

ACICE Issue 5/22 (May)

ACICE Monthly Digest

A monthly round-up of significant news around the world



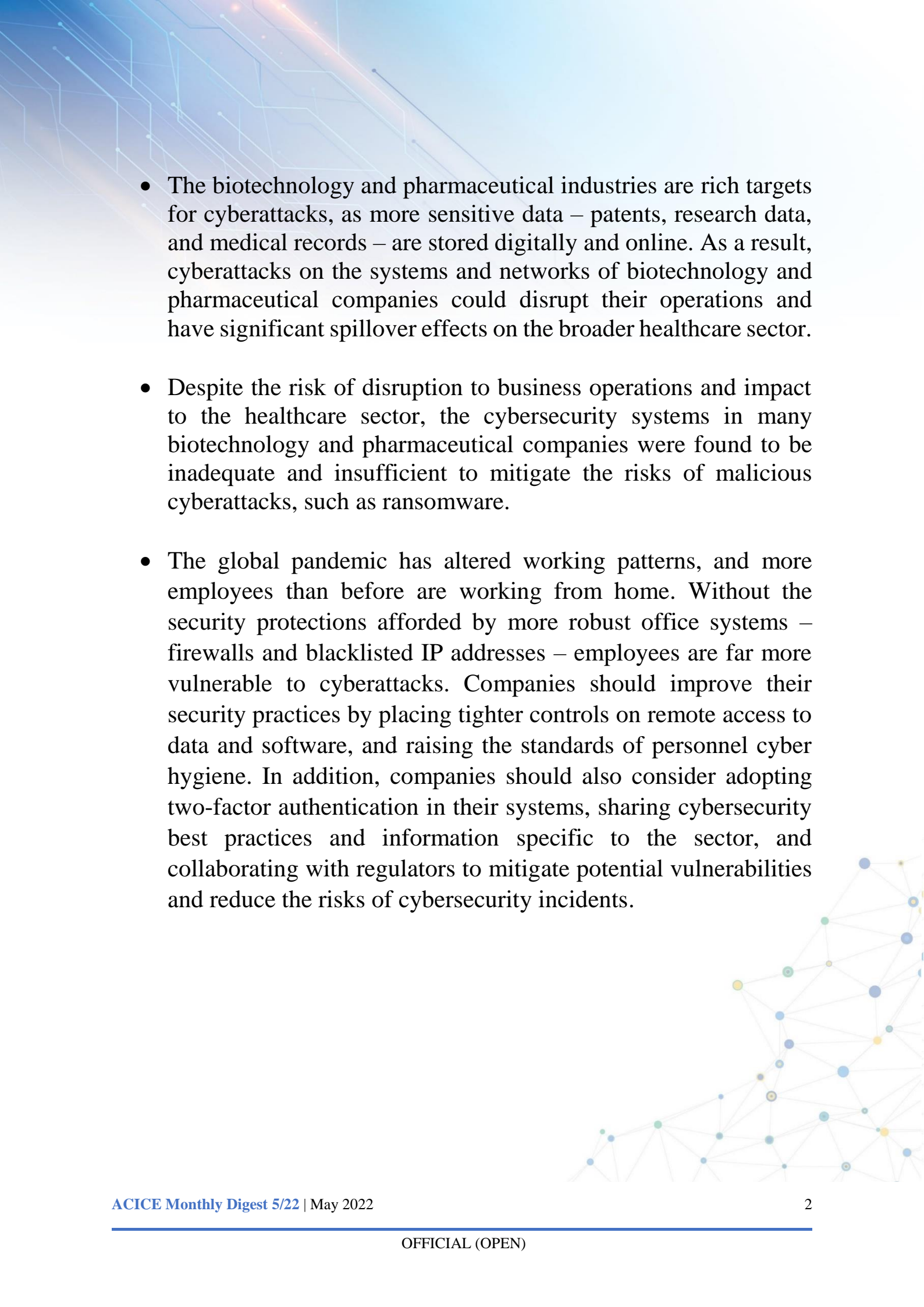
ADMM Cybersecurity and
Information Centre of Excellence

Biotechnology and Cybersecurity

Cybersecurity concerns in the Biotechnology and Pharmaceutical industries

- Cybersecurity experts are increasingly coming to the realisation that the biotechnology and pharmaceutical industries, which include vaccine development, agriculture, and biofuels, are particularly vulnerable to cyberattacks.
- For instance, in the early stages of the COVID-19 pandemic, data on the Pfizer-BioNTech vaccine was stolen during a cyberattack, and subsequently released online. Separately, Black Kite, a cyber risk monitoring company, reported that the NotPetya ransomware attack on Merck, a German multinational pharmaceutical company, crippled more than 30,000 computers and 7,500 servers, causing researchers to lose up to 15 years of research data. The cyberattack also halted Merck's production facilities for the leading vaccine against human papillomavirus. It was reported that Merck's insurance claims could amount to US\$1.3 billion.



- 
- The biotechnology and pharmaceutical industries are rich targets for cyberattacks, as more sensitive data – patents, research data, and medical records – are stored digitally and online. As a result, cyberattacks on the systems and networks of biotechnology and pharmaceutical companies could disrupt their operations and have significant spillover effects on the broader healthcare sector.
 - Despite the risk of disruption to business operations and impact to the healthcare sector, the cybersecurity systems in many biotechnology and pharmaceutical companies were found to be inadequate and insufficient to mitigate the risks of malicious cyberattacks, such as ransomware.
 - The global pandemic has altered working patterns, and more employees than before are working from home. Without the security protections afforded by more robust office systems – firewalls and blacklisted IP addresses – employees are far more vulnerable to cyberattacks. Companies should improve their security practices by placing tighter controls on remote access to data and software, and raising the standards of personnel cyber hygiene. In addition, companies should also consider adopting two-factor authentication in their systems, sharing cybersecurity best practices and information specific to the sector, and collaborating with regulators to mitigate potential vulnerabilities and reduce the risks of cybersecurity incidents.

Humanitarian Assistance and Disaster Relief

Using technology to aid humanitarian work

- KoboToolbox is a free and open source platform, developed by Kobo Inc with funding from the Cisco Foundation, to support disaster relief efforts.
- Used by multiple agencies such as the United Nations, the World Bank, and Doctors Without Borders, KoboToolbox helps to improve data collection, management, visualisation, and analysis in environments with little to no infrastructure and limited access to critical resources. KoboToolbox has been used in every conflict or large-scale natural disaster in the world since its inception in 2014, with the most recent being the Russia-Ukraine conflict. As of May 2022, the number of KoboToolbox users has increased by 130% compared to the year before.
- KoboToolbox is particularly useful in helping humanitarian organisations and relief workers coordinate efforts on the ground and allocate resources effectively. These processes were previously carried out manually in the field, and often resulted in errors and delays.
- During the COVID-19 pandemic, Kobo Inc realised that aid workers were struggling to communicate with their recipients, who may not share a common language. In response, Kobo Inc partnered with CLEAR Global to enhance KoboToolbox with audio capture and speech recognition technology as well as machine learning translation capability.

- These additional features would automatically transcribe speech into text, before translating it into relevant languages, helping aid workers better communicate with local partners and recipients.

Terrorism

Updates on Terrorism in Southeast Asia

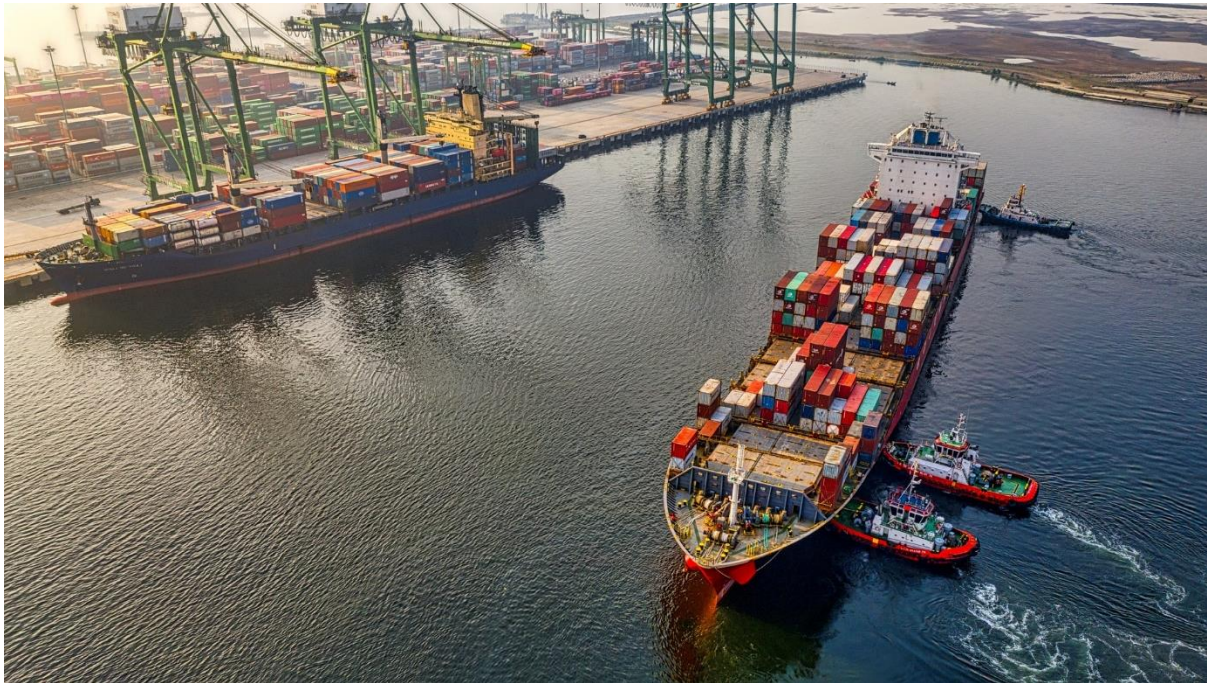
- On 28 Apr 2022, the media arm of ISIS' East Asia Province (ISEAP), a term coined by ISIS to refer to a region within Southeast Asia, issued a communique claiming an attack that took place on 27 Apr 2022.
- According to ISEAP, ISIS fighters had ambushed a Philippine army patrol, killing and wounding nearly 20 soldiers. The high death toll reported by ISEAP was in contrast to the two army casualties reported in the Philippine mainstream media.
- The announcement by ISEAP was likely an attempt to portray the commitment and strength of ISIS fighters in the Southern Philippines, and to boost the confidence of ISIS supporters in Southeast Asia.
- Relatedly, ISIS has claimed responsibility for 346 attacks globally during the Ramadan period. 70% of these attacks took place after ISIS called for “The Revenge of the Battle of the Two Sheikhs” on 17 Apr 2022.¹

¹ ISIS announced its “The Revenge of the Battle of the Two Sheikhs” campaign to call on supporters to take advantage of the conflict in Ukraine to stage attacks in Europe, in response to the deaths of its former leader Abu Ibrahim al-Hashimi al-Quraishi, who was killed during a US Special Forces raid, and its former spokesman, Abu Hamza al-Quraishi.

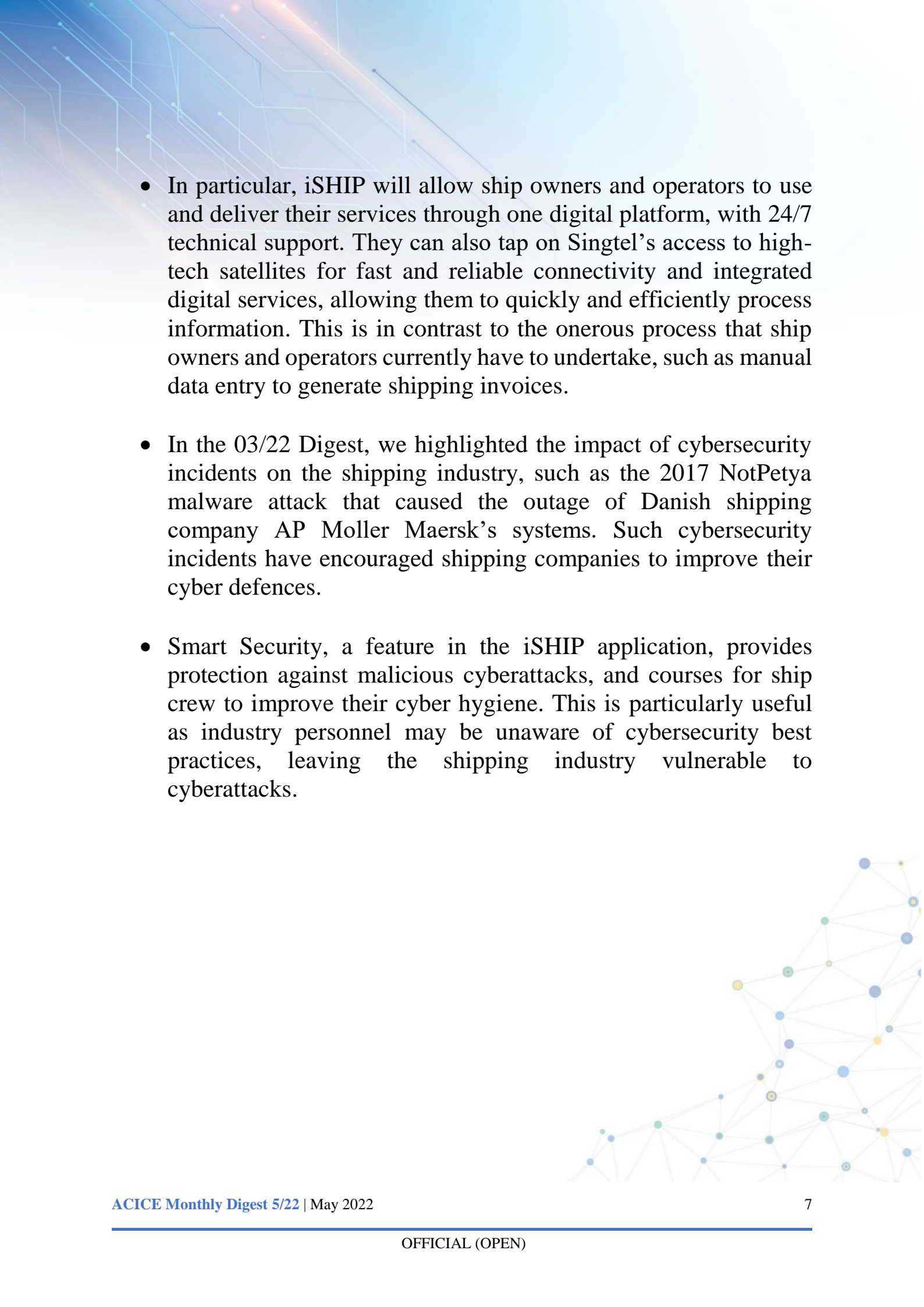
Maritime Security

Satellite-enabled connectivity and digital services for the maritime industry

- With advancements in technology, the shipping industry has been rapidly digitalising its critical operations, such as navigation, power supply, and cargo management, which hitherto were mostly performed manually.



- iSHIP, a new application developed by Singtel, combines satellite-enabled connectivity with digital services for operations, cybersecurity, and crew welfare. In addition, iSHIP provides solutions for shipping companies that are accelerating digital adoption, and working towards being more sustainable.

- 
- In particular, iSHIP will allow ship owners and operators to use and deliver their services through one digital platform, with 24/7 technical support. They can also tap on Singtel's access to high-tech satellites for fast and reliable connectivity and integrated digital services, allowing them to quickly and efficiently process information. This is in contrast to the onerous process that ship owners and operators currently have to undertake, such as manual data entry to generate shipping invoices.
 - In the 03/22 Digest, we highlighted the impact of cybersecurity incidents on the shipping industry, such as the 2017 NotPetya malware attack that caused the outage of Danish shipping company AP Moller Maersk's systems. Such cybersecurity incidents have encouraged shipping companies to improve their cyber defences.
 - Smart Security, a feature in the iSHIP application, provides protection against malicious cyberattacks, and courses for ship crew to improve their cyber hygiene. This is particularly useful as industry personnel may be unaware of cybersecurity best practices, leaving the shipping industry vulnerable to cyberattacks.

Annex

Sources

Biotechnology and Cybersecurity

- Cybersecurity concerns in the Biotechnology and Pharmaceutical industries
 - <https://www.wired.com/story/biotech-security-threats/>
 - <https://www.ecuron.com/cybersecurity-in-biotechnology/>
 - <https://www.biospace.com/article/security-strategist-automation-makes-pharma-a-prime-target-for-cyberattacks-/>

Humanitarian Assistance and Disaster Relief

- Using technology to aid humanitarian work
 - <https://blogs.cisco.com/csr/kobotoolbox-transforming-humanitarian-work-through-voice-capture-and-translation>
 - <https://www.kobotoolbox.org/blog/kobo-and-twb-develop-speech-recognition-software-marginalized-languages>
 - <https://blackkite.com/wp-content/uploads/2021/05/The-2021-Ransomware-Risk-Pulse--Pharmaceutical-Manufacturing.pdf>

Terrorism

- Updates on Terrorism in Southeast Asia
 - <https://www.pna.gov.ph/articles/1173244>

Maritime Security

- Satellite-enabled connectivity and digital services for the maritime industry
 - <https://smartmaritimenetwork.com/2022/05/12/singtel-launches-ishop-platform/>
 - <https://www.telecomreviewasia.com/index.php/news/network-news/2758-singtel-launches-ishop-to-provide-industry-s-first-all-in-one-maritime-service>

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