

ACICE Issue 01/23 (Jan)

ACICE Monthly Digest

A monthly round-up of significant news around the world

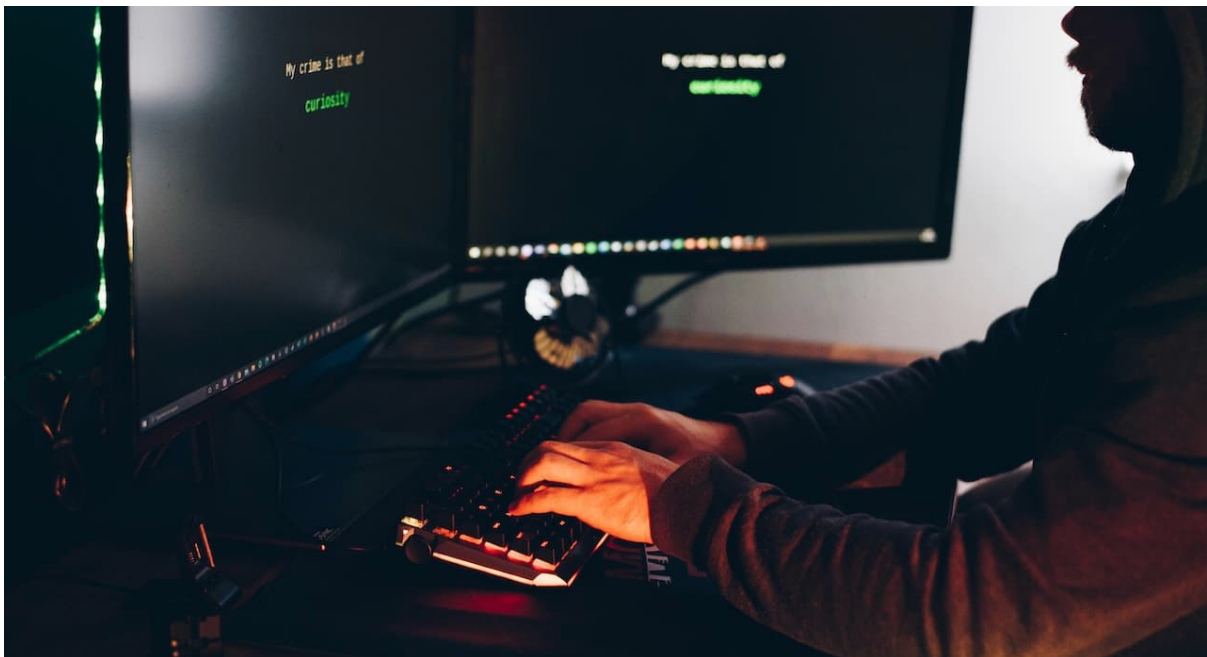


ADMM Cybersecurity and
Information Centre of Excellence

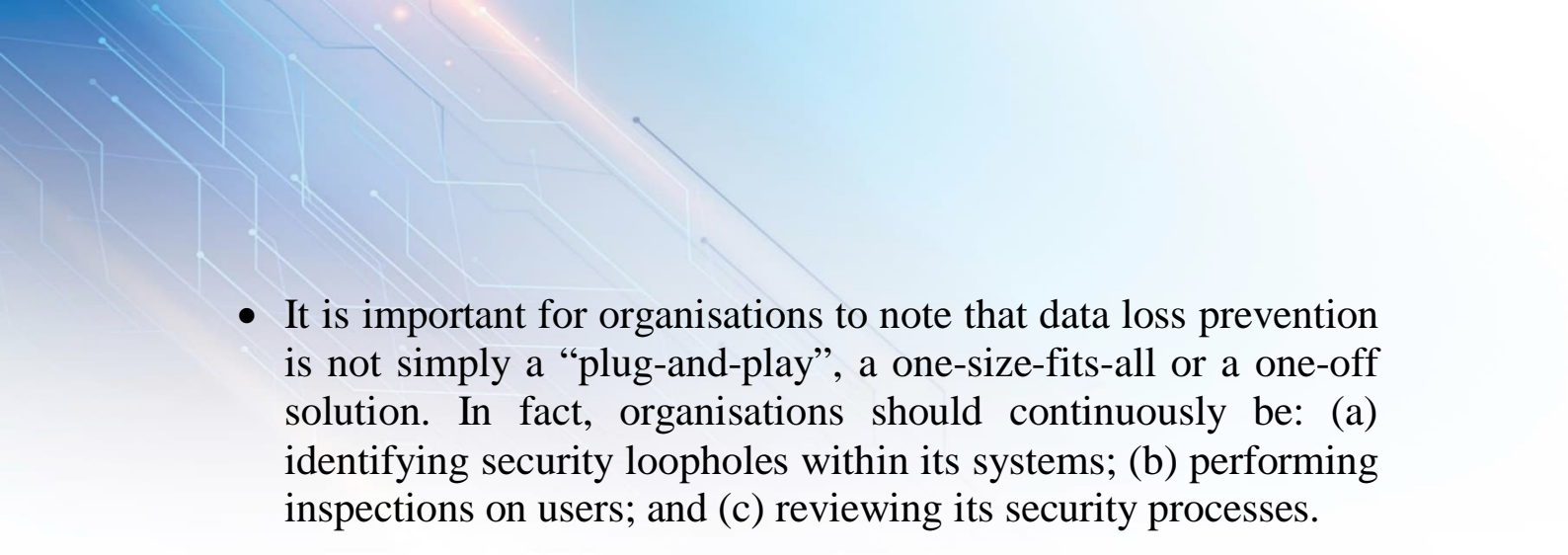
Cybersecurity

Data Loss Prevention

- Cybersecurity threats like phishing and ransomware have been on the rise globally. This trend has corresponded to an increase in the number of data breaches in businesses.
- A recent high-profile data breach involving LastPass, a popular password manager application which allows users to store sensitive data on its platform, offers a case in point. In 2022, hackers breached LastPass not once, but twice – in August and November. According to LastPass, hackers first gained access to its network through a compromised account held by a software developer in August. In November, the hackers subsequently used information gained from its illegal access back in August to get their hands on important user data like passwords and IP addresses.

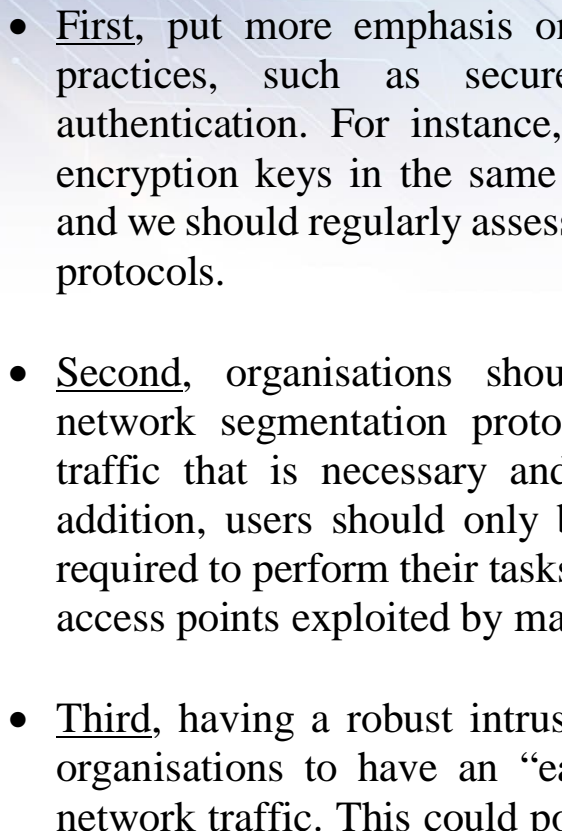


- The key reason for the breach is LastPass' weak data loss-prevention policies, such as its cryptography and security processes. First, LastPass' cryptography is not as secure as what users had thought it would be. Contrary to what people might think, LastPass does not fully encrypt all of users' data. Instead, it only encrypts data it deems "important", such as users' passwords, leaving data like website URLs unencrypted, which could still give malicious actors an idea of the passwords that are stored, and prioritise their attacks accordingly.
- Second, LastPass was not diligent in ensuring that its users followed the best practices of a strong master password. For instance, despite the fact that it had increased the minimum length of master passwords from 8 characters to 12, they neither enforced nor prompted users to regularly change their passwords. This meant that users were still allowed to log in with their previous 8 character passwords, which were less secure.
- While LastPass is currently under immense public scrutiny due to this data breach, it is not the only company guilty of lapses in its security practices. In fact, security analysts have found that many organisations frequently invest in a cybersecurity solution solely to meet regulations / requirements, without considering whether it actually works for them.
- Such poor security practices, compounded by lack of attention to security, can quickly compound into a huge loss for companies when their systems are breached. This is made worse when people are fired and replaced when cybersecurity breaches happen. Without institutional memory and experience, the cycle repeats all over again.

- 
- It is important for organisations to note that data loss prevention is not simply a “plug-and-play”, a one-size-fits-all or a one-off solution. In fact, organisations should continuously be: (a) identifying security loopholes within its systems; (b) performing inspections on users; and (c) reviewing its security processes.

How Organisations Can Mitigate Cloud Security Risks

- Cloud services and technologies have become a crucial backbone for many organisations today, which are increasingly migrating their data and workflows into these platforms. In 2022, 94% of companies used cloud services as compared to 61% in 2020. In addition, the global cloud computing market, which is already worth USD 445.3 billion in 2021, is expected to grow to USD 947.3 billion by 2026 – half a billion USD in only five years.
- Cloud adoption has become increasingly common over the years due to the many benefits that it brings to businesses. First, cloud users enjoy greater convenience when accessing their data as compared to retrieving data from local / physical sources. Second, storing data in the cloud is more reliable than storing data locally, as the cloud offers backup and disaster recovery features. These could help prevent data loss in emergencies. Third, cloud computing gives organisations more flexibility in scaling-up resources and storage to meet business demands without having to invest in physical infrastructure.
- However, there are also drawbacks to the cloud which organisations should be aware of. For instance, cloud services have a large attack surface area as they have multiple points of connectivity. As a result, cloud services are susceptible to cyber threats such as data breaches / losses, and denial of service (DoS) attacks.
- Organisations should therefore conduct their own thorough research before deciding whether cloud solutions work best for them. Should they decide to adopt cloud services, they should consider the following best practices to keep their data secure.

- 
- First, put more emphasis on having good data security best practices, such as secure encryption, and multi-factor authentication. For instance, organisations should never keep encryption keys in the same program as sensitive information, and we should regularly assess the efficacy of existing encryption protocols.
 - Second, organisations should consider implementing good network segmentation protocols, and only allowing network traffic that is necessary and appropriate to pass through. In addition, users should only be granted access to data that are required to perform their tasks. This will minimise the number of access points exploited by malicious cyber actors.
 - Third, having a robust intrusion detection system would allow organisations to have an “early warning system” for unusual network traffic. This could potentially be crucial in preventing a DoS attack.

Terrorism

Updates on Terrorism in Southeast Asia

Development of Regional Pro-ISIS Media Group

- Since early 2022, the regional media group that started as the East Asia Knights (EAK) media group was observed to have taken steps to establish itself as a leading media group in the region.
- Since pledging its allegiance to then-ISIS leader Abu al-Hassan in Mar 2022, EAK has released propaganda in different languages used in the region, such as Bahasa Melayu, Bahasa Indonesia, Tagalog and English.
- Apart from using vernacular languages to expand its reach, the group also announced its merger with al-Nibras News Agency, a pro-ISIS media unit that claimed to be from Thailand, in May 2022.
- In style and in substance, EAK was observed to have drawn inspiration from official ISIS media and other regional media groups. This included releasing claims, photosets, eulogies, posters and videos. Most recently, on 7 Jan 2023, EAK began using the name “Al Faris (Knights) Media Center”. The switch to an Arabic name is likely a bid to increase their credibility.

Arrest of Indonesian Pro-ISIS Elements Following Suicide Attack

- The Indonesian Police have arrested seven individuals suspected to have been involved in the 7 Dec 2022 suicide bombing at the Astana Anyar Police HQ in Bandung, which killed two and injured nine.
- The perpetrator of the attack, Agus Sujatno, was identified to have been linked to pro-ISIS group Jamaah Ansharut Daulah. He was previously arrested for his involvement in the 2017 Cicendo Bombing.¹

¹ On 27 Feb 2017, a pressure cooker bomb exploded at Pandawa Park in Cicendo, Bandung. Agus was arrested by police in Mar 2017 for his involvement in the attack.

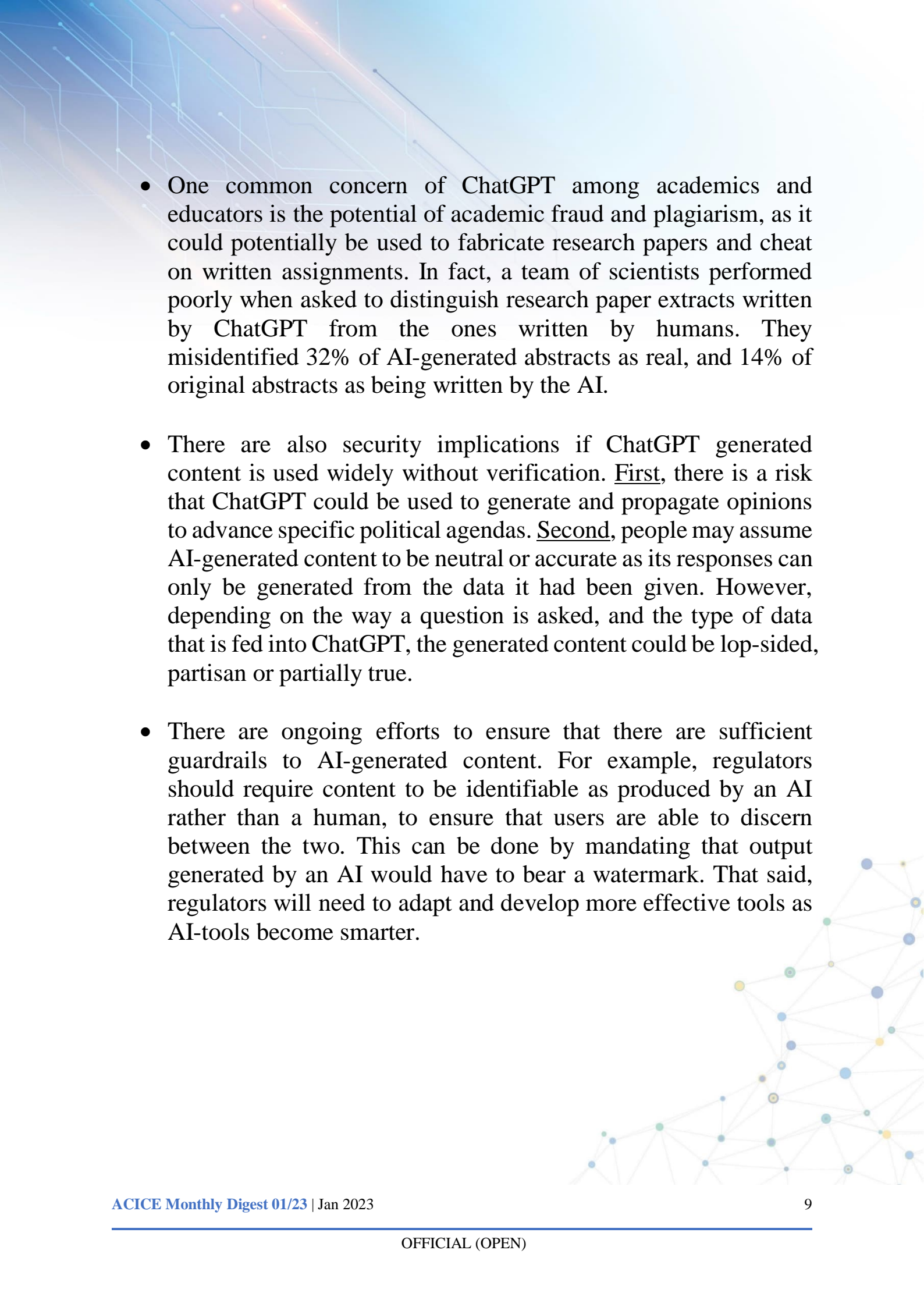
Artificial Intelligence and Disinformation

Is ChatGPT an Eloquent Robot or a Misinformation Machine?

- ChatGPT (or Chat Generative Pre-trained Transformer), a chatbot launched by the artificial intelligence (AI) company OpenAI in Nov 2022, has recently garnered international attention for its generative AI technology.²
- ChatGPT is able to provide a suitable answer to questions posed to it across many disciplines. Since its release, ChatGPT has been used to write a children's book, cover letters, academic essays, and even generate responses to dating application matches.



² Generative AI is the ability to generate text, images and other media in response to short prompts provided by the user.

- 
- One common concern of ChatGPT among academics and educators is the potential of academic fraud and plagiarism, as it could potentially be used to fabricate research papers and cheat on written assignments. In fact, a team of scientists performed poorly when asked to distinguish research paper extracts written by ChatGPT from the ones written by humans. They misidentified 32% of AI-generated abstracts as real, and 14% of original abstracts as being written by the AI.
 - There are also security implications if ChatGPT generated content is used widely without verification. First, there is a risk that ChatGPT could be used to generate and propagate opinions to advance specific political agendas. Second, people may assume AI-generated content to be neutral or accurate as its responses can only be generated from the data it had been given. However, depending on the way a question is asked, and the type of data that is fed into ChatGPT, the generated content could be lop-sided, partisan or partially true.
 - There are ongoing efforts to ensure that there are sufficient guardrails to AI-generated content. For example, regulators should require content to be identifiable as produced by an AI rather than a human, to ensure that users are able to discern between the two. This can be done by mandating that output generated by an AI would have to bear a watermark. That said, regulators will need to adapt and develop more effective tools as AI-tools become smarter.

Annex

Sources

Cybersecurity

- The Right Approach to Data Loss Prevention
 - <https://www.helpnetsecurity.com/2023/01/02/dlp-done-right/>
 - <https://www.lexology.com/library/detail.aspx?g=b3857d8e-7c00-44c4-9aee-3af7ba042d58>
 - <https://www.theverge.com/2022/12/28/23529547/lastpass-vault-breach-disclosure-encryption-cybersecurity-rebuttal>
- How Organisations Can Mitigate Cloud Security Risks
 - <https://www.cloudcomputing-news.net/news/2023/jan/03/views-from-the-field-shifting-left-in-enterprise-cloud-security/>
 - <https://www.analyticsinsight.net/top-10-cloud-computing-trends-to-look-out-for-in-2023/>
 - <https://appinventiv.com/blog/cloud-security-risks-and-solutions/>

Healthcare and the Metaverse

- The Possibilities of Healthcare in the Metaverse
 - <https://insights.omnia-health.com/technology/metaverse-unlocks-new-opportunities-healthcare>
 - <https://www.politico.com/newsletters/digital-future-daily/2022/12/13/mental-health-in-the-metaverse-00073728>
 - <https://gulfbusiness.com/emirates-health-services-to-use-metaverse-technology-to-deliver-healthcare-services/>

- <https://www.forbes.com/sites/bernardmarr/2022/02/23/the-amazing-possibilities-of-healthcare-in-the-metaverse/?sh=1a0175209e5c>

Terrorism

- Development of Regional Pro-ISIS Media Group
 - <https://www.militantwire.com/p/the-rise-of-the-islamic-state-aligned>
- Arrest of Indonesian Pro-ISIS Elements Following Suicide Attack
 - <https://www.thejakartapost.com/indonesia/2022/12/22/police-arrest-seven-suspects-in-bandung-bombing.html>

Artificial Intelligence and Disinformation

- Is ChatGPT an Eloquent Robot or a Misinformation Machine?
 - <https://www.theguardian.com/technology/2022/dec/31/ai-assisted-plagiarism-chatgpt-bot-says-it-has-an-answer-for-that>
 - https://www.washingtonpost.com/business/is-chatgpt-aneloquent-robot-or-a-misinformation-machine/2023/01/12/05da34a6-92c8-11ed-90f8-53661ac5d9b9_story.html
 - <https://www.straitstimes.com/opinion/ai-generated-content-is-taking-over-the-world-but-who-owns-it>

Contact Details

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

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence