

ACICE Issue 11/22 (Nov)

ACICE Monthly Digest

A monthly round-up of significant news around the world



ADMM Cybersecurity and
Information Centre of Excellence

Sustainability and Cybersecurity

The Role of Cybersecurity in a Sustainable Energy Transition

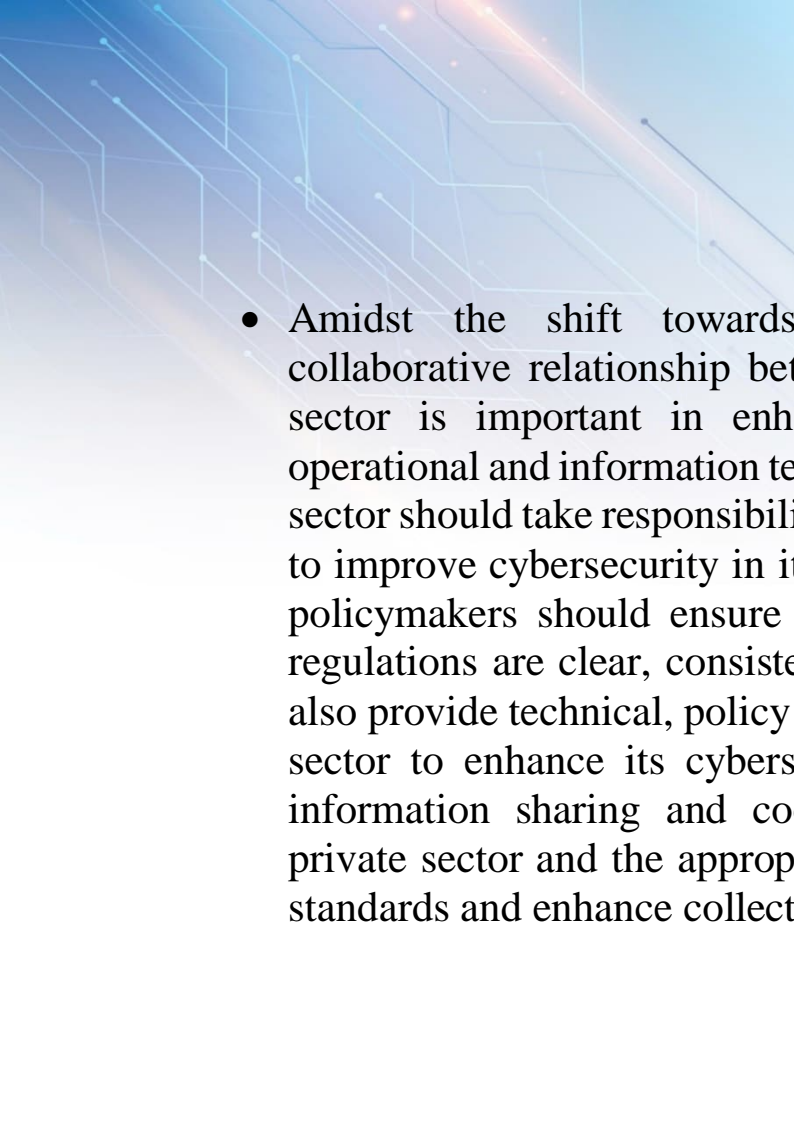
- The global focus on environmental sustainability has accelerated the trend towards digitalisation by transforming personal, commercial and administrative processes and management. For instance, many industries are doing away with manual and labour-intensive processes, including the use of physical forms and documents. These traditional practices and processes are now being digitalised to streamline processes, reduce carbon footprint and minimise the generation of waste.
- The focus on green technology and climate change has cast a spotlight on the energy sector. At the industry level, digitalisation is key to integrating renewables into electricity systems, improving reliability of power grids and reducing cost. Digitalisation also helps to generate and distribute energy in a sustainable and efficient manner. At the retail level, digitalisation allows power generation companies to provide individuals (e.g. smart homes) and businesses (e.g. facility management) a suite of solutions to optimise energy efficiency, reduce wastage and improve user experience with the help of data.

- As the pace of digitalisation increases in society and industries, there is greater urgency to enhance the cybersecurity of operational and information technologies. With critical infrastructure and technologies gradually being brought online, it also inadvertently creates more points of exposure for cyberattacks. Ongoing efforts to build a sustainable future through digitalisation are unlikely to be successful if people and businesses do not have confidence in the systems and technologies that are available.



- A report by the Atlantic Council’s Global Energy Center suggests that the feasibility of a sustainable energy transition will depend on having a strong cybersecurity. Global efforts to build climate resilience could be derailed if cyber threats disrupt the provision of services and undermine user confidence in the availability and utility of systems. This vulnerability was revealed by the single ransomware attack that shut down the Colonial Pipeline in the US in May 2021, paralysing the movement of over half of liquid fuels in the US East Coast.¹

¹ The Colonial Pipeline spans more than 5,500 miles (8,852 km) from Houston, Texas to Linden, New Jersey. The ransomware attack caused massive fuel shortages across several states on the East Coast.

- 
- Amidst the shift towards digitalisation, a healthy and collaborative relationship between the government and private sector is important in enhancing the cybersecurity of our operational and information technology systems. First, the private sector should take responsibility in securing critical infrastructure to improve cybersecurity in its own sector. Second, government policymakers should ensure that existing and future laws and regulations are clear, consistent and robust. Governments could also provide technical, policy and financial support to the private sector to enhance its cybersecurity. Third, there should open information sharing and cooperation between the respective private sector and the appropriate regulators. This will raise the standards and enhance collective awareness within each sector.

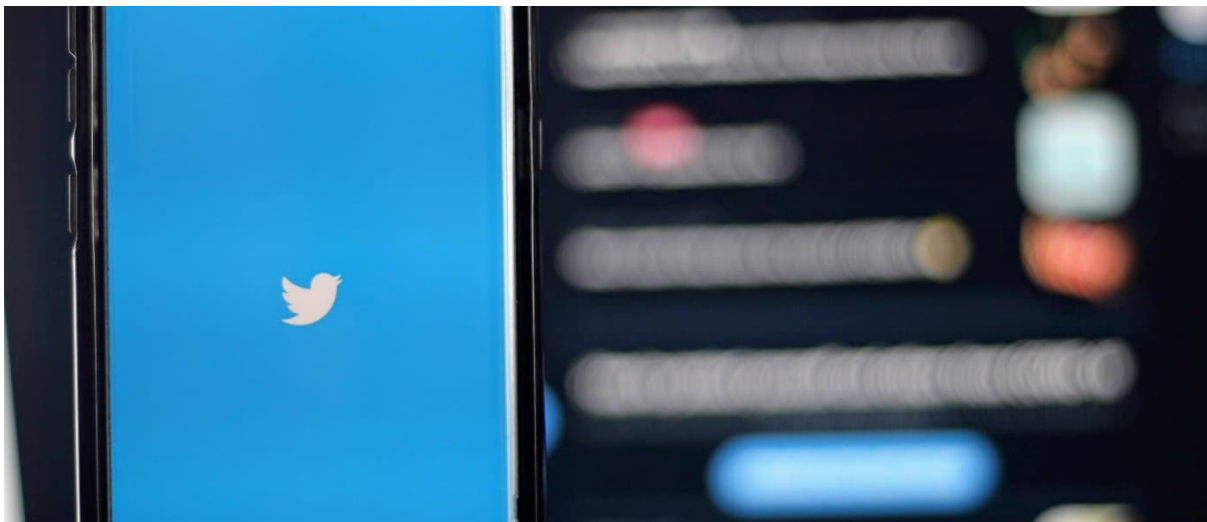


Social Media and Cybersecurity

Big Tech vs Governments

- The world's largest technology companies have made significant contributions to the world we live in today. These companies – commonly known as Big Tech – design, build, and manage platforms and critical infrastructure which we use on a daily basis.
- Big Tech has also been helpful in times of crisis, such as during the Russia-Ukraine conflict. Apple and Google disabled live features in their maps applications, such as real-time satellite imagery and traffic updates, to protect local communities and citizens in Ukraine. Microsoft also helped the Ukrainian government manage cyberattacks directed at the country's critical infrastructure.
- The rapid advance of digital technologies, the privatisation of digital tools and platforms, the opacity of their algorithms, coupled with their enormous wealth, have enabled Big Tech to wield immense power. Often, policymakers and regulators are playing catch up. One example of Big Tech's rise is in the social media domain – where social media companies have the ability to shape what viewers get to see and hear, and even influence their perceptions as well as choices. As a result, there is growing chorus among politicians and civil society for governments to regulate and supervise Big Tech, including their policies.

- In Oct 2022, Elon Musk completed a USD 44 billion deal to buy Twitter, and announced plans to implement his own take on free speech with a slew of changes to how content is moderated on the platform. Twitter had hitherto used a combination of automated and human methods to ensure the credibility of the content put out on its platform, and slow down the viral spread of harmful or misleading content. This, however, will change with Musk's new content moderation policies.



- Creating an online space that fosters free expression is not a zero sum game, but a constant balancing act. Ineffective governance could potentially be detrimental to society. In that light, the European Union (EU) has passed a law, known as the Digital Services Act, to impose new rules on how Big Tech should handle misinformation and regulate content on social media. Governments should consider regulating social media platforms via a combination of moral suasion, self-regulation, as well as legislative or policy levers to safeguard society.

Terrorism

Updates on Terrorism in Southeast Asia

ISIS Claims Attack in the Philippines

- In its 27 October issue of its newsletter, ISIS claimed an attack that took place on 24 October in Kauswagan, Lanao del Norte, Southern Philippines. The attack targeted a communications tower with explosives.
- This is the second such attack against critical infrastructure in the Southern Philippines this year, the first being in February. The attack has been claimed by ISIS as “within the economic war”.
- “Economic war” refers to a common ISIS tactic of targeting the energy and critical infrastructure sectors, to cause financial loss and discontent with local governance over failure to protect such essential sites.

Education and Cybersecurity

Why Everyone needs to be Trained in Cybersecurity

- According to the 2022 Data Breaches Investigation Report published by Verizon, the human element continues to be a key factor in data breaches. While Verizon found that only 2.9% of employees may actually click on phishing emails and fall victim to them, the total absolute number is sizeable enough for cyber criminals to exploit and deliver disproportionate consequences.
- Strengthening an entity's cybersecurity hygiene and posture requires coordination on multiple fronts, such as people, processes, tools and systems. However, there is often too much attention on hardware and processes, instead of human-related factors, such as those that influence people's judgement and responses.
- Training can help to improve security hygiene and best practices, which includes both employees' day to day habits as well as systems' design. Regular training coupled with practical tests and exercises have been proven to make a real difference.
- As Europe's top-ranked country in digital education, Estonia has focused on educating all its citizens on the importance of cybersecurity. This has included informing the elderly on cybersecurity best practices, to teaching kindergarten pupils how to code, and showing teenagers how to run security checks on their smart devices at home.

- For instance, the Estonian Ministry of Defense had collaborated with Estonian companies to organise cyber exercises for students as young as ten. Schools in Estonia also utilise innovative digital tools to allow students, teachers, and parents to collaborate and make teaching and learning more conducive.



- The private sector should also provide cyber awareness and training materials for all, with the aim of benefitting society. Some companies, such as Spanish multinational financial services company Santander, have taken the lead in opening and sharing free cybersecurity training on their websites.

Annex

Sources

Sustainability and Cybersecurity

- The Role of Cybersecurity in a Sustainable Energy Transition
 - [Securing the Energy Transition Against Cyber Threats, Atlantic Council Global Energy Center, 12 Jul 2022](#)
 - <https://www.forbes.com/sites/johntough/2022/09/29/sustainability-and-cybersecurity-the-unexpected-dynamic-duo-of-the-energy-transition/?sh=6318ae58514f>
 - <https://wedocs.unep.org/bitstream/handle/20.500.11822/37439/FB027.pdf>

Social Media and Cybersecurity

- Big Tech vs Governments
 - <https://time.com/6228045/elon-musk-twitter-free-speech-future/>
 - <https://fortune.com/2022/11/16/elon-musk-makes-up-mind-twitter-blue-official-if-enough-verified-followers/>
 - <https://www.nature.com/articles/d41586-022-03552-4>

Terrorism

- ISIS Claims Attack in the Philippines
 - <https://www.benarnews.org/english/news/philippine/philippines-bus-blast-isis-11072022120244.html>
 - <https://globalnews.ca/news/9193385/abu-sayyaf-murder-canadians-philippines/>

Education and Cybersecurity

- Why Everyone needs to be Trained in Cybersecurity
 - <https://www.weforum.org/agenda/2022/11/how-user-experience-and-behavioural-science-can-guide-smart-cybersecurity/>
 - <https://securityintelligence.com/articles/estonia-trust-digital-government/>
 - [2022 Data Breach Investigations Report, Verizon](#)

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