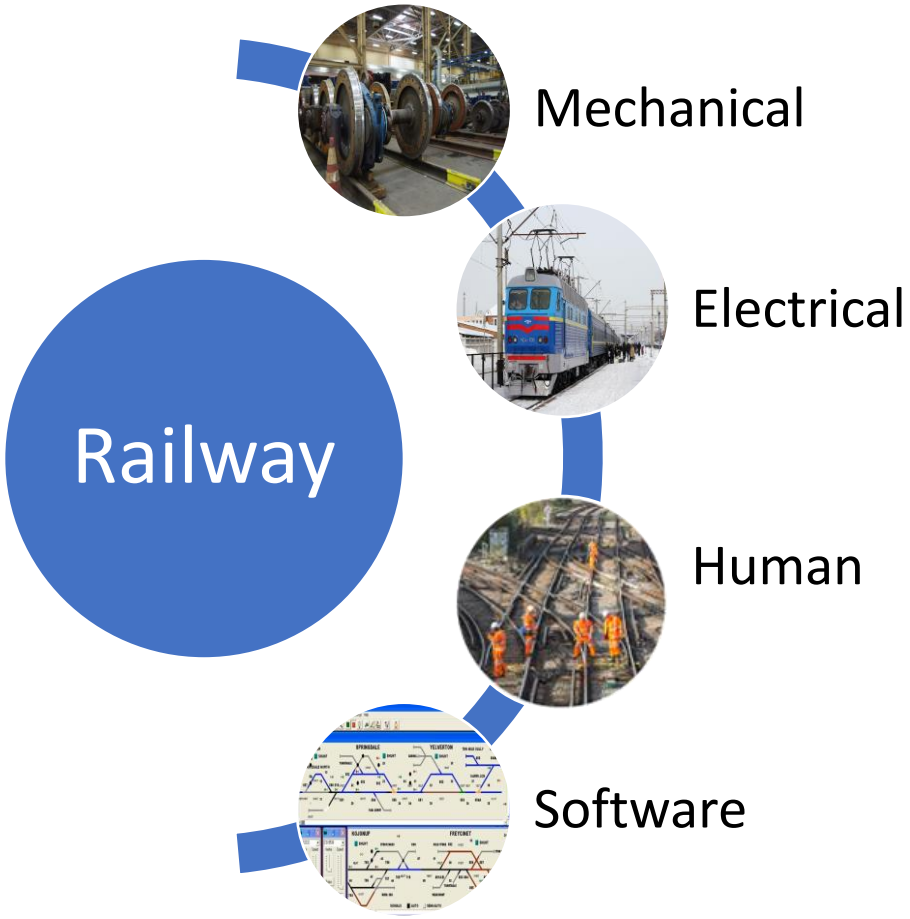
Cyber Resilient approach for Railways

Ravdeep Kour, Amit Patwardhan, and Ramin Karim

Division of Operation and Maintenance Engineering,
Luleå University of Technology

Railway and Cybersecurity

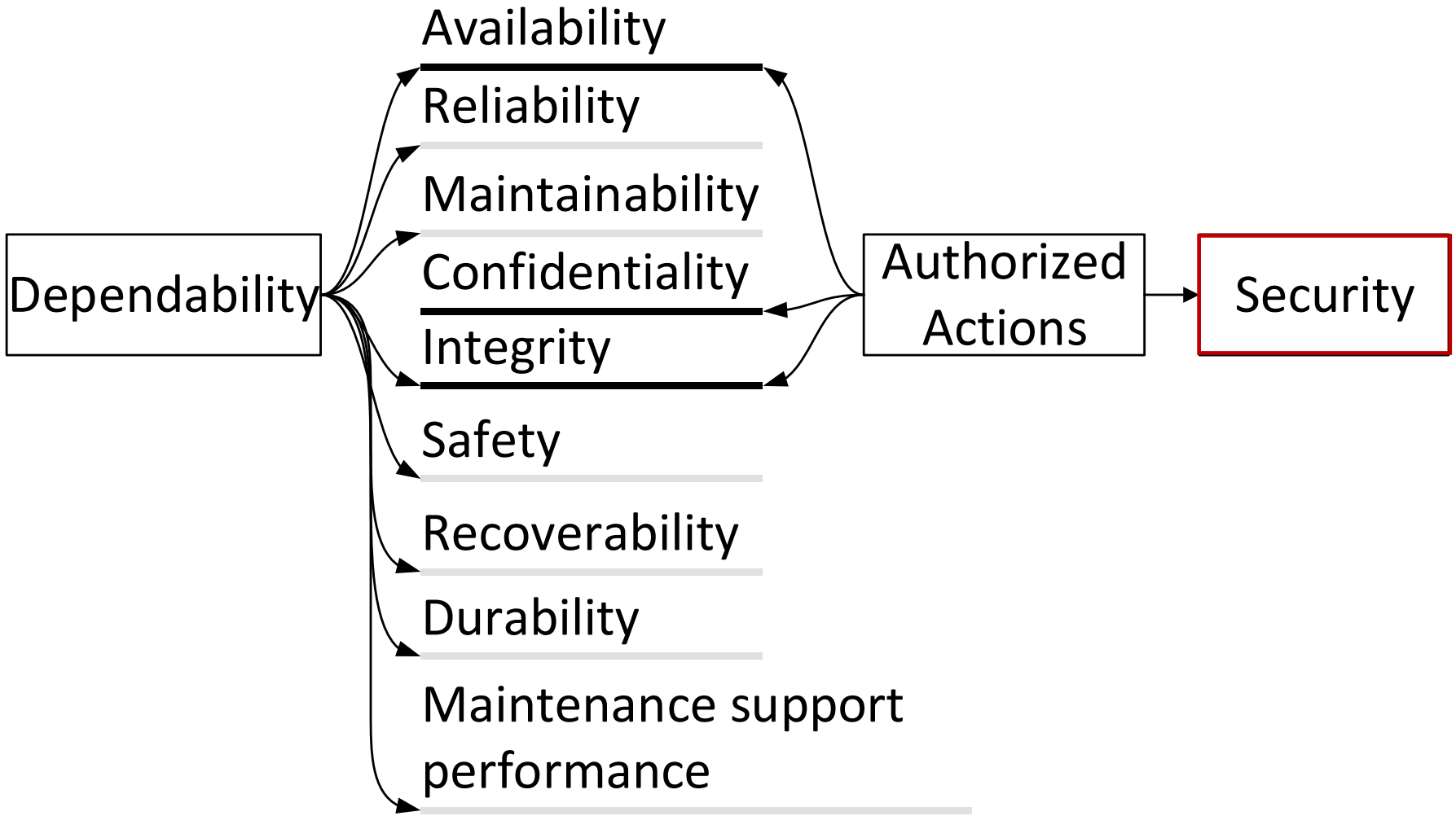


Confidentiality
Only authorized personnel may disclose or observe information

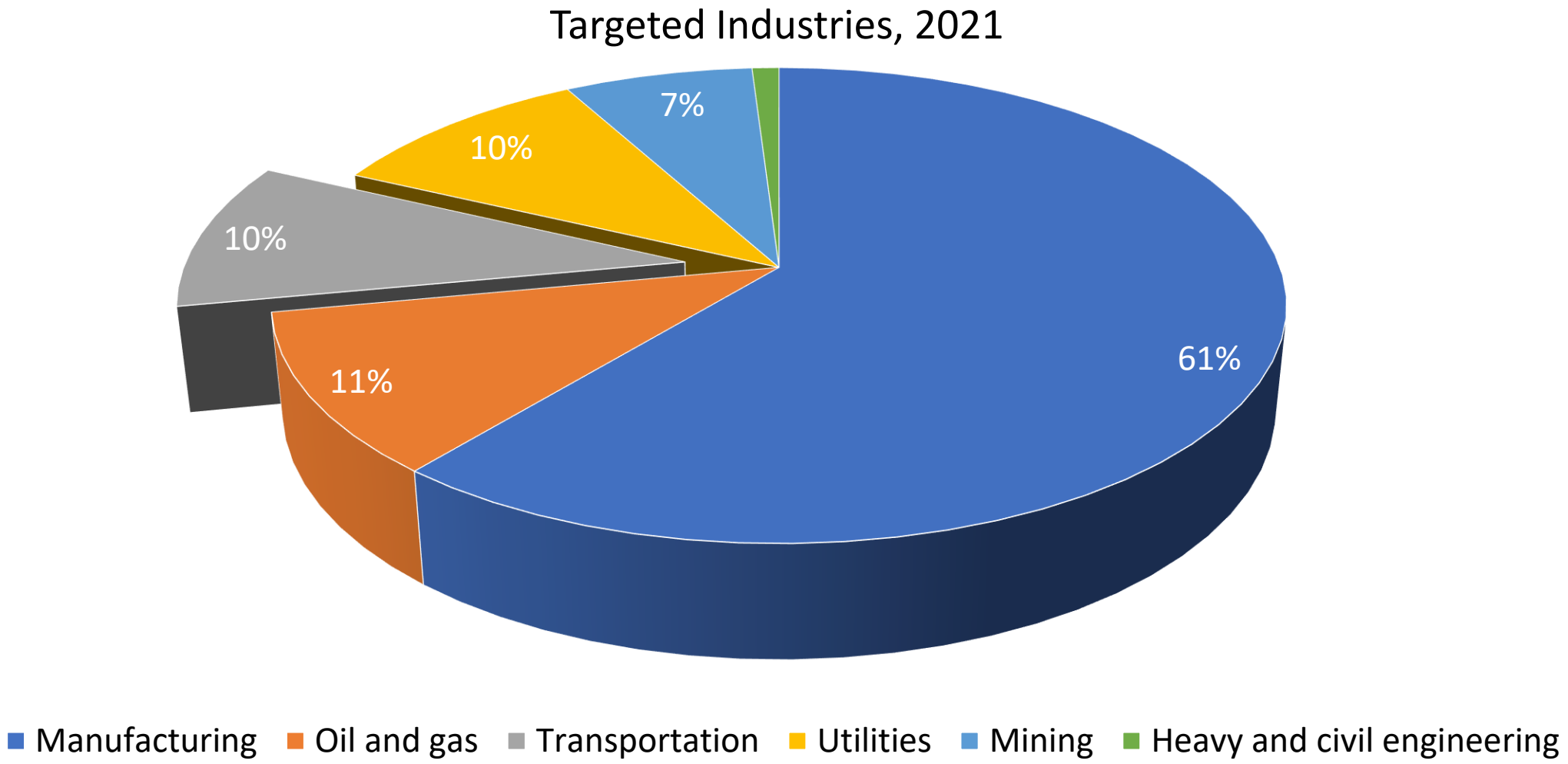
Integrity
Information cannot be modified in an unauthorized manner

Availability
Information should be readily available for the authorized users

Dependability and Security Attributes

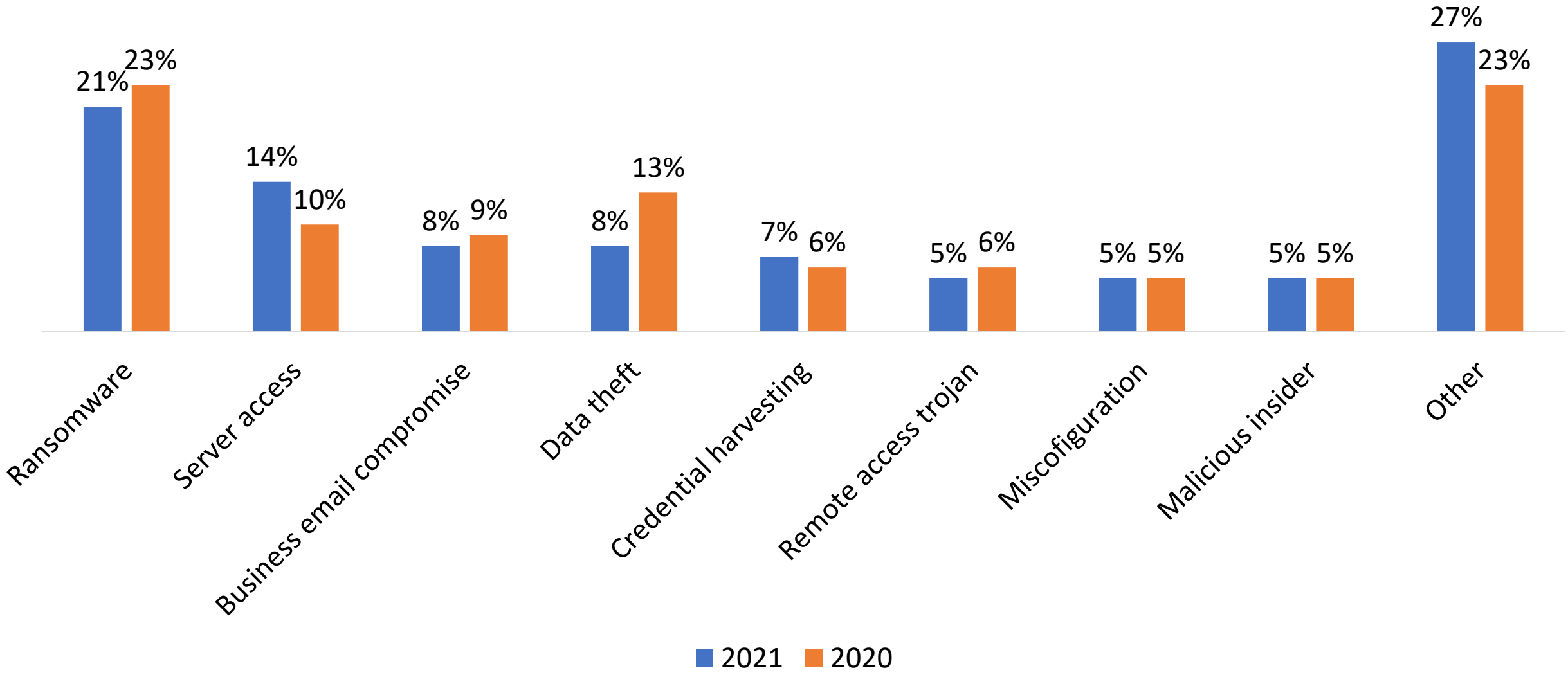


Cybersecurity statistics

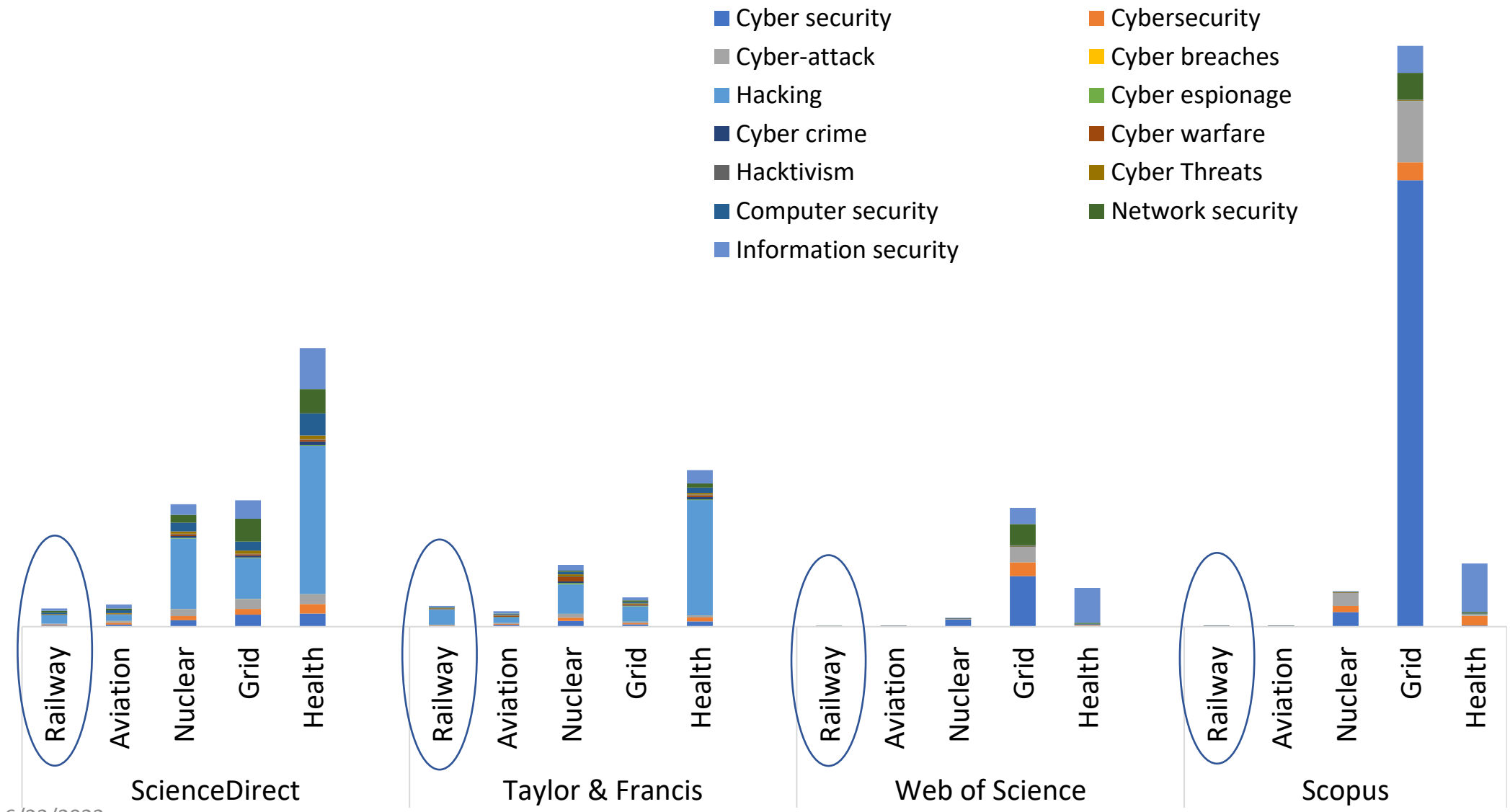


[ravdeep.kour@ltu.se]

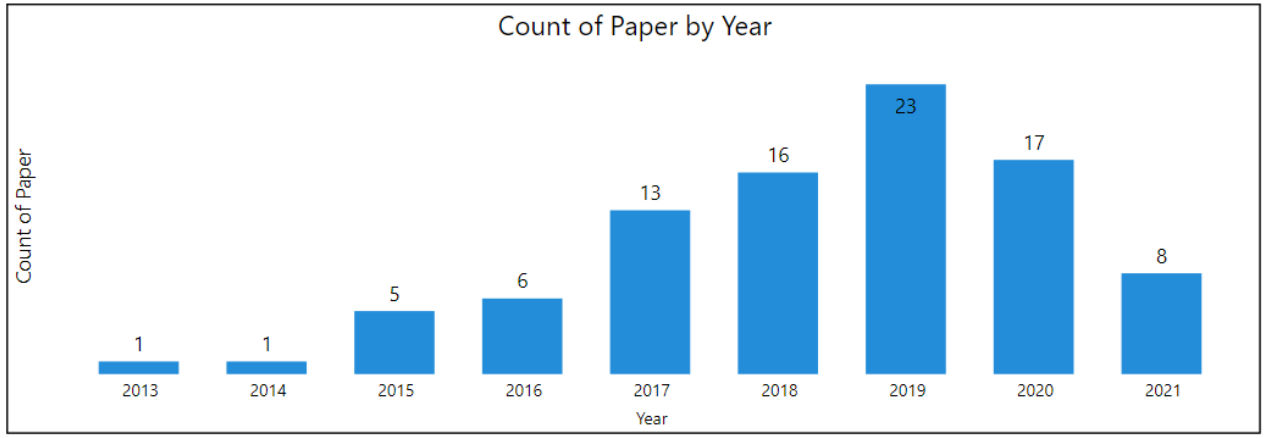
Top attack types, 2021 vs. 2020

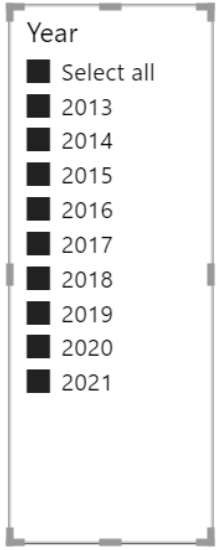


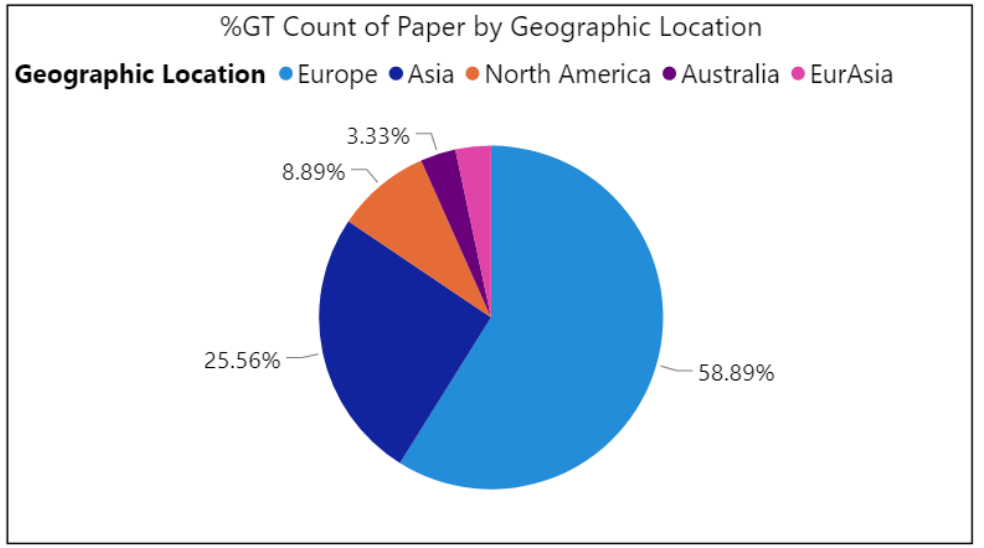
Cybersecurity research gap within railways

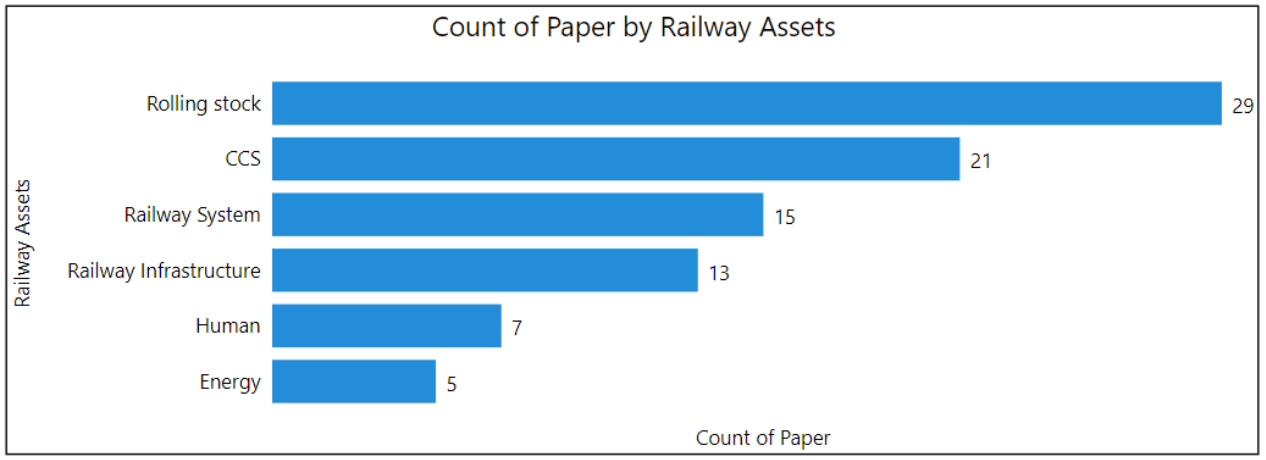


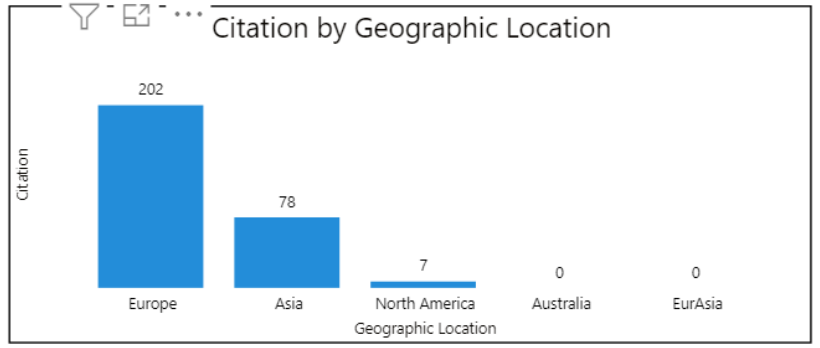
Trends in cybersecurity research in Railway





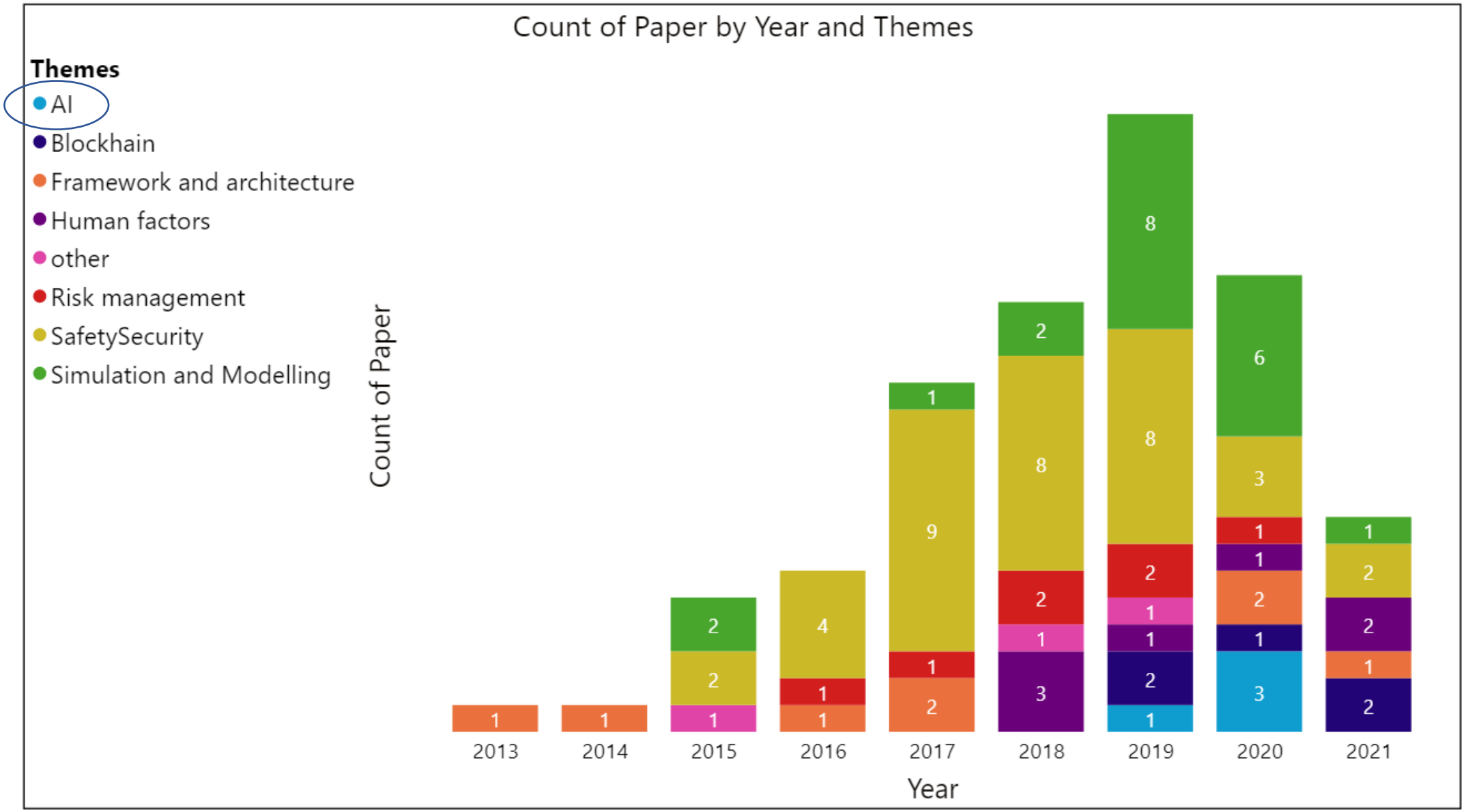






country	Citation
Singapore	59
UK	42
Spain	36
Sweden	32
Italy	31
France	20
China	19
Germany	19

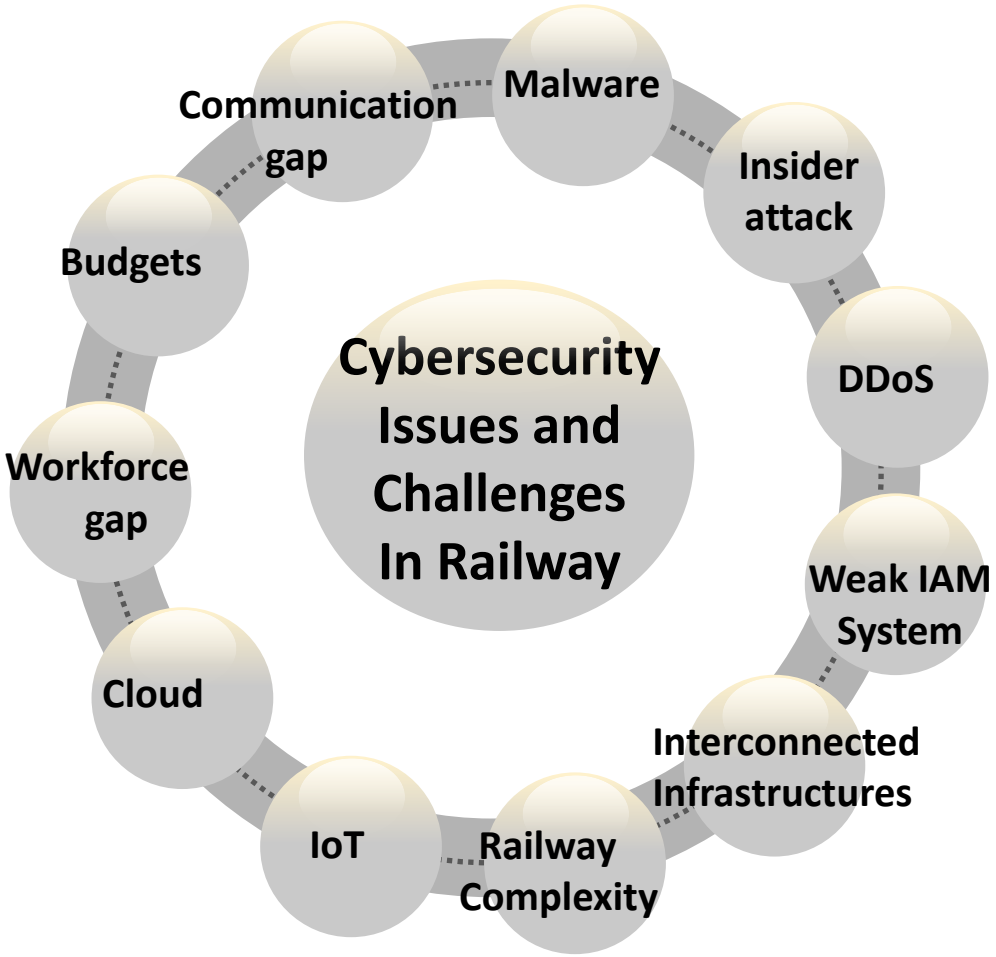
Review results by research themes



Why do these attacks happen?

- Software systems are buggy
- Users make mistakes (unintentional/ accidental)
- Security may make things harder to use
- Unpatched systems vulnerabilities
- Lack of security training for software engineers or workforce
- Insider attacks

Cybersecurity issues & challenges



DDoS- Distributed Denial of Service
IAM- Identity & Access Management System
IoT- Internet-of-Things

Purpose

To develop and provide a conceptual model to improve the cyber resilience of railway system from cyberattacks

Cyber resiliency

(NIST Definition, 2021)

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources

Cyberattack Sources (origin)

- Internal cyberattacks are from people working within the organisation with authorized access to the network, including employees and business partners.

- External cyberattacks are from people working outside the organisation without authorized access to the network. External incidents occur through wired or wireless networks and physical intrusion.

Actors

- responsible for the cause of the attack
- humans, technology, and natural disasters
- human actors such as internal (insiders) or external (hackers) can cause harm to the systems and gain physical access to restricted areas such as buildings, cabins, rooms, or any other area to steal or damage hardware and software
- technology includes the failure of hardware, software, and information systems
- natural disasters include earthquakes, hurricanes, wind, floods, tsunamis, fires, lightning, animals, and wildlife which can cause severe damage to system’s assets.

Actions

- intentions of the actors

- malicious or non-malicious

- Malicious intentions modify information of an organisation using malicious code. If the authentication mechanism is not properly implemented, a malicious intruder can act as a genuine user and monitor the network traffic.

- Non-malicious intentions occur when inadequate security policies allow vulnerabilities and errors. They are caused unintentionally by employees who are not seeking to harm the system.

Security goals

- the core principles or security elements which provide fundamental objectives for managing risks

- the operational goals of Information Technology (IT) security are Confidentiality, Integrity, and Availability (CIA)

- the operational goals of Operational Technology (OT) security are Safety, Reliability, and Availability (SRA)

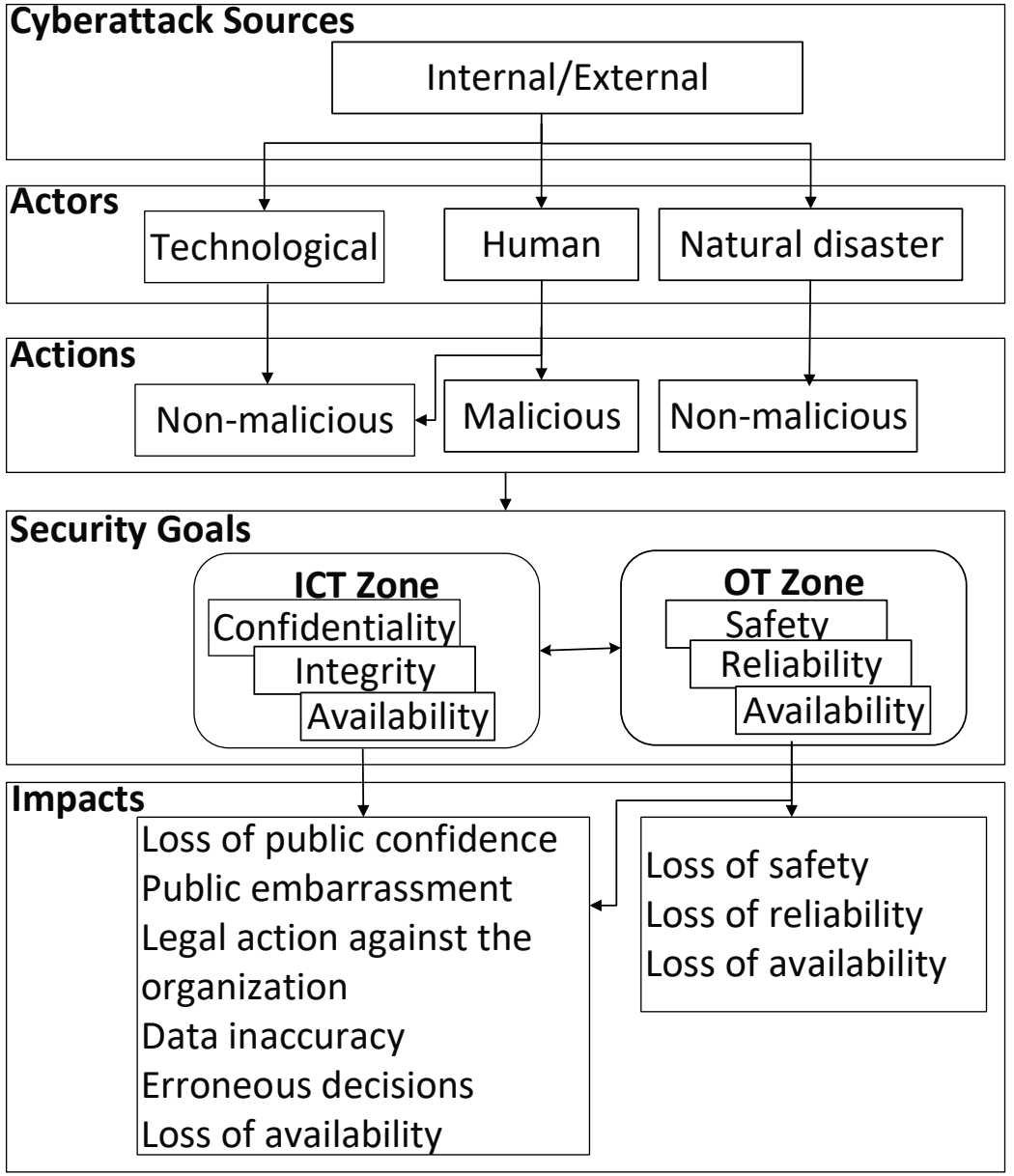
Impacts

- Financial loss
- Loss of public confidence
- Public embarrassment
- Legal action against the organisation
- Data inaccuracy
- Erroneous decisions
- Loss of reliability, safety, and continuity

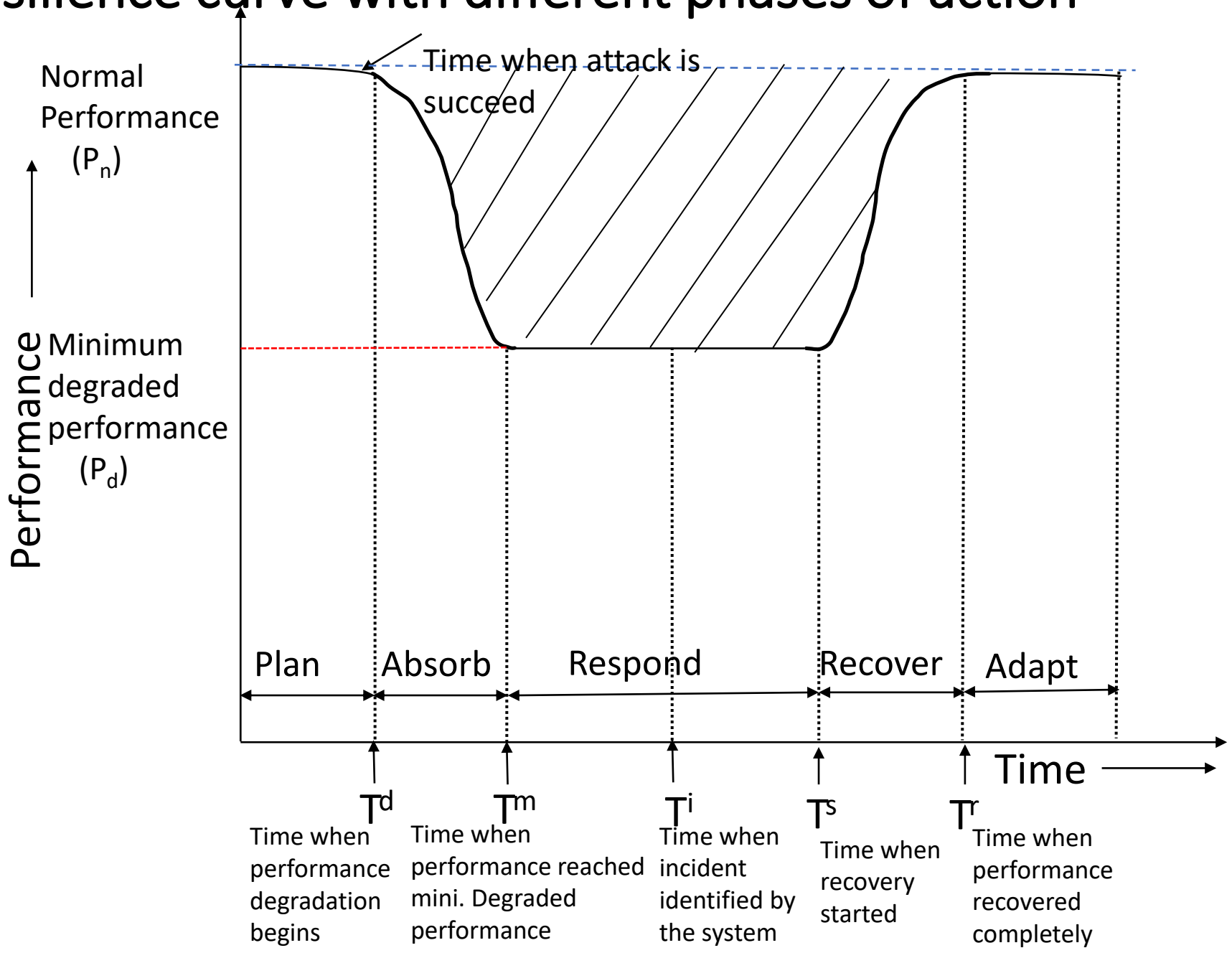
Multi-level cyberattack model

Identified cyberattacks and their impacts before their occurrence

- Assist in understanding cyberattack characteristics
- Beneficial for cybersecurity risk assessment using cause-effect analysis
- Help in determining severity of cyberattacks

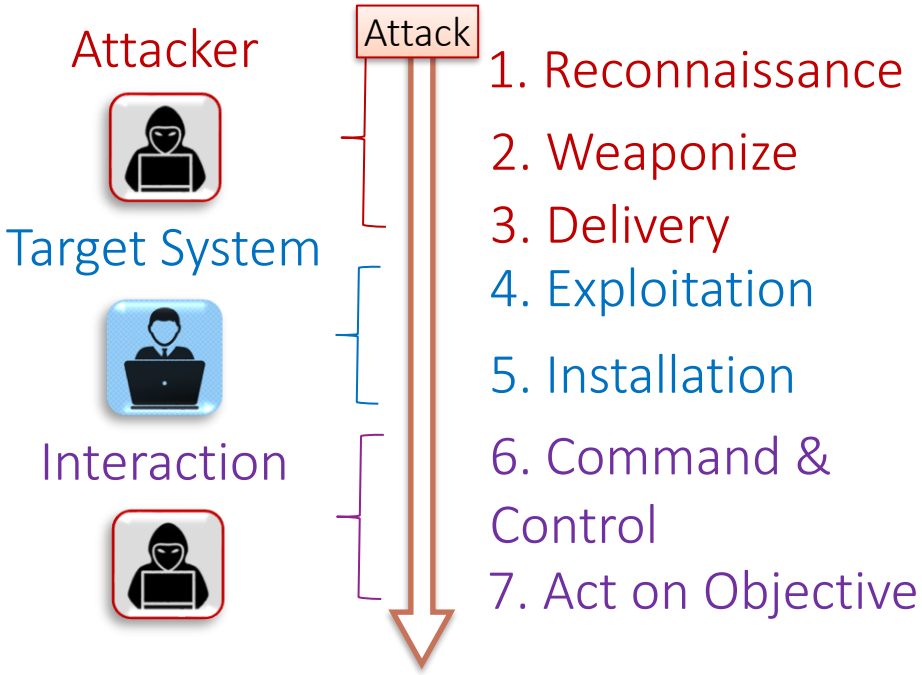


Resilience curve with different phases of action

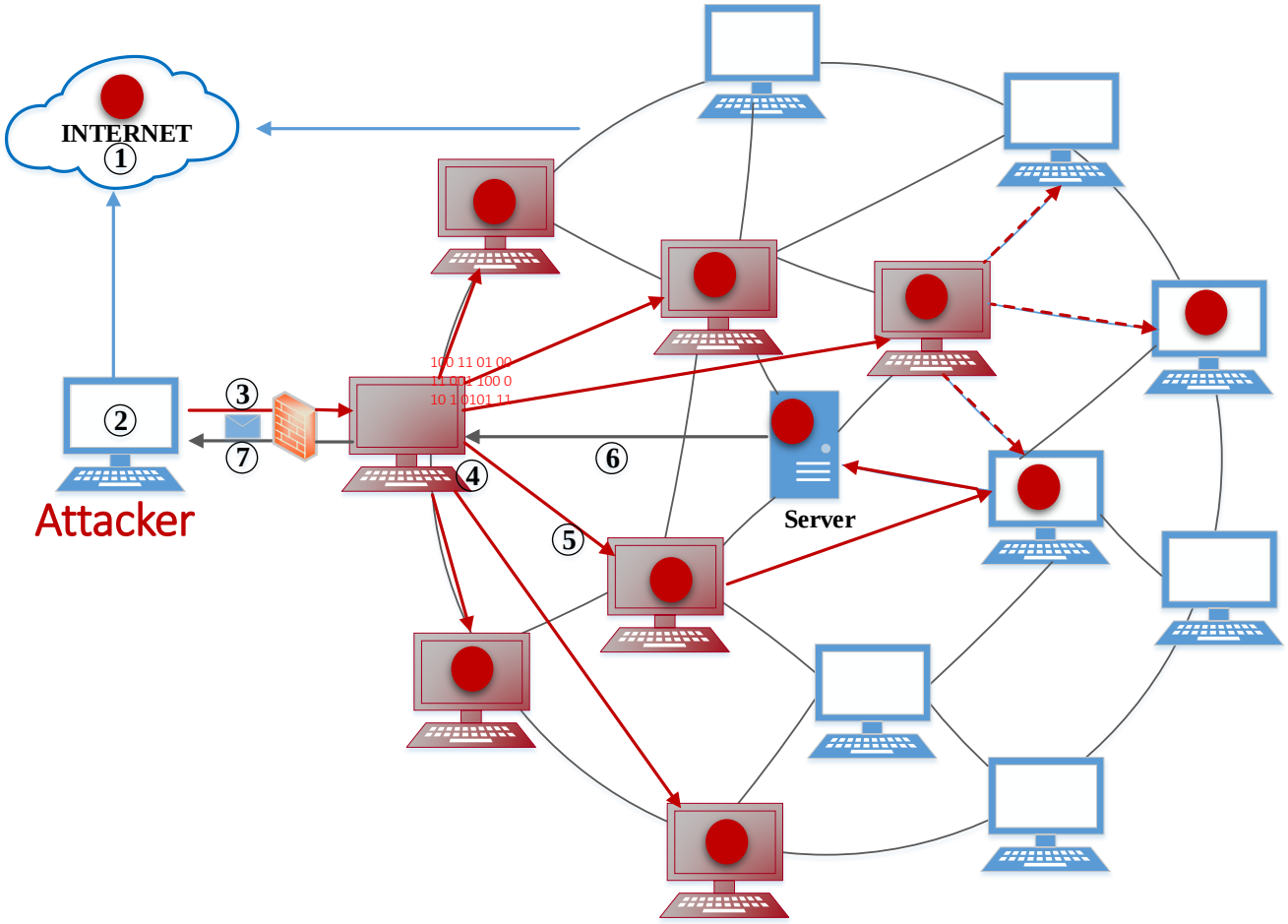


Cyber Kill Chain (CKC) Model

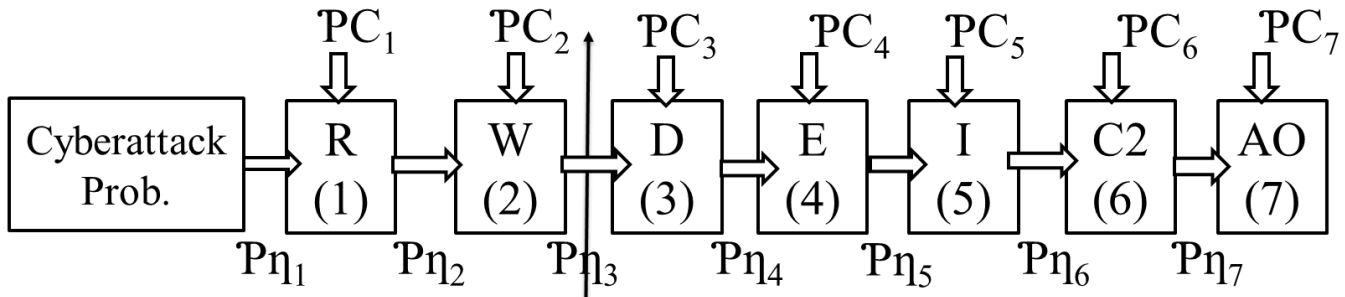
CKC Model

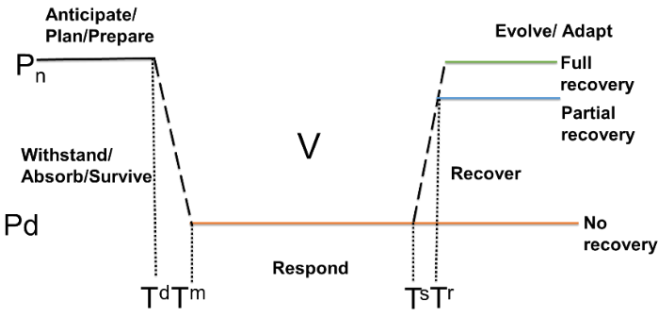


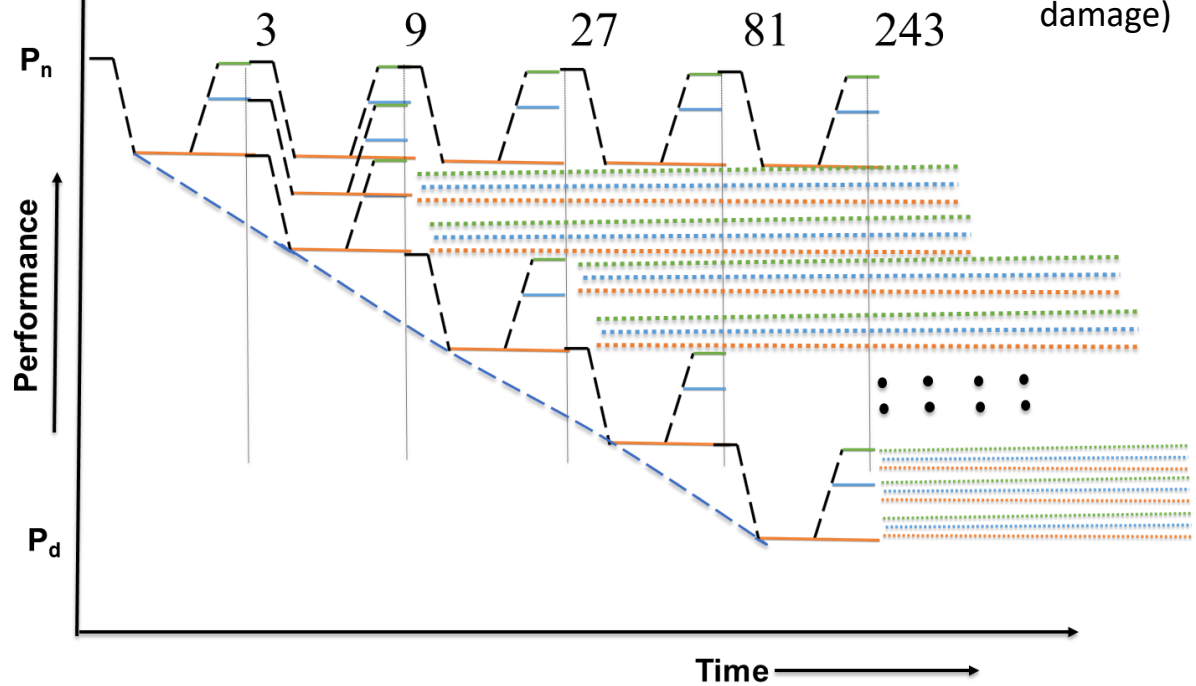
Target System



Resilience curve within each stage of the CKC model

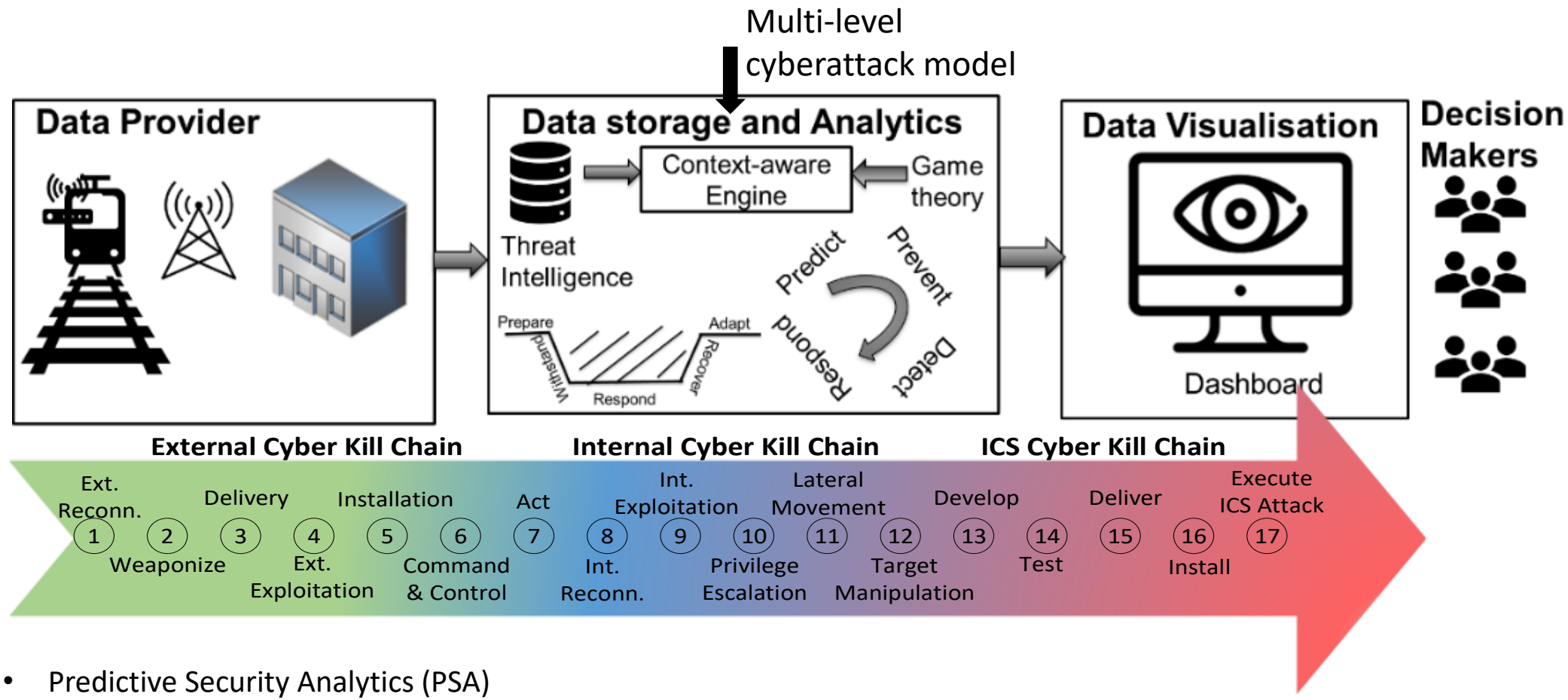






- V "Exploitation of Vulnerability" shows loss of performance
- area of a trapezoid with the assumed shape, i.e., Performance loss = [(Ts – Tm) +(Tr – Td)] * [(Pn - Pd)]/2
- Total loss = f(Performance loss, cost of SCs, asset damage)

Conceptual model for improving cyber resilience



- Predictive Security Analytics (PSA)
- Threat intelligence, MITRE ATT&CK Matrix
- Zero trust policy
- Learn from the breach attempt and continuously adapt the system to the changing conditions (resiliency)
- Stress test the incident response plan to increase cyber resilience

Cybersecurity framework

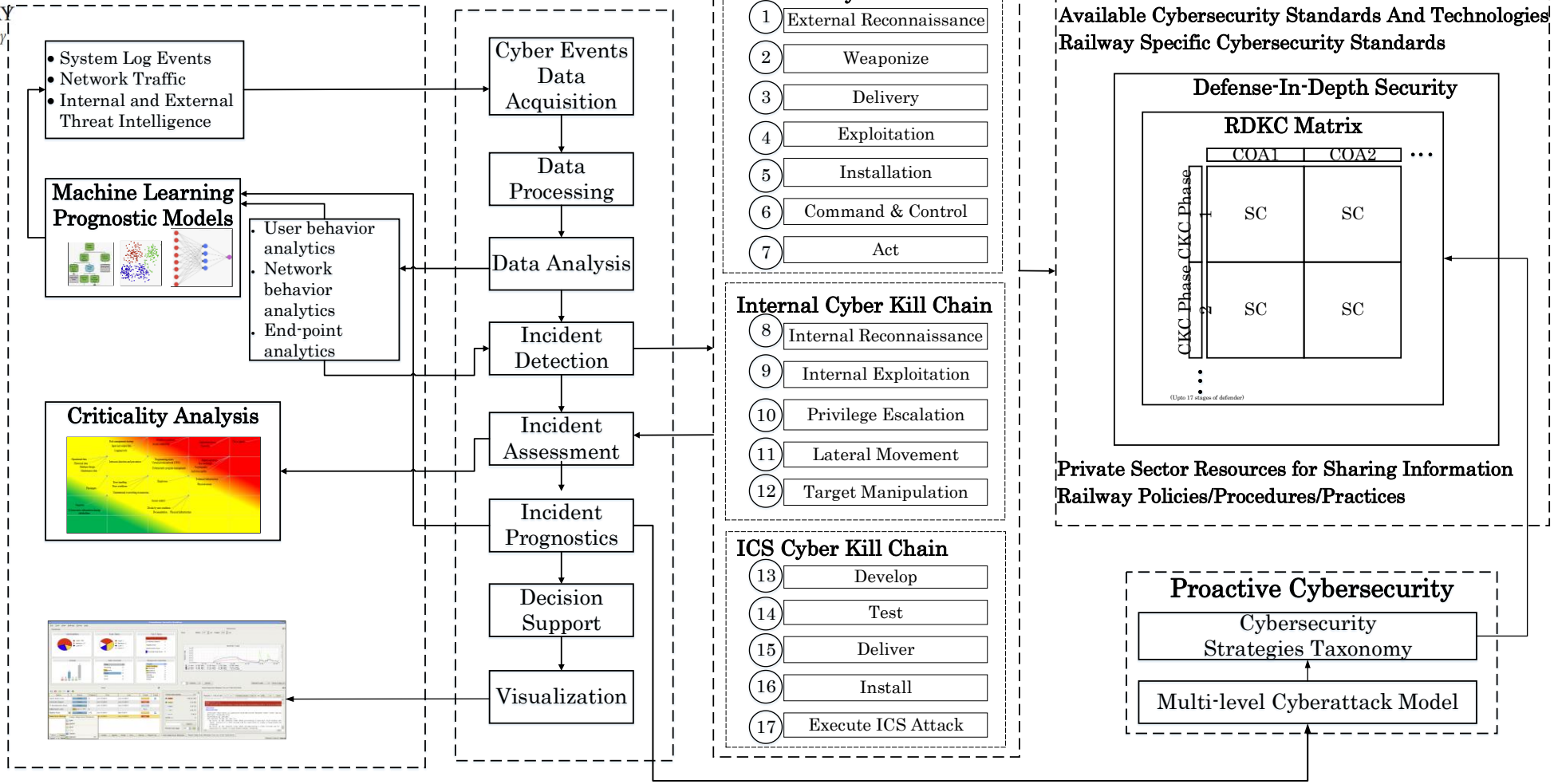
DOCTORAL THESIS

CYBERSECURITY IN RAILWAY
A Framework for Improvement of Digital Asset Security

Ravdeep Kour

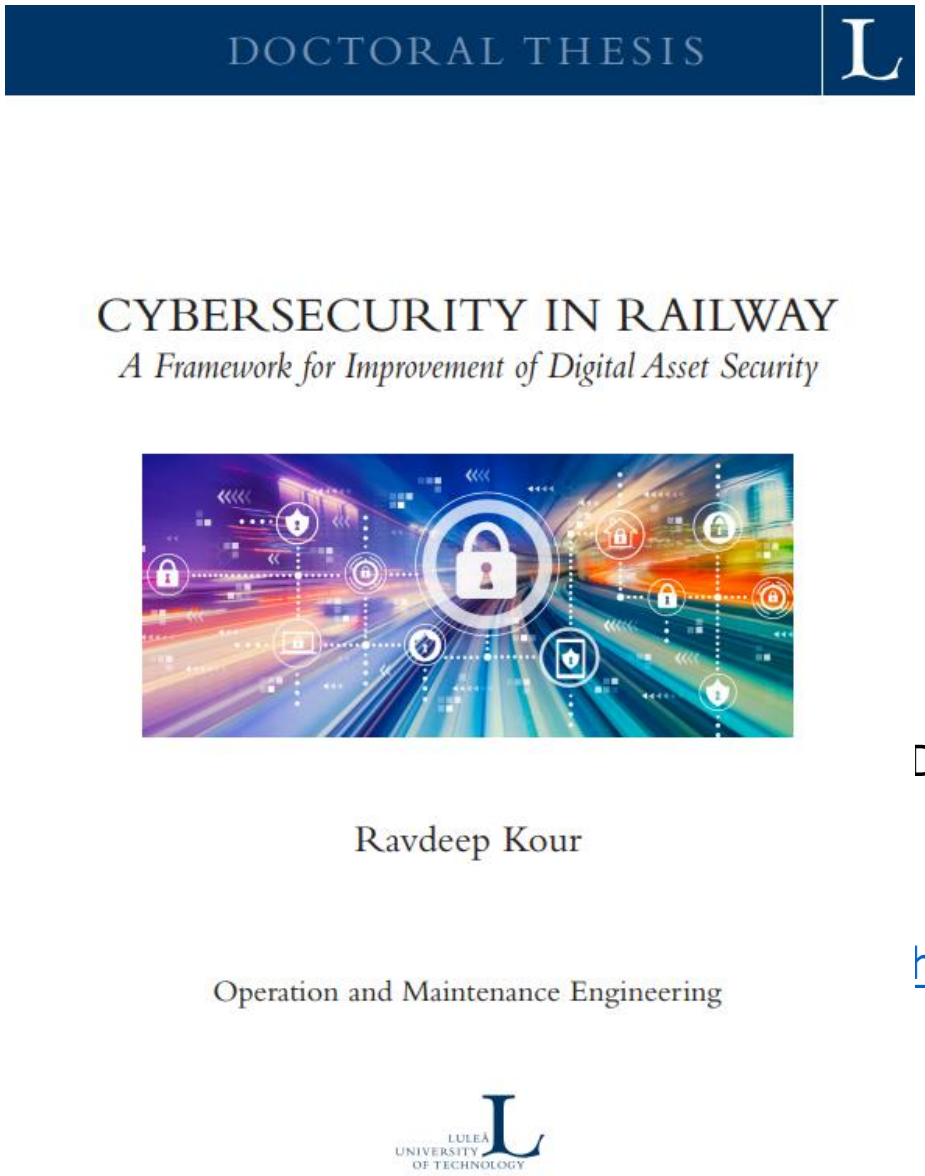
Operation and Maintenance Engineering

LULEÅ UNIVERSITY OF TECHNOLOGY



References

1. ISO/IEC 27032, 2012. ISO/IEC 27032: 2012–Information technology—Security techniques—Guidelines for cybersecurity.
2. IEC, 2015. International electrotechnical vocabulary—Part 192: Dependability. International standard IEC, , pp. 60050-60192.
3. Avizienis et al. (2004). Basic concepts and taxonomy of dependable and secure computing. IEEE transactions on dependable and secure computing, 1(1), 11-33.
4. Haque, M. A., Shetty, S., Gold, K., & Krishnappa, B. (2021). Realizing cyber-physical systems resilience frameworks and security practices. In Security in cyber-physical systems (pp. 1-37). Springer, Cham.
5. Wei, D., & Ji, K. (2010, August). Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights. In 2010 3rd international symposium on resilient control systems (pp. 15-22). IEEE.
6. Kour, R., 2020. Cybersecurity in Railway: A Framework for Improvement of Digital Asset Security, Luleå University of Technology. (PhD dissertation).
7. Heinrich M, Renkel D, Arul T, et al. Predicting Railway Signalling Commands Using Neural Networks for Anomaly Detection. In: *Computer Safety, Reliability, and Security*, 2020 Sep 15 (pp. 164-178). Springer, Cham.
8. Mikhailova U, Lukyanov G and Kalugina O. Intelligent and Secure Wireless Network Management of a Railway Transportation. In: *2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, 2020 Jun 12 (pp. 1-6). IEEE.
9. Fan Y, Tian K, Wang X, et al. Detecting Intrusions in Railway Signal Safety Data Networks with DBSCAN-ARIMA. In: *Frontiers in Cyber Security,* 2020 Nov 15 (pp. 254-270). Springer, Singapore.
10. Perales Gomez AL, Fernandez Maimo L, Huertas Celdran A, et al. On the Generation of Anomaly Detection Datasets in Industrial Control Systems. IEEE Access, 2019 Dec 6;7:177460-73.



Thank You!

Ravdeep Kour

ravdeep.kour@ltu.se

Division of Operation and Maintenance Engineering

Department of Civil, Environmental and Natural Resources Engineering

Luleå University of Technology

This doctoral thesis can be downloaded at the following link:

https://www.diva-portal.org/smash/get/diva2:1423651/FULLTEXT01.pdf