ACICE Issue 10/22 (October)

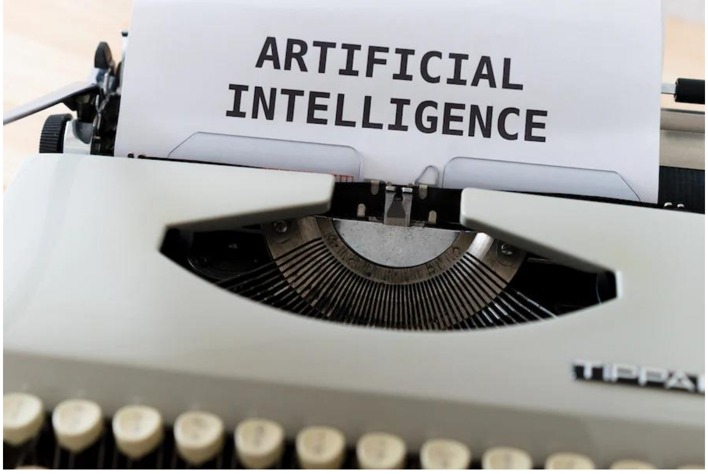
# ACICE Monthly Digest

A monthly roundup of significant news around the world

ADMM Cybersecurity and
Information Centre of Excellence

# Information and Cybersecurity

## The Use of AI and its Impact on Data Privacy



- Artificial intelligence (AI) is widely used around the world to improve users' online experiences. Common applications such as smart assistants, spam filters and search engines, are largely powered by AI.

- While AI offers many benefits, the technology also poses significant risks to privacy, including the potential to de-anonymise data. According to *Information Age*, as AI systems are heavily reliant on large datasets, there is a high probability that these AI systems could expose individuals' private information if they were compromised. With the increasing usage of AI in everyday applications like credit-scoring, AI systems have also become attractive targets for cyberattacks.

- That said, experts have pointed out that AI can have a positive impact on privacy as well. It can be used as a form of privacy enhancing technology (PET)[1] to help organisations comply with data-protection-by-design obligations. AI can also be used to encrypt personal data to minimise the risk of privacy breaches and to detect potential cyber security incidents before they occur.

[1] Privacy-enhancing technologies are technologies that embody fundamental data protection principles by minimising personal data use, and maximising data security for individuals.

- Ultimately, AI is a game-changing technology that is likely to have an increasing presence in the world, but it must be managed responsibly to avoid potential privacy intrusions. For instance, the European Union (EU) is currently developing AI-related privacy protections in law. Similarly, the AI Bill of Rights was recently released in the US, with data privacy as one of the five keystone categories.

## Combatting the Rise of Deepfake Audios

- With the advancement of deepfake technology, there has been a rise in cyber scams using audio deepfakes.[2] According to *The Conversation,* attacks using pre-recorded audio fabrications have already occurred, and audio deepfakes capable of conducting a real-time conversation might not be far off.

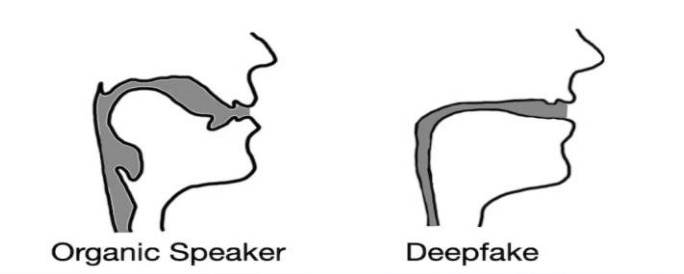
- Audio deepfakes pose a significant threat as people often communicate through phone calls, radio or voice recordings, without visuals of who, or what they are speaking to. These voice-only communications increase the possibilities for malicious actors to use such deepfakes.

- As *Analytics Insight* reported, many researchers have turned to analysing audio artefacts such as minute glitches and inconsistencies to detect audio deepfakes. These analyses found that audio deepfakes are first created by allowing a computer to extract key information about the unique aspects of the target's voice. Thereafter, the attacker would use a modified text-to-speech algorithm to generate an audio sample that sounds like the target saying the selected phrase.

- According to *The Conversation*, in order to detect such deepfakes, researchers extracted vocal tract estimations from deepfake audio and compared those estimations to that of organic human speakers. In contrast to organic human vocal tracts, which are wider and more variable, deepfake audio have estimations that are consistent and narrow – almost akin to a drinking straw (see Figure 1).

[2] A type of artificial intelligence used to create convincing speech sentences that sound like specific people saying things they did not say.

Figure 1: Comparison of Vocal Tracts between Organic Speaker and Deepfake Estimation



- Ultimately, it is challenging for individuals to spot an audio deepfake because most people are not trained to disbelieve their ears. According to *security magazine*, as science and technology leaders continue to develop defences to detect the influence of deepfakes, individuals can adopt the following measures: (a) to remain vigilant, especially if something seems off; (b) do not be afraid to ask questions to verify the caller's identity; (c) to be aware and informed of such threats; and (d) to adopt a zero-trust approach online. Other tell-tale signs include choppy sentences, varying inflection in speech, low quality and lack of conversational flows.

# Humanitarian Assistance and Disaster Relief

### Disaster Mapping through AI Satellite Techniques

Photo of a damaged area caused by hurricane

- Satellite mapping is increasingly being used to identify high-risk areas for floods, wildfires, landslides, and other disasters, as well as to pinpoint the damages after these disasters strike.

- According to *Prevention Web*, AI satellite-based technology could hasten the disaster management process by capturing anomalies over large areas. These anomalies could be water or sand, where the water or sand could be displaced into new areas following a natural disaster. For instance, yellow alert polygons were showed on the map covering all over South Florida five days after Hurricane Ian passed through South Carolina on 1 Oct 2022.

- The machine-learning model also predicts disturbance probabilities, which measures the influence of natural disaster on land surfaces. As such, disaster mapping can be automated and analysts would be able to provide the full coverage of an entire state.

- However, such images are often released publicly only days after the disaster. To improve the effectiveness of the mapping techniques, researchers and analysts should prioritise real-time monitoring features that could provide timely and latest land information in preparation for the next natural disaster.

## Disaster Relief Management Through Satellite Connectivity

- In the last couple of years, the number and magnitude of natural disasters has been overwhelming, as climate change has caused an upward trajectory in the occurrence of such natural disasters.

- According to *IoT Business News*, governments around the world have begun conducting research into developing a holistic disaster management strategy. Recently, there have been breakthroughs in satellite technology that not only reduce the impact of disasters, but can also avert any potential damage right from the start.

- *Interactive Satellite* reported that satellite technology can be an effective tool in combating emergencies. Satellite technology is crucial in providing network redundancy in disaster-critical facilities like hospitals and fire stations. This is extremely useful as it could ensure that service delivery and communication lines within these facilities – especially during life-threatening situations – remain uncompromised.

- For instance, temporary communications network for emergency responders were set up by mounting antennas and equipment on any available surfaces during the aftermath of a mining dam collapse in southern Brazil in Dec 2021. This allowed people who were involved in the rescue mission to respond more effectively to the demands of the situation.

- As satellite systems continue to be an invaluable tool in disaster management, governments around the world – especially those in disaster-prone areas – could consider proactively implementing ways to facilitate such critical satellite connectivity.

# Terrorism

## Varied Recruitment Tactics by Terrorist Organisations

- *Xinhua net* reported that far-right terrorism-related activities have increased over the years. To expand its reach, extremist groups or terrorist organisations have utilised various ways to manipulate and recruit like-minded individuals.

- One of the most common recruitment methods would be through influential preachers. According to reports, ISIS media group al-Furqan Media Foundation[3] published a speech[4] by an ISIS spokesperson who called for Muslims in countries like the Philippines and Indonesia, to join the mujahideen[5] in the Islamic State and support their fight.

- With technological advancements, recruitment tactics are no longer confined to video speeches. There are new recruitment trends observed, such as recruiting young people via gaming platforms. Extremist groups would target young gamers and expose them to dangerous content such as violent re-creations of actual terrorist events. As part of creating recruitment collaterals, terrorist groups have also used drones to capture footages of its operatives carrying out suicide car bombings.

- As terrorist organisations and extremist groups refine their recruitment methods, and tailor them according to information or technological trends, governments and relevant counter-terrorism agencies need to be aware of these latest trends, as well as the possible channels and platforms that may be used.

[3] Al-Furqan Media Foundation is the media wing for the Islamic State and its prior incarnations.

[4] The speech was translated and disseminated by regional pro-ISIS media groups and individuals to their followers on 13 September 2022, demanding them to obey.

[5] Is the plural form of Mujahid, which refers to people who engage in jihad, interpreted in a jurisprudence of Islam as the fight on behalf of God, religion, or the community.

# Maritime Security

## Global Shipping Industry Faces Increasing Risks of Cyberattacks

- As maritime activities in ports around the world gradually return to pre-pandemic levels, the global shipping industry is increasingly susceptible to cyber incidents. *Tech Economy* and *Dark Reading* reported that the issue of cyber threats remains a significant challenge for the sector despite the continued long-term positive safety trend in the industry over the past year.

- According to *Business Day*, the growing reliance on computer systems and software, as well as increasing inter-connectivity within the sector, has made it highly vulnerable to cyberattacks. To date, most cyber incidents in the shipping industry have been shore-based, such as ransomware and malware attacks against shipping companies and port database systems.

- In other words, the longer a ship is docked, the more vulnerable the port is to a cyberattack. This is because docked ships regularly interact digitally with shared-based operations and service providers. Marine insurers have been issuing warning about the potential cyber risks to these shipping ports. According to *Business Day*, the risk could be as significant and dangerous as a terrorist attack, or a nation state group targeting shipping, in bid to inflict damage or cause major disruption to trade.

- While such a severe scenario may seem like a remote possibility, this security challenge remains a serious concern for the shipping industry and marine security sectors to monitor and to develop adequate preparedness measures for.

# Annex

## Sources

### Information and Cybersecurity

- The Use of AI and its Impact on Data Privacy
  - https://www.information-age.com/how-ai-could-be-a-game-changer-for-data-privacy-123500056/
- Combatting the Rise of Deepfake Audios
  - https://www.analyticsinsight.net/fluid-dynamics-will-put-an-end-to-deepfake-audio-scams-soon/
  - https://theconversation.com/deepfake-audio-has-a-tell-researchers-use-fluid-dynamics-to-spot-artificial-imposter-voices-189104
  - https://www.securitymagazine.com/articles/98394-deepfakes-when-seeing-is-no-longer-believing

### Humanitarian Assistance and Disaster Relief

- Disaster Mapping through AI Satellite Techniques
  - https://www.preventionweb.net/news/these-ai-and-satellite-mapping-techniques-are-speeding-process-disaster-management
  - https://theeagle.com/news/science/new-ai-satellite-mapping-can-quickly-pinpoint-hurricane-damage-to-spot-where-people-may-be/article_0d139211-468b-5647-b451-c51cfdb78496.html
  - Photo: WeForum https://www.weforum.org/agenda/2022/10/new-satellite-mapping-with-ai-can-quickly-pinpoint-hurricane-damage-across-an-entire-state-to-spot-where-people-may-be-trapped

- Disaster Relief Management Through Satellite Connectivity
  - https://iotbusinessnews.com/2022/09/02/70352-satellite-iot-helps-make-the-best-of-the-worst/
  - https://interactive.satellitetoday.com/via/september-2022/minimizing-the-impact-of-disasters-through-satellite-connectivity/

Terrorism

- Varied Recruitment Tactics by Terrorist Organisations
  - https://eeradicalization.com/the-use-of-drones-by-terrorist-organizations/
  - https://english.news.cn/asiapacific/20221017/73313368b1794f779c4b054ce753a95d/c.html

Maritime Security

- Global Shipping Industry Faces Increasing Risk of Cyberattacks
  - https://businessday.ng/insurance/article/insurers-see-shipping-face-more-cyber-threats-despite-long-term-safety-trends/
  - https://techeconomy.ng/2022/09/global-shipping-industry-faces-wave-of-cyber-threats-article-by-rahul-khanna/
  - https://www.darkreading.com/attacks-breaches/why-ports-are-at-risk-of-cyberattacks

**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**