Draft regional framework for enhancing rail cybersecurity in Asia-Pacific

Sandeep Raj Jain
Transport Division

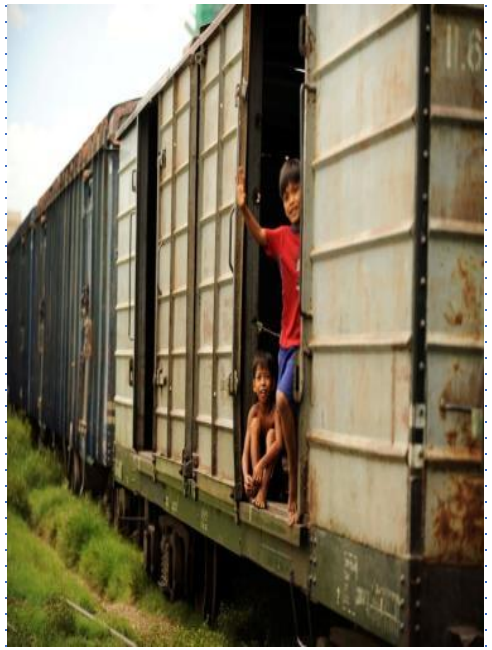
ESCAP
Economic and Social Commission for Asia and the Pacific

Outline

- Background
- Challenges to rail cybersecurity
- Key areas for action and proposed suggestions



Background

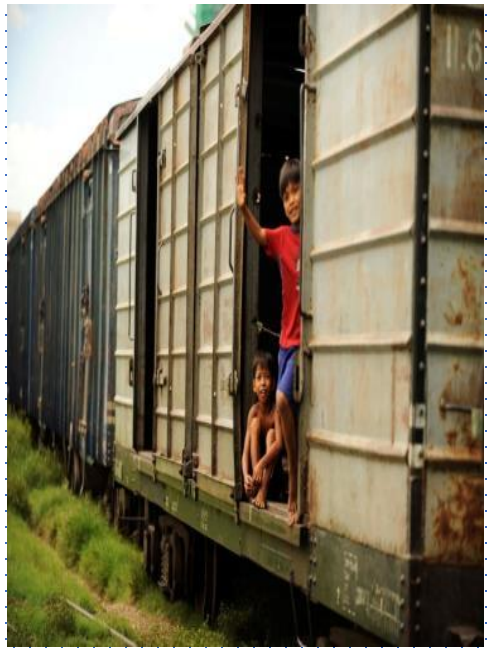


- ✓ Strategy 2030 on Accelerating Rail Digital Transformation in Asia-Pacific provides for rail cybersecurity as one of the cross-cutting issues - Recommends developing a regional framework to leverage regional cooperation in addressing cyberthreats to rail

- ✓ Growing digitalization and artificial intelligence capabilities no doubt increase efficiency and reduce costs however they would expose rail systems to cyber threats. According to Gartner, by 2025, one third of critical infrastructure organizations such as rail will experience a security breach

- ✓ Growing cyberattacks in the form of ransomware, malware can lead to disruption of services with attendant economic and other losses, damage to

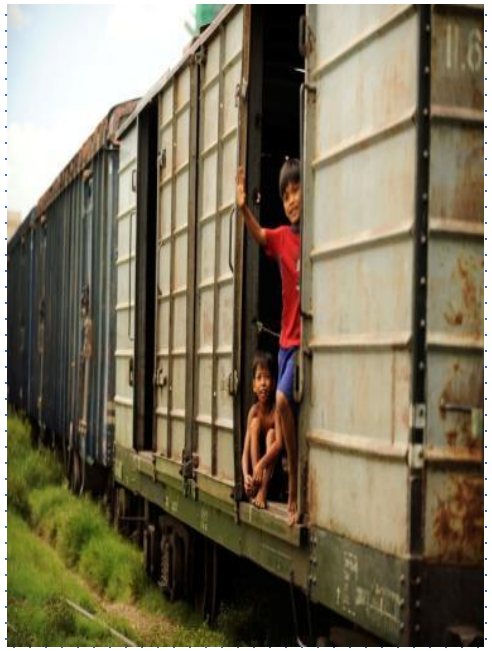
Challenges for rail cybersecurity



- ✓ Longevity and legacy of rail assets
- ✓ Prevalence of wide range of stakeholders
- ✓ Analyzing rail safety due to cyber threats
- ✓ Wide geographical spread of rail assets
- ✓ Low capacity of rail officials on cybersecurity issues
- ✓ Making rail cybersecure would need additional investments

Key actions for enhancing rail cybersecurity

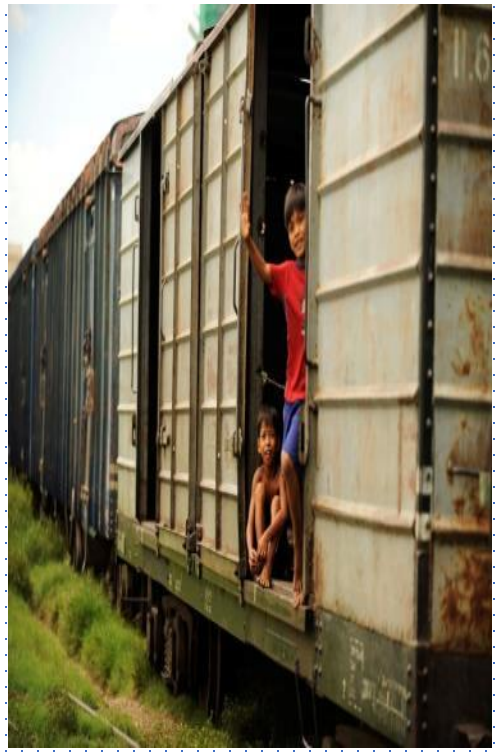
1. Develop a comprehensive policy for rail cybersecurity that is aligned to national cybersecurity policy



- Rail should be part of critical national infrastructure if not included already
- Comprehensive understanding of rail digital ecosystem including inventory digital assets and cyber-interfaces and a risk-based approach to secure to manage cyber threats
- Governance structure that apart from others aim to address the legal and fiscal responsibilities
- Means to secure OT systems, train to trackside interfaces, IT system protection, data protection and procurement policy

Key actions for enhancing rail cybersecurity

2. Consider developing subregional/regional standards/regulations on rail cybersecurity

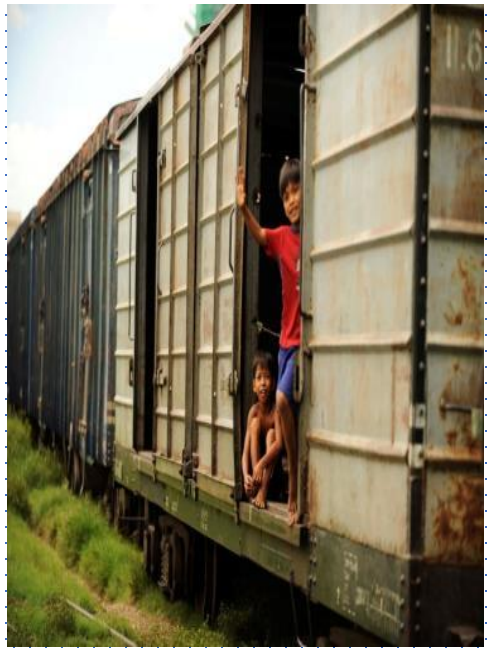


- Unique rail environment in Asia-Pacific characterized by existence of
  - ✓ Different rail gauges, rolling stock and operational practices
  - ✓ Integrated infrastructure and operations; and
  - ✓ Three types of rail, namely, high-speed and highly digitalized, digital metro systems and traditional heavy rail used for freight and passenger

- Globally several regulations/standards have been developed on rail cybersecurity
  - ✓ European Union Network and Information Systems (NIS) Directive
  - ✓ European Union General Data Protection Regulation (GDPR)
  - ✓ IEC 62443 suite of standards for cyber security of industrial automation
  - ✓ CENELEC TS 50701 technical standard apply to the railway

Key actions for enhancing rail cybersecurity

2. Consider developing subregional/regional standards/regulations on rail cybersecurity



- ✓ None of the existing standards/regulations address all aspects of rail cybersecurity
- ✓ It appears countries in the region have different approaches on rail cybersecurity
- ✓ Consider developing subregional standards/regulations/specifications or principles
- ✓ Constitute a *group of experts* from interested countries to consider this and present recommendations at the Working Group

Key actions for enhancing rail cybersecurity

3. Enhance capacity for rail cybersecurity



- ✓ With digitalization, apart from traditional engineering skills, digital competencies and capabilities are essential for operation and maintenance of railway systems and assets
- ✓ Skills are needed to understand, advise and quantify cyber risks to stakeholders in an organization
- ✓ A cyber security culture needs to be developed -where in a digital ecosystem any erroneous events are reviewed and across an organization the role of cyber security
- ✓ Upskilling the workforce with strong cyber security capability can require significant investment and time
- ✓ **Develop a dedicated regional capacity building programme on rail cybersecurity**

Key actions for enhancing rail cybersecurity

4. Establish regional rail cybersecurity group (RRCG)



Establishing collaborations between member states can provide significant opportunities and mutual benefits on addressing rail cybersecurity threats

- Information sharing – sharing relevant information about emergent cyber security threats, indicators of compromise/attack, and threat intelligence which other member states who may not possess or have access to
- Knowledge exchange – to promote mutual development of knowledge, skills, and expertise

Key actions for enhancing rail cybersecurity

4. Establish regional rail cybersecurity group (RRCG)



- Identifying and resolving shared issues – a specific challenge in railway cyber security within one member state may be shared by other states. Through collaborative efforts, these burden of addressing an issue is shared across many parties, each bringing their knowledge, expertise, and insight to address these challenges

- Suggested that member countries establish a **regional rail cybersecurity group** as a mechanism to address the common challenges

Key actions for enhancing rail cybersecurity

5. Engage private sector and OEMs through collaborative arrangements



- Private sector and OEMs have significant rail cybersecurity experience and therefore it is critical to engage them throughout the lifecycle of rail assets
- Their engagement would ensure that the common approaches to cybersecurity requirements developed at a regional, sub-regional level and at national level are agreed by end users and suppliers
- Suppliers can then inform their product roadmaps and develop solutions early to meet these requirements, rather than on a per-project basis leading to economies of scale

Key actions for enhancing rail cybersecurity

5. Engage private sector and OEMs through collaborative arrangements



- At the regional level the proposed regional railway cybersecurity group should consider including or inviting the private sector and OEMs in their deliberations to inform security requirements
- Engagement of private sector, however, should be based on knowledge and in the interests of rail cyber security within the region rather than for pushing specific supplier solutions



Next Steps

Thank you
for
your attention

http://www.unescap.org/our-work/transport

