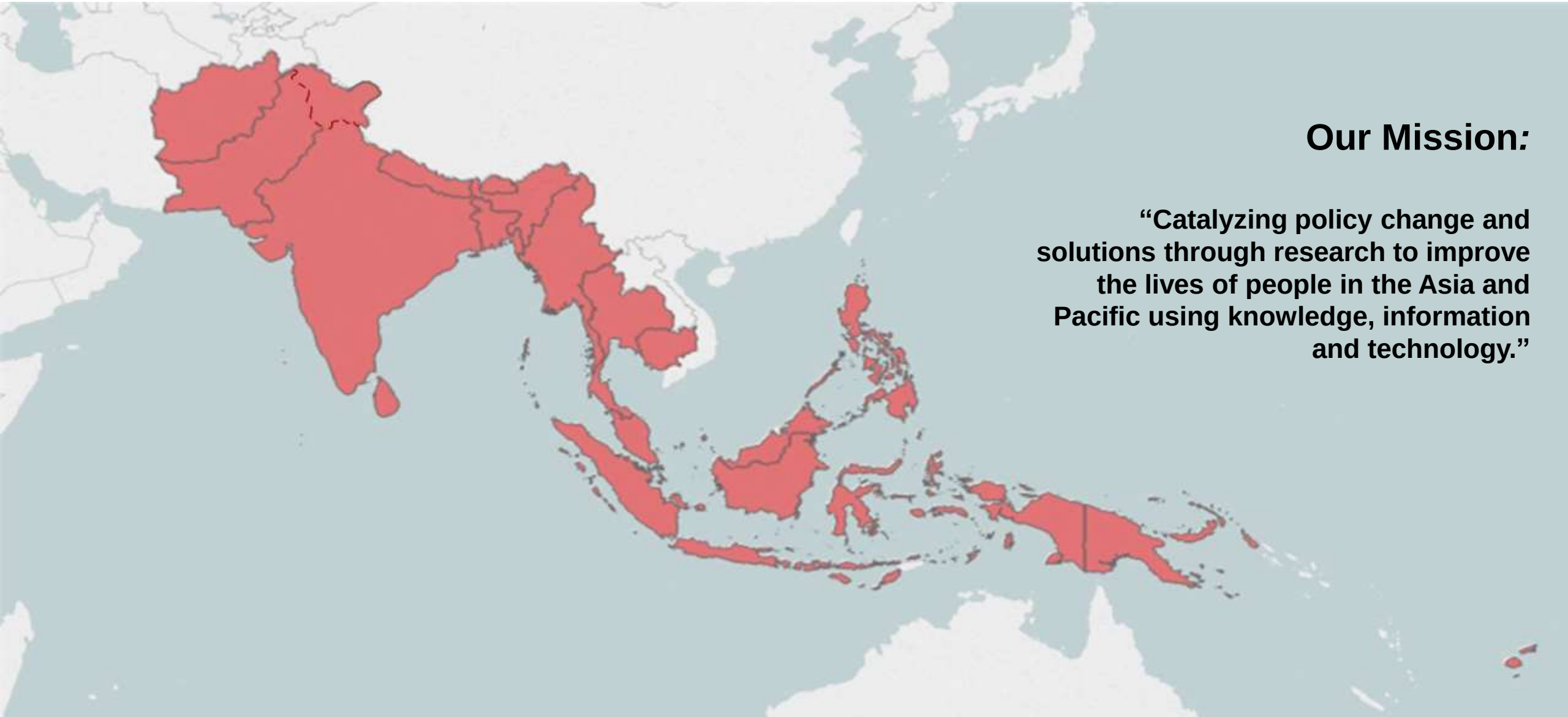
LIRNEasia
Pro-poor. Pro-market.

CONSIDERATIONS FOR CYBER SECURITY IN SRI LANKA

24 November 2025

Colombo

LIRNEasia is a regional think tank, focusing on digital inclusion, governance, and data for development



Our Mission:

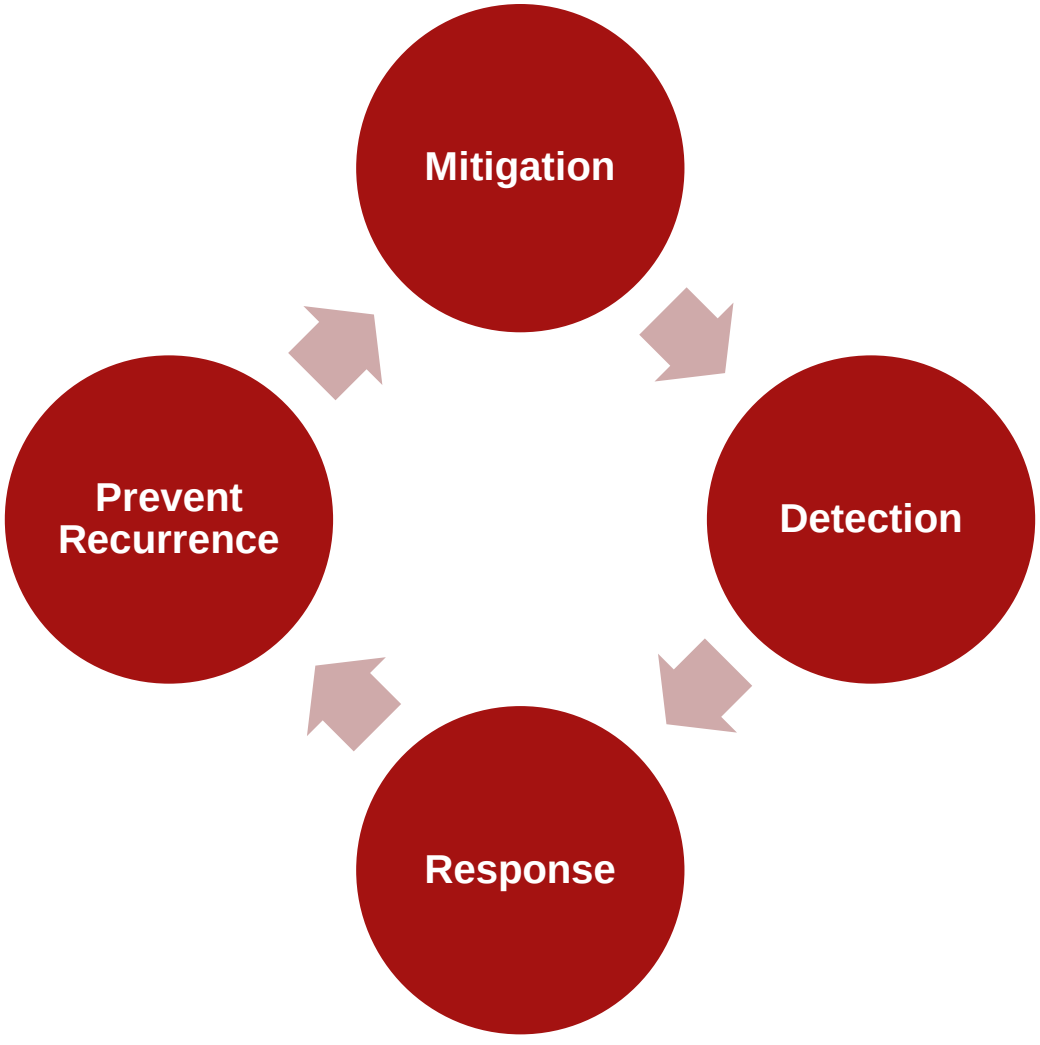
"Catalyzing policy change and solutions through research to improve the lives of people in the Asia and Pacific using knowledge, information and technology."

Varying definitions of cyber security

- **SL 2023 Cybersecurity Bill** [1] **: Protection** of information **in transit, in process and in storage** … from any form of attacks, unauthorized access, use…also includes any activities to make cyberspace safe and secure
- **EU 2022 NIS2 Directive** [2] ***: Protecting** networks, information systems and the user of such systems against Cyber Threats (events or actions which can **damage, disrupt** or otherwise **adversely impact** them).
- **US Committee on National Security Systems (CNSS)** [3] **: Prevention** of damage to, **protection** of and **restoration** of computers, electronic communications systems and services and the information they contain to ensure availability, integrity, authentication, confidentiality, and nonrepudiation.
- **International Telecommunications Union (ITU)** [4] **:** Collection of tools, policies, security concepts…assurance and technologies that can be used to **protect** the cyber **environment, organization** and **users'** assets.

Sources: *[1] TRCSL, [2] EU , [3] US NIST/CNSS, [4] ITU ;*
*Notes: *The 2022 NIS2 Directive is the latest EU Cybersecurity Act. It uses the definition of cybersecurity from EU regulation 2019/881 [https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng] ; **In the 2023 SL Cybersecurity Bill; the objectives of cybersecurity are "to prevent, detect, mitigate, and respond to cybersecurity th incidents".*

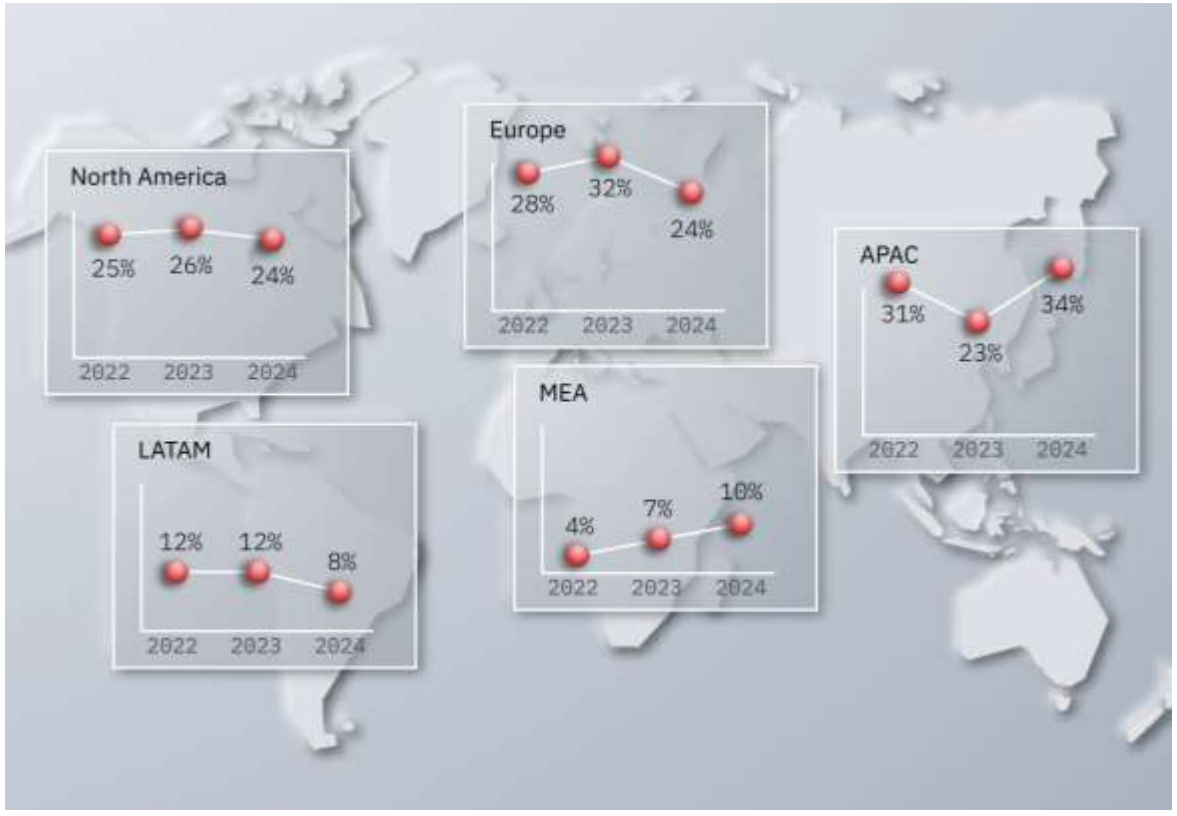
A comprehensive approach requires mitigating, detecting, responding to & preventing recurrence of cyber threats



- **Mitigation:** Proactive measures to reduce the likelihood and impact of cyber incidents. E.g. strengthening systems, applying security controls, managing vulnerabilities, and improving organizational resilience.
- **Detection:** Identifying malicious activity or system compromise as early as possible.
- **Response:** The actions taken once an incident is detected. Aiming to contain the threat, minimize damage, prevent further spread, preserve evidence, and restore normal operations.
- **Prevent Recurrence:** Ensuring that similar incidents do not happen again. E.g. conducting root-cause analysis, addressing system and process vulnerabilities, strengthening controls, and enforcing accountability.

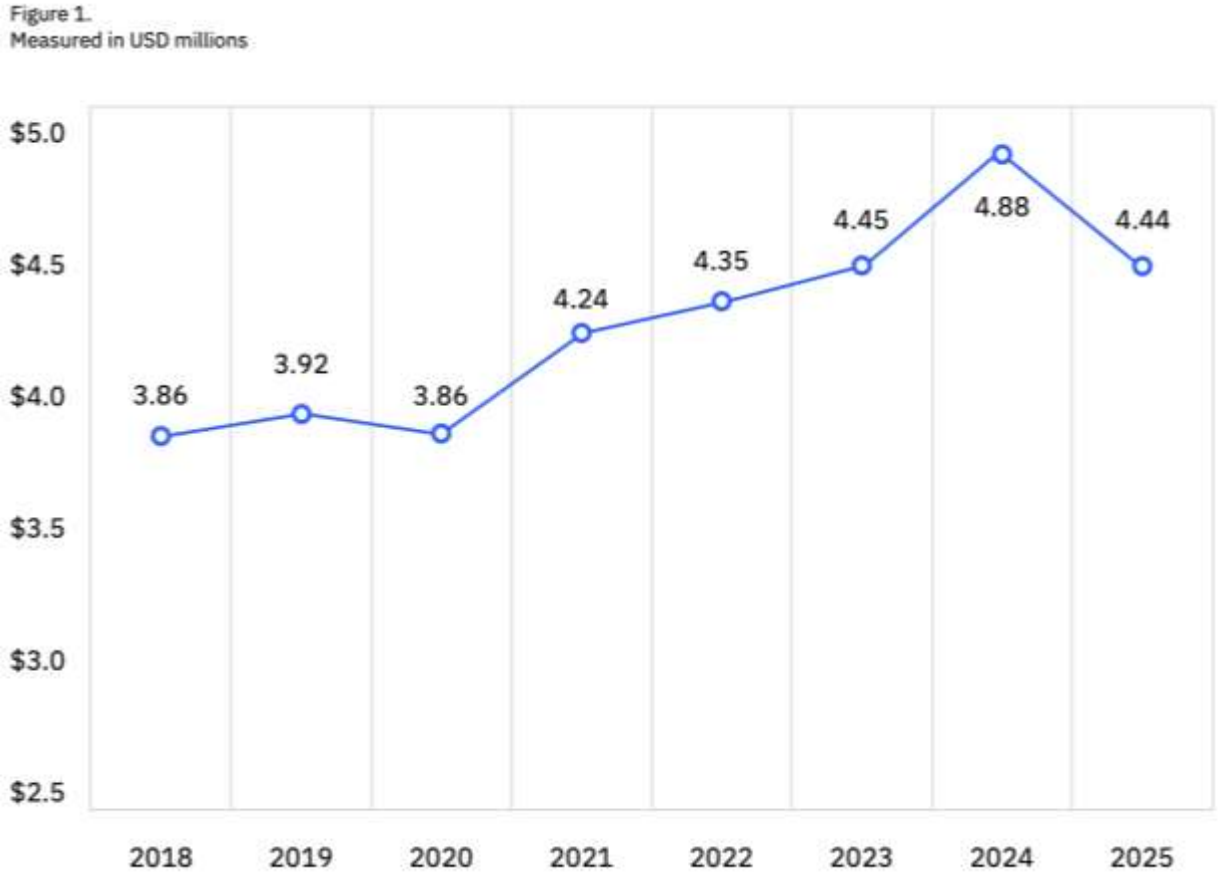
Recent global and regional trends show a worsening cyber threat landscape. APAC faces 1/3rd of global incidents

Global share of cyber response incidents by region [1]



e.g. in 2024 **APAC (34%)**, Europe (24%), MEA (10%), Latin America (8%) and N. America (24%).

Global average cost of data breach per incident (USD millions) [2]



Sources: *[1]* *IBM & Red Hat*, *[2]* *IBM & Ponemon Institute*

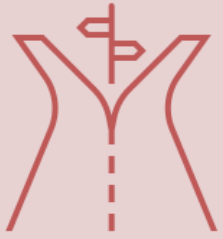
LIRNEasia
Pro-poor. Pro-market.

Increasingly, critical infrastructure is going digital. Cyber incidents can have population-scale consequences

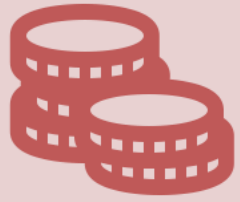
Sri Lanka Computer Emergency Response Team | Coordination Centre (SLCERT | CC) has **designated 37 Critical Information Infrastructure (CII) Systems [1]. They include:**

ELECTRICITY

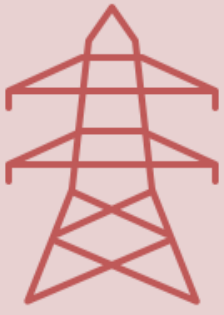
TRANSPORTATIO N



FINANCE



COMMUNICATION



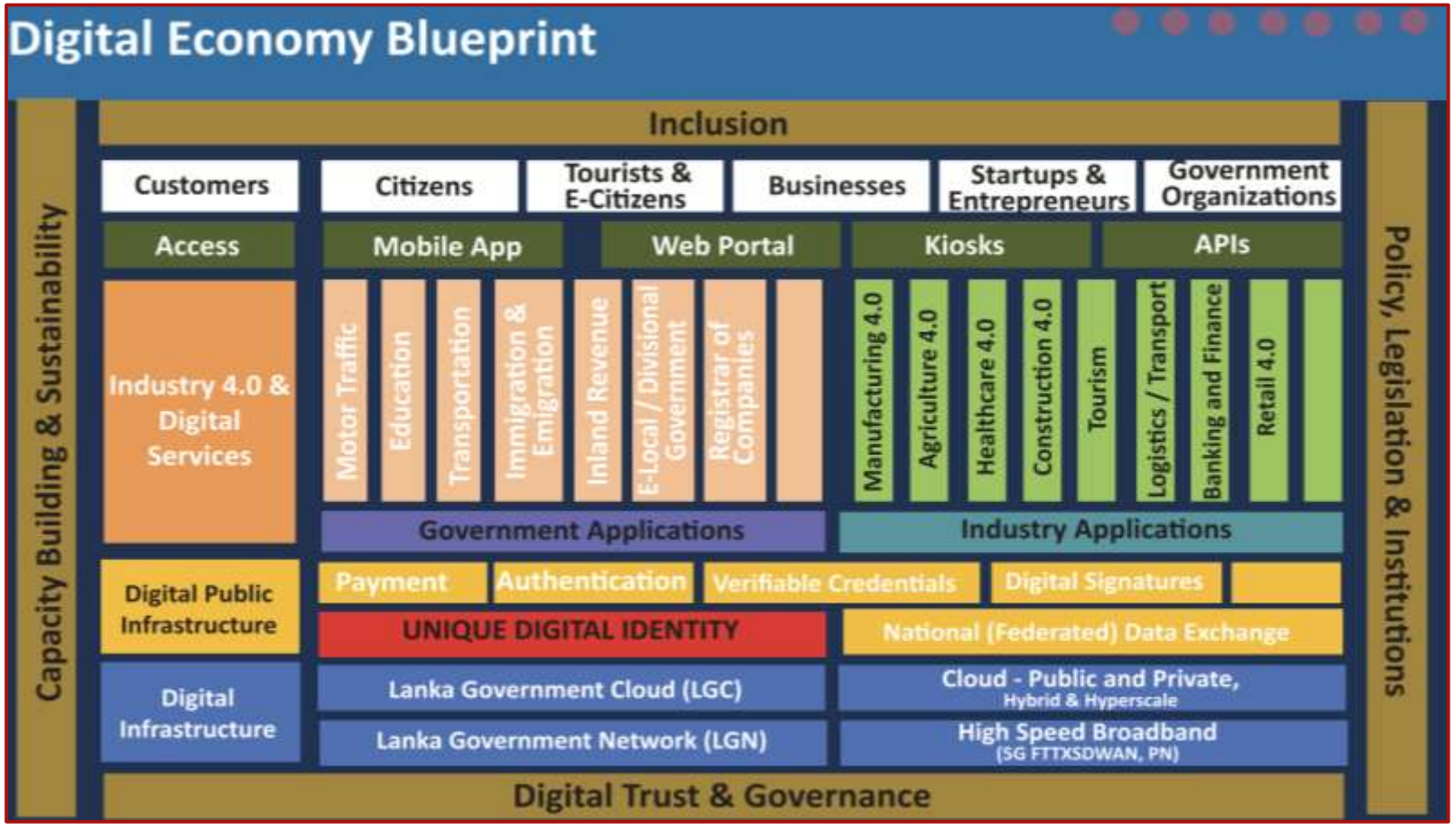
WATER

Source: [1] SLCERT | CC

LIRNEasia
Pro-poor. Pro-market.

Government of Sri Lanka has ambitious digital plans. A secure cyberspace is key to success

- Ambitious plans for "**digital transformation to be a cross-cutting enabler of macroeconomic growth** [1] ".
- **Unique Digital ID** (SLUDI) system.
- **National Data Exchange (NDX)** to enable interoperable data sharing between government institutions.
- **Lanka Government Network** (LGN) and **Lanka Government Cloud** (LGC) expanding digital infrastructure and connectivity across the public sector.



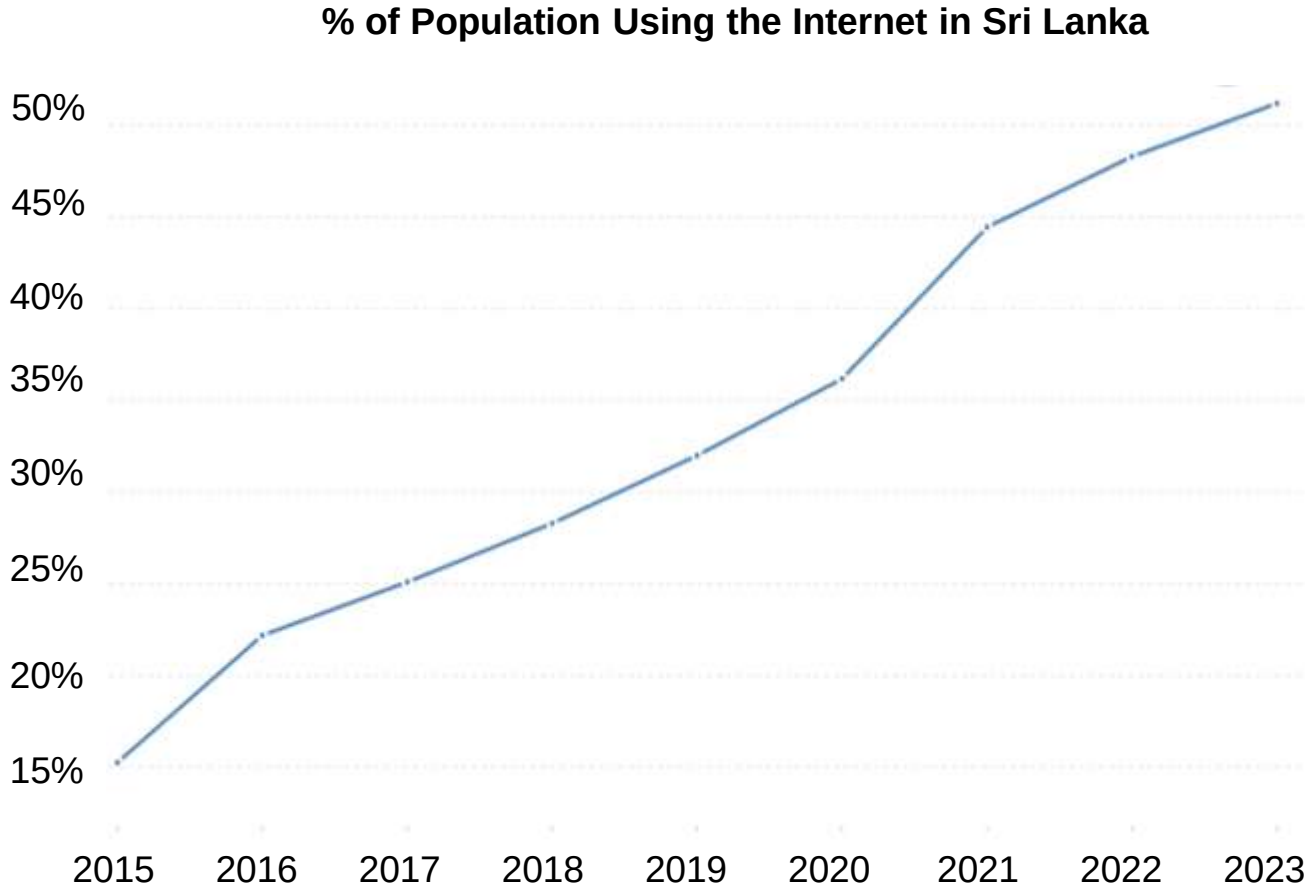
Plan for Digital Economy [2]

Sources: [1] DailyFT, [2] SLCERT | CC

LIRNEasia
Pro-poor. Pro-market.

Individual Sri Lankans are increasingly online and transacting digitally

- 31% of Sri Lankans made digital bank payments via a card or phone in 2024 [1]
  - Another 47% have financial accounts but don't make digital payments (yet)
- Over 65% of Sri Lankans used Social Media in 2024 [2].
- ~ 36% of Sri Lankans were Computer Literate & ~ 64% were Digitally Literate in 2024 Q4: [3]
- New Digital Literacy definition "the ability to access, manage, understand integrate, communicate, evaluate and create information safely and appropriately through digital technologies for employment, decent jobs and entrepreneurship"



Sources: *[1] World Bank, Sri Lanka – Inclusive digital financial services. https://digitalfinance.worldbank.org/country/sri-lanka [2] TRCSL Telecom statistics of Sri Lanka – Q4 2024 . Calculation of social media users: From TRCSL pg. 10, the platform with the highest number of users is Facebook with ~15 Mn. % = 15/23 [the pop. of SL] = 65%; [3] DCS, [4] LIRNEasia, [5] World Bank*

LIRNEasia
Pro-poor. Pro-market.

Like Other Countries, Sri Lankan Organizations Have Faced Cyber Incidents

Lanka Government Network (LGN) Breach [1]

- "All government offices using the 'gov.lk' email domain, including the cabinet office…lost data from May 17 – August 2023"
- In May 2023 LGN was still using the 2013 version of Microsoft Exchange.
- On 26 Aug 2023 there was a ransomware attack and LGN was restored within 12 hours. Some old emails were lost.

Cargills Bank Data Breach [2] [3]

- Announced by Cargills Bank in March 2025
- "Hackers reportedly dumped over 1.9 TB of data online"
- Included "NIC and passport photo [and] specimen signatures"

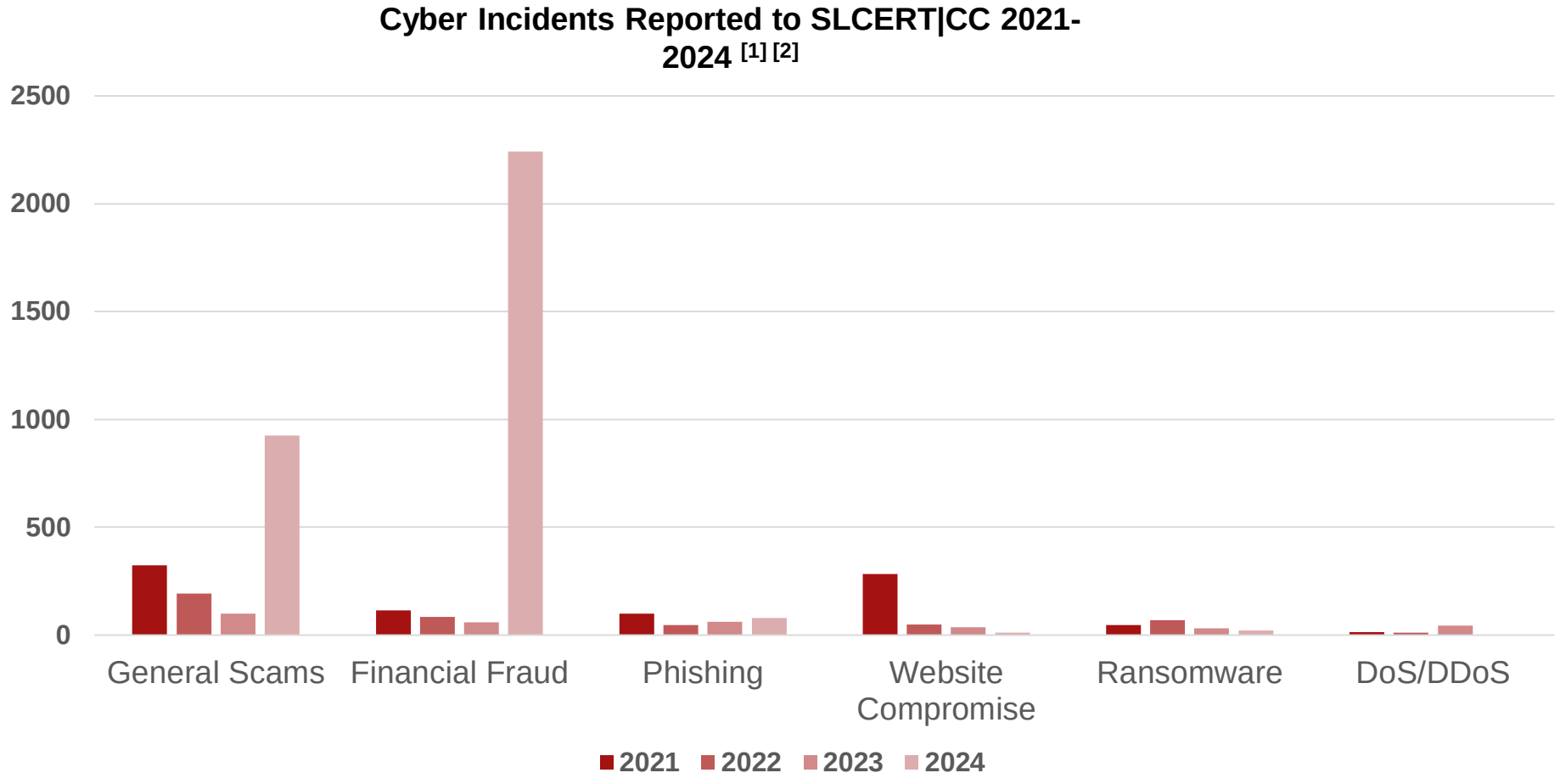
Department of Pensions Breach [4]

- First reported to SLCERT | CC in April 2025
- Pensioner data was compromised
- In May over 600 GB of data was uploaded to the dark web
- Department sent out warning texts to registered pensioners.

Sources: [1] The Sunday Times, [2] Ceylon Daily News, [3] Newswire, [4] The Sunday Times

LIRNEasia
Pro-poor. Pro-market.

Scams and financial frauds are the most common Incidents reported by Sri Lanka CERT | CC



Sources: *[1] 2021-2023 Data from SLCERT | CC , [2] 2024 Data from SLCERT | CC;*
Definitions: Scams: Common ways that digital accounts are compromised, Financial Fraud: Crimes involving illicitly gained funds, Phishing: Using fraudulent communication to trick people, Website Compromise: When a party has unauthorized access to a website, Ransomware: Malware which prevents access of files and allows them to be held for ransom, DDoS/Dos (Distributed/Denial of Service) Attack: Flooding a server with traffic.
Links for the above: https://www.cyber.gov.au/learn-basics/watch-out-threats/types-scams, https://www.uspis.gov/tips-prevention/financial-fraud, https://www.ibm.com/think/topics/phishing, https://csrc.nist.gov/glossary/term/compromise, https://www.ncsc.gov.uk/ransomware/home, https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/

Data is not 100% comparable over the years due to changes in definitions, new categories being reported by CERT|CC

Cyber Incidents Reported to SLCERT|CC Between 2018-2023 [1]

Type of Incidents	Number of Incidents					
	2018	2019	2020	2021	2022	2023
Cyber Security Incidents						
Phishing	12	5	17	98	46	61
Ransomware	8	11	24	45	68	31
Scams	7	5	157	322	191	98
Malicious Software	11	3	9	10	16	2
Financial Fraud	21	28	57	115	85	58
Website Compromise	9	175	85	282	49	37
DoS/DDoS	1	2	1	13	12	44
Phone Compromise	-	1	6	7	119	9
Server Compromise	-	2	6	13	11	11
Cloud Related Incidents	-	-	-	-	17	1
Other Cyber Security Incidents	-	364	48	144	7	56
Total Cyber Security Incidents	69	596	410	1049	621	408
Social Media Compromises and Other Content-related Incidents						
Social media Related Incidents	2505	2969	15965	17157	15674	20219
Intellectual Property Violation	6	1	1	8	6	1
Total Incidents	2580	3556	16376	18214	16301	20628

Figure 1: Summary of Incidents Reported to SLCERT|CC in 2023 Annual Report

Cyber Incidents Reported to SLCERT|CC in 2024 [2]

Category	Number of Incidents	Category	Number of Incidents
Cyber Security Incidents (Total)	4,347	Social Media Incidents (Total)	17,396
Financial Scams	2,241	Hacked Account	7,468
General Scams	926	Fake Account	4,011
Phishing	79	Hateful/Abusive Content	2,883
Ransomware	22	Adults Sexual Harassment/Content	1,411
Data Breach	42		
Website Compromise	11	Harmful & Dangerous Act	673
Database Compromise	4	Child Sexual Harassment	58
Malware Infection	6	Child Non-Sexual Harassment	60
Malicious Software	4	Suicide or Self-Harm	16
Technical Issues	638	False Information	767
Internal Inquiries	198	Copyright Violation/DMCA	49
System Failure	3		
Total Incidents (Social Media + Cyber Security)			**21,743**

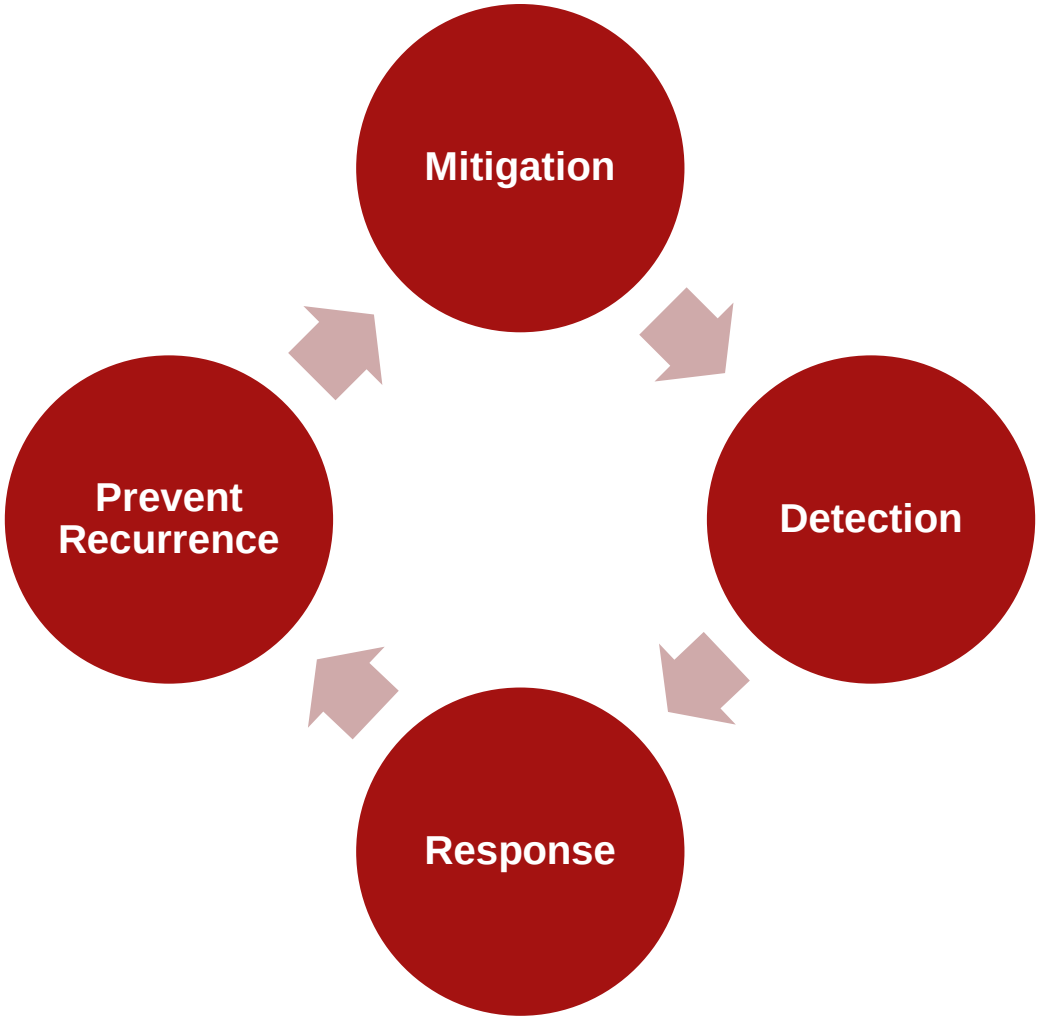
Figure 2: Summary of Incidents Reported to SLCERT|CC in 2025-2029 Strategy

Sources: [1] SLCERT | CC , [2] SLCERT | CC

LIRNEasia
Pro-poor. Pro-market.

LOOKING BEYOND OUR BORDERS

Countries taking a comprehensive approach: mitigating, detecting, responding to & preventing recurrence



- **Mitigation:** Proactive measures to reduce the likelihood and impact of cyber incidents. E.g. strengthening systems, applying security controls, managing vulnerabilities, and improving organizational resilience.
- **Detection:** Identifying malicious activity or system compromise as early as possible.
- **Response:** The actions taken once an incident is detected. Aiming to contain the threat, minimize damage, prevent further spread, preserve evidence, and restore normal operations.
- **Prevent Recurrence:** Ensuring that similar incidents do not happen again. E.g. conducting root-cause analysis, addressing system and process vulnerabilities, strengthening controls, and enforcing accountability.

United Kingdom

(1) MITIGATION

Key Laws

- The Computer Misuse Act 1990
- Network and Information Systems Regulations 2018
- Product Security and Telecommunications Infrastructure Act 2022

Range of guidance published by National Cyber Security Centre (NCSC)

- Cyber Aware (for SMEs)
- Cyber Essentials
- Cyber Essentials Plus
- 10 Steps to Cyber Security (broader organizational good practice guidance)
- Board Toolkit
- Cyber Essential Plus (independent technical verification of basic cyber hygiene)
- Cyber Assessment Framework to assess cyber resilience of essential services

(2) DETECTION

Active Cyber Defence (ACD) monitoring tools: Protective DNS, Host Based Capability, Suspicious Email Reporting Service

NCSC Early Warning Service: alerts organisations when their IPs show signs of compromise.

Cyber Security Information Sharing Partnership: joint govt–industry threat-intel sharing platform to increase situational awareness across sectors. Discontinued in 2025 and incorporated with ACD 2.0.

(3) RESPONSE

NCSC coordinates major incidents and issues technical response guidance.

NCSC Cyber Incident Response scheme: certifies providers to support organisations during incidents.

Active Cyber Defence Exercise in a Box: free simulation environment for testing response playbooks

(4) PREVENT RECURRENCE

National Audit Office & NCSC reviews: findings feed into updated security policies

Proposed Ban on ransom payments to sanctioned entities to curb repeat ransomware harms.

ACD Takedown Service: Removes UK-hosted malicious content, preventing re-abuse of infrastructure.

Sources: Adam Clark pg 26-28, 35-36, 47-50, 62-64, NCSC, NCSC, National Audit Office

Singapore

(1) MITIGATION

Key Laws
- Cybersecurity Act 2018
- Personal Data Protection Act 2012
- Computer Misuse Act 1993

Cybersecurity Labelling Scheme : security rating labels for Internet of Things devices

SG Cyber Safe Programme: initiative providing toolkits, self-assessment resources, and targeted guidance to help businesses raise their cybersecurity readiness.

Cybersecurity Code of Practice for Critical Information Infrastructure (CII): Prescribes minimum mandatory security controls for operators of CII.

Singapore Common Criteria Scheme: government certification of IT products against international Common Criteria standards.

Public Awareness Campaigns: Cyber Security Authority (CSA) of Singapore runs nationwide cyber hygiene campaigns targeting phishing, scams, and device security.

(2) DETECTION

National Cyber Threat Analysis Centre: Enhances early detection of national-level threats through intelligence sharing and analysis.

Government Bug Bounty Programme: Uses ethical hackers to identify vulnerabilities in government systems before exploitation.

Red Teaming in Government: Systematic adversarial testing of critical systems to proactively uncover weaknesses.

(3) RESPONSE

SingCERT as national incident contact point: national contact point offering incident alerts, advisories, and coordination support.

CSA Incident Advisories: rapid response guidance (e.g., during the CrowdStrike outage)

Critical Infrastructure Defence Exercise (CIDeX): national cyber response exercise co-organised by Ministry of Defence and CSA simulates simulating real-world attacks.

(4) PREVENT RECURRENCE

Post-incident investigations and strengthened standards after major breaches
Example: learning after 2018 SingHealth breach, which led to stronger CII requirements and sector-specific directives.

Singapore Police Force Cybercrime Command: Integrates investigation, forensics, intelligence, and training to systematically improve Singapore's ability to prevent repeat cybercrime.

Sources: Cyber Security Agency of Singapore (1) (2) (3), The StraightsTimes

LIRNEasia
Pro-poor. Pro-market.

Estonia

(1) MITIGATION

Key Laws
- Cybersecurity Act (2018, amended 2022)

Estonian Information Security Standard (E-ITS): mandatory baseline controls for public and private organisations

X-Road secure data-exchange layer: decentralised architecture that reduces single-point failures and strengthens systemic resilience

Planned cyber hygiene requirement (by 2026): users in state agencies must pass cyber-awareness tests before accessing government systems.

(2) DETECTION

Information System Authority's (RIA) incident handling unit (CERT-EE): continuously monitors and records cyber incidents across Estonia.

Nationwide vulnerability scanning: CERT-EE scans Estonian cyberspace and notifies organisations of exposed or vulnerable systems.

(3) RESPONSE

Voluntary cyber reserve: to be called upon if needed

RIA/CERT-EE as national coordinator: authority for assurance, prevention, coordinated resolution of cyber incidents under the Cybersecurity Act.

Int'l & Domestic Exercises: Prticipates in EU Cyber Europe, NATO Cyber Coalition, CyberSOPEx, and CCDCOE's Locked Shields.

Cyber Range Capability: CR14 Cyber Range supports hands-on training for agencies and CII operators.

(4) PREVENT RECURRENCE

Annual updates to E-ITS: RIA updates the standard based on implementer feedback and incident lessons.

Mandatory elimination of known vulnerabilities: system owners must fix vulnerabilities listed in CERT-EE threat notices.

Sources: RIA pg 6, 16, 24, 33, 42, , e-Estonia, RIA pg 8, 10, 23, 26, 34, 46,

LIRNEasia
Pro-poor. Pro-market.

Thailand

(1) MITIGATION

Key Laws
- Cybersecurity Act B.E. 2562 (2019)
- Personal Data Protection Act B.E. 2562 (2019)
- Computer Crime Act (Amended 2017)

Website Security Standard v1.0: sets mandatory technical and organisational requirements for government and CII websites

Thailand National Cyber Academy: builds nationwide workforce capacity and strengthens cyber resilience.

CII security standards: CII operators must prepare inspection plans, risk assessments, and internal cybersecurity procedures.

(2) DETECTION

ThaiCERT: key agency responsible for monitoring, detecting emerging incidents and alerting organizations

National Cyber Security Agency (NCSA) of Thailand partnership with Google Cloud Cyber Defence: enhances national threat-intelligence sharing using cloud-based detection tools.

(3) RESPONSE

ThaiCERT: coordinates national incident response across agencies, give remediation assistance

CII incident-response obligations: operators must maintain response plans, report incidents within defined timelines, and cooperate with authorities.

(4) PREVENT RECURRENCE

Cybercrime division in the Criminal Court: handles crimes involving ransomware, extortion, illegal access, and technology-enabled fraud, enabling faster, specialised adjudication.

Sources: Legal 500, PKF Thailand, The Nation, Tilleke & Gibbins, Google, Chandler MHM

There are several best-fit principles/practices Sri Lanka might learn from from

	Mitigation	Detection	Response	Prevention
United Kingdom	Apex authority provides tools and standards to the public	Active Cyber Defence 2.0 threat sharing platform	Apex authority certifies cybersecurity companies	Proposed ban on ransom payments
Singapore	Building a talented workforce through programs like SG Cyber Talent	Bug Bounty Programmes by the government	Coordinating responses to major cybersecurity incidents through SingCERT	Post incident legal reforms after major breaches
Estonia	E-ITS and X-Road secures national information and data exchange architecture	National level threat detection programs by National Cyber Security Centre	Voluntary cyber reserve through the military	Regular update of Estonian Information Security Standard (E-ITS) based on lessons learned
Thailand	Mandatory security standards for CII websites	Partnership with Google Cloud Cyber Defence	ThaiCERT as the national incident response team	Cybercrime division in Criminal Court for faster investigation and adjudications

LIRNEasia
Pro-poor. Pro-market.

CONSIDERATIONS FOR SRI LANKA

Sri Lanka Has Revised its Cybersecurity Bill Several Times - Alongside a Growing Set of Related Laws

2006 — **Electronic Transactions Act of 2006 [1]:** Legal framework for electronic commerce.

2007 — **Computer Crimes Act of 2006 [1]:** Criminalizes certain forms of cyber-enabled offenses

2019 — **Cybersecurity Bill [1]:** First version of the Act published. Not brought to Parliament.

2022 — **Personal Data Protection Act [1]:** To safeguard individual data. Not enforced yet

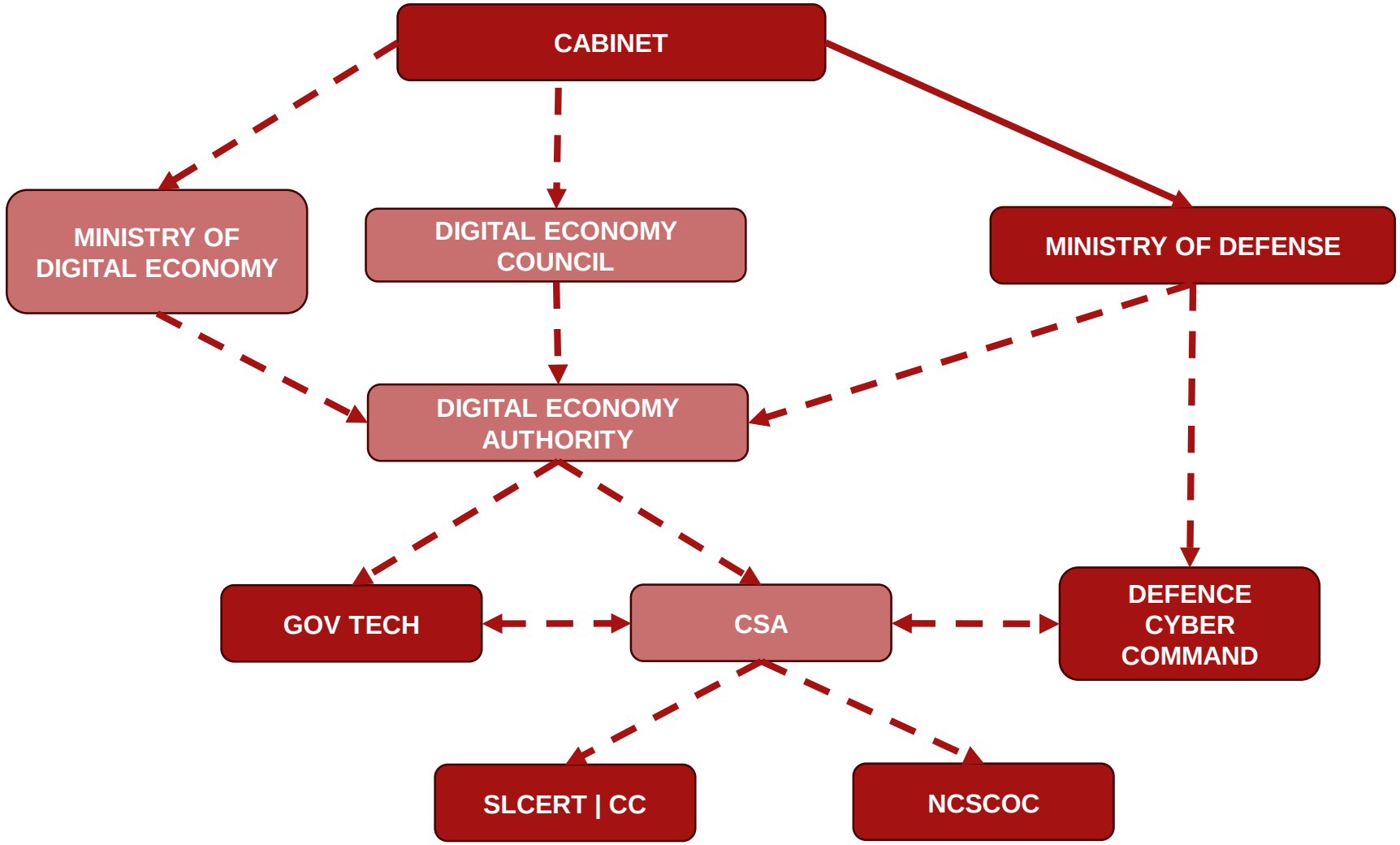
2023 — **Cybersecurity Bill [2]:** Sixth draft published. A new draft is expected in 2026.

2024 — **Online Safety Act [1]:** Regulates online behaviour.

Source: [1] ICTA, [2] TRCSL

LIRNEasia
Pro-poor. Pro-market.

Establish Institutions with an Overarching Governing Authority and clear lines of communication



- **Digital Economy Authority:** Develop Strategies, Policies and Legal Advice with the input of CSA and Defence Cyber Command.
- **(CSA) Cyber Security Authority*:** Coordinating operations, building public awareness and deploying guidelines and tools.
- **(NCSCOC) National Cyber Security Operations Centre:** Monitoring threats and building resilience of Critical Information Infrastructure (CIIs).
- **SLCERT | CC:** Assist public sector with security and conduct some incident response.
- **Defence Cyber Command:** Respond to major incidents.

Source: *ICTA [2019, Cyber Security Bill] TRCSL [2023, Cyber Security Bill]'.*
*Note: *In the 2023 Cybersecurity Bill this is called the "apex regulatory authority" is called the Cyber Security Regulatory Authority (CSA). This version also calls for a Cyber Defence Bill to clarify the role of the military. It states that SLCERT | CC will be wound down and incorporated into the CSA.*

LIRNEasia
Pro-poor. Pro-market.

An Agency is needed to coordinate (for mitigation, detection, response, prevention)

- Cyberspace: when one node is compromised the surrounding ecosystem is threatened.
- Therefore, need to **coordinate information sharing** between:
  - Private Sector
  - Public Sector
  - Critical Information Infrastructure
  - Civil Societies
  - Intelligence & Defence Networks
  - International Actors
- Others (SLCERT/NCSCOC) to actively **monitor CIIs** (Critical Information Systems)

Note: 2023 Bill refer to this Agency as the Cyber Security Regulatory Authority

LIRNEasia
Pro-poor. Pro-market.

Enable this Agency to offer competitive renumeration

- Competent staff are essential.
- Salaries must be competitive with the private sector and foreign countries(*)
- The standard public sector salary scales are insufficient.
- The authority can accomplish this if given a block grant and allowed to structure their own salaries.
- Job continuity can be pegged to performance.

Global Cybersecurity Workforce Gap of 4.8 million [1].
As of 2024: International Information System Security Certification Consortium (ISC2)

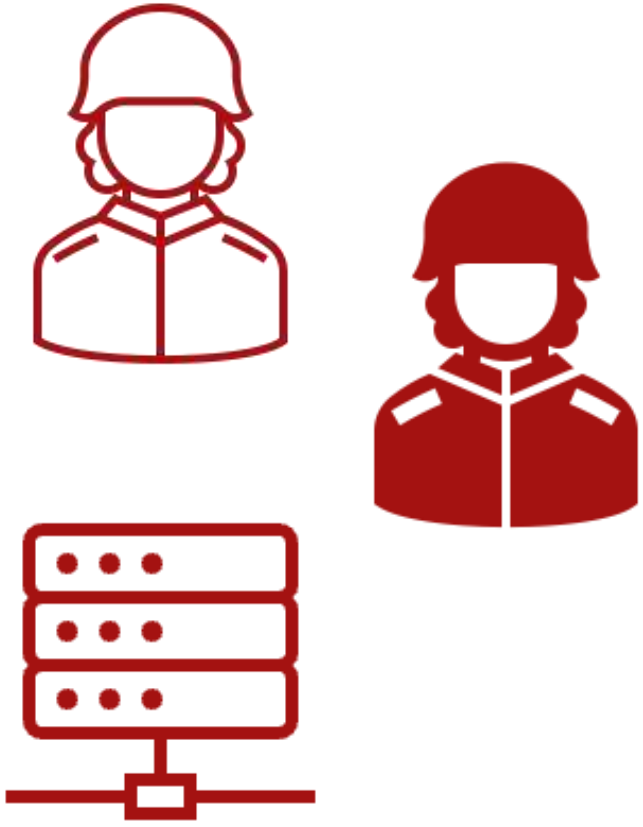
In the US, **Employment** of Information Security Analysts is projected to **grow 29% between 2024 to 2034.** Much faster than the average for all occupations [2].
Occupational Outlook Handbook by the US Bureau of Labor Statistics (BLS)

Sources: *[1] ISC2, [2] BLS.GOV;*
*Note: *Developing countries struggle to retain skilled cyber security professionals who often find attractive opportunities in the private sector in more developed countries. See https://documents1.worldbank.org/curated/en/099111023150023703/pdf/P17785208994aa06d08eca094513904323a.pdf?*

LIRNEasia
Pro-poor. Pro-market.

Develop a Civilian Reserve to respond to major incidents

- Major incidents require highly skilled cybersecurity experts.
- Keeping them in full-employment is impractical.
- Professionals from the private sector (and the diaspora) can be enlisted as reserves.
- The military has best expertise with managing a reserve force.
- The reserves can join the Defence Cyber Command in responding to major incidents.



Sources: [1] WBG, [2] OECD

LIRNEasia
Pro-poor. Pro-market.

Policy Considerations for Cybersecurity

Designate an Overarching Cybersecurity **Governing Body (DEA?)**

Establish an **Agency to Coordinate** for Prevention, Mitigation, Response & Prevention (CSA?)

Enable the Cybersecurity Authority to Offer **Competitive Renumeration**

Develop a **Civilian Reserve** to Respond to Major Incidents

LIRNEasia

Pro-poor. Pro-market.