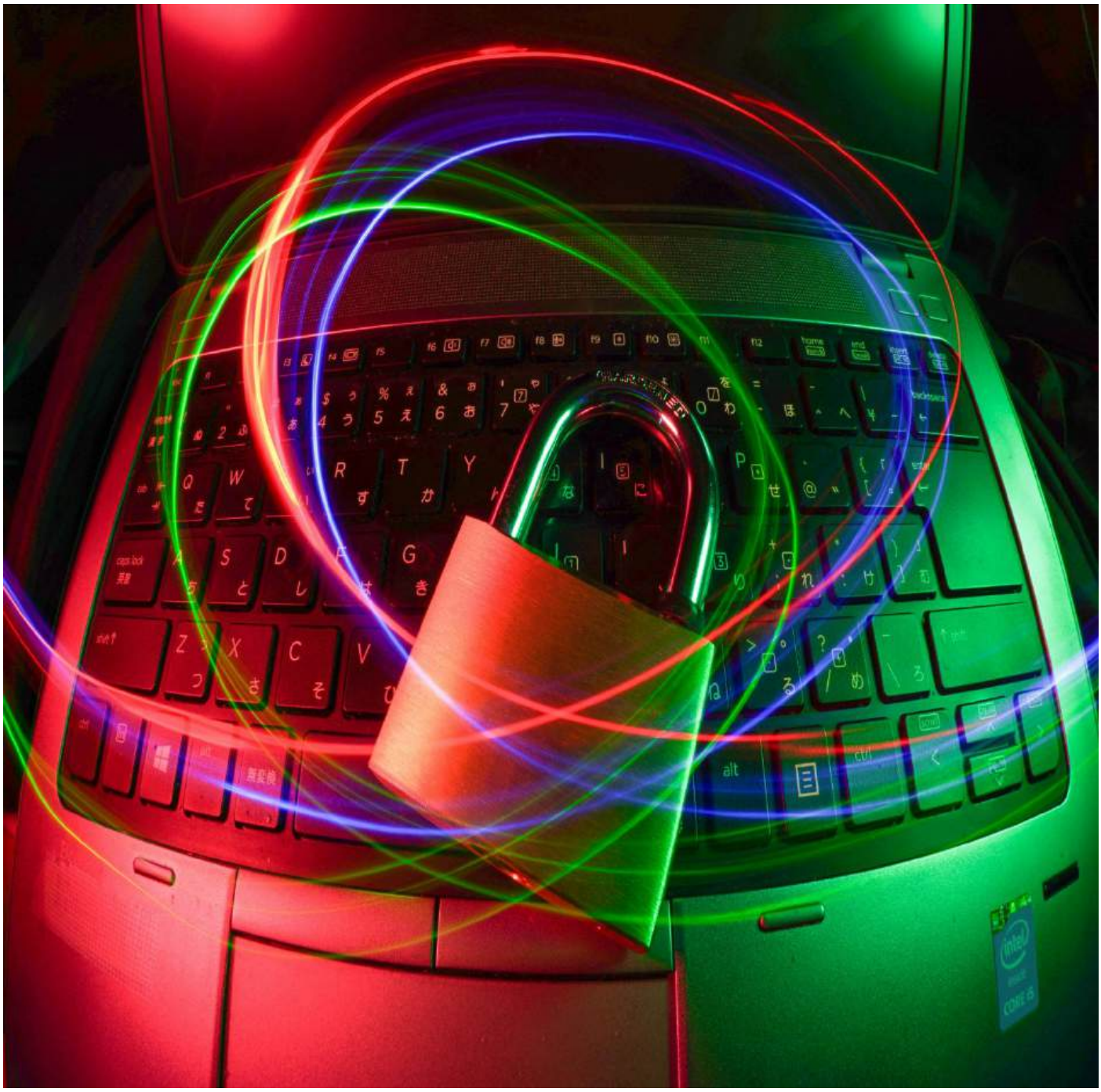
SEP
2025
Vol 6 Issue 9

CILT Buzz

THE CHARTERED INSTITUTE OF LOGISTICS AND TRANSPORT SINGAPORE



Building Cyber Resilience

The Chartered Institute of Logistics and Transport

CONTENTS

Click on title to go to page

3 Chairman's message

9 Cyber attacks on Singapore's Infrastructure

14 Military logistics in cyber threat landscape

23 Vulnerabilities in transport & logistics

27 Supply chain security & third-party risks

31 Tech vulnerabilities in land transport

35 Regulations & governance

37 Harnessing AI

40 Blockchain for secure data exchange

FOR FULL HYPERLINK FEATURES IN CILT BUZZ

- DOWNLOAD PDF file. Open with Adobe Acrobat (recommended).
- Current and past issues of CILT Buzz are downloadable at: https://www.cilt.org.sg/post/cilt-buzz-archive

CHAIRMAN'S MESSAGE

LISTEN 5 min

Dear Colleagues,

It was with great pride that Singaporeans celebrated its 60th birthday with a vibrant and colourful National Day Parade (NDP), featuring national songs and cultural performances. Distinguished leaders from closest neighbouring countries - Brunei, Indonesia, Malaysia - graced the occasion.

The Global Tariffs (BASELINE and RECIPROCAL tariffs) imposed by USA, appear to have "stabilised" for now but uncertainty over SECTORAL tariffs e.g. Semiconductors and Pharmaceuticals still remain. Singapore's Economic Resilience Taskforce (SERT) has since announced its Economic Strategy Review (ESR) to help businesses, unions and other stakeholders navigate after strategically assessing the implications and impacts of the new Tariffs, Changing Global Trade flows and shifting Regional Supply Chains.

As a Major Transhipment Port, it is still unclear how the US will apply its additional "Transhipment Tariffs" of 40% for any imported intermediate goods or finished products originating from China and transhipped via Singapore to the US Market.

AIR — SATS has announced a new air cargo handling facility at the Airport's Changi Airfreight Centre. The new 3,000 sqm BULK UNITISATION PROGRAMME (BUP) Handling Centre simplifies and improves the handling process. Outbound shipments can now be processed within 2 hours, thereby saving half an hour. The facility also serves as a testbed for new systems and processes that may be deployed for air cargo handling at the future Terminal 5 and Changi East Industrial Zone.

SUSTAINABLE AVIATION FUEL (SAF) — DHL EXPRESS SINGAPORE and NESTE (Finland's Renewable Fuel Refinery in Singapore) recently concluded a deal whereby DHL will use sustainable aviation fuel produced in Neste's TUAS refinery in Singapore on Cargo flights out of Changi Airport until June 2026.

Approximately 7,400 tonnes or 9.5 million litres of sustainable aviation fuel will be supplied to DHL, accounting for 35-40% of the total fuel used by DHL's fleet of 5 Boeing 777 Freighter aircraft. Neste's local refinery can produce up to a million tonnes of sustainable aviation fuel. Sometime in

2026, ALL outbound flights departing Singapore will be obliged to use sustainable jet fuel, with an INITIAL National Target of 1% use. Meanwhile, CAAS, in consultation with the industry, is developing the legislative framework and operational details for the proposed Passenger Fuel Levy charge to fund the bulk purchase of SAF, to kick-start its adoption.

MILITARY LOGITICS

SAF — The SAF coordinated the integrated and complex NDP Logistics, Events Planning and Execution at the Padang/Marina Bay sites. The military units included the RED LION's PARACHUTE TEAM and NAVAL DIVERS, RSAF AERIAL FLYPAST, RSN MARITIME DISPLAY, ARMY INTEGRATED MOBILE COLUMN and the HOME TEAM's special assets.

Involving several rehearsals and final execution of the NDP Parade (and related SG60 celebrations, festivities and fireworks), the multi-domain military display marshalled 170 assets and over 800 participants from the defence and security agencies. The ARMY's MOBILE COLUMN journeyed from the City Centre along 5 routes as part of its Outreach to the public at various Heartland Celebrations sites.

RSAF — The RSAF C-130 aircraft recently participated in airdrop operations to deliver Humanitarian Aid, including Medical and Food Supplies, in GAZA. A total of 58 Defence and Military personnel were deployed in support of these Humanitarian Aid operations. Medical supplies were contributed by the Ministry of Health. Food Aid came from NGOs (Humanity Matters, Caritas Humanitarian Aid, Relief Initiatives Singapore, Mercy Relief and the Rahmatan Lil Alamin Foundation). Since March 2024, the RSAF has performed 9 such operations and contributed $22million in assistance to GAZA.

RSN — The Singapore and Indian Navies recently concluded a 5-day Bilateral Exercise involving Ships from both Navies and Aircraft from the RSAF. The Maritime Exercise (SIMBEX) was conducted at the RSS Singapura-Changi Naval Base and at South China Sea (southern reaches). The RSN deployed a Formidable-class Frigate, RSS SUPREME and a Victory-class Missile Corvette, RSS VIGILANCE, supported by Cargo Ship MV Mentor. An S-70B Naval Helicopter, 2 Fokker-50 Maritime Patrol aircraft and 2 F-15SG fighter jets from RSAF were also involved.

The Indian Navy deployed its Shivalik-class Frigate INS SATPURA. The participating forces conducted complex warfare serials, including gunnery firing, air defence exercises and maritime security drills.

Karmjit Singh
Chairman

Taking place in the vibrant city of Colombo, Sri Lanka, this year's convention promises to bring together our global community to connect, learn and celebrate.

What to Expect:

- Inspiring keynote sessions from world-renowned industry experts.
- Interactive workshops and panels addressing the latest trends, challenges, and innovations.
- Networking opportunities with global leaders and professionals.
- Cultural experiences that showcase the rich heritage of Sri Lanka.
- Annual awards ceremony honouring excellence within our profession.

READ: CILT CONVENTION 2025 BROCHURE

REGISTER

CILT International AGM

14 Sep 2025

The Chartered Institute of Logistics and Transport will hold its 2025 Annual General Meeting on Sunday 14 September 2025 at 10:00 hrs (local time) at the Cinnamon Life City of Dreams Hotel, Colombo, Sri Lanka, with online participation available via Zoom.

Members are invited to attend, review the Council of Trustees' report, consider financial statements, and take part in formal business, including the appointment of auditors and approval of revised Bye Laws.

How to attend

- In-person - Join us at the Cinnamon Life City of Dreams Hotel, Colombo
- Online - Register via Zoom

Who can vote

Chartered Members, Chartered Fellows, Emeritus Fellows and Honorary Fellows.

aBuzz

WiLAT Singapore Networking Session
11 September 2025

Join us for an engaging evening as we delve into the sustainability and ESG legal compliance requirements and challenges shaping today's supply chains.

Speaker:

Ms Luo Ling Ling is the Managing Director of Luo Ling Ling LLC. With extensive experience in litigation, arbitration and mediation, she has represented listed companies, government agencies and individuals in complex legal disputes ranging from construction claims and asset management to white-collar crime and regulatory compliance. She has also served as Amicus Curiae in the High Court and is active in pro bono work with the Supreme Court of Singapore, Ministry of Law and Law Society Pro Bono Services.

Ticket (includes light refreshments):

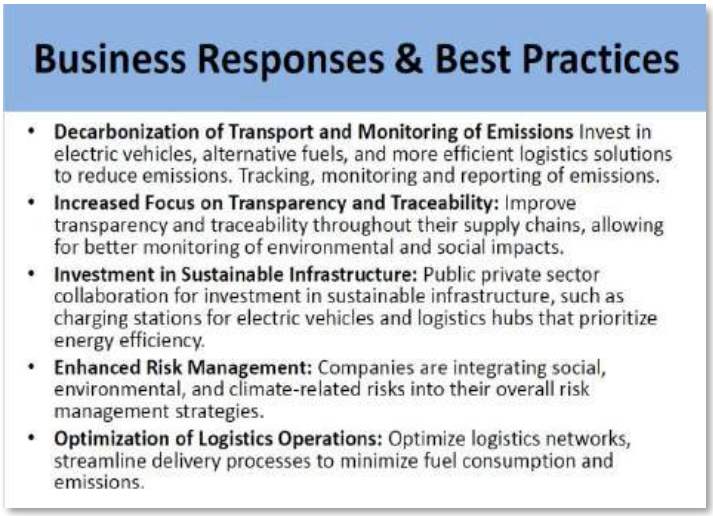
- **CILT Member/Friend of WiLAT: $38**
- **Student Affiliate: $12**

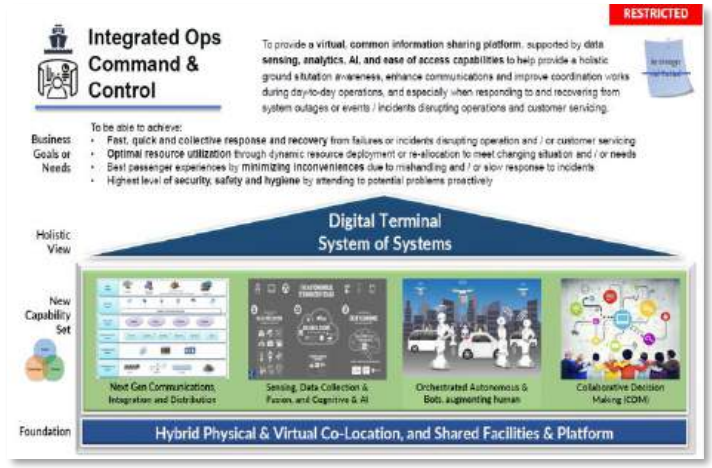
CILTS Transformation & Digitalisation in Supply Chain Webinar Series 2025

The third webinar in the **CILTS Transformation & Digitalisation** webinar series held on 21 August 2025 featured **Sustainable Supply Chains Through Digital Solutions**.

We extend our warmest appreciation and thanks to all our distinguished speakers and participants.

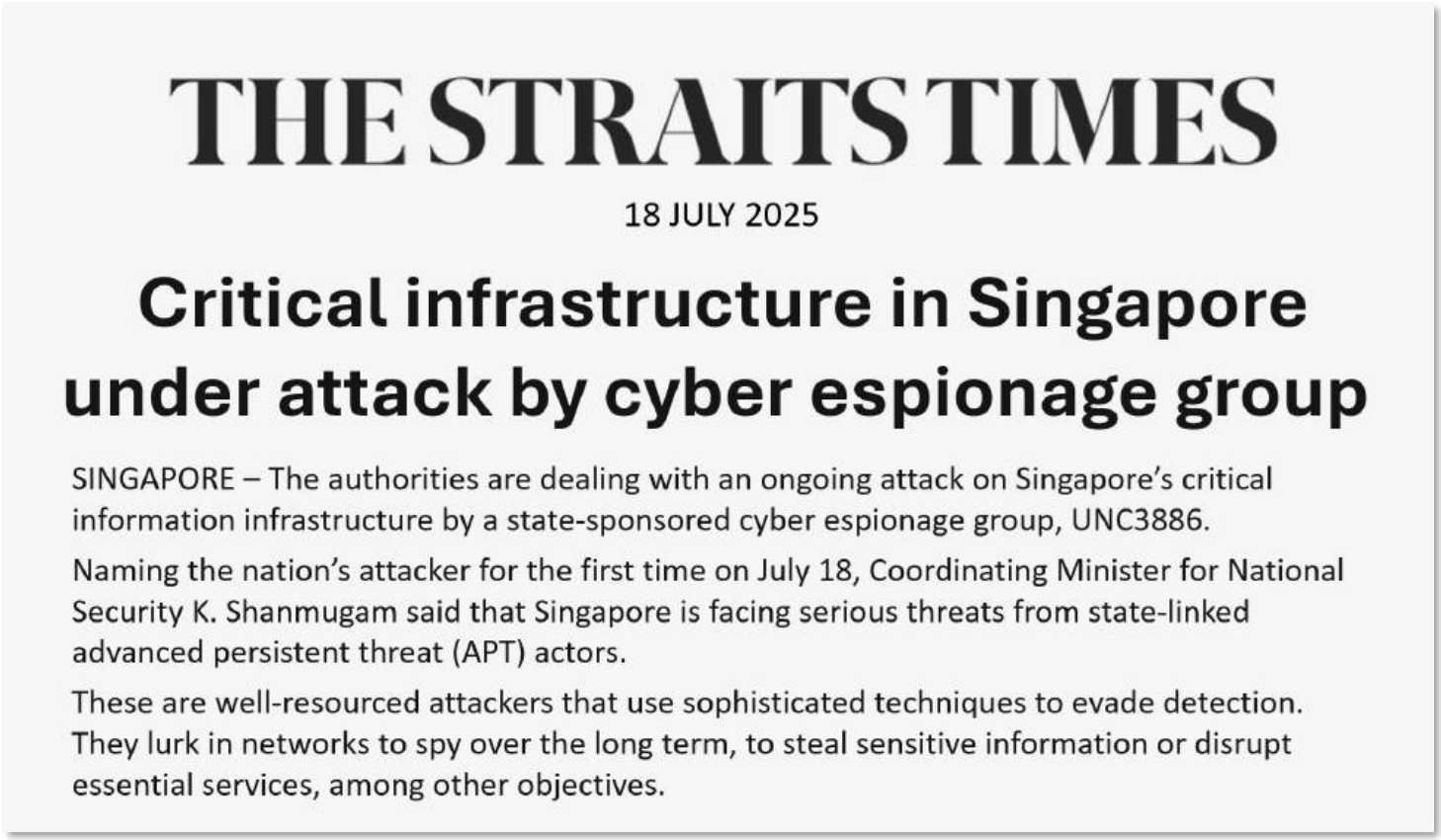
PICTORIAL HIGHLIGHTS OF WEBINAR





WATCH THE WEBINAR
(1:01 hr)

Exclusively for Members
WEBINAR PRESENTATION SLIDES
(requires login to CILTS Knowledge Centre)



THE STRAITS TIMES

18 JULY 2025

Critical infrastructure in Singapore under attack by cyber espionage group

SINGAPORE – The authorities are dealing with an ongoing attack on Singapore's critical information infrastructure by a state-sponsored cyber espionage group, UNC3886.

Naming the nation's attacker for the first time on July 18, Coordinating Minister for National Security K. Shanmugam said that Singapore is facing serious threats from state-linked advanced persistent threat (APT) actors.

These are well-resourced attackers that use sophisticated techniques to evade detection. They lurk in networks to spy over the long term, to steal sensitive information or disrupt essential services, among other objectives.

LISTEN 6 min

UNC3886 Cyber Attacks on Singapore's Infrastructure – Overview and Timeline

Singapore stands at a vital crossroads of global trade, acting as a critical hub in transport and logistics for Southeast Asia and beyond. This strategic positioning also makes it a prominent target for sophisticated cyber adversaries.

In July 2025, the island state publicly disclosed that its critical infrastructure was subject to ongoing cyberattacks attributed to UNC3886, an overseas Advanced Persistent Threat (APT) group.

This article offers a comprehensive overview and timeline of these attacks, setting the context for deeper exploration of technical, regulatory and resilience perspectives in this edition of the CILT Buzz.

UNC3886: The Threat Actor Defined

UNC3886 is recognised in the cybersecurity community as a highly sophisticated, state-backed espionage group with a reputation for persistence and long-term intelligence gathering.

First detected by Mandiant in 2022, with operations observed as early as 2021, UNC3886 primarily targets defence, technology, telecommunications and now increasingly, logistics and critical infrastructure organisations across the US and Asia, including Singapore. The group stands out for its capability to exploit zero-day vulnerabilities in widely deployed network devices (Fortinet, Juniper Networks), virtualisation platforms (VMware), and evade detection through stealthy, customised malware toolsets.

The Singapore Attacks: Public Disclosure and Timeline

The first public acknowledgment of the cyberattacks in Singapore came on July 18, 2025. Coordinating Minister for National Security K. Shanmugam addressed the nation, naming UNC3886 as the group actively targeting Singapore's critical information infrastructure (CII) and underscoring the seriousness and ongoing nature of the threat.

Timeline of Critical Events

DATE	EVENT
Late 2021 – 2022	Initial global campaign tied to UNC3886, focused on IT/OT, telcos, technology and defence sectors.
September 2022	Malware discovered within ESXi hypervisors, prompting deeper investigation by Mandiant.
Early 2023	Observations of zero-day exploitation in VMware and Fortinet devices.
Mid 2023 – 2024	UNC3886 targets Juniper Networks routers with new tailored backdoors, extending to Singapore sectors.
July 2025	Singapore's government publicly names UNC3886 as the active threat against CII (including logistics).
July–August 2025	Ongoing monitoring, sector-wide coordination and incident response by CSA and affected organisations.

This timeline underscores a pattern of persistent and evolving intrusion attempts. Authorities have indicated that UNC3886's presence in affected networks might have predated the public announcement, reflecting typical APT dwell times where attackers maintain protracted, clandestine access for as long as possible.

Sectoral Impact in Transport and Logistics

Singapore's Cyber Security Agency (CSA) did not specify affected sectors in initial statements but highlighted that monitoring and remediation efforts were underway across **all 11 sectors classified as critical information infrastructure—of which land transport, maritime and aviation are prominent.** These sectors are not only economically significant, but also represent potential risks for cascading impacts across supply chains and public operations should they suffer disruption or compromise.

The industry context is especially notable, as Singapore's logistics and transport sectors have continued to thrive amid global headwinds, investing heavily in digitalisation, smart infrastructure and sector expansion. The infiltration of these increasingly digitised environments by state-level cyber adversaries like UNC3886 demonstrates the urgent necessity of robust, adaptive cyber defences that extend beyond traditional perimeter models.

The Fourfold Rise: Escalating APT Threats

Singaporean authorities and industry experts have noted a fourfold increase in suspected APT incidents between 2021 and 2024—a trend mirrored globally as sophisticated groups pivot from data theft to targeting operational technology and infrastructure for both strategic espionage and coercive influence. The escalating scale, ambition and stealth demonstrated by UNC3886 underscore a growing cyber threat landscape that no longer spares even the most prepared digital economies.

Lessons from Previous Incidents

Singapore's recent confrontation with UNC3886 is part of a continuum that includes attacks on:

- The **Ministry of Foreign Affairs** in 2014 (targeting sensitive diplomatic data)
- **National University of Singapore and Nanyang Technological University** attacks in 2017 (espionage targeting transport and defence research)
- The **SingHealth** breach of 2018 (compromising personal/medical records of 1.5 million people)
- Multiple attacks on **financial, infocomm and infrastructure sectors** through third-party and supply chain vectors as recently as 2024.

These prior events have been instrumental in shaping Singapore's current cybersecurity posture, tightening critical infrastructure reporting requirements and catalysing national security investments.

Immediate and Strategic Implications

The ongoing UNC3886 campaign has prompted increased government vigilance, expedited threat intelligence sharing and tighter coordination with private sector operators. Authorities have signalled that preserving operational security may limit the release of detailed forensics or attribution, reflecting best practices in live APT response.

More broadly, Singapore's public attribution of UNC3886 marks a shift toward greater cyber threat transparency—a move with significant regional and geopolitical implications, especially given the unresolved diplomatic debates around direct state attribution for cyber operations.

Singapore's battle against UNC3886 is emblematic of the new reality confronting transport and logistics organisations worldwide—where nation-state threat actors target not just data, but the critical physical infrastructure underpinning economic security and societal stability.

The ongoing timeline of these attacks, and the lessons already emerging, emphasize the need for adaptive resilience strategies, sector-specific defence and coordinated public–private response.

In the following articles of this CILT Buzz edition, we discuss the sector vulnerabilities, evolving regulatory frameworks and global best practices in building digital resilience for the logistics and transport industry.

CYBER DEFENCE

Military Logistics

LISTEN 15 min

Singapore's Military Logistics in a Cyber Threat Landscape: Challenges, Risks and Opportunities

The watershed UNC3886 event underscores the evolving nature of modern conflict where the digital and physical worlds are intimately interconnected, and where military success hinges on both operational prowess and the resilience of the digital backbone underpinning logistics and supply chains.

Singapore's military logistics, long lauded for its efficiency and integration, now faces a new generation of threats. These extend beyond physical interdiction to digital manipulation and sabotage, targeting not only the "tip of the spear" but also the "tail that wags the dog."

This article uses the backdrop of the UNC3886 cyber threats to provide a comprehensive analysis of the challenges, risks and opportunities facing Singapore's military logistics and cyber defence sector.

I. CHALLENGES

1. UNC3886: A Paradigm Shift in Threat Landscape

UNC3886 represents a new breed of state-linked advanced persistent threat (APT) actors. What sets UNC3886 apart is its knack for exploiting zero-day vulnerabilities, often before vendors are aware of flaws in their products. Such vulnerabilities are especially difficult to patch and monitor, representing significant blind spots in security oversight.

Attackers like UNC3886 moved beyond conventional hacking-transitioning to a campaign of digital espionage targeting network devices, hypervisors, routers and virtual machines that constitute the nerve centres of military and logistics networks. The use of custom malware, blending with native system tools to evade detection, and employing living-off-the-land techniques has enabled them to persist, even after their presence is detected and initial cleanup operations are performed.

Key Challenge: Singapore's military logistics must adapt to a landscape where patching known vulnerabilities is necessary but not sufficient. Real-time detection, anomaly monitoring, behavioural analytics and proactive threat hunting have become imperative.

2. Systemic Vulnerabilities in Military Logistics Networks

Logistics is the lifeblood of military readiness, encompassing everything from supply depots to last-mile delivery and maintenance operations via interconnected networks of information technology (IT) and operational technology (OT) systems. The digitalisation of Singapore's logistics architecture brought gains in efficiency and flexibility, but also expanded the attack surface.

Specific architectural challenges include:

- **Network segmentation gaps:** Allowing APTs lateral movement once inside a logistics network.
- **Unpatched and outdated infrastructure:** Especially in OT devices such as SCADA (Supervisory Control and Data Acquisition), programmable logic controllers (PLCs), and warehouse automation systems.
- **Integration of civilian and military supply chains:** Third-party dependencies, IoT devices and shared APIs can serve as convenient attack vectors.
- **Legacy systems and end-of-life hardware/software:** These often exist in logistics due to the high cost or complexity of upgrades, but act as weak links.

Over time, "shadow IT" (unapproved hardware/software) and complex supply chain relationships amplify these challenges, creating internal blind spots for threat detection.

3. Operational Technology (OT) and ICS Vulnerabilities

OT systems underpin the smooth functioning of logistics warehousing, fuel distribution, transportation and facility management. These comprise SCADA systems, building management systems and IoT-enabled devices that are now prime targets for threat actors seeking to disrupt critical services. Unlike IT, OT system vulnerabilities can manifest as physical disruptions, from halting warehouses to manipulating shipments or even causing physical equipment failures.

OT security remains a specific challenge because:

- Many OT protocols lack modern authentication and encryption.
- Patching windows in live, always-on railway networks, energy distribution or logistics hubs can be small or risky.
- Supply chain and OT network monitoring tools are less mature compared to IT security stacks.

4. Complexity of Supply Chain Ecosystem

Singapore's military supply chain extends well beyond government agencies, encompassing private logistics firms, cloud vendors, hardware suppliers and even small subcontractors. While public-private partnerships with firms like ST Logistics have delivered scale and efficiency, they have also woven a dense web of dependencies.

Global case studies such as the 2017 NotPetya attack on Maersk and ransomware attacks on FedEx's TNT Express serve as stark reminders that vulnerabilities in one part of a deeply networked logistics chain can ripple across the globe in minutes, affecting not only shipping but also mission readiness and civilian economy.

5. Human Factor and Cyber Hygiene

Even the most advanced security controls are only as strong as their weakest (often human) link. Inadequate training, poor password management and a lack of awareness about phishing and social engineering attacks remain perennial challenges.

With the proliferation of IoT devices, bring-your-own-device policies and distributed workforces, enforcing consistent cyber hygiene becomes ever more difficult.

II. RISKS

1. Strategic Risks: Weaponising Military Logistics

The strategic intent of groups like UNC3886 extends beyond data theft to degrading military readiness, delaying force projection or even undermining public confidence in national defence.

For a highly networked hub like Singapore where the military, economy and society are tightly interwoven, cyberattacks on logistics can quickly escalate into critical national security events.

Attack scenarios include:

- **Supply chain poisoning:** Insertion of compromised components or manipulated data into the logistics stream.
- **Cascading failures:** Manipulation of fuel, ammunition, or maintenance logistics to slow or halt ongoing operations.
- **Disruption of C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance):** Through attacks on logistics nodes, disrupt the broader operational tempo.

These risks are compounded in a world of "hybrid" conflict where digital disruption can precede, accompany or replace physical attacks.

2. Operational Risks: Mission Impact and Lost Readiness

From an operational viewpoint, a successful cyberattack can:

- **Halt shipment tracking and asset visibility:** Preventing just-in-time supply, as seen with Maersk's global meltdown where thousands of shipments were stuck.
- **Corrupt maintenance schedules or requisition orders:** Leading to missed maintenance windows, equipment downtime or misallocation of resources.
- **Manipulate sensor data in OT/ICS:** Wilful misreporting of inventory levels or rerouting shipments.

Rapid, trusted recovery is critical. However, legacy backup strategies often fail to meet real-world attack scenarios where malware can wipe domain controllers, rendering rapid reconstruction impossible. The risk, therefore, is not just disruption but prolonged loss of capability.

3. National Security Risks: Compromising "Total Defence"

Singapore's "Total Defence" doctrine weaves together military, economic, civil, social, psychological, and digital dimensions. Cyber-enabled attacks can simultaneously challenge all six pillars:

- **Military Defence:** By degrading logistics, adversaries can weaken deterrence and warfighting capability.
- **Economic Defence:** Logistics is foundational to trade, finance and daily life in Singapore.
- **Civil and Digital Defence:** Attacks can spread into civilian sectors (e.g. healthcare, transport), as seen in past APT activity against Singapore's universities and hospitals.
- **Psychological and Social Defence:** Prolonged outages or perception of vulnerability can undermine public trust.

4. Supply Chain and Third-Party Risks

Compromised suppliers, digital service providers or outsourced logistics partners offer adversaries an alternative route into military networks. The globally distributed, multi-country nature of logistics partners means that adversaries can exploit weak links, often those least resourced in cyber defence.

NotPetya, for instance, did not directly target Maersk, but an infection in a Ukrainian tax software supplier quickly crippled the globe's largest shipping operator. The total cost of disrupted operations was estimated at US$250-$300 million for Maersk alone, with tens of millions more in knock-on effects for logistics partners.

5. Evolving Risk: AI, Autonomous Systems, and Supply Chain 4.0

The integration of AI, digital twins and advanced automation into military logistics, while promising for efficiency, introduces new risks. AI-driven predictive maintenance relies on large datasets which, if tampered with, can lead to wrong decisions about equipment health. Adversarial "data poisoning" attacks can corrupt models or skew supply chain forecasts, amplifying operational risks.

III. OPPORTUNITIES

1. Advancing Cybersecurity Resilience in Military Logistics

Faced with relentless cyber adversaries, Singapore's military and logistics sectors must turn crisis into a platform for innovation and future advantage.

Key opportunities include:

A. Proactive Supply Chain Risk Management and Modernisation

The digital transformation journey underway in MINDEF/SAF-integrating AI, cloud and advanced analytics must be matched with cyber supply chain risk management at every node, from data centres to "last mile" IoT sensors. **Zero trust architectures** should become standard, allowing only verified users and devices access to sensitive functions, even within "trusted" internal networks.

B. Embedding AI and Digital Twins for Resilient Logistics

AI-driven predictive maintenance, already used to streamline equipment upkeep, also enables real-time anomaly detection in logistics, flagging subtle indicators of cyber and physical tampering. Digital twin technology - virtual replicas of supply chains - can run scenario-based stress tests, enabling logistics planners to rehearse responses to

disruptions ranging from cyberattacks to natural disasters, improving readiness and resilience.

C. Enhanced Cyber Training and Workforce Development

Singapore has taken major steps in building a cyber-savvy workforce, expanding training through dedicated Cyber NSF schemes, digital and AI-focused "Work-Learn" programmes, and the establishment of a national Cyber Defence School and Cyber Defence Test and Evaluation Centre (CyTEC). Exercises such as CIDeX expose defenders to real-world OT/IT attack simulations, including emerging threats against AI-powered and cloud-based systems.

Continued investment in training, "red teaming," cross-sector exercises, and international knowledge exchange (e.g. with Dragos, Microsoft, Google and regional counterparts) will strengthen Singapore's operational and strategic "cyber muscle".

D. Partnerships and Ecosystem Collaboration

Singapore's strategy stresses **whole-of-government** and **public-private** cooperation-linking MINDEF/SAF, the Cyber Security Agency (CSA), major logistics firms (e.g. ST Logistics), academia and international partners in the tech industry. The CIDeX exercise and joint MOUs with academic institutions and cybersecurity partners build a bench of expertise and support a "network of networks" approach to defence, coordination and recovery.

---

2. Innovating Logistics Practices: From Automation to Secure-by-Design

Digital Logistics Innovations:

- **Cloud and AI-Integrated Supply Chains:** Oracle's recent partnership with Singapore brings air-gapped, encrypted cloud and AI services to MINDEF, setting a new benchmark for secure "data room" operations in logistics.
- **Blockchain and Distributed Ledger Technologies:** Promising for secure tracking and validation of logistics transactions, mitigating risks from data tampering or supply chain poisoning.
- **Smart contract automation:** Can optimise procurement, inventory and compliance, while integrating cyber-physical security controls from the outset.

Resilience-by-Design: Learning from crisis, organisations like Maersk have embraced "security as competitive advantage," embedding cyber resilience as a foundational requirement in contracts, operations and international partnerships.

3. Mitigation Strategies: From Theory to Practice

Based on recent research and best practices, the following table summarises key cybersecurity vulnerabilities in military logistics and recommended mitigation strategies:

Vulnerability	Description	Mitigation Strategy
Zero-day exploits on network and OT devices	Attacks on routers, hypervisors, IoT/OT devices via unpatched vulnerabilities	Threat intelligence sharing, rapid patching, anomaly detection
Persistent APT presence	Use of custom malware and living-off-the-land techniques	Continuous monitoring, AI-based threat hunting, EDR solutions
Credential harvesting and lateral movement	Credential theft via rootkits or phishing enables movement across systems	Multifactor authentication, credential rotation, strict access controls
OT/ICS vulnerabilities in logistics environments	Outdated protocols in SCADA/PLCs, lack of encryption/authentication	Network segmentation, security audits, OT-specific patch management
Supply chain/third-party compromise	Insecure digital interfaces, vendor/partner breaches	Vetting of third parties, zero trust, blockchain for supply verification
Human error and cyber hygiene gaps	Poor password discipline, phishing, inconsistent training	Cyber awareness training, simulated phishing, strict security protocols
Systemic lack of resilience and recovery planning	Flat networks, unsegmented backups, slow disaster recovery	Micro-segmentation, rapid recovery playbooks, geo-redundant backups

These strategies echo the lessons learned from global incidents: robust prevention, adaptive detection and resilient, rapid recovery must all be in place-and continuously tested.

---

4. Policy and Strategic Developments

- **Operational Technology Cybersecurity Masterplan 2.0:** Singapore's latest strategy incorporates a "secure-by-deployment" approach-embedding security from

the design and procurement stages through to deployment and operations, especially for critical digital and logistics infrastructure.

- **DIS Leadership in Digital Transformation:** The Digital and Intelligence Service now serves as both the nerve centre and innovation catalyst for SAF's digital defence and logistics transformation, consolidating command, control, cyber and AI capabilities for holistic defence.
- **Total Defence with a Digital Pillar:** The explicit addition of Digital Defence as the sixth pillar in Singapore's Total Defence doctrine signals the recognition that cyber resilience is critical to national survival-on par with military, civil, economic, social, and psychological defence.

Singapore's response to the UNC3886 cyberattacks represents both a moment of vulnerability and a crucible for national resilience and innovation.

In an interconnected age, where military logistics and digital infrastructure are the foundation of both deterrence and day-to-day survival, Singapore must continue to lead in cyber resilience-melding vigilance, innovation and collaboration.

From patching zero-days to imagining resilient AI logistics, from exercising the whole-of-nation in crisis response to embedding digital defence into every link of the supply chain, Singapore's military sector is charting a way forward.

The lessons of UNC3886, like those of NotPetya and other global attacks, are clear: In the age of digital warfare, the battle for logistics is as much about bits and bytes as brute force and battalions. National security now means defending and continually reinventing the digital lifeblood that enables the nation's readiness, resilience and prosperity.

Cybersecurity in Transport & Logistics

LISTEN 6 min

Vulnerabilities in Transport and Logistics Operational Technology (OT) Systems

Singapore's digital transformation in transport and logistics—embracing smart ports, automated warehouses and intermodal hubs—has delivered world-class efficiency, but also radically expanded the attack surface exposed to cyber adversaries.

With APT groups like UNC3886 deliberately probing these systems, it is critical to understand both IT and OT vulnerabilities specific to this sector. This analysis explores the unique technical and organisational exposures present in Singapore's operational technology landscape and highlights strategies to reduce risks.

Core Vulnerabilities in OT Systems

1. Legacy Devices and Lack of Security by Design

Much of Singapore's OT depends on industrial control systems (ICS) and supervisory control and data acquisition (SCADA) components engineered at a time before IT/OT convergence. Such devices:

- Often run outdated OS with limited patching options;
- Rely on proprietary protocols lacking secure authentication or encryption;
- Feature limited onboard monitoring or logging capabilities;
- Are difficult to segment or upgrade without costly, disruptive replacement.

2. IT–OT Convergence and Expanded Attack Surface

Driven by an imperative for centralised management and analytics, logistics operators are linking warehouse, fleet and port OT to enterprise IT and cloud platforms. This delivers productivity gains but also allows intrusion at the IT perimeter to quickly propagate to core control or safety systems.

3. Unpatched Vulnerabilities and Supply Chain Risk

Globally, many leading Singaporean companies suffered a third- or fourth-party breach in 2024–2025, exposing indirect routes for attackers like UNC3886 to access CII via suppliers, outsourced IT or digitally connected logistics partners. Lack of supply chain

visibility, patching of embedded devices and weak contract enforcement are persistent problems.

4. Insufficient Segmentation and Accidental Exposure

Logistics organisations sometimes operate "flat" or poorly segmented networks, leaving OT devices reachable from broader corporate environments. Cloud misconfigurations, exposed IoT endpoints and inadequate access controls further compound the risk of lateral movement by sophisticated adversaries.

Technical Case Example: SWaT Testbed

Singapore University of Technology and Design's SWaT testbed, widely referenced for ICS research, demonstrates in practice common weak points in OT security:

- PLCs and sensor controllers exposed via poorly protected network links.
- Lack of patching in proprietary industrial devices.
- Weak admin credentials and ability to spoof sensor data leading to physical consequence (e.g., water treatment failure).

Modern Threats Profile

Top Attack Vectors in OT for Transport and Logistics:

VULNERABILITY	EXAMPLE IMPACT
Unpatched legacy device	RCE enables backdoor/rootkit installation
Insecure remote access	VPN exploited for initial access/lateral movement
Weak credential management	Admin account compromise, loss of control
Lack of network segmentation	Malware moves from IT to OT environments
Supply chain (third-party software)	Malware in vendor update disables systems
Cloud misconfiguration	Exposed storage allows data exfiltration

These factors were exploited in case studies such as the Maersk NotPetya incident, where a combination of legacy OS, unpatched software and lack of segmentation led to worldwide operational paralysis despite "good" internal cyber hygiene.

Singapore's National Approach

Singapore has proactively launched dedicated OT Cybersecurity Masterplans (2019, 2024), incorporating input from 60+ organisations to ensure alignment between regulatory expectations and practical security controls. The updated plans prioritise:

- Building a pipeline of specialised OT security talent;
- Improving situational visibility and logging;
- Mandating risk reporting and incident response preparation for CII in critical sectors;
- Strengthened public–private and cross-sector collaboration.

OT–IT Risk Convergence: Key Lessons

Analysis of breach data (2024–2025):

- Most organisations with top internal ratings (A grade) still suffered breaches via vendors or unmonitored fourth-party suppliers, demonstrating security "is only as strong as the weakest link".
- Segmentation, strong asset management and validated incident response plans are now recognised as essential—not optional—controls.

Recommendations

- **Asset Inventory and Network Segmentation**: Keep precise records of every ICS/OT device; use firewalls to restrict traffic and prevent lateral movement. Micro-segmentation for essential devices.
- **Patch Management and Monitoring**: Regularly update where possible, and monitor for signs of tampering or exploitation in systems where patching is impractical.
- **Multi-factor Authentication**: Across all remote and privileged access points, including vendor/contractor accounts.

- **Continuous Supply Chain Auditing and Incident Drills**: Ongoing validation of vendor practices, scenario-based tabletop exercises including cross-sector simulation of supply chain disruptions.
- **Enable Secure IT–OT Integration**: Architect secure data flows, limit exposure of OT controls to internet or enterprise IT without layered controls.

The vulnerabilities exposed in Singapore's digital infrastructure are a mirror of global trends—where technical progress and interconnection drive operational efficiency, but create new and sometimes unexpected entry points for attackers.

The resilience of the sector will depend on converging best practices in IT and OT security, relentlessly addressing supply chain risk, and investing in both human capital and innovative monitoring solutions.

LISTEN 6 min

Exposing the weakest link: Supply chain security and third-party risks in transport and logistics

Singapore's transport and logistics sector runs on trust between tightly coupled partners—3PLs, carriers, ground handlers, freight tech platforms and cloud/SaaS providers. That trust is under strain.

Recent supply-chain-driven breaches have shown that even mature operators can be compromised through weaker vendors, leading to data loss, operational disruption and regulatory scrutiny. Turning this Achilles heel into a resilience driver requires clear visibility across dependencies, disciplined risk governance and shared responsibility with partners.

The anatomy of a supply chain breach

Attackers increasingly prefer the vendor side door—one compromise, many victims. In logistics, common patterns repeat:

- **Ransomware via managed service providers:** Compromise of a small IT vendor's remote management tools propagates ransomware to multiple warehouse sites, encrypting WMS servers and handheld endpoints. Recovery stalls because backups are co-located or not tested for restores.
- **Data loss through SaaS integrations:** A freight visibility platform's misconfigured S3 bucket or token leakage exposes shipment manifests, client PII and customs documentation. Downstream re-use of API keys turns a single leak into multi-tenant exposure.
- **Credential pivot from facilities contractors:** A building management firm with VPN access to cold-chain SCADA networks gets phished; attackers use contractor accounts to move into refrigeration control systems, risking spoilage and safety impacts.
- **Point-of-sale and loyalty vendor compromise:** Retail tenants within logistics hubs face breach through a payments vendor, triggering PDPA notification duties and reputational fallout for the estate operator despite indirect involvement.
- **Regulatory response themes:** Mandatory incident reporting timelines, expectations for due diligence on vendors and evidence of corrective actions (e.g. segmentation, Multi-Factor Authentication (MFA), improved contracting). Firms that can demonstrate robust third-party risk management (TPRM) see better regulatory outcomes.

The ecosystem problem in logistics

Interconnectivity is intrinsic to modern logistics—and a multiplier for cyber risk.

- **Dense partner graphs:** Freight forwarders, NVOCCs, ground handlers, trucking fleets, customs brokers, and e-commerce platforms exchange real-time data via APIs, EDI and file drops. Each connection is a potential ingress.
- **Shared platforms and identity:** Single sign-on across multiple partner portals and shared API keys for multi-party workflows inflate blast radius. Credential reuse and weak token scoping worsen exposure.
- **OT/IT convergence:** Warehouse control systems, cold-chain telemetry and yard management increasingly hook into ERP/WMS and cloud analytics. Weak

segmentation can allow lateral movement from a low-value IoT sensor to high-value planning systems.

- **Shadow integrations:** "Temporary" file shares, one-off SFTP users and contractor tools often bypass formal review, leaving undocumented pathways into core networks.

Singapore's regulatory and programmatic response

The direction of travel is clear: more accountability for supply chain risk and stronger baseline controls.

- **CII supply chain expectations:** Critical Information Infrastructure (CII) owners are expected to exercise oversight of vendors that can impact essential services, including supply-chain incident reporting, assurance over outsourced operations and evidence of risk assessments.
- **Vendor risk rating and tiering:** Operators are adopting tiered categorisations (e.g. Tier 1 providers with network access or sensitive data; Tier 2 with limited data; Tier 3 with no connectivity) to calibrate controls, reviews and contract strength.
- **Zero-trust mandates:** Identity-centric access, least privilege, strong authentication, continuous verification and micro-segmentation are increasingly baseline for connections into critical environments, including vendor access.
- **Programmatic uplift:** Sector exercises, guidance for third-party assurance and information-sharing forums are pushing convergence on practices like MFA coverage for vendors, secure remote access and incident notification clauses.

Fourth-party risk and the expanding attack surface

Your vendors' vendors can be your downfall. Visibility and enforceable flow-downs are key.

- **Map critical dependencies:** Identify sub-processors and critical libraries/services used by Tier 1 vendors. Require notification of material changes to fourth-party ecosystems.
- **Quantify concentration risk:** Watch for single points of failure (e.g. reliance on a single identity provider, cloud region or logistics data broker).

- **Assure upstream controls:** Require that Tier 1 vendors impose equivalent security obligations on their sub-processors, with transparency into audits where feasible.
- **Automate discovery:** Periodically scan for new external services, leaked credentials and exposed development artifacts tied to your vendor domains.

Resilience through collaboration

Security is a team sport across the chain.

- **Joint audits and tabletop exercises:** Include key vendors in incident simulations—test breach notification pathways, log sharing and coordinated response.
- **Shared detection rules and IOCs:** Exchange indicators of compromise, TTPs and hardening guidance across partner networks to close common gaps quickly.
- **Sector playbooks:** Align on common minimum controls for shared platforms (e.g. WMS, TMS, freight visibility) to reduce variance and upgrade friction.
- **Incentivise good behaviour:** Preferred-vendor status, longer contract terms or co-marketing for partners who meet higher security benchmarks.

Supply chain risk cannot be eliminated, but it can be operationalised.

With clear tiering, stronger contracts, continuous monitoring and collaborative drills, logistics operators can contain blast radius, satisfy regulators and build commercial advantage from demonstrable resilience.

LISTEN 6 min

Technological vulnerabilities in land transport: Safeguarding IoT, ITS and urban mobility

Singapore's land transport ecosystem blends intelligent transport systems (ITS), public transit and urban logistics into a hyper-connected network. That connectivity accelerates efficiency—and expands the attack surface.

From smart sensors and fare systems to fleet telematics and V2X pilots, a single weak device or integration can offer adversaries a pivot into mission-critical operations. Defending this landscape requires disciplined engineering, data-driven detection and public vigilance.

The ITS landscape and exposure points

- **Real-time data fabric:** Traffic signals, adaptive junction control, electronic road pricing and public transport telemetry feed centralised platforms for planning and incident response. Integration across agencies and operators increases dependency on shared identity, APIs and message brokers.
- **Multi-modal integration:** Fare systems, journey planners and mobility-as-a-service (MaaS) apps connect buses, MRT, micromobility and ride-hailing. Weaknesses in token handling, SDKs or third-party analytics libraries can cascade across services.
- **Edge-heavy operations:** Roadside units, cameras, environmental sensors and connected vehicles generate massive edge footprints with physical exposure and diverse firmware baselines.

IoT proliferation and threat vectors

- **Insecure endpoints:** Default credentials, open management interfaces and outdated firmware leave cameras and sensors susceptible to compromise.
- **Protocol weaknesses:** Unencrypted or unauthenticated protocols (e.g. legacy RTSP, Modbus variants) allow interception or manipulation of data streams.
- **Supply chain risks:** Drivers' devices, contractor laptops and aftermarket telematics add opaque software and cloud dependencies.
- **V2X experimentation:** Early deployments must contend with certificate lifecycle, misconfiguration and privacy risks if pseudonymisation fails.

Notable vulnerabilities and case patterns

- **Botnets and DDoS:** Compromised cameras and routers conscripted into botnets can both disrupt services and hide lateral movement attempts.
- **Credential stuffing and token theft:** Reuse of passwords across operator portals and SaaS leads to session hijacking; inadequate token scoping in APIs magnifies the impact.
- **Patch gaps:** Mixed vendor fleets and long maintenance cycles slow updates; "never-reboot" cultures keep exploitable versions in the field.

- **Poor vendor oversight:** Integrators ship devices with insecure defaults, hard-coded credentials or disabled logs—issues missed without acceptance testing.

AI and machine learning for defence and reliability

- **Anomaly detection at scale:** Models trained on network flows, SYSLOG and sensor baselines can spot deviations (e.g. jitter spikes, sudden credential reuse, odd API call sequences) faster than manual triage.
- **Predictive maintenance:** Telemetry from vehicle subsystems and roadside devices supports failure prediction, lowering downtime and narrowing patch windows through planned interventions.
- **Computer vision safeguards:** On-device analytics can validate camera integrity (e.g. lens occlusion, feed tampering) and flag spoofed inputs.
- **Model assurance:** Guard against data poisoning and drift with curated datasets, canary models and human-in-the-loop validation; protect model artifacts and inference APIs with strong access controls.

Sectoral response and initiatives

- **Security uplift programs:** Hardening guidelines for ITS and fare systems, red-teaming of operator networks and sector-wide cyber exercises to test coordination and incident communications.
- **Technology upgrades:** Migration to zero-trust architectures, secure remote access for contractors and phased replacement of legacy roadside units with secure-by-design hardware.
- **Public-private collaboration:** Operators, vendors and research institutions co-develop detection analytics and share indicators of compromise relevant to transport tech.

Recommendations for resilience

- **Segment critical OT assets:**
  - **Network design:** Separate control networks (signals, SCADA) from enterprise IT and public internet; enforce one-way gateways where possible.
  - **Identity:** Use dedicated, scoped identities and MFA for admin access; adopt just-in-time elevation.

- **Validate vendor integrations:**
  - **API security:** Enforce mTLS, OAuth2/OIDC with least-privilege scopes, token rotation and per-client rate limiting; perform schema validation and input sanitisation.
  - **Acceptance testing:** Security test hardware/firmware and app updates before deployment; require SBOMs and vulnerability disclosures.

- **Harden endpoints and gateways:**
  - **Baseline controls:** Disable default accounts, close unused ports, enable signed firmware and secure boot and centralise logs.
  - **Patching:** Define maintenance windows and over-the-air (OTA) update pipelines; track patch SLAs by device class.

- **Detection and response:**
  - **Telemetry:** Collect NetFlow, syslogs and endpoint telemetry; baseline normal behaviour per site and device type.
  - **Playbooks:** Create runbooks for device quarantine, rapid re-provisioning and safe failover of control systems.

- **Public vigilance and cyber literacy:**
  - **User education:** Educate commuters on phishing, fake apps and QR code risks for mobility services.
  - **Reporting:** Provide simple channels for reporting suspicious devices or app behaviour; run periodic awareness campaigns.

Hyper-connected mobility demands hyper-disciplined cybersecurity.

By segmenting critical controls, validating every integration and pairing AI detection with public vigilance, Singapore's land transport can stay safe, reliable and resilient as it innovates.

LISTEN 3 min

Regulations and Governance: Singapore's Cybersecurity Act & sector-specific mandates in transport

Regulatory guardrails in Singapore are evolving to match an increasingly complex threat landscape. Updates to the Cybersecurity Act and sector-specific controls for transport are reshaping governance, risk and compliance expectations—especially for firms operating critical logistics, public transit and aviation or maritime interfaces.

Leaders need a clear map of obligations, practical compliance strategies and a view of what's next.

The Cybersecurity Act and 2024 amendments

- **Expanded scope of oversight:** The regime extends beyond traditional CII boundaries to encompass digital infrastructure and services whose disruption would affect essential functions, recognising cloud, managed services and key platforms.
- **Supply chain incident visibility:** CII owners are accountable for outsourced operations and must report material incidents that occur at vendors if they impact essential services, including loss of visibility or data integrity.

- **Operational assurance expectations:** Authorities can require audits, technical information, incident data and remediation plans; owners must maintain evidence of risk assessments, protections and continuity measures.
- **Tighter timelines and obligations:** Clearer expectations for prompt incident reporting, preservation of logs and artifacts, and cooperation during investigations.

Transport Sector (Critical Firms) Act and targeted operational controls

- **Designation of critical firms:** Selected operators in air, land and sea segments can be designated due to systemic importance, triggering obligations beyond baseline corporate compliance.
- **Operational controls:** Requirements may include ownership transparency, security leadership accountability, vetted outsourcing, crisis resource management and assured supply chain oversight.
- **Cross-sector coordination:** Aligns with national incident response, ensuring that critical transport players integrate with sector response plans and coordinated communications.

Looking ahead: Digital Infrastructure Act and integrated approaches

- **Convergence of regimes:** Expect tighter integration between cybersecurity, data protection and incident response obligations, reflecting reliance on cloud and platform ecosystems.
- **Platform accountability:** Clearer duties for providers of foundational digital services and intermediaries, with standardised reporting and assurance obligations.
- **Measurement and transparency:** Movement toward outcome-based metrics (e.g. time to contain, resilience of critical services) and sector benchmarking.

Compliance is not paperwork—it's engineered assurance.

By aligning design, operations and evidence to evolving mandates, transport leaders can turn regulatory pressure into durable resilience and public trust.

LISTEN 4 min

Harnessing AI: Threat Detection, Anomaly Response and Digital Transformation in Transport Logistics

Artificial intelligence and data analytics are revolutionising cyber defence in Singapore's transport and logistics sector.

Gone are the days of purely reactive security operations; AI now drives proactive anomaly detection, accelerates incident response and enables automated remediation workflows.

This article unpacks how organisations are applying AI, highlights leading case studies, addresses challenges and previews future directions where AI will continue to multiply resilience.

AI for predictive anomaly detection and real-time monitoring

AI and machine learning elevate signal-to-noise ratio in massive logistics networks:

- **Behavioural baselining:** Unsupervised models learn normal patterns of API calls, data flows and device telemetry — flagging deviations often invisible to signature-based tools.
- **Predictive alerts:** Time-series analysis anticipates hardware failures or anomalous login bursts before they morph into outages or credential stuffing attacks.
- **Automated triage:** Natural language processing (NLP) classifies alerts by severity and suggests response steps, slashing mean time to respond (MTTR).

Case studies in AI-driven intrusion detection

Maritime transport network

- Deployed graph-based ML to map container-ship communication patterns.
- Detected lateral-movement "beaconing" that indicated an insider threat exfiltrating cargo manifests.
- Automated quarantines of affected segments before manifest tampering could occur.

Air cargo handling

- Integrated AI into baggage-handling control networks.
- Anomaly detection identified unusual command-sequence spikes in conveyor PLCs, tracing back to a compromised maintenance terminal.
- AI-guided playbooks disabled remote access and rolled out EMERGENCY shutdown scripts within minutes.

Land logistics hub

- Real-time clustering of fleet telematics exposed subtle GPS spoofing attempts on high-value vans.
- Correlated adverse weather patterns with sensor anomalies to reduce false positives, improving trust in automated alerts.

Best practices: AI for phishing prevention and identity assurance

- **Adaptive phishing simulations:** AI crafts lures that mirror real-world threats, measuring user susceptibility and tailoring training content dynamically.
- **Behavioural biometrics:** ML models analyse typing cadence and mouse movements for continuous identity verification on broker and carrier portals.
- **Adaptive MFA:** Risk-based authentication raises step-up prompts when behavioural anomalies occur, reducing friction without sacrificing security.

Industry adoption and collaborative R&D

Singapore stands at the forefront of AI-powered logistics resilience:

- **FedEx–Cisco–SUTD lab:** Joint R&D on reinforcement learning for dynamic network segmentation in cargo handling.
- **NUS AI4Logistics initiative:** Publishes open datasets and hosts annual hackathons to prototype intrusion-detection models for maritime corridors.
- **Government co-funding:** Grants channel private investment into proof-of-concept testbeds at Changi Air Freight Centre and Tuas Mega Port.

Future trends: Beyond today's AI

- **Quantum-resistant AI:** Exploring post-quantum cryptography integrated with ML to secure future transports' key exchanges.
- **Autonomous response:** Multi-agent systems that can isolate compromised segments end-to-end — from revoking certificates to re-provisioning clean device images without human intervention.
- **Self-healing networks:** AI-orchestrated micro-segmentation adjustments in real time, automatically rerouting traffic around emerging threats.

AI as a force multiplier

Artificial intelligence is no longer a futuristic concept but a practical necessity for cyber-resilient transport logistics. By marrying advanced ML models with robust data governance, collaborative R&D and vigilant privacy practices, Singapore's transport ecosystem can detect threats earlier, respond faster, and outpace adversaries — ensuring supply chains remain both efficient and secure.

LISTEN 4 min

Blockchain for Secure Data Exchange – Innovation Opportunities in Logistics

Blockchain's promise of immutable, transparent ledgers is fuelling a wave of innovation in Singapore's supply chains.

From port terminals to customs clearance and warehouse management, distributed-ledger technologies enable trusted data sharing among diverse stakeholders.

This article examines blockchain fundamentals, walks through sector-specific deployments and assesses the challenges and prospects of integrating blockchain into real-world logistics.

Blockchain fundamentals for logistics

- **Immutability:** Every transaction—shipment handoff, customs declaration, temperature log—is cryptographically chained, preventing tampering.
- **Transparency with privacy controls:** Shared ledgers ensure provenance while enabling selective disclosure via zero-knowledge proofs or permissioned chains.
- **Secure data trails:** Auditable histories help regulators, insurers, and customs authorities verify authenticity and compliance in real time.

Sector-specific use cases

TradeLens and port/shipping data exchange

- Joint venture between Maersk and IBM rolled out in Singapore for TEU tracking and terminal invoicing.
- Achieved 20% reduction in document delays by automating port release notifications on-chain.
- Piloted integration with PSA's yard-management systems for synchronised gate manifests.

Customs and inventory processes

- Proof-of-concept with Singapore Customs to anchor Single Administrative Document (SAD) submissions on a Hyperledger Fabric network.
- Warehouse operators trial distributed proof of storage: IoT temperature sensors sign logged readings to the ledger, ensuring cold-chain integrity for pharmaceuticals.

Smart contracts for automated workflows

- **Programmed settlements:** Once a shipment's on-chain status hits "delivered" and temperature logs remain within range, smart contracts auto-trigger invoicing and payment release.
- **Load-management automation:** Blockchain-driven slot allocation for container unpacking optimises yard usage without manual coordination.
- **Regulatory compliance:** On-chain rules enforce origin checks and embargo controls, rejecting non-compliant shipments before arrival.

Anti-fraud and trust enhancement

- **Document forgery prevention:** Bill of Lading (BoL) and certificates of origin hashed on-chain guard against unauthorised edits.
- **Shipment manipulation detection:** GPS logs and custody handoffs recorded in the ledger create an unbroken chain of custody—raising the cost of illicit diversions.

- **Counterfeit mitigation:** Serial numbers and supplier attestations on-chain verify genuine parts in automotive and electronics supply chains.

Future prospects: SGTraDex and beyond

- **SGTraDex platform:** Singapore's national trade data exchange leverages a permissioned DLT to unify e-certificates, permits and logistics events across agencies.
- **End-to-end digital corridors:** Pilots with Malaysian and Indonesian partners to extend blockchain-backed trade-finance flows across the Strait of Malacca.
- **Convergence with AI and IoT:** Secure oracles feed trusted sensor data into ledgers, while AI audits on-chain metadata to detect anomalies or compliance drifts.

Implementation and integration challenges

- **Pilot-to-scale transitions:** Proofs-of-concept often stall at 3–5 participants. Scaling requires governance bodies, cost-sharing models and robust SLA frameworks.
- **Stakeholder alignment:** Harmonising data models, permissions and governance policies across shippers, carriers and regulators is a major coordination effort.
- **Complementary technologies:** IoT, AI and API gateways must integrate seamlessly with DLT networks; architecture blueprints and reference implementations accelerate adoption.

From promise to production

Blockchain offers a transformative foundation for secure, transparent data exchange in transport and logistics—but only if real-world constraints are managed.

By building hybrid architectures, forging cross-industry governance, and integrating IoT/AI services, Singapore's logistics community can convert blockchain's theoretical benefits into practical resilience, efficiency, and trust that propel the nation's trade frontier forward.

PURSUE CPL & SCPD PROFESSIONAL CERTIFICATES WITH SKILLSFUTURE

*Use Your SkillsFuture Credits – Pay No Cash**

Up to 90% Government Subsidy from *SkillsFuture*

You pay only $63.50 per SCPD module (UP: $545)* with your SkillsFuture Credits

*Subject to SkillsFuture eligibility

Singapore Citizen (SC) aged 40 and above	$63.50
Singapore Citizen aged below 40 Singapore Permanent Resident (PR)	$163.50
SC or PR sponsored by SME	$63.50
Non-SC/PR *(no subsidy)*	$545

COURSE FEES PER SCPD MODULE

Additionally, NTUC members are eligible for Union Training Assistance Programme (UTAP) funding.

PROGRAMME STRUCTURE

The CILTS Supply Chain Professional Development (SCPD) Programme comprises two levels, the **Advanced Professional Certificate** (four modules: SCPD05-08) and the **Professional Certificate** (four modules: SCPD01-04).

The SCPD modules, progressively updated to keep abreast of advancements in the industry, have a substantial fit with the Skills Framework for Logistics published by *SkillsFuture*, a Singapore Government initiative and the Key Knowledge Areas published by CILT International.

The syllabus for the Advanced Professional Certificate level also addresses the knowledge competency for the **Certified Professional Logistician (CPL)** certification, which is exclusively awarded by CILT Singapore.

CPL candidates taking the four advanced SCPD modules shall proceed to sit for the CPL Examination upon meeting eligibility conditions of work experience and qualifications. Successful candidates shall be awarded the CPL certificate.

Click on image for more information:

Enrol for SCPD

Certified Professional Logistician (CPL)

SCPD modules

CPL RENEWAL

Successful completion of an SCPD module is accepted as proof of Continuous Professional Development for CPL renewal.

Enquiries: secretariat@cilt.org.sg

MY CAREER PORTAL

Click on image for details:

AMAZON ASIA-PACIFIC RESOURCES PRIVATE LIMITED
TYPICALLY REPLIES IN 30 DAYS
Supply Chain Manager , Infrastructure Supply Chain
Central | Permanent | Manager | Logistics / Supply Chain
$11,000 to $20,000 Monthly

FLINTEX CONSULTING PTE. LTD. TYPICALLY REPLIES IN 30 DAYS
Regional Supply Chain Manager
Central | Permanent | Manager | Logistics / Supply Chain
$10,000 to $15,000 Monthly

SEARCHASIA CONSULTING PTE. LTD.
Senior Supply Chain Manager (Planning)
Islandwide | Permanent | Middle Management | Logistics / Supply Chain
$10,000 to $14,000 Monthly

BEATHCHAPMAN (PTE. LTD.) TYPICALLY REPLIES IN 30 DAYS
Supply Chain & Demand Analyst (6 Months Contract)
Central | Contract | Middle Management | Logistics / Supply Chain
$7,500 to $8,000 Monthly

RECRUITPEDIA PTE. LTD. TYPICALLY REPLIES IN 30 DAYS
Head of HR (Supply Chain)
Islandwide | Permanent ... | Senior Management | Human Resources
$12,000 to $18,000 Monthly

For more career search:

SOURCE	My Careers Future

EDUCATION

EVENTS ON CILTS WEBSITE

To keep up with the latest developments and sharing in the Supply Chain, Logistics and Transport industry, check out the **EVENTS** section of our website, which includes the following insightful webinars:

- **DIGITAL TRANSFORMATION IN SUPPLY CHAINS: FROM AI TO E-INVOICING COMPLIANCE**

17 SEP 2025

As global e-invoicing mandates continue to evolve, staying ahead of regulatory changes and understanding their broader business implications is more critical than ever. This webinar will explore the intersection of e-invoicing and supply chain optimization.

Takeaways:

1. Understand how e-Invoicing improves supply chain efficiency
2. Learn how AI is transforming invoicing processes
3. Get up to speed on France and Germany's AR mandates
4. Identify steps to ensure global compliance

- **UNIFYING SYSTEMS, POWERING GROWTH: FUTURE-PROOF YOUR DELIVERY OPERATIONS**

11 SEP 2025

Join us for an executive-level discussion on how building supply distributors are transforming their operations by uniting best-in-class technologies from Descartes, Geotab, Lytx and Zebra. Learn how this partner network supports a connected workflow that simplifies operations from dispatch to delivery, giving your teams the tools they need to perform with greater precision and consistency.

- **AI IN ACTION - ENHANCING GROUND OPERATIONS AT FRANKFURT AIRPORT**

30 SEP 2025

The discussion will highlight two real-world implementations currently active at **Frankfurt International Airport**. The first use case involves using computer vision to monitor over 30 aircraft turnaround events in real time, providing a live operational overview and data-driven alerts to support efficient management. The second use case tackles one of the most common sources of boarding delay: carry-on baggage.

Key points for discussion:

- Discover how AI and computer vision are being applied
- Understand the challenges of digital transformation in high-pressure, regulated environments
- Learn from real-world case studies at Frankfurt Airport, including turnaround monitoring and carry-on baggage assessment

KNOWLEDGE CENTRE

CILTS Members have **exclusive access** to our online Knowledge Centre, a rich repository of more than **1,600 publications and webinars on SUPPLY CHAIN, TRANSPORT, MILITARY LOGISTICS AND MANAGEMENT / SELF DEVELOPMENT.**

To access Knowledge Centre, use your CILTS member-registered email address to log in at www.cilt.org.sg/account/knowledge-centre

If you have not set your password yet, click on "Forgot Password". If you need help to log in, please contact secretariat@cilt.org.sg.

PUBLICATIONS

Click on image to read:

AI can and will transform how organizations operate — including security. In the meantime, as the challenges of AI become more apparent and AI applications continue to mature, turn your focus toward:

- Rightsizing AI's impact
- Prioritizing key areas of risk
- Maximizing AI's value
- Anticipating future changes

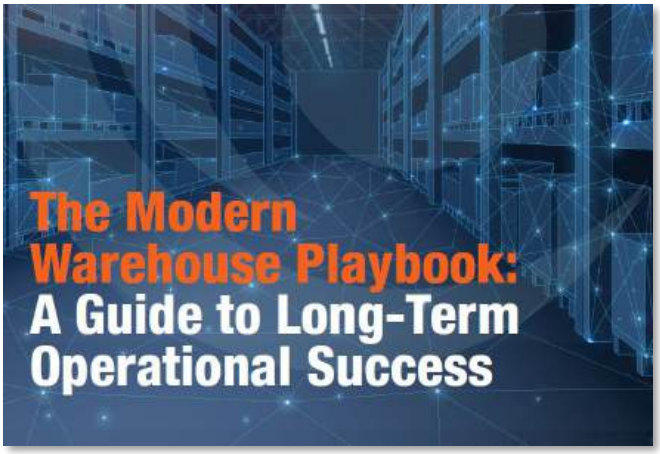
Cybersecurity incidents are a matter of "when," not "if." They result in more adverse media coverage than ever before, and auditors, regulators and other stakeholders expect organizations to demonstrate a clear plan for managing these incidents to minimize the impact on brand, reputation, staff, customers and shareholders.

The imperative for security and risk management leaders is to prepare. The key tools are a documented response plan and a detailed playbook for the incident type.

Cyber security is absolutely essential if we are to become a smart nation. You can't have electronic medical records, you can't have financial technology, you can't have large databases with information that could be abused or misused, you can't afford a breach of privacy. Cyber security is the flip side of the coin of being a smart nation.

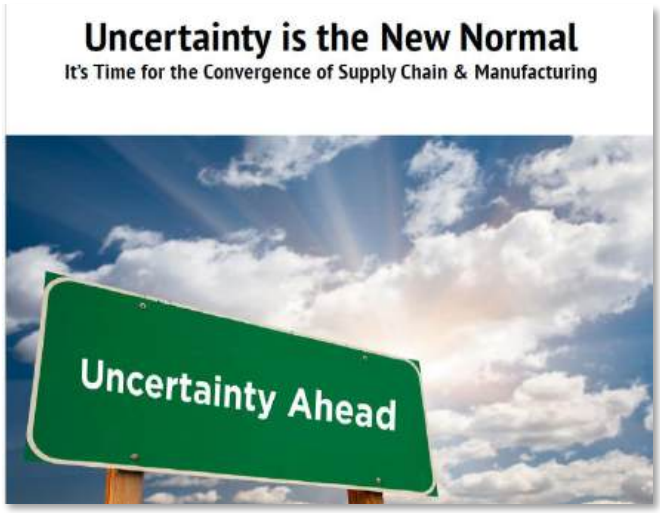
We were guided in the development of the Roadmap, by best practice guidance from the European Civil Aviation Conference (*ECAC*) and the International Civil Aviation Organization (*ICAO*).

With the help of the Sustainable Aviation Fuel Task Force and wider bilateral engagements, this Roadmap identifies four policy pathways to advance between 2025 and 2035. For each of these policy areas, we have set out a policy approach and detailed a number of actions to advance these policies, that build upon a suite of EU initiatives.



By embracing automation, connectivity, and proactive maintenance, operators can build a flexible, data-driven infrastructure that enhances efficiency, improves safety, and minimizes disruptions.

In today's volatile environment, the ability to adapt and respond quickly to risks in this intricate supply chain network has become one of the most important factors in determining long-term success. Over the past few years, we've seen firsthand the turbulence caused by global events: the disruption of the COVID-19 pandemic, growing labor shortages, rising inflation, geopolitical instability, the ongoing conflict in Ukraine, cybercrime and the increasingly visible impact of climate change on supply chains.



What seemed normal a few years ago no longer exists. Yet consumers still expect their purchases to be delivered on time, and at an affordable cost. Reconciling these apparently opposing forces requires finding ways to adapt to a world in a continuous state of flux.

Who We Are

The Chartered Institute of Logistics and Transport Singapore is part of the leading, global professional body for those engaged in supply chain, logistics and transport – covering all sectors of the industry, namely air, land and sea, for both passenger and freight transportation.

Our primary objectives are to support our members in continuous professional development to future-proof their careers, as well as to work in close collaboration with the public and private sectors, Government agencies and the academia to develop opportunities and synergy for industry transformation and growth, underpinned by strategic thrusts in digitalisation and sustainability.

Contact Us

The Chartered Institute of Logistics and Transport Singapore

5 Jalan Kilang Barat
#06-03 Petro Centre
Singapore 159349
Email: secretariat@cilt.org.sg

CILTS Personal Data Protection Policy

For advertising interest in CILT Buzz, please contact: secretariat@cilt.org.sg