ACICE Issue 02/23 (February)

ACICE Monthly Digest

A monthly roundup of significant news around the world

ADMM Cybersecurity and Information Centre of Excellence

Information

The Use of AI to defend against Fake News

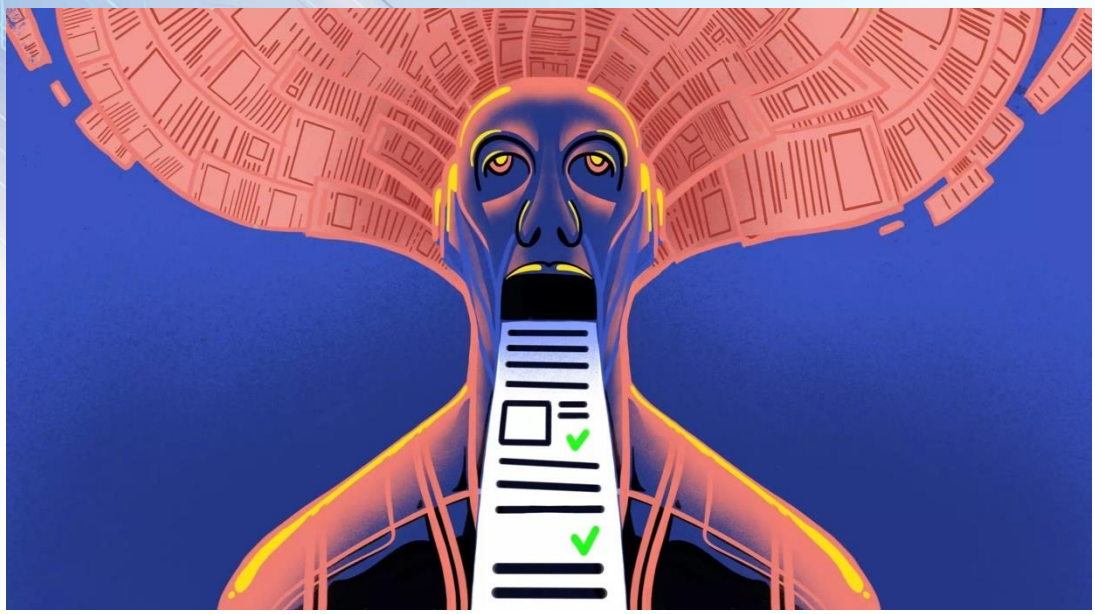
- The modern-day battlefield is multi-dimensional, spanning across domains such as the kinetic, digital and psychological realms. In the rising trend of disinformation operations, countries have upped their game in dealing with information-related threats with the latest technologies, including the use of Artificial Intelligence (AI) to keep tabs on foreign disinformation campaigns.

- In Asia, Japan has ramped up efforts to counter disinformation campaigns. The Japanese Foreign Ministry aims to launch an AI-enabled system in 2023 to collect and analyse 'fake' information on social media and other online platforms. The Japanese hope to use this to track foreign influence operations that may unduly influence public opinion. In conjunction with the Foreign Ministry's efforts, the Japanese Ground and Maritime Self Defence Force will also introduce a specialised information unit and a combined cyber and communications capabilities respectively.

- In the US, the authorities have worked with civil and commercial entities to build technologies to monitor social media platforms. The Cybersecurity and Infrastructure Security Agency monitors and alerts the general public on disinformation threats.

- AI engines such as FactCheck, FaceSwap and DeepFaceLab can be used to sieve out propaganda, manipulate news articles and journalists' opinions. Data analysts can also use AI-enabled forensics tools to discover coordinated influence campaigns by using raw online data to draw network link analyses.

- However, the limitations of AI include the difficulty in discerning human emotions such as satire and humour, which may lead to incorrectly flagged posts. Deep fakes also confuse AI engines and disrupt machine learning to detect disinformation propagated by foreign threat actors.



- To overcome the limitations of AI, states can consider the sharing of information on the development of AI engines, which can enhance their respective AI capabilities in detecting and disrupting disinformation campaigns.

New Features on Social Media Platforms

- Apart from incorporating AI into their defence mechanisms, the governments can also tap onto the new features on social media platforms to guard against undesirable content and fake news from reaching impressionable audiences, such as the younger ones, within their populace.

- Some social media platforms such as Instagram have begun rolling out features that offer users more control over their feeds. For example, users now have the option to block posts containing specified keywords. Along with continued raising of awareness of fake news, the keywords restrictions may have longer term positive impact on the mental health of younger users, including reducing their social anxiety/peer pressure when exposed to unrealistic images of "success", among other things. TikTok has developed a programme to restrict content from reaching teenage users by requiring content creators to specify their target audience's age groups.

- Twitter, under Elon Musk, has announced plans to incorporate Tinder-like swiping on its user interface to allow ease of browsing recommended and followed tweets. Twitter will also roll out long-form tweets from February 2023, which will allow users to post beyond the current 280 character limit,

and reduce the risk of short tweets being misunderstood or taken out of context.

- These protection measures keep advanced aggressors on their toes and deter high-level scammers from manipulating content on social media and other online platforms. Governments can consider further legislation to counter potential security threats to its population or engage in multilateral discussions to promote coordination to tackle disinformation threats in the information domain.

Humanitarian Assistance and Disaster Relief

The Rise of Disaster Relief Scams

- There have been observed incidents of threat actors using disaster relief efforts to scam victims. Emergency management officials are warning residents to beware of unexpected phone calls or home visits from people claiming to work for government agencies providing relief.

- In the US, it was reported that impersonators of government officials had offered to give disaster victims relief grants, while scamming them into providing personal information such as signatures, insurance numbers.

- Similarly in Turkiye and Syria, the BBC reported that scammers had been capitalising on the earthquake tragedies and corresponding outpouring of

sympathy to cash in on donations, including using phrases such as “Pray for Turkey (sic)” and “Donate for earthquake victims” steal donations by diverting funds to their own Paypal accounts/cryptocurrency wallets.

- These disaster scams typically used disinformation tactics such as misleading pictures of previous disasters and warzones to stoke emotional responses from their targets. Hence, there is a need to educate individuals to discern the legitimacy of the donation requests. The governments play an important role to increase media literacy towards donation scams, especially amid advancing technologies to facilitate the creation of deep fakes for disinformation tactics.

Terrorism

Responses to Desecration of the Quran

- The recent burning of the Quran in some European cities had given terrorist groups a reason to galvanise support among those sympathetic to their cause to rise up in defiance of this desecration. The pro-ISIS supporters cited incidents such as Rasmus Paludan, a leader of the Danish far-right political party Stram Kurs (Hard Line), burning a copy of the Quran in Sweden outside the Turkish Embassy in Stockholm on 21 Jan 2023. Days later, Edwin Wagensveld, a Dutch leader of the far-right Pegida movement in the Netherlands, tore pages out of a Quran near the Dutch Parliament and stomped on them. On 27 Jan 2023, Paludan again burned a copy of the Quran in Denmark, in front of a mosque.

- Since these incidents, ISIS and Al Qaeda (AQ) supporters have exploited the Quran burning incidents and called for revenge attacks against Europe and Christians in Europe. This included calls for "lone wolf" attacks with the intent to "strike terror", and attacks against Paludan. The beheading of Samuel Paty in 2020[1] and the 2015 Charlie Hebdo shootings[2] were used as examples to rally supporters to conduct their own attacks. Regional pro-ISIS social media groups such as Al-Faris Media Center have also propagated posters depicting attacks against Paludan.

- Pro-ISIS supporters have justified that a stabbing on a train in Germany (25 Jan 2023), a machete attack in two church in Spain (26 Jan 2023) and mass protests by over 12,000 Islamists from the Tehreek-e-Labbaik Pakistan party people in Lahore, Pakistan were held in retaliation for the desecration of the Quran.

- There have been far-reaching implications of the Quran burnings. Most notable of all was of Turkiye, who have refused to ascent to Sweden and Norway's bid to join NATO. Turkiye previously stated that the withdrawal of support for Kurdish groups whom it deems as terrorist groups was

[1] The beheading of Samuel Paty on 16 October 2020 was carried out by a Russian Muslim refugee in response to allegations that Paty, a school teacher, had shown pictures of Charlie Hebdo's infamous 2012 cartoon caricature of the Prophet Muhammad's face. The French government responses included the promulgation of bill to fight Islamic extremism which was approved by the National Assembly in 2021.

[2] On 7 Jan 2015, gunmen from AQ on the Arabian Peninsula stormed the headquarters of Charlie Hebdo, murdering 12 people, including Charb, the artist responsible for the caricatures of the Prophet Muhammad

paramount for Turkish support. However, since the incidents of the Quran burnings, Turkiye has taken a heavier approach, citing the insensitive and blasphemous nature of the burnings as a step that impedes constructive dialogue at the international level.

Arrest of Pro-ISIS Suspect

- Pro-ISIS suspect Agus Wijayanto was arrested in Yogyakarta, Indonesia on 22 Jan 2023.

- He was active in sharing pro-ISIS propaganda on social media platforms such as Facebook and Telegram and making provocative and consist calls for people to commit acts of violence. He was also suspected of intending to carry out attacks with two homemade bombs that were recovered from his residences.

- In Singapore, a self-radicalised 18 year-old student was detained in December 2022 after it was discovered that he had intentions to incite armed violence in Singapore and declare an Islamic caliphate province on Coney Island. He was radicalised after watching videos online, including videos of foreign preachers and ISIS online propaganda. He was arrested under the Internal Security Act before he could make his oath of allegiance to ISIS.

- This serves as a strong reminder for governments to stay vigilant in the face of self-radicalisation via social media platforms. Monitoring of these spaces can filter out groups which are intent on propagating radical and terrorist-friendly ideology to the impressionable audiences. Governments should take the lead in safeguarding their populace against terrorist groups, such as through working with social media companies to create filters to prevent disinformation from reaching impressionable audiences.

Cyber and Maritime Security

The Danger of Ransomware Attacks on Maritime Software

- The maritime industry has been hit by a number of high-profile cyber-incidents in recent years which might cause substantial economic disruption, as most ships do not have up-to-date technological infrastructure to combat ransomware attacks.

- In 2020, CMA CGM, a French container ship firm was forced to temporarily shut its website and applications due to a ransomware attack. Similarly, in 2017, Maersk, the Danish shipping giant was attacked and close to USD 300 million was lost. It was reported that data gathered from shipping companies could be used to gain insight into their operational systems. This left the companies and their fleets heavily susceptible to any malicious attacks on their software, which could lead to shutting down of shipping lines and possible global shipping delays.

- Major industry players have raised the issue of the high costs of refurbishing older ships with modern technology that is able to resist ransomware attacks. Industry players and governments/multilateral international organisations could consider coming up with joint venture safety protocols, investment in anti-ransomware technology, as well as firewall systems that could be specially developed for the industry.

OFFICIAL (OPEN)

Annex

Sources

Information

- The Use of AI to defend against Fake News
    - https://asia.nikkei.com/Business/Technology/Japan-taps-AI-to-defend-against-fake-news-in-latest-frontier-of-war
    - https://www.spiceworks.com/tech/artificial-intelligence/guest-article/ai-rid-the-internet-of-fake-news-and-bias/
    - https://abcnews.go.com/Politics/trump-signs-order-impose-sanctions-election-interface/story?id=57770888
    - https://www.skynettoday.com/overviews/misinfo

- New Features on Social Media Platforms
    - https://techcrunch.com/2023/01/03/tiktok-ability-creators-restrict-videos-adult-viewers/
    - https://economictimes.indiatimes.com/magazines/panache/long-form-tweets-bookmark-button-swipe-tool-elon-musk-announces-new-twitter-features-rolling-out-in-january/96849912.cms
    - https://www.cnbc.com/2023/01/19/instagram-got-an-update-that-gives-users-more-control-over-their-feeds.html
    - https://www.skynettoday.com/overviews/misinfo

Humanitarian Assistance and Disaster Relief

- The Rise of Disaster Relief Scams
    - https://www.wrbl.com/news/troup-country-officials-warn-avoid-disaster-relief-fraudulent-scams
    - www.bbc.com/news/world-europe-64599553
    - https://my.infotex.com/awareness-poster-disaster-scams-02/

Terrorism

- Responses to Desecration of the Quran
    - https://www.aa.com.tr/en/politics/danish-far-right-leader-burns-copy-of-quran-in-swedish-capital/2793776
    - https://www.thehindu.com/news/international/protests-against-quran-burning-held-across-the-middle-east/article66440061.ece
    - https:www.bbc.com/news/topics/c8grk9gm6nzt
    - https://apnews.com/article/protest-and-demonstrations-denmark-pakistan-islamabad-islam-eeb9b836645a9967c08c2c9fa39c89d0
    - www.britannica.com/event/Charlie-Hebdo-shooting

- Arrest of Pro-ISIS Suspect
    - https://www.manado.tribunnews.com/2023/01/22/agus-wijayanto-ditangkap-densus-88-antiteror-di-diy-punya-dua-bom-rakitan-didgua-simpatisan-isis
    - https://www.straitstimes.com/singapore/teen-detained-under-isa-planned-to-declare-caliphate-on-coney-island-bomb-army-camp-stab-people

Cyber and Maritime Security

- The Danger of Ransomware Attacks on Maritime Software
    - https://www.infosecurity-magazine.com/news/shipping-vessels-ransomware-attack/
    - https://www.seatrade-maritime.com/cyber-security/dnv-ransomware-attack-concerning-cyber-threat-analyst
    - https://splash247.com/up-to-1000-ships-affected-by-dnv-ransomware-attack/

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