ADMM Cybersecurity and Information Centre of Excellence

Monthly Digest

Issue 05/24 (May)

A monthly round-up of significant news around the world

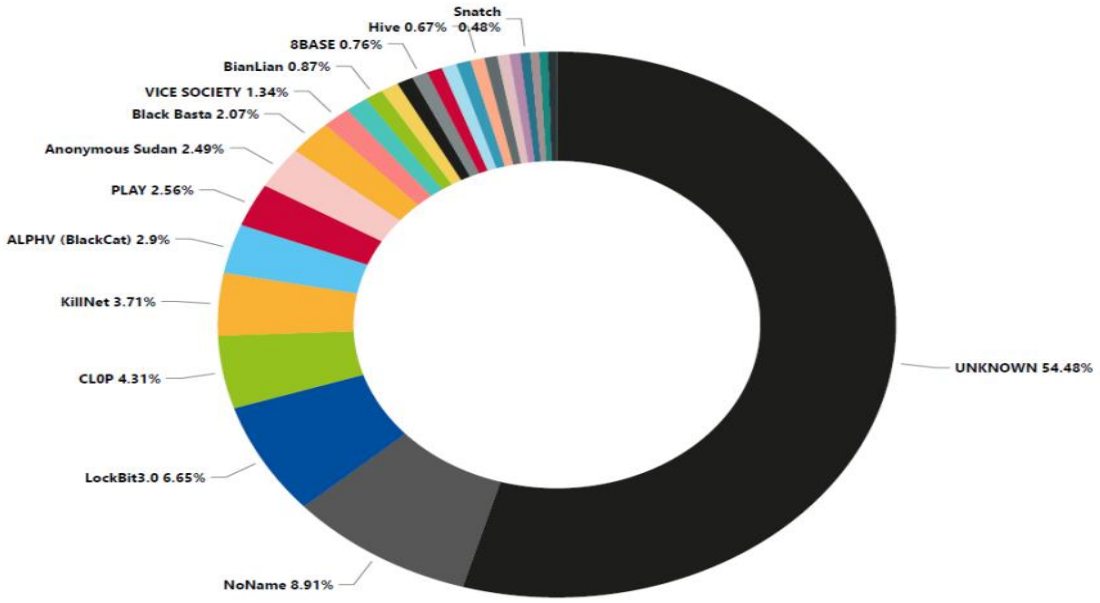
Cybersecurity

Cybersecurity in Supply Chain Resilience

1. Supply chains refer to the systems and relationships between buyers, sellers and suppliers in the production and sale of products. SAP defines supply chain resilience as the ability to anticipate, respond and recover from disruptions in any part of this chain. The fast-evolving technological landscape has created new challenges for supply chain resilience. This section discusses the factors contributing to supply chain resilience, and suggestions to enhance the robustness of supply chains in the face of growing cybersecurity threats.

Cybersecurity Challenges to Supply Chain Resilience

2. Cyberattacks are a major threat to supply chain resilience. As global supply chains rely heavily on technology to expedite their production and logistical processes, any stage of the supply chain process might become vulnerable to cyberattacks. Given the multiple stakeholders and actors within supply chains, technical attribution becomes complicated, if not impossible. European Union Agency for Cybersecurity (ENISA)'s Threat Landscape Report of 2023 found that 54.48% of the cyberattacks were unknown actors. This reflects the complexity in attribution of attacks to the supply chains (see diagram below).

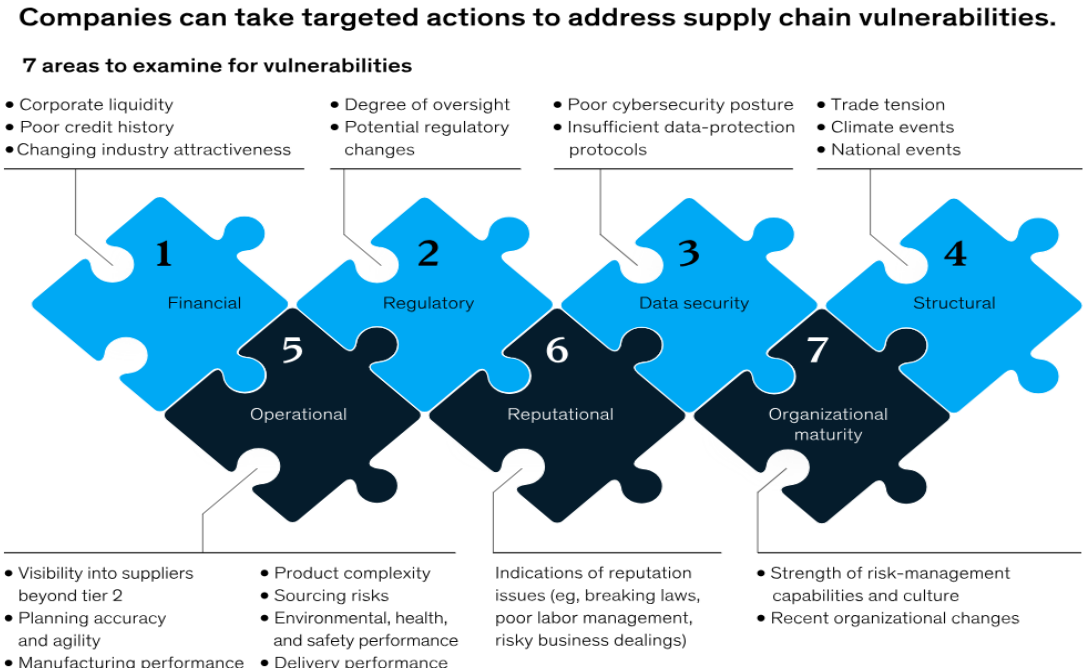


Most attributed threat actors - ENISA's Threat Landscape for Supply Chain Attacks
(Source: ENISA, 19 October 2023)

3. According to the BCI Supply Chain Resilience Report of 2023, cyberattacks and data breaches were ranked the highest in terms of factors comprising supply chain resilience. ENISA reported that malware is the preferred mode of cyberattack, accounting for 62% of all attacks on supply chains. Malicious actors also stole large amounts of data, contributing to 58% of attacks on supply chains.

ENISA's Threat Landscape for Supply Chain Attacks
(Source: ENISA, 29 July 2021)

4. Global e-commerce entities are particularly susceptible to supply chain attacks. For example, Amazon has one of the world's largest supply chains, consisting thousands of suppliers and sellers on their platforms. When operating at such a large scale, supply chains could be vulnerable to breakdowns. According to McKinsey and Company, there are seven main areas that are likely to expose vulnerabilities in supply chains, as shown in the diagram below.



Future Proofing the Supply Chain
(Source: McKinsey and Company, 14 June 2022)

5. A cyberattack on supply chain can have devastating effects. In 2021, Sonatype, an open-source security company based in the US, highlighted a new form of supply chain attack using "dependency confusion" packages, which utilises familiar corporation names such as Amazon to create fictitious codes. These malicious codes were used to steal passwords and credentials, targeted at big corporations' applications such as Amazon, Zillow and Slack. Microsoft thereafter published a research paper on ways to counter such risks to supply chain processes.

Increasing Resilience of Supply Chains

5. Ensuring supply chain resilience is even more critical in the military domain to ensure that operational requirements are protected from potential cyberattacks. In Singapore, the Defence Science and Technology Authority (DSTA) has partnered with Interos to strengthen supply chain resilience through the use of technology. DSTA and Interos will work together to test and adopt digital tools to identify and detect risks in supply chains to mitigate risks to

Singapore's critical defence infrastructures. In another example, the US military has adopted a Digital Twin concept to improve supply chain resilience for semiconductors. The Digital Twin concept allows the US military to simulate changes made to their supply chain ecosystem and assess the possible vulnerabilities proactively, before implementing them in real life.

6. States and militaries can introduce legislative and regulatory frameworks to enhance supply chain resilience. An example is the National Defence Authorisation Act (NDAA), introduced by the US in 2024. The NDAA contains supply chain and stockpile management provisions that seek to reduce vulnerabilities in the Department of Defense's (DoD) supply chain networks. It also includes provisions to build supply chain resilience in critical industries such as semiconductors; as well as provisions to overhaul DoD systems for tracking and managing supply chains. The NDAA will increase coordination among the US government agencies such as the National Security Agency's Cybersecurity Collaboration Centre and private sector manufacturers to improve the cybersecurity of semiconductor design and manufacturing process. Governments around the world can learn from the best practices of other states and militaries to enhance their supply chain resilience, so as to ensure the continuity of essential services, and preserve peace and stability in the societies.

Information

Misinformation and Disinformation in the Spread of Terrorism

1. Extremist activities in Southeast Asia had shown signs of returning to pre-COVID-19 pandemic levels, according to the Southeast Asia Report in 2021. The pandemic had accelerated the growth of digitalisation as many of our daily activities had moved online. The surge of online activity provided a viable platform for extremists to reach out to their target audiences and advance their agenda. This section discusses the common tactics and techniques used by terrorists to spread disinformation and misinformation, and their potential impacts on national security.

2. Sparking Fear Through Threats of Attacks. Terrorists were observed to spread narratives of threats of attacks to heighten social tensions and fears. Commonly used tactics could include (a) distributing pre-recorded videography of historical events such as those used by al-Qa'ida; or (b) disseminating high-quality manipulated images as used by ISIS. These threats sometimes juxtapose actual locations with unrelated terrorism-related content. For example, in December 2017, ISIS-Somalia released a video of a sniper on top of a building in Denver, Colorado to instil fear in the populace. The image was found later to be fake.

Terrorist threats of attacks in New York and Denver
(Source: Joint Counterterrorism Assessment Team (JCAT), 9 August 2018)

3. Leveraging Anxiety and Panic During Times of Uncertainty. During times of heightened uncertainty, such as natural disasters or political instability, the populace might search for information to make sense of the situation. XCEPT, a cross border evidence and policy research group reported on 12 April 2023 that terrorist groups tended to convey distinct ideologies and explanations about event happenings that might affirm people's existing beliefs. Terrorists might also leverage strong emotions of anxiety and anger to fuel extremist narratives by undermining the narratives of government authorities.

4. Targeting Youths' Susceptibility to Extremism Ideologies. Extremist groups are also known to target youths and children as they tended to be more easily influenced and impressionable. Feelings and perceptions of social exclusion and discrimination as well as having low self-esteem are factors that might contribute to the possibility of radicalisation. For example, in January 2024, a Singaporean youth was detained under the Internal Security Act and issued a restriction order. He was found to have been self-radicalised since 2022 after chancing upon videos by far-right Internet personality Paul Nicholas Miller[1]. The youth subscribed to white supremacist beliefs, and believed that African Americans were responsible for the crimes in the US. He hoped to be recruited for violent attacks to "fight for the whites". Case officers and psychologists from the Internal Security Department (ISD) are working with the youth, his family and school to equip him with relevant cyber-wellness skills.

Potential Impacts on National Security

5. According to Singapore's ISD, far-right extremist rhetoric promotes an 'us-versus-them' narrative against members of other communities who are perceived as the enemy. When individuals become self-radicalised, they might identify more with their extremist groups and less with their nation. This might result in reduced social resilience to national security threats, according to a paper titled "Self-radicalisation and national security: new threat, new response" by the Centre of Excellence for National Security (CENS), S Rajaratnam School of International Studies (RSIS).

6. There is hence a need to improve public resilience through regular communication and engagements to socialise the public, especially the youths, to the common tactics used by terrorists to radicalise individuals. For example, the US Global Engagement Center and the Department of Homeland Security released "Harmony Square," a virtual game drawing on an "inoculation theory" that exposes players to various misinformation and disinformation related to elections, including those by terrorists. Similarly, the Game Resource Kit curated by the Singapore Ministry of Defence invites players to reflect on their considerations and responses to various terrorism-related scenarios, such as terrorists' cyberattacks and lone wolf attacks. Governments can consider learning from the best practices of other nations to continuously improve their programmes and initiatives to fight terrorism and extremism, including developing robust and engaging communication platforms.

[1] Paul Nicholas Miller, also known as "GypsyCrusader", gained notoriety for streaming extremist discussions promoting white supremacist and neo-Nazi ideologies. He has a significant social media following on platforms such as like Telegram and Gab.

Terrorism

Malay Media Group *At-Tamkin Malay Media Foundation* Joins Global Translation Group *Fursan Al-Tarjuma*

1. On 25 April 2024, global translation group *Fursan Al-Tarjuma (FaT)* announced the launch of its Malay translation arm, *At-Tamkin Malay Media Foundation (ATMMF)* via Telegram and Rocketchat. *FaT* focuses on translating official ISIS propaganda into various languages; it currently offers official ISIS materials in 23 languages through 16 media units.

2. With this latest addition, *FaT* will possess the capability to produce translations in three key regional languages: Bahasa Indonesia, Tagalog and Malay.

3. *ATMMF* has produced a few translations of *Al-Naba* since its launch.

Statement announcing the addition of ATMMF into FaT

Pro-AQAP Media Group *Malahem Cyber Army* References Southeast Asia

4. Between 8 to 17 April 2024, pro-Al Qaeda in the Arabian Peninsula (AQAP) media unit, *Malahem Cyber Army (MCA)*, released two statements referencing the region, specifically Malaysia and Indonesia.

5. On 8 April 2024, *MCA* released a statement commending the perpetrators of the Molotov cocktail attacks carried out on KK Mart outlets in Malaysia between 26 to 31 March 2024, in response to the sale of socks printed with the word "Allah". *MCA* highlighted that the KK Mart attacks had resulted in the owner of the mart having to "apologise and withdraw the offensive product" which achieved "a great victory for Islam and Muslims", thus underscoring the value of such lone-wolf actions.

6. On 17 April 2024, *MCA* released a statement celebrating the 15 April 2024 Sydney stabbing attack and exhorting lone-wolf attackers to carry out more of such attacks. *MCA* stated that "(d)uring the past two weeks, the world has seen the freedom of actions of the heroes of Islam on three continents, from Indonesia to France to Australia". However, there were no reported recent terror attacks in Indonesia.

Latest Attacks Claimed by ISIS-East Asia

7. ISIS-East Asia (ISIS-EA) claimed three attacks between 4 to 7 April 2024. The attacks included (a) a 31 March 24 attack against the Armed Forces of the Philippines (AFP) personnel in Maguindanao del Sur; (b) an undated attack against AFP forces in Lanao del Norte; and (c) a 5 April 2024 attack against Moro Islamic Liberation Front (MILF) personnel. Of the three attacks, only the 31 March 2024 attack was reported by mainstream media.

8. ISIS-EA has claimed eight attacks in 2024 thus far. Notably, all ISIS-EA attacks since December 2023 have occurred in Maguindanao del Sur and Lanao del Norte provinces.

ISIS-EA attack claims published in Al-Naba 437 and IS-East Asia Province

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

REFERENCES

Cybersecurity

1. DSTA and Interos join forces to advance supply chain resilience through AI-powered intelligence and risk monitoring https://www.interos.ai/press/press-dsta-and-interos-advance-supply-chain-resilience-for-defense-infrastructure/

2. 2024 NDAA maintains focus on supply chain https://www.nationaldefensemagazine.org/articles/2024/2/1/2024-ndaa-maintains-focus-on-supply-chain

3. What is a supply chain attack? https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/

4. What does supply chain resilience mean in 2024? https://www.thebci.org/news/what-does-supply-chain-resilience-mean-in-2024.html

5. Understanding the increase in supply chain security attacks https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks

6. ENISA threat landscape 2023 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

7. Future-proofing the supply chain https://www.mckinsey.com/capabilities/operations/our-insights/future-proofing-the-supply-chain

8. Collaboration, agility and visibility: the supply chain trifecta? https://www.pelico.ai/ressources/our-articles/collaboration-agility-and-visibility-the-supply-chain-trifecta#:~:text=By%20promoting%20agility%2C%20organizations%20can,increase%20efficiency%2C%20and%20reduce%20costs

9. Strategies for achieving pre-emptive resilience in military supply chains https://doi.org/10.1016/j.procir.2022.05.186

10. New malicious NPM packages attack Amazon & Slack https://www.cybersecuritynews.com/new-malicious-npm-packages-attack-amazon-slack/

11. Malicious NPM packages target Amazon, Slack with new dependency attacks https://www.bleepingcomputer.com/news/security/malicious-npm-package-target-amazon-slack-with-new-dependency-attacks/

Information

1. Can uncertainty make us violent? The role of uncertainty in encouraging violent and extremist ideologies https://www.xcept-research.org/can-uncertainty-make-us-violent-the-role-of-uncertainty-in-encouraging-violent-and-extremist-ideologies/

2. The link between misinformation and radicalisation: current knowledge and areas for future inquiry https://www.jstor.org/stable/27209215?seq=12#PT%20-%20Issue%20XVII%2C%20Volume%20I%20-%20March%202023.indd%3A21084

3. Violent extremists likely will continue to use disinformation on social media outlets to instill fear and radicalize others https://www.hsdl.org/c/view?docid=818976

4. Prevention of radicalization on social media and the Internet https://www.icct.nl/sites/default/files/2023-01/Chapter-12-Handbook_0.pdf

5. Countering and exposing terrorist propaganda and disinformation https://www.washingtoninstitute.org/policy-analysis/countering-and-exposing-terrorist-propaganda-and-disinformation

6. Terrorism and self radicalisation https://www.sg101.gov.sg/defence-and-security/current-threats/terrorism-and-self-radicalisation/

7. Armed and explosive? An explorative statistical analysis of extremist radicalization cases with military background https://www.tandfonline.com/doi/full/10.1080/09546553.2021.1957675

8. Mis-and disinformation: extremism in the digital age https://www.london.gov.uk/sites/default/files/2023-12/CTPN%20Report%202023%20-%20Mis-and%20Disinformation%2C%20Extremism%20in%20the%20Digital%20Age%20%28Single%20Pages%29.pdf

9. Self-radicalisation and national security: new threat, new response https://www.rsis.edu.sg/rsis-publication/cens/1031-self-radicalisation-and-nation/

10. The impact of natural disasters on violent extremism https://www.jstor.org/stable/resrep31258.24

Terrorism

1. Marcos condemns ‘cowardly ambush’ of Philippine troops https://www.benarnews.org/english/news/philippine/soldiers-killed-03182024114726.html

2. IS launched ‘official’ Malay media group with IED drone manual, firm warns https://www.scoop.my/news/192555/is-launched-official-malay-media-group-with-ied-drone-manual-firm-warns/

3. Another Malaysian store attacked over sale of offensive socks https://www.straitstimes.com/asia/se-asia/another-malaysia-store-attacked-over-allah-socks