03/21/googles-bard-lags-behind-gpt-4-and-claude-in-head-to-head-comparison/
- https://apnews.com/article/ai-misinformation-trump-putin-new-york-42ac9c41c5504d05412b492e48bcaded
- https://www.businessinsider.com/chatgpt-cyber-crime-phishing-malware-artificial-intelligence-2023-2
- https://www.chinadaily.com.cn/a/202304/13/WS643742baa31057c47ebb9cf4.html
- https://www.chinadaily.com.cn/a/202304/12/WS6436037ea31057c47ebb9a15.html
- https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper
- https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4072436
- https://www.istockphoto.com/photo/ai-speaks-letters-text-to-speech-or-tts-text-to-voice-speech-synthesis-applications-gm1458045238-492706670

Terrorism

- Continued Interest in Migration Among Terror Elements
  - https://en.antaranews.com/news/277704/four-uzbek-terror-suspects-picked-up-by-police
  - https://en.antaranews.com/news/278424/three-uzbek-terror-suspects-attack-indonesian-immigration-officers

Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/

For any queries and/or clarifications, please contact ACICE at ACICE@defence.gov.sg

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence