

ACICE Issue 3/21 (November)

# ACICE Monthly Digest

A monthly roundup of significant news around the world

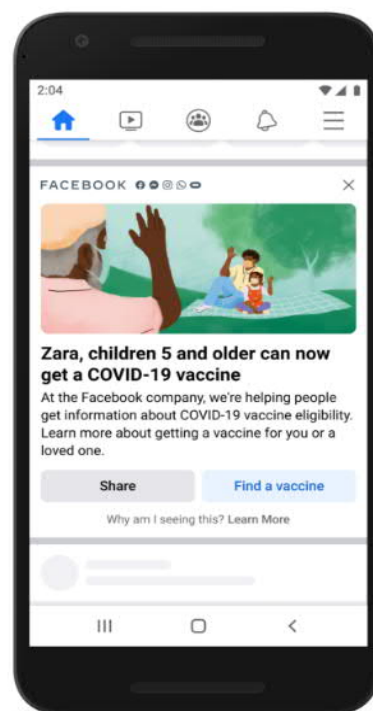


ADMM Cybersecurity and  
Information Centre of Excellence

# Information and Cybersecurity

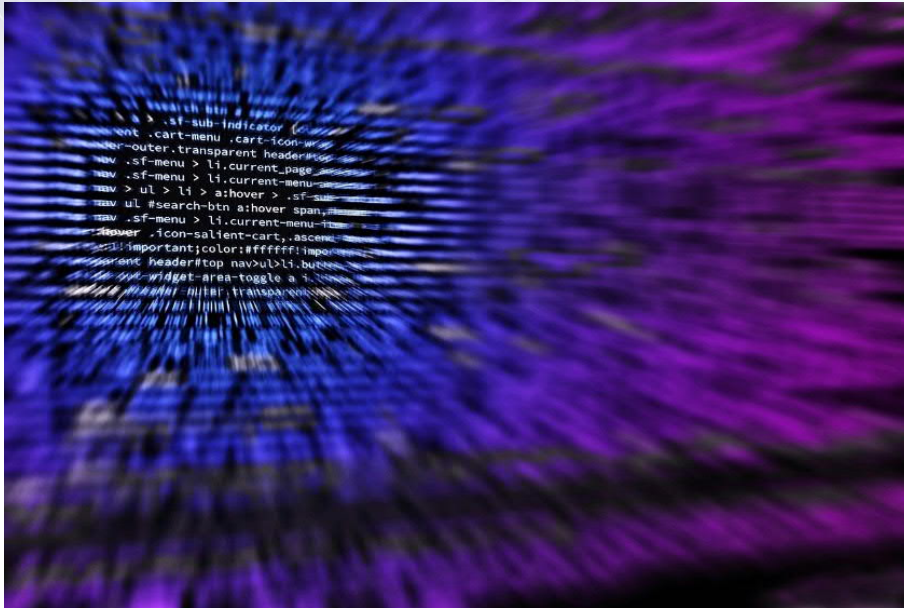
## Facebook puts Tighter Restrictions on Vaccine Misinformation Targeted at Children

- On 29 Oct 2021, Meta, Facebook's parent company, announced that it was rolling out stricter policies for vaccine misinformation targeted at children.
- Meta said that it was partnering with the Centres for Disease Control and Prevention (CDC) and the World Health Organisation (WHO) to take down harmful content related to children and the COVID-19 vaccine. This included any posts that imply the COVID-19 vaccine was unsafe, untested or ineffective for children.
- It would also send in-feed reminders to users in the US that the COVID-19 vaccine was now available for children and the nearest location where they were available.



Facebook's In-feed Reminder about the COVID-19 Vaccine

## Microsoft Warns That Hacker Group behind SolarWinds Hack is Striking Global IT Supply Chains



- On 24 Oct 2021, Microsoft said in an advisory that Nobelium, the hacking group behind the SolarWinds hack, had targeted at least 140 resellers and technology service providers in global IT supply chains.
- It added that Nobelium had turned its attention to software and cloud service resellers in order to “piggyback on any direct access that resellers may have to their customers’ IT systems”.
- Nobelium’s latest attempt was discovered by Microsoft in May 2021, with an estimated 14 confirmed cases of compromise out of the 140 companies that had been targeted.
- The latest round of attacks appeared to not make use of any specific vulnerabilities or security flaws. Rather, Nobelium was relying on spray-and-pray credential stuffing, phishing, API abuse and token theft in attempts to obtain account credentials and privileged access to victims’ systems.

# Humanitarian Assistance and Disaster Relief

## Natural Disasters Can Set the Stage for Cyberattacks



- According to a *Stateline* article, an initiative of The Pew Charitable Trusts, experts said that “it’s only a matter of time” that cybercriminals would take advantage of natural disasters such as hurricanes, wildfires and tornadoes to severely disrupt critical infrastructure such as transportation, emergency response, water and sewer systems, and hospitals.
- A cyberattack during a natural disaster could greatly affect first responders, hospitals, utilities and government agencies. A “domino effect” such as loss of electrical power, water, telecommunications and other infrastructure could be created.
- Experts also added that government agencies should be prepared for such an incident, especially with climate change causing more natural disasters.

## Chinese Tech Giants Contribute to Flood Relief Efforts in Shanxi

- In early Oct 2021, heavy flooding hit the Chinese provinces of Shanxi and Shaanxi.
- More than 1.75 million people in 76 counties in Shanxi were affected by the floods, with over 120,000 people evacuated and five deaths.
- China's big tech companies, including the Alibaba Group Holding, social media and gaming giant Tencent, Beijing-based ByteDance, and search engine and artificial intelligence company Baidu had announced donations of over 300 million yuan (US\$46.6 million) towards flood relief efforts in Shanxi.
- Besides donations, the big tech companies are also using their platforms to help. For example, ByteDance's short video platform Douyin, video-sharing platform Xigua Video and news aggregator Jinri Toutiao had launched special pages on Shanxi's inclement weather so that the population was aware of the situation on the ground.



A flooded area after heavy rainfalls in Jiexu, China's northern Shanxi province

# Terrorism

## Taliban Supreme Leader Makes Rare Public Appearance

- Taliban officials announced on 31 Oct 2021 that the Taliban's supreme leader, Haibatullah Akhundzada, had made a rare public appearance in the city of Kandahar, contradicting widespread rumours of his death. He had not been seen in public since the Taliban's takeover of Afghanistan in Aug 2021, giving rise to the speculation.



A picture of Haibatullah Akhundzada released in 2016

- According to Taliban officials, Akhundzada addressed supporters and visited Jadia Darul Aloom Hakimia, a religious school in Kandahar.
- Although security was tight at the event and no photographs or videos emerged, a 10 minute audio recording was shared on Taliban social media accounts.
- A few days after Akhundzada's public appearance, he also issued a warning to the Taliban that there might be infiltrators among their ranks who were working against them. The warning came in a statement attributed to him and was circulated widely on Taliban social media accounts.

## Continued Use of Social Media Platforms by Pro-ISIS Users in the Region

- Pro-ISIS users in the region continue to use social media platforms to call for violent attacks and martyrdom. An example is regional pro-ISIS supporters praising the brutal stabbing of a lawmaker in the UK who was meeting his constituents in October. Regional social media users praised the attacker as a “lion” with calls for other pro-ISIS supporters to conduct similar operations in Indonesia.
- The most prominent of regional pro-ISIS media unit aggressively spreading violent propaganda is the an-Najiyah Media. The media unit has been spreading propaganda widely via multiple platforms and has launched a “streaming” service known as Jihadflix on Telegram. Users can reach out to specific contacts to obtain the Jihadflix video to view offline, or other propaganda materials.
- In addition, an-Najiyah Media has also launched an app that allows their followers access to a blog, without the need for email addresses or cell phone numbers to use the app. This is with the knowledge that their followers’ accounts are often blocked or shut down on social media and chat platforms. Followers were also reminded to use VPN at all times.



# Maritime Security

## US Lawmakers Back Mandatory Standards for Transport and Logistics Cybersecurity

- In Oct 2021, the US House Committee on Homeland Security hearing on “Transportation Cybersecurity: Protecting Planes, Trains, and Pipelines from Cyber Threats” heard that hackers were increasingly targeting the transport sector, including aviation, rail, shipping and ports.
- During the hearing, members of congress called for mandatory cybersecurity measures for the transport and logistics sectors, in the wake of an increase in ransomware and other cyber-attacks. Examples included the Colonial Pipeline ransomware attack, and cyber-attacks targeting New York’s public transport authority, the Massachusetts ferry system and the Port of Houston, Texas.
- Witnesses to the hearing highlighted that more cooperation and collaboration between operators and government agencies was needed.





# Annex

## Sources

### Information and Cybersecurity

- Facebook puts Tighter Restrictions on Vaccine Misinformation Targeted at Children
  - <https://about.fb.com/news/2021/10/supporting-covid-19-vaccine-children/>
  - <https://www.engadget.com/facebook-covid-19-vaccine-misinformation-kids-074628334.html>
- Microsoft Warns That Hacker Group behind SolarWinds Hack is Striking Global IT Supply Chains
  - <https://www.bloomberg.com/news/articles/2021-10-25/solarwinds-hackers-targeting-tech-supply-chain-microsoft-says?srnd=technology-vp>

### Humanitarian Assistance and Disaster Relief

- Natural Disasters Can Set the Stage for Cyberattacks
  - <https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/10/25/natural-disasters-can-set-the-stage-for-cyberattacks>
- Chinese Tech Giants Contribute to Flood Relief Efforts in Shanxi
  - <https://www.scmp.com/tech/big-tech/article/3151924/chinese-tech-giants-led-alibaba-and-tencent-donate-millions-towards>
  - Photo credits: AFP, <https://www.straitstimes.com/asia/east-asia/thousands->

[evacuated-as-heavy-rain-and-flooding-hit-shanxi-and-shaanxi-in-china](#)

## Terrorism

- Taliban Supreme Leader Makes Rare Public Appearance
  - <https://www.reuters.com/world/asia-pacific/talibans-reclusive-supreme-leader-appears-belying-rumours-his-death-2021-10-31/>
  - <https://www.aljazeera.com/news/2021/11/4/afghanistan-taliban-leader-warns-against-turncoats-infiltrators>
  - Picture credits: AFP, <https://www.straitstimes.com/asia/south-asia/taliban-supreme-leader-makes-first-public-appearance>
- Continued Use of Social Media Platforms by Pro-ISIS Users in the Region
  - <https://www.scmp.com/news/world/europe/article/3152623/britain-orders-security-review-after-mp-stabbed-death-terror>
  - Picture credits: Reuters, <https://www.rand.org/blog/2018/12/isiss-use-of-social-media-still-poses-a-threat-to-stability.html>

## Maritime Security

- US Lawmakers Back Mandatory Standards for Transport and Logistics Cybersecurity
  - <https://homeland.house.gov/activities/hearings/transportation-cybersecurity-protecting-planes-trains-and-pipelines-from-cyber-threats>
  - <https://portswigger.net/daily-swig/inaction-isnt-an-option-us-lawmakers-back-mandatory-standards-for-transport-and-logistics-cybersecurity>

## Contact Details

For any queries and/or clarifications, please contact ACICE at [ACICE@defence.gov.sg](mailto:ACICE@defence.gov.sg)

Prepared by:  
**ADMM Cybersecurity and Information Centre of Excellence**