

ACICE Issue 9/22 (Sep)

ACICE Monthly Digest

A monthly round-up of significant news around the world



ADMM Cybersecurity and
Information Centre of Excellence

Ransomware and Cybersecurity

The Evolving Threat of Ransomware

- Ransomware attacks have evolved from being sporadic and isolated incidents into national security risks capable of massive disruption. 2021 saw several significant ransomware incidents in terms of the scale and extent of disruption caused. For instance, two separate ransomware attacks on the IT networks of Colonial Pipeline and JBS Foods prompted both companies to shut down their operations momentarily, leading to temporary shortages and price hikes.



- According to the Cybersecurity Agency of Singapore's (CSA) annual Singapore Cyber Landscape 2021 report, more local firms fell prey to ransomware last year compared to the year before. There were a total of 137 ransomware cases reported in 2021 – a 54% increase from 2020, which had only 89 reported cases. In addition, it was reported that small and medium enterprises in the manufacturing and IT industries were among the most affected.

- Although authorities have generally discouraged organisations from making payment to cyber criminals, some organisations still prefer to pay to get their data back. There are several reasons why organisations are willing to pay when hit by ransomware attacks. First, certain organisations would like to quickly resume their business operations to minimise their losses. Paying the ransom is thus seen as less expensive than the cost incurred by the ongoing disruption. Second, organisations would be willing to make payments to avoid damage to their reputation. Some may be embarrassed about being hacked due to poor cyber hygiene standards or are fearful that threat actors would release or share stolen business-critical intellectual property or other sensitive proprietary information. Third, some organisations are willing to pay the ransom because their insurance providers are prepared to cover the cost.
- Besides ransomware, CSA's report also highlighted the rising threat of cybercrime in Singapore, as it accounted for 48% of overall crime in 2021. This included threats like phishing, online cheating and cyber extortion, which increased significantly from 2020 to 2021.
- The global threat landscape is evolving rapidly, and ransomware has grown to become the most significant and systemic threat in the world today. Organisations, in particular those managing critical infrastructure, should focus its efforts on preventing ransomware attacks, and investing its money and resources in strengthening its cybersecurity measures. Specifically, they should monitor all devices that are connected to their networks, and take further steps to segregate their networks to ensure that attacks can be contained. Employees should also be held to good cyber hygiene practices, such as ensuring that their systems are regularly patched, and avoiding the use of simple passwords.

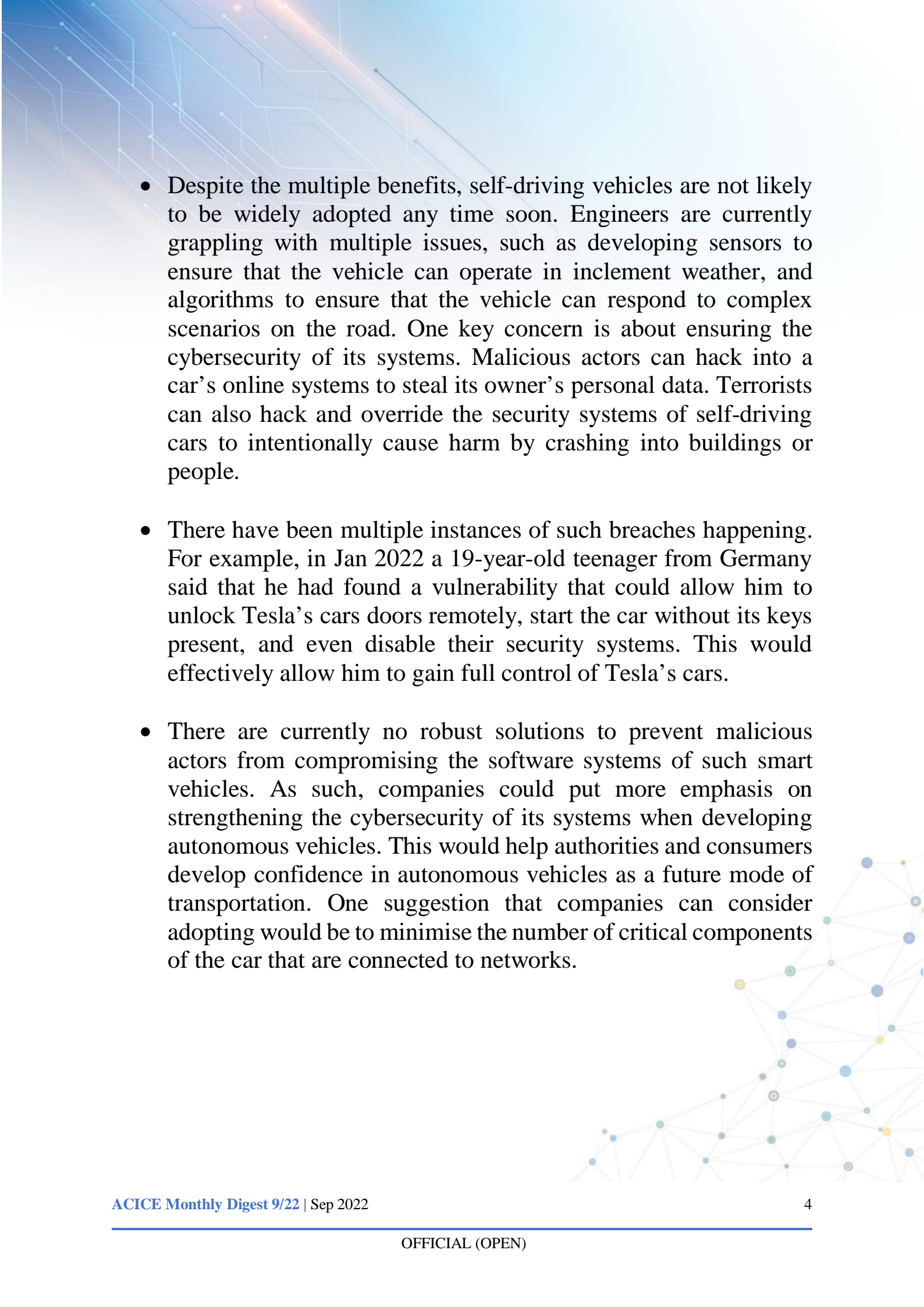
Autonomous Vehicles and Cybersecurity

Self-Driving Vehicles: A Serious Security Risk?

- Apollo Go, the robotaxi arm of Baidu, recently deployed 14 fully driverless robotaxis in Yongchuan, a district in south-west Chongqing, China. Of these 14 robotaxis, five of them are fully driverless, while the other nine have a human safety driver on board to intervene, if necessary.
- There are many potential benefits of self-driving, or autonomous vehicles. First, these self-driving vehicles are reportedly safer and less prone to make judgement errors than human-operated cars. They have been statistically proven to help reduce traffic accidents. Second, they are able to drive more closely to each other as they are equipped with high-tech sensors that allow them to react faster than humans. This would lead to a reduction in travelling time and help ease traffic congestion. Third, self-driving vehicles are more fuel efficient than a human operator as they are able to regulate speed better, through software development.



Photo Credit: Baidu

- 
- Despite the multiple benefits, self-driving vehicles are not likely to be widely adopted any time soon. Engineers are currently grappling with multiple issues, such as developing sensors to ensure that the vehicle can operate in inclement weather, and algorithms to ensure that the vehicle can respond to complex scenarios on the road. One key concern is about ensuring the cybersecurity of its systems. Malicious actors can hack into a car's online systems to steal its owner's personal data. Terrorists can also hack and override the security systems of self-driving cars to intentionally cause harm by crashing into buildings or people.
 - There have been multiple instances of such breaches happening. For example, in Jan 2022 a 19-year-old teenager from Germany said that he had found a vulnerability that could allow him to unlock Tesla's cars doors remotely, start the car without its keys present, and even disable their security systems. This would effectively allow him to gain full control of Tesla's cars.
 - There are currently no robust solutions to prevent malicious actors from compromising the software systems of such smart vehicles. As such, companies could put more emphasis on strengthening the cybersecurity of its systems when developing autonomous vehicles. This would help authorities and consumers develop confidence in autonomous vehicles as a future mode of transportation. One suggestion that companies can consider adopting would be to minimise the number of critical components of the car that are connected to networks.

Terrorism

Updates on Terrorism in the Region

ISIS Spokesperson Urges Muslims in Southeast Asia Province to Join the Fight

- On 13 Sep 2022, ISIS media group al-Furqan Media Foundation published a speech by ISIS spokesperson Abu Umar al-Muhajir, titled “*And Hold Fast, All of You Together, to the Rope of Allah, and Be Not Divided Among Yourselves*”. In the speech, ISIS praised their fighters in the Central Africa Province and West Africa Province, for operations carried out in their respective regions, including raids on prisons.
- Of note, he specifically mentioned Singapore, the Philippines, Malaysia, Indonesia, India, Bangladesh and Pakistan, and called for Muslims in these countries to join the mujahideen in the Islamic State and support their fight.

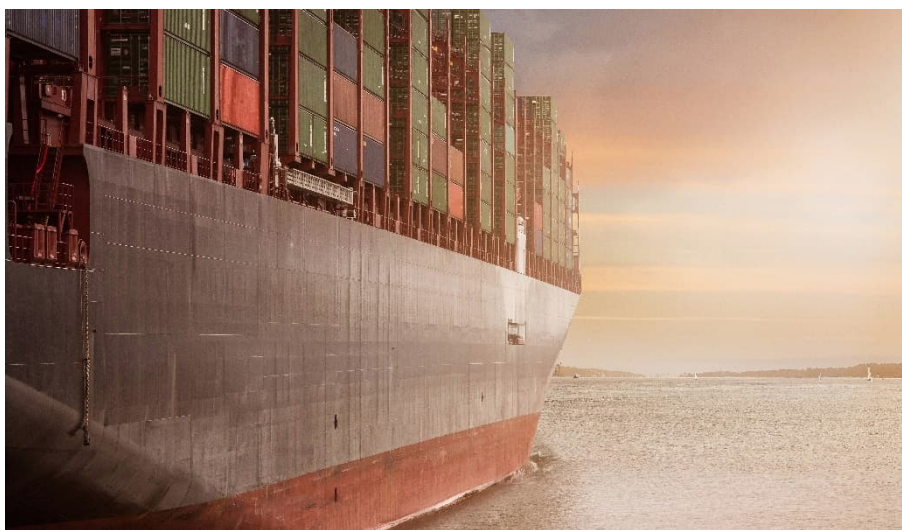
Regional Extremists Commemorate the 9/11 Attacks

- In the days leading up to the anniversary of the 9/11 attacks, regional extremists posted propaganda to commemorate the 9/11 attacks and called for more attacks.
- On 7 Sep 2022, a pro-ISIS media group, *Tamkin Media*, posted two videos of al-Qaeda founder Osama bin Laden detailing the 9/11 operation from its training phase to the bombings. The group also shared photos of the perpetrators. On 10 Sep 2022, another pro-ISIS media group *Milisi Tauhid Media*, published a message titled “Blessed Attacks 9/11” and expressed hope for a similar attack to take place.

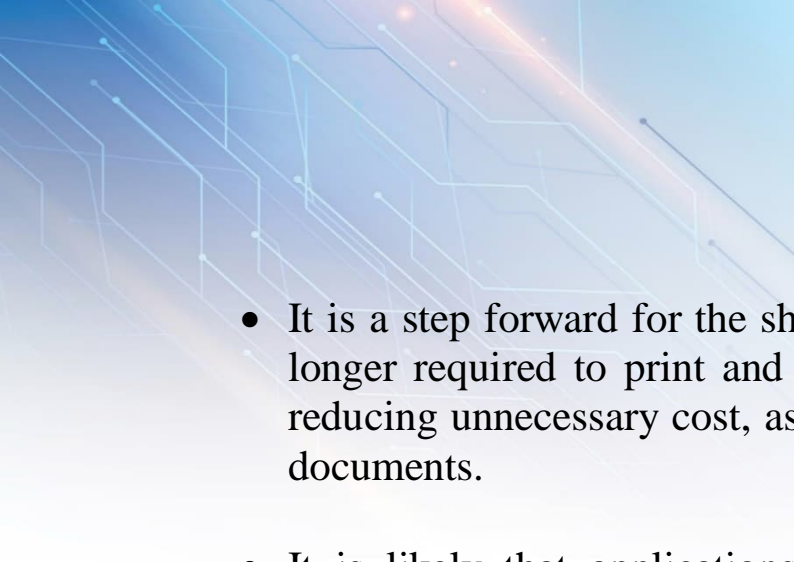
Blockchain Technology and Shipping

Europe's First Electronic Shipping Transaction

- Italian freight forwarder and shipping agency Roberto Bucci has recently completed the first electronic bill of lading¹ transaction in Europe. This was achieved using TradeLens – a supply chain management tool based on blockchain technology.
- TradeLens was created by AP Moller-Maersk, a Danish shipping company, and IBM Blockchain. TradeLens digitised and expedited the shipping process, making it more efficient and cost effective than the conventional way of shipping, which has always involved transmitting physical documents to its intended recipient, which could take days. TradeLens also allowed stakeholders to be constantly coordinated, as shipment information and authorisations are updated automatically through the system and visible to all parties.



¹ A bill of lading is a legal document which outlines the following three information: (a) the exact content of the shipment, (b) the location the shipment is coming from, and (c) the destination of the shipment.

- 
- It is a step forward for the shipping industry, as shippers are no longer required to print and deliver these physical documents, reducing unnecessary cost, as well as the risk of potentially lost documents.
 - It is likely that applications like TradeLens will continue to improve as it becomes widely adopted by shipping companies and ports worldwide. TradeLens can also be integrated with other platforms, to provide a wider range of services for users. One such example is its integration with Skyangel, which allows users to trace the location of its cargo.

Annex

Sources

Ransomware and Cybersecurity

- The Evolving Threat of Ransomware
 - Singapore Cyber Landscape 2021, Cyber Security Agency of Singapore
 - <https://sloanreview.mit.edu/strategy-forum/ransomware-attacks-are-on-the-rise-should-companies-pay-up/>

Autonomous Vehicles and Cybersecurity

- Self-Driving Vehicles: A Serious Security Risk?
 - <https://www.straitstimes.com/asia/east-asia/taking-a-ride-in-a-driverless-taxi-in-chinas-chongqing>
 - <https://securityboulevard.com/2022/08/self-driving-vehicles-a-serious-security-risk/>
 - <https://fortune.com/2022/01/12/teen-hacker-david-colombo-took-control-25-tesla-ev/>

Terrorism

- Updates on Terrorism in the Region
 - <https://www.terrorism-info.org.il/en/isis-spokesman-abu-umar-al-muhajir-calls-on-muslims-around-the-world-to-join-the-organizations-ranks-and-criticizes-other-islamist-organizations/>
 - <https://thesoufancenter.org/intelbrief-2022-september-12/>

Blockchain Technology and Shipping

- Europe's First Electronic Shipping Transaction
 - <https://smartmaritimenetwork.com/2022/08/25/roberto-bucci-introduces-electronic-bill-of-lading-process/>
 - <https://www.pymnts.com/news/blockchain-distributed-ledger/2022/italys-bucci-line-deploys-tradelens-sends-europes-first-electronic-bill-of-lading/>
 - <https://www.pymnts.com/shipping/2022/shipping-dlt-tradelens-touts-q2-integrations-but-few-new-users/>

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