ACICE Issue 8/22 (August)

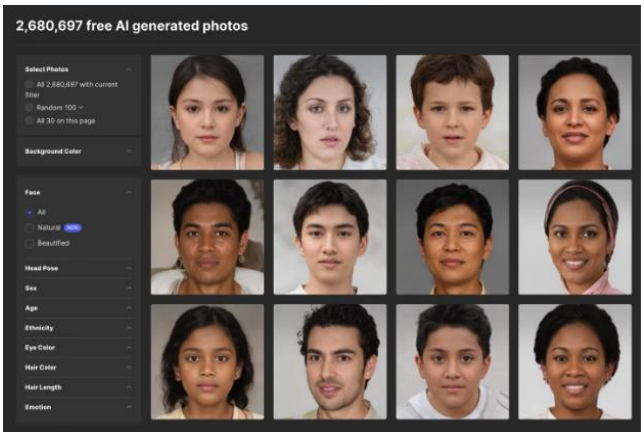
ACICE Monthly Digest

A monthly roundup of significant news around the world

ADMM Cybersecurity and Information Centre of Excellence

Information and Cybersecurity

Proliferation of Artificial Intelligence (AI)-Generated Faces May Lead to Greater Problems



Example of AI-Generated Faces

- By definition, AI is the simulation of human intelligence processes by machines, or computer systems.

- According to *Digital Trends*, social media platforms are cracking down on faceless trolls. However, a growing threat has emerged - AI equipping malicious actors and bots that appear alarmingly authentic.

- Compared to past practices where trolls simply ripped real faces off the internet and anyone could unmask them using reverse-imaging technology, it is now almost impossible to do the same for AI-generated photos.

- For instance, according to *Analytics Indian Mag*, platforms like DALL-E2[1] and StyleGAN2[2] are able to generate images of AI-faces at hyper-speed, resulting in quantities and quality that far exceed human capabilities. These images make it challenging for social media companies or agencies to track and analyse online deceptive content from bots.

[1] DALL-E2 is a text-to-image generative model that creates realistic images and abstract art from a description in natural language.
[2] StyleGAN2 is a generative adversarial network that uses machine learning tools to create images that resemble the distribution of real images.

OFFICIAL (OPEN)

- With the proliferation of AI-generated faces, threat actors are expected to impersonate trusted sources using such images. Experts also believe that the most significant threat posed by AI-generated photos is the “liar’s dividend”, in which the mere existence of such technology allows any media to be dismissed as fake.

- However, AI-generated forgery tools are still relatively new, and these technologies have not yet been completely effective. For instance, a video depicting Ukrainian President Volodymyr Zelensky surrendering was quickly debunked. It is therefore imperative for the private and public sectors to work together to develop strategies to combat potential AI-enhanced disinformation.

- Just as machine learning can be used to amplify disinformation operations, governments could work with technology companies to develop other forms of machine learning capabilities. This could include, for example, using media authentication technologies to protect the information realm.

Humanitarian Assistance and Disaster Relief

The Use of Supercomputer Technology for Disaster Relief

- As technology evolves over the years, countries such as Japan have utilised supercomputers and AI technologies to develop applications that could be used to mitigate the impact of natural disasters[3].

- *Asahi Shimbun* reported that these supercomputer-powered applications could provide real-time countdowns upon being triggered by natural disasters such as tsunamis. These models can also generate flood predictions and send the forecast information to smartphones in each areas within seconds.

- However, the use of such applications do require governments' approvals as the data generated may conflict with official warnings issued by government agencies and could cause public confusion.

- As such, governments could partner relevant technology companies to develop a joint system that could allow for the dissemination of timely and accurate information.

[3] Supercomputer technology refers to the processing of massively complex or data-laden problems using the concentrated computing resources of multiple computer systems.

Terrorism

The Future of al-Qaeda

- *The News Minute* reported that Ayman al-Zawahiri, the leader of al-Qaeda (AQ), was killed in Kabul on 31 July 2022. As one of the prominent leaders of AQ for over a decade, al-Zawahiri was successful in spreading extremist content. His death can be said to signal the end of an era at AQ. It also exposed the underlying "partnership" between AQ and Taliban, where the Talibans were revealed to be sheltering al-Zawahiri despite their security assurances that Afghan territory would not be used as a launch pad by AQ or Islamic State.

- Taliban's violation of the 2020 Doha Agreement (signed with the United States) provides an opportunity for Islamic State to intensify its propaganda war against the Taliban.[4] The Khorasan Province (IS-K)[5], in particular, has been trying to undermine Taliban's ruling of Afghanistan. According to *Politico*, IS-K is now one of the "most vigorous" regional networks of the Islamic State. As IS-K seeks to spread its influence, its radicalised ideologies are likely to spill over to Central and South Asian countries.

- AQ remains an organisation of concern. Several reports indicated that Saif al-Adel, a former Egyptian colonel who is presently living in Iran, will be the next leader of AQ. Other names in contention include Yezid Mebarek, Ahmad Diriye and, Abd al Rahman al Maghrebi.

[4] Under the 2020 Doha Agreement, the US withdrawal of forces from Afghanistan was conditional on Taliban security assurances that Afghan territory would not be used as a safe haven by any Islamic militant groups for attacks against US.

[5] An affiliate of the Islamic State militant group active in South Asia and Central Asia. IS-K aims to establish a global Islamic empire and to undermine Taliban's assurances to the international community that militants from Afghanistan will not target any other countries.

- Given AQ's enduring ties with the Taliban and the Haqqani Network [6], intelligence agencies fear that a Taliban-ruled Afghanistan [7] would remain a fertile ground for AQ and other global jihadist organisations to orchestrate 9/11-esque attacks.

[6] The Haqqani network is an Afghan Islamist guerrilla insurgent group that has used asymmetric warfare in Afghanistan to fight against Soviet Forces in the 1980s, and US-led NATO forces and the Islamic Republic of Afghanistan government in the 21st century.

[7] Under the Taliban's rule in Afghanistan, al-Qaeda has enjoyed 'greater freedom' and some of its members were even advising the de facto regime. However, the partnership between Taliban and al-Qaeda is seen as a violation of the 2020 Doha agreement by the United States in which Taliban has assured NATO that Afghanistan would not serve as a haven for al-Qaeda under its rule.

OFFICIAL (OPEN)

Maritime Security

Increased Cyber-Attacks on Shipping Ports

- According to *Daily Cargo News*, cyber-attacks targeting the maritime sector have increased in the Asia-Pacific region. Ransomware, malware, spear phishing as well as credential harvesting attacks are just some of the threats made against shipping facilities.

- *BBC* also reported that Los Angeles (LA) Port, which is the busiest port in the Western hemisphere, has seen an increase in cyber-attacks since the start of COVID-19 pandemic. It has now developed a Cyber Resilience Centre for heightened protection against cyber threats in the maritime domain. The Port also partners the Federal Bureau of Investigation (FBI) to analyse and share threat intelligence.

- If cyber threats are not properly managed, supply chains could be severely affected as it takes time for the system to recover and for the blockages at the ports to be fully cleared. It remains imperative for the cyber defence of such critical infrastructure to be enhanced. The protection of shipping data centres' operations should be strengthened as well.

Annex

Sources

Information and Cybersecurity

- Proliferation of AI-Generated Faces May Lead to Greater Problems
  - https://analyticsindiamag.com/the-societal-dangers-of-dall-e-2/
  - https://www.digitaltrends.com/social-media/ai-generated-faces-misinformation/
  - https://www.justsecurity.org/82246/the-existential-threat-of-ai-enhanced-disinformation-operations/
  - Photo credits: Digital Trends https://www.digitaltrends.com/social-media/ai-generated-faces-misinformation/

Humanitarian Assistance and Disaster Relief

- The Use of Supercomputer Technologies for Disaster Relief
  - https://www.asahi.com/ajw/articles/14657738
  - https://www.forbes.com/sites/cyrusfarivar/2022/07/05/can-ai-predict-if-your-house-is-going-to-burn-to-the-ground/?sh=14f2edfed171

Terrorism

- The Future of al-Qaeda
  - https://www.thenewsminute.com/article/death-al-zawahiri-and-future-al-qaeda-166863?amp
  - https://www.politico.com/news/magazine/2022/08/02/zawahiris-death-and-afghanistans-future-00049239

Maritime Security

- Increased Cyber-Attacks on Shipping Ports
  - https://www.portlincolntimes.com.au/story/7832830/has-the-government-done-enough-to-protect-against-cyber-warfare/?cs=9397
  - https://www.infosecurity-magazine.com/news/cyberattacks-on-port-of-la-double/
  - https://www.bbc.com/news/business-62260272
  - https://www.thedcn.com.au/news/info-tech/research-shows-increase-in-asia-pacific-maritime-cyber-attacks/

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