Railway Defender Kill Chain to Predict and Detect Cyber-Attacks

Ravdeep Kour*, Adithya Thaduri and Ramin Karim

Division of Operation and Maintenance Engineering, Luleå University of Technology 97187 Luleå, Sweden
E-mail: ravdeep.kour@ltu.se, adithya.thaduri@ltu.se, ramin.karim@ltu.se
**Corresponding Author*

Received 04 August 2019; Accepted 26 November 2019;
Publication 14 December 2019

Abstract

Most organizations focus on intrusion prevention technologies, with less emphasis on prediction and detection. This research looks at prediction and detection in the railway industry. It uses an extended cyber kill chain (CKC) model and an industrial control system (ICS) cyber kill chain for detection and proposes predictive technologies that will help railway organizations predict and recover from cyber-attacks. The extended CKC model consists of both internal and external cyber kill chain; breaking the chain at an early stage will help the defender stop the adversary's malicious actions. This research incorporates an OSA (open system architecture) for railways with the railway cybersecurity OSA-CBM (open system architecture for condition-based maintenance) architecture. The railway cybersecurity OSA-CBM architecture consists of eight layers; cybersecurity information moves from the initial level of data acquisition to data processing, data analysis, incident detection, incident assessment, incident prognostics, decision support, and visualization.

The main objective of the research is to predict, prevent, detect, and respond to cyber-attacks early in the CKC by using defensive controls called the Railway Defender Kill Chain (RDKC).

The contributions of the research are as follows. First, it adapts and modifies the railway cybersecurity OSA-CBM architecture for railways. Second,

Journal of Cyber Security and Mobility, Vol. 9_1, 47–90.
doi: 10.13052/jcsm2245-1439.912

it adapts the cyber kill chain model for the railway. Third, it introduces the Railway Defender Kill Chain. Fourth, it presents examples of cyber-attack scenarios in the railway system.

Keywords: Cybersecurity, cyber kill chain, railway, cyber-attack, OSA-CBM, predict.

1 Introduction

The railway is a complex system which consists of railway infrastructure and rolling stock. Railway infrastructure is divided into technical subsystems, including, signalling system, track, electrical system, and telecommunication system [1]. Rolling stock consists of both powered and unpowered vehicles that move on the rail track. Supervisory Control and Data Acquisition System (SCADA) is an operational technology (OT) that provides centralized monitoring and control of the railway system. It is designed to collect field information (such as the status of the trains, signal systems, traction electrification systems, and ticket vending machines), transfer it to operator consoles at an HMI (Human Machine Interface) station at the rail control center [2]. The received information is displayed graphically or textually, thereby allowing the operator to monitor or control the railway system from a central location in near real time. The SCADA system also sends high-level operator commands to the rail section components based on condition monitoring (e.g., stopping a train to prevent it from entering an area that has been determined to be flooded or occupied by another train) [2]. Figure 1 shows subsystems of a railway system.

The convergence of the railway system with Information Technology (IT) and Operational Technology (OT) has brought significant benefits in reliability, maintainability, operational efficiency, capacity and passenger experience, as the use of Internet-connected sensors and devices can provide

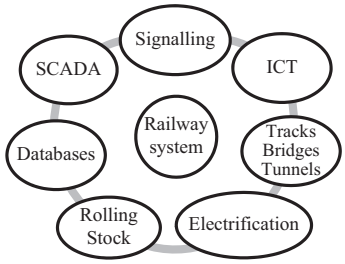

Figure 1 The Railway system.

timely and accurate information about the physical world. The railway is adapting Information and Communication Technology (ICT) to take advantage of cloud technology to integrate, analyze and visualize data for effective decision-making [3]. European Union and Shift2Rail [4] programs have proposed to include ICT in transportation because they expect potential benefits. Railway maintenance data can be collected and integrated within the cloud computing infrastructures to facilitate condition-based maintenance (CBM), a strategy that predicts future failures based on the condition of an asset; in CBM, maintenance actions are performed on the defective elements only [5]. However, these innovative developments are not without risks. Transfer of data from the field to the cloud causes some concern, as adversaries can attack network, servers and communication channels. Subramanian and Jeyaraj [6] have explored various security challenges faced by cloud service providers, data owners, and cloud users.

NATO (North Atlantic Treaty Organization) ranks phishing and malware cyber-attacks among its greatest concerns [7]. According to Patel [8], one of the top cyber threats is phishing scams. Other threats are: ransomware attacks (like WannaCry), system vulnerability due to unchecked gaps (nearly 50% of alerts and logs are never investigated), new threats and dangers from and to AI (Artificial Intelligence) powered systems, and human weaknesses [9–12]. In 2018, HelpSystems [13] surveyed more than 600 IT and cybersecurity professionals to determine the main cybersecurity risks and mitigation strategies. It found the top five cyber-threats were ransomware, phishing, weak/stolen credentials, system misconfigurations, and unsecure file transfers [13]. Hackmageddon [14] lists malware, account hijacking, unknown attacks, targeted attacks and vulnerability as threats and says such attacks are growing. Worldwide statistics show the dominant type of cyber-attack is a malware attack, including in the railway [15]. 'Unknown' cyber-attacks, which means the reason for an attack is unknown, are increasing as well. These unknown attacks are even more dangerous because we do not know the motives for them. Targeted attacks are also increasing day-by-day. According to Symantec [16], Formjacking was a breakthrough threat in 2018; it uses malicious code to steal credit card details and other information from a payment form submission. As the railway is being digitalized, all these types of attack can occur. The railway requires a cyber-resilient system to counteract malware and advanced persistent threats (APT) to continue in the case of an attack. NIST says an APT is:

"An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives

by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of filtrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat:

(i) pursues its objectives repeatedly over an extended period of time;
(ii) adapts to defenders' efforts to resist it; and
(iii) is determined to maintain the level of interaction needed to execute its objectives." [17]

Cyber kill chain (CKC) is one of the most widely used frameworks to detect cyber-attacks in IT network; it is based on the kill chain tactic of the US military's F2T2EA (find, fix, track, target, engage and assess) [18]. The extension of this kill chain concept has been proposed to gather threat intelligence by allowing the attacker to continue his activities even after he is detected [19]. The gathered threat intelligence can be used to detect future advanced persistent threats. Mrabet et al. [20] have identified four steps used by attackers to attack and get control of a smart grid: reconnaissance, scanning, exploitation, and maintain access. This IT CKC model has been expanded and improved for use in industrial control systems (ICS) called ICS Cyber Kill Chain to understand the attackers' activities and provide effective security measures [21]. Researchers are analyzing cyber-attacks by applying ICS cyber kill chain [21]; one example of such research is an analysis of a cyber-attack on the Ukrainian power grid [22]. The railway is converging IT and OT technologies, so similar types of cyber-attacks can happen here as well. Thus, as an initial step, instead of going into detail on different kill chains, this research applies Lockheed Martin's (LM) CKC model [18, 23], ICS cyber kill chain [21, 24] and extended cyber kill chain [25] model to the railway to detect cyber-attacks. Lockheed Martin's (LM) CKC model [18, 23] has a seven-stage attack path. It is very important to break this path or chain at any stage using defensive controls instead of focusing on defending the organization's perimeter alone. It is always beneficial to break the chain as early as possible. The disadvantage of LM's CKC (external cyber kill chain) is that it does not fully address insider threats. Therefore, this research adapts extended cyber kill chain [25] to be able to consider internal threats as well.

Hence, the main objective of this research is to predict, prevent, detect and respond to cyber-attacks early in the chain by using the proposed

Railway Defender Kill Chain (RDKC). RDKC uses cybersecurity controls, technologies, standards, and defenses to mitigate security risks that can be characterized in terms of threats that could cause harm to railway assets. Northcutt [26] defines security controls as "technical or administrative safeguards or countermeasures to avoid, counteract or minimize loss or unavailability due to threats acting on their matching vulnerability, i.e., security risk". Understanding each phase of the chain will help the analyst and incident responder identify proper courses of defensive action. The US Department of Defense [27] has identified six basic tactics: detect, deny, disrupt, degrade, deceive and destroy. Hutchins et al. [28] say these tactics can design a course of action (CoA) matrix to detect, deny, disrupt, degrade, deceive and destroy the effectiveness of the adversary events along the kill chain phases. This research uses a CoA matrix called RDKC matrix that considers DoD's [27] course of action, along with an additional course of action, i.e., predict, prevent, and response and recover, in addition to the CKC phases. These CoAs are used in RDKC matrix as defensive controls. As mentioned above, the scope of this research is that it does not go into the detail on the various kill chain models. Rather, it applies a combination of external cyber kill chain, extended cyber kill chain, and ICS cyber kill chain model to the railway as an initial step.

2 State of the Art of Currently Used Technologies in Railway

Many activities related to cybersecurity in the railway are ongoing, for example, the RAILway (CYRAIL) project, a Shift2Rail sub-project [4]. Thales [29] is supporting the Shift2Rail program of the European Commission by participating in the development of CERTs (computer emergency response teams). According to European Union (EU) Shift2Rail project report [30], the list of currently used security technologies in railway are divided into three parts: networks security, signalling security and deployment security. The detail of these security technologies is provided in the EU report [30] and the list is given below:

- Virtual private networks (VPN)
- Wavelength-division multiplexing (WDM)
- Cryptography (PE26)
- Firewall
- Demilitarized Zone (DMZ)

- Intrusion detection systems and intrusion prevention system
- Network segmentation
- Redundancy
- Internal and external intrusion tests
- Contingency plans for cyber attack
- Adoption of security standards
- Real-time functional monitoring system
- Double check of received commands by onboard units
- Network intrusion detection system/host intrusion detection system that checks the signalling traffic
- Intrusion tests
- Collaboration with national Community Emergency Response
- Software and hardware testing
- White box policy

Shift2Rail project report [30] also provided list of cybersecurity standards that should be considered and tailored with respect to the security requirements for railway system. In addition to these technologies and standards, some railway-specific cybersecurity standards, practices, and guidelines are also available [15]. Furthermore, some private sector resources for sharing cybersecurity information can be used by railways to enhance their cybersecurity capabilities. These resources can be NIST Computer Security [31], ICS cyber emergency response teams [32], US Computer Emergency Readiness Team (US-CERT) [33], Information Sharing and Analysis Organizations (ISAOs) [34], The Public Transportation Information Sharing and Analysis Center (PT-ISAC) [35], CIS®(Center for Internet Security, Inc.) [36], and Minimum Cyber Security Standard [37].

At the point of publication of this research, there is only one research article related to application of ICS cyber kill chain that consists of multiple-scenario ICS testbed for thermal power plant, rail transit, smart grid, and intelligent manufacturing with two typical attack scenarios [38]. Although modified versions of cyber kill chain model have been applied in other domains like multimedia service environments [39], Internet-of-Things (IoT) systems [40], security information and event management (SIEM) software [41], and cyber-physical system [42]. The proposed framework in this research is an attempt to integrate and collaborate all these existing technologies, standards, frameworks, models, and methodologies to detect and minimize the risks of cyber-attacks and to communicate cybersecurity information in the railway system. In addition to this, our proposed

framework will provide defensive controls at each stage of IT and OT/ICS cyber kill chains.

3 Conceptual Methodology and Framework

3.1 Unified Extended Cyber Kill Chain and ICS Cyber Kill Chain

Cyber kill chain (CKC) is one of the most widely used frameworks for the identification, prevention and detection of advanced persistent cyber threats [43–47]. Some of the researchers have proposed methodologies to detect cyber threats early in the stages of CKC [48, 49]. Cyber kill chain is focused on malware-based intrusion and APTs [50]. The CKC model has been expanded and improved for use in industrial control systems (ICS) and internal threats, i.e., the ICS cyber kill chain [21, 24] and extended cyber kill chain [25] respectively. A combination of both these kill chains can be applied in the railway (Figure 2).

3.1.1 External cyber kill chain model

An initial CKC model was developed by Lockheed Martin [18, 23] to attack the corporate network. The seven stages of this model are:

- Reconnaissance: The first stage of the model, one of the most difficult stages to detect from a security monitoring perspective, is the planning stage of the cyber-attack. The adversary searches for and gathers information about the organization background, resources, and individual employees through social sites, conferences, blogs, mailing lists and

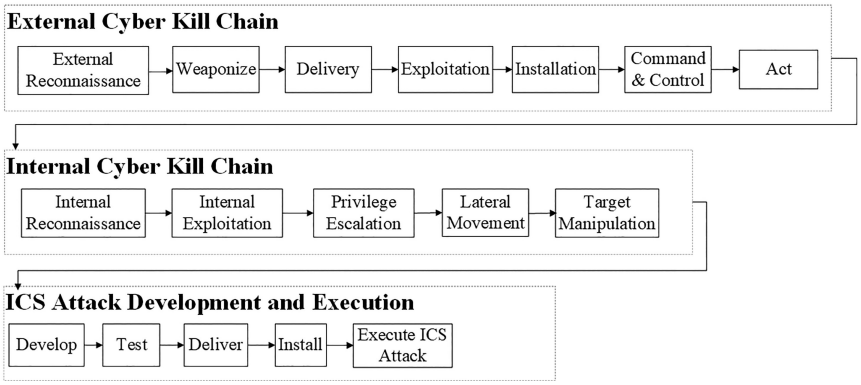

Figure 2 Unified extended cyber kill chain [25] and ICS cyber kill chain [21, 24].

other network tracing tools [51]. The collected information is useful in the later stages to deliver payload (the actual intended message that performs malicious action) to the target system.

- Weaponize: The second stage of the model is the operation preparation stage. This stage involves the coupling of a remote access Trojan (RAT) with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer) [28]. The detailed information related to RAT and an exploit are well explained by Yadav and Rao [52].
- Delivery: The third stage of the model is the operation launch stage when an organization can implement technology as a mitigating control [49]. At this stage, the weapon is transmitted to the targeted environment.
- Exploitation: At this stage, exploit is triggered to silently install/execute the delivered payload. The most frequent exploits are operating system, network and application/software level vulnerabilities [52]. One of the most popular viruses, WannaCry, uses the operating system exploit.
- Installation: This stage involves the installation of back door remote access Trojans (RATs) and the maintenance of persistence inside the targeted environment. The techniques used by malware authors to install a back door include anti-debugger and anti-emulation, anti-antivirus, rootkit and bootkit installation, targeted delivery and host-based encrypted data exfiltration [52].
- Command & Control (C2): After the successful installation of a back door, the adversary tries to open a two-way communication channel to enable the attacker to control the targeted environment remotely. Once the C2 channel is established, the adversary has "hands on the keyboard" access inside the targeted environment.
- Act on Objective: In the last stage of the model, the adversary achieves the desired attack goals. These goals can be a loss of confidentiality, integrity or availability of the assets. Velazquez [49] says an APT threat actor may live in an organization for years until detected.

According to Heckman [53], the pre-exploit steps offer opportunities for intrusion detection and mitigation, and the post-exploit steps offer opportunities to deploy incident response and forensics. Cyber forensics or computer forensics is defined as "the science of locating, extracting and analyzing types of data from difference devices, which specialists then interpret to serve as legal evidence" [54]. Incident response helps defenders detect and respond to breaches with minimal potential damage. The previous research has provided recommendations to railway organizations to improve event and incident

response domain that can further improve their capabilities to reduce the impacts of cyber-attacks and eradicate vulnerabilities [55].

3.1.2 Internal cyber kill chain

The internal cyber kill chain is part of an extended cyber kill chain [25]. It consists of almost the same steps as external kill chain but is preceded by the word internal [25]. Internal cyber kill chain follows a chain of steps to gain access to the ICS system, go from workstations to servers using privileged escalation, move laterally within the network, and then manipulate individual targeted machines [25] (Figure 2). Considerable work has already been done on ICS security [2, 56–58].

3.1.3 ICS cyber kill chain

After gaining knowledge from the corporate network (external cyber kill chain) and the ICS system (internal kill chain), the attacker starts developing a specific attack tool for the ICS system and validates it for reliable impact. After successful testing, the attacker delivers the tool, installs it, and executes the attack [21] (Figure 2).

3.2 Railway cybersecurity OSA-CBM overview

The proposed railway cybersecurity OSA-CBM (open system architecture for condition-based maintenance) framework delivers cybersecurity information from a technological point of view. This cybersecurity information flow is strongly related to the open system architecture for condition-based maintenance, developed in accordance with the functional specifications of ISO-13374 on the condition monitoring and diagnostics of machinery [59]. It is considered one of the most important standards of eMaintenance systems [60]. The railway sector also advocates Smart Maintenance Initiatives [61] and uses ICT in maintenance to develop artifacts (e.g. frameworks, tools, methodologies, and technologies) to support maintenance decision-making [62]. The adoption of ICT in railway maintenance makes it vulnerable to cyber threats. Thus, there is a need for standards or frameworks that can help minimize these threats.

The OSA-CBM standard can be modified and adapted for use in the railway to deliver cybersecurity information. The modified cybersecurity OSA-CBM architecture has eight layers: cyber events data acquisition, data processing, data analysis, incident detection, incident assessment, incident prognostics, decision support, and visualization. Table 1 shows

Table 1 A mapping between OSA-CBM based on ISO-13374 standard and cybersecurity information delivery system (modified cybersecurity OSA-CBM architecture)

OSA-CBM		Railway Cybersecurity OSA-CBM	
Layers	Description	Layers	Description
Data Acquisition	Provides the CBM system with digitized sensor or transducer data.	Data Acquisition	Provide the railway system with cyber events occurrence data that can be acquired from internal and external threat intelligence, network traffic and from the history of cyber event logs.
Data Manipulation	This step corresponds to the data preparation stage in a normal data mining process. Techniques such as data cleansing, feature selection, feature extraction, and standardization can be applied to process the raw data for analysis.	Data Processing	This layer involves all the activities to build a final dataset from the first raw data. For example, each IP address is stored in the dotted-quad notation or each IP address has been geo-located into the latitude and longitude pair, but they are in a single field separated by a comma.
		Data Analysis	This layer involves the analysis of data like user behavior analytics, network behavior analytics, and end-point analytics by using machine-learning algorithms. The predicted results are feedback to the data sources and used during the detection phase of the architecture.
State Detection	This step focuses on comparing data with expected values or control limits; an alert is triggered if these limits are exceeded.	Incident Detection	This layer involves the application of RDKC for the detection of cyber incidents within the railway system.

Table 1 Continued

OSA-CBM		Railway Cybersecurity OSA-CBM	
Layers	Description	Layers	Description
Health Assessment	The focus of this step is to prescribe if the health in the monitored system has degraded. This should be able to generate diagnostic records and propose fault possibilities.	Incident Assessment	This layer is a proactive approach with a focus on prevent and prepare. This step performs a qualitative assessment of cybersecurity incidents with cause-effect analysis and lessons-learned activities and focuses on determining the level or severity of the cyber events. It should also consider the trends of event history along with its operational context. Thus, it will help to predict early indicators to statistically predict potential future cyber-threats.
Prognostics	The focus of this step is to calculate the future health of an asset and report the remaining useful life (RUL) of that asset.	Incident Prognostics	This layer involves the use of machine learning prognostic models to analyze or monitor future cyber incidents on the system and estimate the remaining secure life of the system based on cyber-attacks on the system.
Advisory Generation	Its focus is to generate recommended actions and alternatives based on the predictions of the future states of the asset.	Decision Support	This layer involves recommendations and remedial actions based on the predictions of the future states of the system. These actions may include the immediate shutdown of the system, using back-ups or use of antivirus, etc. Examples of some of available decision support systems in cybersecurity domain are Nexpose, Nessus Home, Security System Analyzer 2.0 Beta, Open Vas, Saint8, Nmap, eEye Retina, QualysGuard, and nCircle IP360.
Presentation	This step provides an interactive human-machine interface (HMI) to visualize pertinent data, information and results obtained in previous steps.	Visualization	This layer involves an interactive human-machine interface (HMI) that facilitates visualization of analyzed cybersecurity information by qualified personnel.

mapping between OSA-CBM based on ISO-13374 standard and the cybersecurity information delivery system (modified cybersecurity OSA-CBM architecture).

Figure 3 shows the proposed cybersecurity information delivery framework to identify, predict, prevent and detect cyber threats and communicate them to internal and external railway organizations.

This research integrates existing technologies, standards, frameworks, models, and methodologies to minimize the risks of cyber-attacks in the railway system. To capture the dynamically changing trend of cyber events, vast amounts of data can be collected via network traffic, threat intelligence and historical cyber event logs using various data sources and technologies as shown in Figure 3. The extended cyber kill chain and ICS cyber kill chain can be applied to detect the cyber incidents, along with various data analysis techniques (e.g., machine learning, data mining, etc.), to assess and predict cyber incidents within the railway system, thereby facilitating the decision support system.

There is a feedback loop after cyber incidents are detected; countermeasures can be reconsidered to minimize similar types of future cyber-attacks. As we move towards the 2020s, cyber-attacks are rapidly adopting new techniques and strategies to circumvent new security measures and evade detection. There is a need to shift towards a type of resilience that has the ability to recover quickly from adversities, including advanced security solutions like automated anomaly detection, cloud-based back-ups, disaster recovery services, security-by-design, and self-healing.

This research uses railway as a case study and proposes a cybersecurity framework adapted and modified from the OSA-CBM framework. It also proposes a railway defender kill chain (RDKC) that offers defensive controls at each stage of LM's cyber kill chain, an extended cyber kill chain, and an ICS cyber kill chain. RDKC involves defense-in-depth security, cybersecurity standards and resources and an RDKC matrix. The RDKC matrix is explained in the results section.

3.3 Defense-in-Depth Security

Defense-in-depth (DiD) is a cybersecurity approach with multi-layered defensive mechanisms to protect valuable railway data and information. Its layered security is like the Swiss cheese model [63] used in risk analysis and risk management. Railway organizations need to develop more complete and complex proactive defensive mechanisms. The benefit of using this

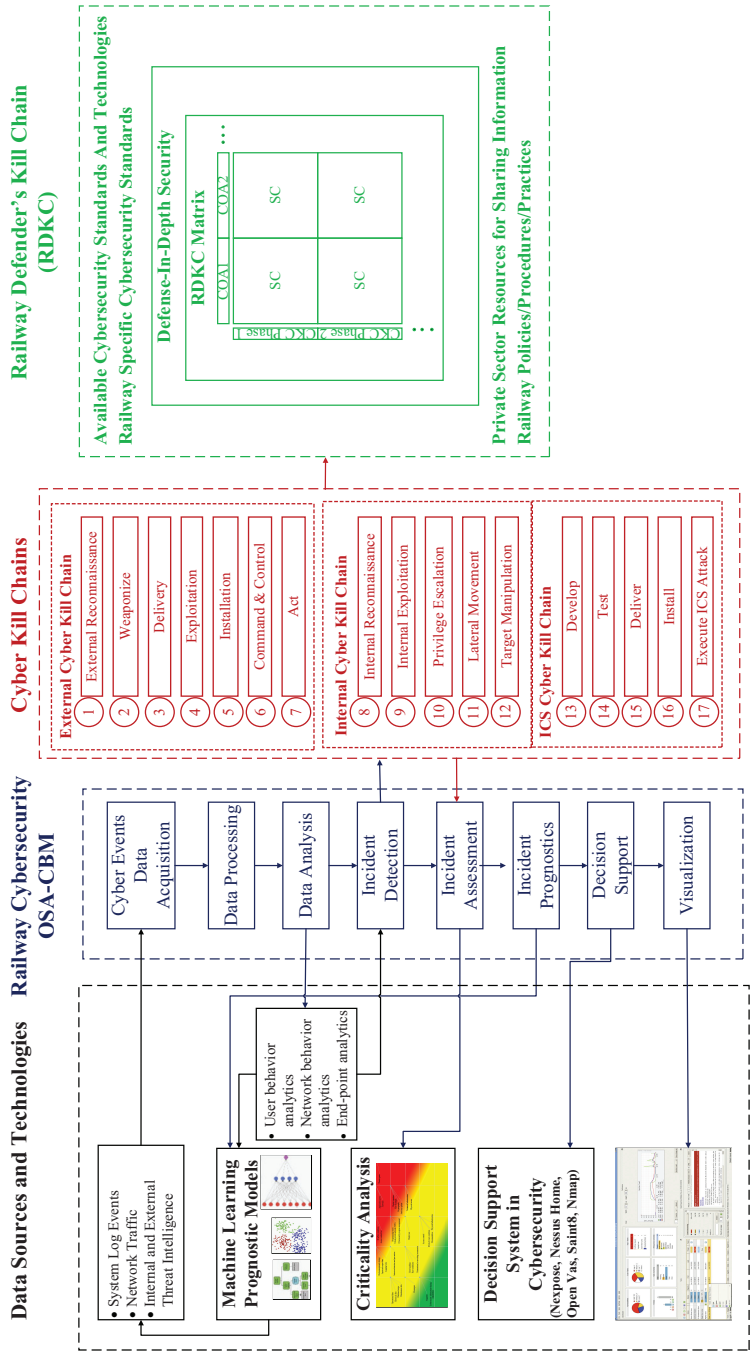

Figure 3 Cybersecurity information delivery framework to predict, prevent and detect cyber incidents in railway, adapted and modified from OSA-CBM framework (Holmberg [60]).

type of multi-layered approach is that if one defensive mechanism fails, another starts immediately. The purpose of the defense-in-depth approach is to defend a system against any particular attack using several independent methods. Different researchers define the layers differently. For example, Starrett [64] deploys a triple-layered defense to control access, infrastructure and data. NSA layers [65] are people, technology and operations, whereas IndustryWeek layers [66] are device, application, computer, network and physical layer. These multi-layered defensive mechanisms do not provide perfect security but can strengthen and complicate the cybersecurity level.

4 Results and Discussion

This section explains how the Railway Defender Kill Chain (RDKC) matrix provides security controls at each stage of CKC using various course of actions.

4.1 Railway Defender Kill Chain (RDKC) Matrix

The convergence of IT and OT technology in the railway has brought significant benefits but at the same time has made it vulnerable to cyber threats. This vulnerability also depends upon the maturity of the integration of IT with OT; e.g., ERTMS (European Rail Traffic Management System) level 3, which is fully digital, is more vulnerable to cyber threats. The operational goals of IT security are confidentiality, integrity, and availability (CIA) and the operational goals of OT security are safety, reliability, and availability (SRA) [67]. OT security generally deals with industrial control systems (ICS) like SCADA systems. The rationale of this research is to introduce a railway defender kill chain that will consider security controls related to both IT and OT technologies. RDKC involves defense-in-depth security, cybersecurity standards and resources, and an RDKC matrix. RDKC matrix describes the logic of a defender to stop the attack by breaking cyber kill chain at any point by implementing appropriate IT/OT security controls from Table 2. Thus, Table 2 show security controls at each stage of the CKC; these defensive controls along with course of actions will help railway organizations predict, prevent, detect and respond to cyber-attacks. The main objective of the defender is to stop or minimize the risk of cyber-attack at the initial stage of the CKC by applying security controls from the RDKC matrix. Cells in the matrix can be viewed as characterizing the types of effect a given defensive control could have on a CKC phase. The Reconnaissance – Detect cell, for instance, is at the intersection of the detect tactic and the

Table 2 RDKC Matrix (modified from Hutchins et al. [28], Tarnowski [69], and Malone [70])

CoA CKC Steps	Predict	Prevent	Detect	Response and Recovery	Deny	Disrupt	Degrade	Deceive	Destroy
External cyber kill chain									
External Reconnaissance	• User behavior analytics • Network behavior analytics • End-point analytics • DPI	• NIPS • Denial of port scanning • Firewall ACL • Cybersecurity education and awareness of railway workforce including IT and OT security personnel • Sensitive and confidential data securely disposed of • Security by design	• NIDS • HoneyPot • Web analytics • Threat Intelligence • Video surveillance • SIEM • Scan the railway network internally and externally by using vulnerability-scanning tools • Penetration testing		• Firewall ACL • Physical locks on critical server rooms • System and service hardening • Network obfuscating • Logical segmentation	• HoneyNet	• Timeout	• HoneyPot	

(*Continued*)

Table 2 Continued

CoA CKC Steps	Predict	Prevent	Detect	Response and Recovery	Deny	Disrupt	Degrade	Deceive	Destroy
Weaponize		• Shared threat information • Penetration testing • Application obfuscation • System and application patching • Version hidden • NIPS	• NIDS • Threats information sharing • Vulnerability intelligence • Honeypots • Identify weaponiza-tion attributes to prevent attacks reaching later stages		NIPS	• Hardening • Version obfuscating	• Application obfuscation • Disabling unused services	Fake weaponize codes to attract adversaries	

Delivery	Block known sources of attacks and compromise (indicators of attacks (IoA) and Indicators of compromise (IoC))	• NIPS • Firewall • Port Knocking • ACL • RBAC to limit who has access to the SCADA or ETCS • Two-person rule that initiates remote maintenance command • Change fabric settings • Network traffic disabled • Update secure sockets layer (SSL) encryption protocols • Prohibit the use of USBs on railway critical systems • Isolate networks serving critical functionality, such as control systems, from the Internet	• NIDS • Firewall • Network analysis • Vigilant users • Context-aware • Endpoint Malware Protection • Blocked attempts alert • Detect anomalous commands not stemming from the normal Remote Control Center • DPI to detect traffic and extract useful metadata such as MAC addresses	• Proxy Filter • Anti-virus • Web browsers and plug-ins must be up-to-date	• Hardening • In-line Anti-virus	• Mandatory Integrity • Email Queuing	• HoneyPot

(*Continued*)

Table 2 Continued

CoA CKC Steps	Predict	Prevent	Detect	Response and Recovery	Deny	Disrupt	Degrade	Deceive	Destroy
Exploitation	Correlate flows and block malicious behavior of devices	• User awareness training • Secure coding training for web developers • Local sandbox • System and application updates • Security toolkits • Turn operating System update ON	• HIDS • Endpoint Malware Protection • Proactive penetration testing for application and operating system vulnerabilities	• Cyber policies/procedures • Cyber laws • Isolation of infected devices • Data loss prevention (DLP) technology • Continuity of Operations Plan • Disaster Recovery Operations Plan • Forensic	• Patch and update the system • Use dedicated anti ransomware utility/blocker	• Hardening • DEP	• Configuration auto-rollback • TARPIT • Remove remote administration capabilities from web platforms	HoneyPot	

Installation	Automatically isolate infected devices to prevent horizontal spread	• Cybersecurity education and awareness • HIPS • Application Whitelisting	• Cybersecurity education and awareness • Generate alarms for unauthorized access to railway critical systems • HIDS • Modification and change alerts/alarms • IP Sonar • Check message integrity (digital signatures) of commands and data received by the network components • Configuration check • Access logs • EDR	• Chroot jail • Multi-factor authentication to gain access to sensitive railway information • Secure password • Authenticate users so that physical access to the railway asset(s) does not automatically grant logical access • Append authentication data (message authentication code (MAC) or digital signature) to the balises • Remove hardcoded credentials on railway CMMS • Require approved cryptographic algorithms for authentication and message integrity on the railway signalling network	• Hardening • Antivirus	• Configuration auto-rollback • TARPIT	• HoneyPot • DNS redirect	EDR

(*Continued*)

Table 2 Continued

CoA CKC Steps	Predict	Prevent	Detect	Response and Recovery	Deny	Disrupt	Degrade	Deceive	Destroy
Command & Control (C2)	• Correlate network traffic against known IoCs • Automatically isolate infected devices	• Whitelisting firewall • IPS	• NIDS • SIEM • Threat intelligence feed • Internal reconnaissance		Firewall ACL	NIPS	Tarpit	• DNS redirect • Honeypots to redirect suspicious network traffic to local traps	EDR
Act on Objective	• Assess damage by analyzing network traffic before and after the infection	• Data loss prevention (DLP) technology • Configure email systems and web proxies to prevent sensitive and confidential railway data from being sent • Block access to sites that facilitate data transfer • Turn off copy/paste over remote desktop connections • Data-at-rest encryption schemes	• Log analysis • Implement internal IDS, IPS and other controls within the railway network to detect and mitigate unauthorized lateral movement		Outbound ACL		Quality of Service throttle	HoneyPot	

		Internal cyber kill chain		
Internal reconnaissance	Use an IPS to check for any active scan alerts	Use host-based intrusion detection system engine for alerting		
Internal exploitation	Patch & vulnerability management	Endpoint protection		
Enterprise privilege escalation	Set alerts for addition or deletion to admin user group	Behavioral analytics		
Lateral movement	Segmented security zones at all layers	• Vulnerability scanning • Behavioral analysis of successful login events		Decoy servers
Target manipulation		• Host level log analysis		
		ICS cyber kill chain		
ICS attack development and testing	• Restrict access to documentation and specifications • Harden/obfuscate applications to make reversing difficult	• Access patterns • Working offline		
Deliver	HIPS	HIDS	Data diode	
Install	Application signing	• File integrity Monitoring • Redundant processing systems	Data diode	

(*Continued*)

Table 2 Continued

CoA CKC Steps	Predict	Prevent	Detect	Response and Recovery	Deny	Disrupt	Degrade	Deceive	Destroy
Execute				• Forensics • Breach insurance					

Explanations of the Table 2:
ACL: Access control list is used to filter incoming and outgoing traffic in the networks by a router.
DEP: Data execution prevention monitors and sends a notification if someone tries to execute malicious code in "non-executable" memory locations.
EDR: Endpoint detection and response is an emerging technology that detects malicious activities by continuously monitoring endpoint and network events and responding to advanced threats.
Hardening: Securing system by reducing its surface of vulnerability.
HIDS: Host-based intrusion detection system examines specific host-based actions, like malicious attempts to rewrite a file.
HIPS: Host-based intrusion prevention system evaluates packets before they are allowed to enter a computer.
HoneyNe**t:** A network set up with intentional vulnerabilities, containing one or more honey pots (mechanism set to detect, deflect or in some manner counteract attempts at unauthorized use of information systems).
RBAC: Role-Based Access Control is a method of restricting system access to unauthorized users.
Port Knocking: A method of externally opening ports by generating a connection attempt on a set of pre-specified closed ports.
DPI: Deep Packet Inspection is a real-time filtering technique.
IDS: Intrusion detection system provides preventive security against any suspicious activity through early warnings.
IPS: Intrusion prevention system is designed to inspect attack data and take the corresponding action, like blocking data.
NIDS: Network-based intrusion detection system analyzes network traffic for suspicious behavior.
NIPS: Network-based intrusion prevention system evaluates traffic before it is allowed into a network or subnet.
Obfuscating: A deliberate act of making something difficult to understand.
Outbound ACL: ACL is placed in the exit interface and filters the traffic after the router makes a forward decision.
Sandbox: Tests unverified programs that may contain viruses or malicious codes.
ETCS: European Train Control System is an automatic train protection system (ATP) to replace the existing national ATP-systems.
ERTMS: European Rail Traffic Management System is standardized communication and signalling system.
CMMS: It is computerized maintenance management system
Data diode: It is a hardware that allows information flow in one direction only.
Decoy server: It is configured to act as a legitimate server.

reconnaissance phase of CKC; this means that to detect cyber incidents at the reconnaissance phase, we must employ the defensive controls noted in the Reconnaissance – Detect cell. Technologies like Chroot Jail, DEP, Firewall ACL, HIDS, Honeypot, In-line AV, NIDS, NIPS and Tarpit are defined in more detail in a white paper by Force CI [68]. One of the advantages of RDKC matrix is that it provides maximum defensive controls at one place to follow quickly.

4.2 Case Study of CDOT Network Breach

To illustrate how a cyber-attack follows the extended cyber kill chain [25], this research uses the case study of ransomware infection in the computers of the Colorado Department of Transportation (CDOT). In March 2018, 2,000 CDOT computers were shut down because of a ransomware infection, SamSam [71, 72]. Unlike many ransomware attacks, SamSam is not distributed in spam emails. Instead, the attacker tries to avoid user interaction and takes a more direct route to infection. In the CDOT ransomware infection, the attacker identified open port 3389, exposing the remote desktop protocol (RDP), and gained access to the company's internal networks by brute-forcing the RDP connections (Figure 4). The impacted employee computers were running Windows and using McAfee security software. The attacker then tried to gain access to as many end-points on the same network as possible, manually running the SamSam ransomware to encrypt the files. In

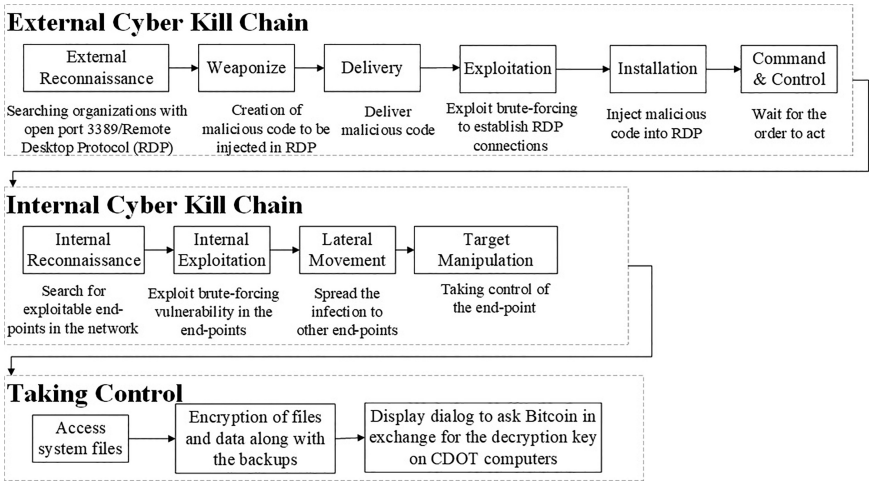

Figure 4 Cyber kill chain steps for SamSam virus using extended cyber kill chain [25].

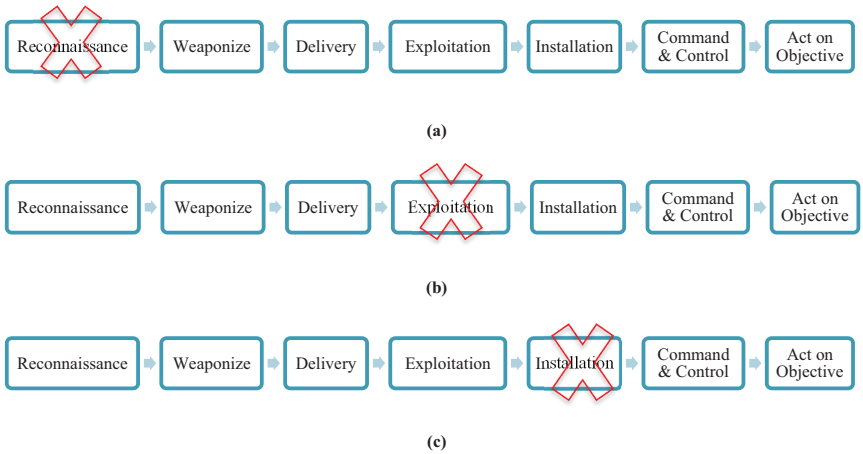

Figure 5 Attack detection and prevention area and external chain break.

the last stage, the attacker demanded Bitcoin in exchange for the decryption key to unlock the system, but CDOT did not pay. As the railway is adopting advanced ICT technologies, it is becoming more vulnerable to cyber-attacks, making it essential to move towards security analytics and automation to predict, prevent, and detect security breaches and to quickly identify and respond to security events.

Figure 5(a–b) shows the attack detection area and chain break if the defender had approached security proactively. As noted above, the SamSam cyber-attack gained access by brute-forcing RDP connections, but cyber defenders could have proactively used the following security measures:

(a) A brute-force attack is very noisy and can be picked up by anomaly detection, behavior analytics, and monitoring systems at the reconnaissance stage of cyber kill chain. Security controls from the reconnaissance-predict cell of the RDKC matrix can notice this attack, and the chain can be broken at the reconnaissance stage (Figure 5(a)).
(b) This attack can be stopped before the exploitation stage by patching the system and using security control from the exploitation-deny cell of the RDKC matrix (Figure 5(b)).
(c) The attack can also be stopped before the installation stage by two-factor authentication on externally facing applications and using security controls from the installation-deny cell of the RDKC matrix (Figure 5(c)).

Thus, to minimize the risk of an attack by malware or ransomware infection, railway workforce must keep software updated, avoid phishing emails and maintain strong passwords.

4.3 Cyber-Attack Scenarios in Railway Operation and Maintenance

With the advanced ICT technologies and tools (e.g., Internet of Things, Cloudification, Big Data Analytics, and Artificial Intelligence, etc) being used in railway operation and maintenance, railway data are collected continuously and sent to the cloud for data analysis and visualization. The security of these data is very important because they will help build data-driven models for operation and maintenance. In addition, the convergence of IT and OT technology in the railway promises significant benefits in reliability, maintainability, operational efficiency, capacity, and passenger experience. But with this convergence, OT technology has the same risk exposures as those of IT practitioners. Thus, there is a need for the security of both IT and OT infrastructures. The following are a few examples of the vulnerabilities:

The signalling system carries critical information and turns it fully digital; it is centrally controlled, making it vulnerable to cyber threats. The system's ICT devices and components are generally interdependent, and any weakness in one linked element in the system (e.g., security gaps left open by system vulnerabilities, vulnerabilities in software or operating systems, or inappropriate security-related decisions by railway staff) can jeopardize the security and dependability of the whole system.

Railway electrification depends on the electric grid infrastructure for the power supply. Any disturbance in the power grid propagates to the whole railway system, causing an immediate stoppage of several trains.

The SCADA system provides centralized monitoring and control of the railway system. This system sends high-level operator commands to the rail section components based on condition monitoring. Any type of cyber-attack on this system will shut down train services and in extreme cases will cause accidents.

Table 3 lists some examples of cyber-attack scenarios in railway operation and maintenance along with their vulnerabilities, risks, and defensive controls.

Table 3 Examples of cyber-attacks scenarios in railway operation and maintenance and defensive controls from RDKC matrix

Cyber-attack	Description	Vulnerabilities	Risks/Consequences	Defensive Controls	RDKC Matrix Cell
Malicious attacks on railway network and infrastructure like: – Signalling – Rolling stock – Power supply – Databases – ICT	A threat agent acting as a maintenance engineer requests physical and logical access to the railway enterprise network using malware. The threat agent installs remote accessible malware allowing remote maintenance command and control of the network accessible from any available Internet connection. Further, physical access can be achieved via poor locks, unlocked doors, stolen credentials or social engineering.	• Weak identity and access control management (physical and logical) • Poor controls on software installation and integrity • Inadequately protected Internet access to the railway enterprise network or ETCS system implementation	• Potential remote command and control capability by a threat agent • Depending on the system's architecture and permissions, degraded railway performance	Require video surveillance (using deep learning) to document who enters the server room	Reconnaissance-Detect
				Use RBAC to limit who has access to the railway enterprise network or ETCS system	Delivery-Prevent
				Generate alerts of who has made software additions or modifications	Installation-Detect
				Check software execution integrity, since software may be compromised when loaded for execution	Installation-Detect

			Authenticate users so that physical access to the system(s) does not automatically grant logical access	Installation-Deny
			Require multi-factor authentication to gain access to sensitive systems	Installation-Deny
			Restrict configuration access to limit who has access and can make configuration changes	Installation-Detect
			Create audit logs of who has made software additions or modifications	Act on Objective-Detect
A threat agent gets access to IT or communications infrastructure via unauthorized access to destroy, disclose or modify railway data or disrupt railway services.	• Lack of access control • Insecure communication protocol that allows unauthenticated changes to sensitive data	• Physical damage to IT or communications infrastructure • Loss of data confidentiality, integrity and availability • Unavailability of railway services • Reputational damage to railway organization • In worse case, train accident due to sending wrong signal	Detect anomalous patterns in the network	Reconnaissance-detect Delivery-Detect
			Require multi-factor authentication	Installation-Deny
			Use RBAC for administrative access, emergency access and shared accounts	Delivery-Prevent
			Monitor anomalous access attempts as indicators of cybersecurity events	Delivery-Detect
			Check message integrity (digital signatures) of commands and data received by the network components	Installation-Detect

(*Continued*)

Table 3 Continued

Cyber-attack	Description	Vulnerabilities	Risks/Consequences	Defensive Controls	RDKC Matrix Cell
	Balises provide no authentication guarantee; therefore, there is a possibility of malicious attack via balise interface (by subverting existing balises or placing a new balise on the track)	Open and accessible public railway infrastructure	• Failure to encounter a linked balise in the expected location will cause the train to halt • Excessive commands from unlinked balises can create hazardous situations	Append authentication data (message authentication code (MAC) or digital signature) to the balises	Installation-Deny
Credential theft attacks on railway assets like: – Databases – ICT	A threat agent acquires railway computerized maintenance management system (CMMS) authentication credentials to visualize railway assets remotely	• Hardcoded passwords • Shared passwords and credentials	• Authenticity of railway CMMS credentials is compromised • Unexpected and perhaps intermittent maintenance service loss • Credibility loss • Revenue loss	Require multi-factor authentication for privileged functionality	Installation-Deny
				Verify absence of hardcoded credentials on railway CMMS	Installation-Deny

"Man-in-the-middle" attacks on railway assets like: – Signalling – Rolling stock – Databases – ICT	EuroRadio protocol uses weak encryption algorithm to encrypt the messages	Possibility of exploiting cryptographic weaknesses in EuroRadio	Weak cryptography exposes GSM-R communication messages on the Internet	Use deep packet inspection (DPI) to detect traffic and extract useful metadata, such as MAC addresses	Delivery-Detect
				Update the SSL encryption protocols (like AES)	Delivery-Prevent
Vulnerability/ ransomware attacks on railway assets like: – ICT – Databases	A threat agent is able to gain access to the railway system by exploiting a known vulnerability that has not yet been patched. The threat agent is unable to access the railway applications but can access other railway devices. The recent WannaCry and Petya ransomware strains exploited a vulnerability in unpatched systems	• Improper or no change/configuration management for the timely deployment of patches and security updates • Unpatched firewall and operating system	• Network shut down • Customer service unavailable • Troubleshooting costs	Scan the railway network internally and externally by using vulnerability-scanning tools	Reconnaissance-Detect
				Implement configuration management including a severity rating (critical, important, moderate, low) and timeframes for patching vulnerabilities based on severity	Exploitation-Deny Exploitation-Degrade

(*Continued*)

Table 3 Continued

Cyber-attack	Description	Vulnerabilities	Risks/Consequences	Defensive Controls	RDKC Matrix Cell
				Monitor access logs on critical systems and servers	Installation-Detect
				Generate alarms for unauthorized access to railway critical systems	Installation-Detect
				Update patches	Exploitation-Deny
Denial of service (DOS) attacks on railway assets like: – Signalling – ICT – Databases – Rolling stock	Cyber-attack on ERTMS/ETCS and railway enterprise network could bring down the ERTMS/ETCS system and railway Web services respectively	• Data-driven property of ERTMS/ETCS • Open communication channel, i.e. "through the air," using radio frequencies which are open and accessible in public railway infrastructure	• Delay or loss of GSM-R communication messages • Stoppage or delay of trains • Passenger discomfort • Disruption of Web services for reservations or updates on delays • Road traffic maps affected	Update SSL encryption protocols	Delivery-Prevent
				Detect anomalous behaviour continuously	Delivery-Detect
				Detect malicious activities by continuous monitoring endpoint and network events using EDR technology	Installation-Detect
				Use Web application firewall	Delivery-Detect

Malicious attack on railway ICS system like: – SCADA	A threat agent breaches a railway SCADA system and causes the SCADA system to issue an unregistered or malicious commands. Since railway systems may react differently to invalid commands, the railway system experiences immediate service shut down	Inadequate authentication and access control mechanisms	• Denial of service attacks • Devices are remotely shut down, affecting train service • Reconfigured instructions, data or code leading to more destructive and costly attacks • In extreme case, possibility of train accident	Restrict remote access to the ETCS	Installation-Deny
				Detect unauthorized connections captured in the communication patterns to and from the ETCS	Installation-Detect
				Require approved cryptographic algorithms for authentication and message integrity on the railway signalling network	Installation-Deny
				Provide cybersecurity training to SCADA system operators	Exploitation-Prevent
				Authenticate users accessing the SCADA system	Installation-Prevent
				Check integrity of messages issued by the SCADA system	Delivery-Degrade Installation-Detect

(*Continued*)

Table 3 Continued

Cyber-attack	Description	Vulnerabilities	Risks/Consequences	Defensive Controls	RDKC Matrix Cell
Insider attacks in railway assets like: – Signalling – Rolling stock – Power supply – Databases – ICT – SCADA	An authorized maintenance team member within the railway maintenance having valid authorization, issues command for remote maintenance of critical railway asset like SCADA	Inadequate system and process checks for railway critical assets	• Equipment damage/sabotage • Temporary stoppage of trains • Loss of customer confidence • In worse case, accident may happen	Detect anomalous commands not stemming from the normal remote control center	Delivery-Detect
				Use RBAC to limit who has access to sensitive functions	Delivery-Prevent
				Require two-person rule that initiates remote maintenance command	Delivery-Prevent
				Generate alarms to issue sensitive commands	Installation-Detect
				Create audit logs to track who issues remote maintenance commands	Act on Objective-Detect

An insider is able to gain access to the network to which an ETCS system is connected and to the ETCS's credentials, assuming credentials are in place. This individual compromises (malicious intent) or misconfigures (accidentally) the ETCS system.	• Firewalls non-existent or improperly configured allowing access to the ETCS system by an unauthorized insider • Weak network security architecture allowing access to the ETCS system • No security monitoring on the railway signalling network • Inadequate authentication and access control for configuration and programming software on the ETCS system • Insecure remote access to the ETCS system	• Delay in taking maintenance and operation actions, when needed • Incorrect maintenance and operation actions taken • Cascading failures • Train accident may happen	Restrict network service access at multiple layers to prevent unauthorized individuals from gaining access to the ETCS	Installation-Prevent
			Restrict remote access to the ETCS	Installation-Deny
			Detect unauthorized connections captured in the communication patterns to and from the ETCS	Installation-Detect
			Require approved cryptographic algorithms for authentication and message integrity on the railway signalling network	Installation-Deny

Explanations of the Table 3.: (RDKC matrix cell) This column is the value from the RDKC matrix cell. This matrix cell can be viewed as characterizing the types of effect a given defensive control could have on a CKC phase. For example, the Reconnaissance – Detect cell is at the intersection of the detect tactic and the reconnaissance phase of CKC; this means that in the reconnaissance phase, to detect cyber incidents, we must follow the defensive controls provided in the Reconnaissance – Detect cell.

4.4 How RDKC will Help to Reduce the Risk of Cyber-Attack: A Case of Railway SCADA Example

Consider an example of multistage cyber-attack on railway SCADA system (one of the scenarios from Table 3) where a threat agent breaches a railway SCADA system and causes this system to issue an unregistered or malicious command. To proactively reduce the risk of this attack, various courses of action from the RDKC matrix can be chosen to reduce the risk of this attack (Figure 6). For example, to defend against the first stage (external reconnaissance), defender may implement detect technologies like NIDS or web analytics. In the second stage (weaponized), defender may deceive the attacker by providing some fake weaponized codes or fake registration. In the third stage (delivery), defender may detect the attacker by using deep packet inspection.

In the fourth stage (exploitation), defender may prevent the attack by using systems & application updates. In the fifth stage (Installation), defender

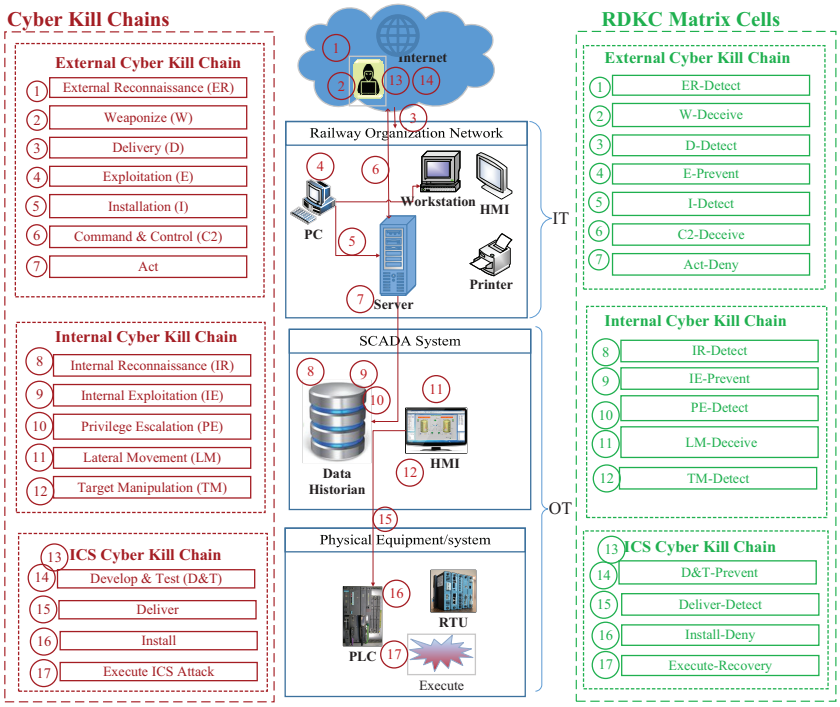

Figure 6 Cyber kill chain and railway defender kill chain to reduce the risk of cyber-attacks: An example of the railway SCADA system.

may detect the attack by using an alarm/alert system. In the sixth stage (command & control), defender may deceive the attacker by using DNS redirect or honeypot. In the seventh stage (act), defender may deny the attack by using outbound access control lists. If the cyber-attack is successful then attacker may move to stage eighth inside the network and starts internal reconnaissance to search for available systems and map the internal network and vulnerabilities (e.g scanning OT to find Human Machine Interfaces). To defend against this, defender may detect this attack by using HIDS for alerting. In the ninth stage (internal exploitation), defender may prevent the attack by using patch and vulnerability management. In the tenth stage (privilege escalation), defender may detect the attack by using behavioral analytics. In the eleventh stage (lateral movement), defender may deceive the attack by using decoy servers. In the twelfth stage (target manipulation), defender may detect the attack by using host-level log analysis. If the attacker will be successful in the manipulation of the railway SCADA system then he will gain access to the physical system via new vulnerabilities. Thus, in the thirteenth and fourteenth stages (develop and test), defender may prevent the attack by harden/obfuscate applications to make reversing difficult. In the fifteenth stage (Deliver), defender may detect the attack by using HIDS systems. In the sixteenth stage (install), defender may deny the attack by using data diode. In the last stage (execute), defender may recover from the attack by using forensics or breach insurance.

4.5 Penetration Probabilities at Each Stage of Cyber Kill Chain

To assess the proposed framework this research has started the simulation of cyber-attack penetration probabilities with varying security controls at each stage of the cyber kill chain. These security controls are the proposed technologies presented in the RDKC matrix (Table 2). Defender can choose these security controls at each stage of the cyber kill chain to defend against the cyber-attack. Figure 7 is one of the simulated results of penetration probabilities at each stage of the cyber kill chain based on the cyber-attack probability. In this case, the probability of defense lies between 11% to 20% (first two stages) and 21% to 30% (rest of the five stages). The penetration probabilities keep on decreasing from first stage to seventh stage. This research has started simulation with seven stages but it will simulate for all the 17 stages in the future.

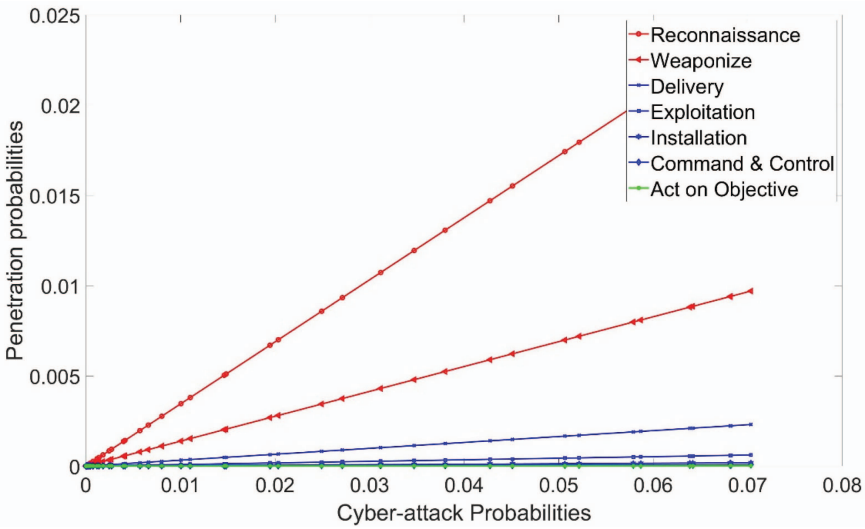

Figure 7 Cyber-attack penetration probabilities at each stage of the cyber kill chain.

5 Conclusions and Future Work

With digitalization, the railway's vulnerability to cyber-attacks is increasing, suggesting the need to focus on cybersecurity. Most organizations are focusing on intrusion prevention technologies, with less emphasis on prediction and detection technologies. This research proposes a Railway Defender Kill Chain (RDKC) to predict, prevent, detect, and respond to cyber-attacks. RDKC uses a course of action matrix, which determines how to predict, prevent, detect, respond to, deny, disrupt, degrade, deceive, and destroy adversary events along the kill chain phases to avoid or minimize loss or unavailability. By being proactive instead of reactive, a defender can mitigate cyber threats, implementing the right defensive strategy provided in the RDKC matrix instead of deploying incident response and forensics after a successful exploit.

Future research will simulate cyber-attack penetration probabilities with varying defensive controls at each stage of the cyber kill chain. The simulation will help railway organizations predict the risk of attack penetrations by applying various security controls at each stage of the cyber kill chain. In addition, a complete set of cyber-attacks along with defensive controls will be sent to the participating railway organizations.

Acknowledgments

The authors would like to thanks Luleå Railway Research Center (JVTC) for sponsoring research work. The authors would also like to acknowledge the contributions of Dr. Phillip Tretten and Robert Beney for their valuable expertise.

References

[1] U. Espling and U. Kumar, "Benchmarking of the maintenance process at Banverket (the Swedish National Rail Administration)," in *Complex System Maintenance Handbook,* Anonymous: Springer, 2008, pp. 559–583.

[2] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams and A. Hahn, "NIST special publication 800–82, revision 2: Guide to industrial control systems (ICS) security," *National Institute of Standards and Technology* 2014.

[3] U. Kumar, R. Kour, P. Tretten and R. Karim, "eMaintenance solution through online data analysis for railway maintenance decision-making," *Journal of Quality in Maintenance Engineering* 2014.

[4] Shift2Rail. *Cybersecurity in the railway sector* [Online]. Available: https://shift2rail.org/project/cyrail/.

[5] R. Ahmad and S. Kamaruddin, "A review of condition-based maintenance decision-making," *European journal of industrial engineering*, vol. 6, no. 5, pp. 519–541, 2012.

[6] N. Subramanian and A. Jeyaraj, "Recent security challenges in cloud computing," *Comput.Electr.Eng.*, vol. 71, pp. 28–42, 2018.

[7] J.R. Nobles, "Cybersecurity threats & challenges," 2018.

[8] D. Patel, "Test utility for live and online testing of an anti-phishing message security system," 2018.

[9] M. Bromiley, "Incident response capabilities in 2016: The 2016 SANS incident response survey," *SANS Institute, June* 2016.

[10] U.D. Ani, H. He and A. Tiwari, "Human factor security: Evaluating the cybersecurity capacity of the industrial workforce," *Journal of Systems and Information Technology*, vol. 21, no. 1, pp. 2–35, 2019.

[11] M. Algarni, S. Almesalm and M. Syed, "Towards Enhanced Comprehension of Human Errors in Cybersecurity Attacks," in *International Conference on Applied Human Factors and Ergonomics*, 2018, pp. 163–175.

[12] S. Kremer, L. Mé, D. Rémy and V. Roca, "Cybersecurity," 2019.
[13] Helpsystems. *Survey Results: 2018 Top Cybersecurity Risks and Mitigation Strategies* [Online]. Available: https://www.helpsystems.com/resources/on-demand-webinars/survey-results-2018-top-cybersecurity-risks-and-mitigation-strategies.
[14] Hackmageddon, "Information security timelines and statistics,". https://www.hackmageddon.com/category/security/cyber-attacks-statistics/.
[15] R. Kour, M. Aljumaili, R. Karim and P. Tretten, "eMaintenance in railways: Issues and challenges in cybersecurity," *Proc.Inst.Mech.Eng.Pt.F: J.Rail Rapid Transit*, pp. 095440971882291 2019. http://dx.doi.org/10.1177/0954409718822915.
[16] Symantec. *2019 Internet Security Threat Report (ISTR): The New Threat Landscape, California, United States* [Online]. Available: https://www.symantec.com/security-center/threat-report.
[17] J.T. Force and T. Initiative, "Security and privacy controls for federal information systems and organizations," *NIST Special Publication*, vol. 800, no. 53, pp. 8–13, 2013.
[18] Lockheed Martin. *Cyber Kill Chain®* [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.
[19] V. Bukac, V. Lorenc and V. Matyáš, "Red queen's race: APT win-win game," in *Cambridge International Workshop on Security Protocols*, 2014, pp. 55–61.
[20] Z. El Mrabet, N. Kaabouch, H. El Ghazi and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," *Comput. Electr. Eng.*, vol. 67, pp. 469–482, 2018.
[21] M.J. Assante and R.M. Lee, "The industrial control system cyber kill chain," *SANS Institute InfoSec Reading Room*, vol. 1 2015.
[22] D.U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)* 2016.
[23] M. Cloppert, "Security intelligence: Attacking the cyber kill chain," *SANS Computer Forensics* 2009.
[24] X. Zhou, Z. Xu, L. Wang, K. Chen, C. Chen and W. Zhang, "Kill chain for industrial control system," in *MATEC Web of Conferences*, 2018, pp. 01013.
[25] Pandasecurity. *Understanding Cyber-Attacks Part I. The Cyber-Kill Chain, Spain* [Online]. Available: http://resources.pandasecurity.com/enterprise/solutions/ad360/1704-WHITEPAPER-CKC-EN.pdf.

[26] S. Northcutt. *Security Controls. SANS Technology Institute, USA* [Online]. Available: https://www.sans.edu/cyber-research/security-laboratory/article/security-controls.

[27] Department of Defense. *JP 3–13 Information Operations* [Online].

[28] E.M. Hutchins, M.J. Cloppert and R.M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research*, vol. 1, no. 1, pp. 80, 2011.

[29] Thales. *Railway Digitalization: Cybersecurity* [Online]. Available: https://www.thalesgroup.com/en/spain/magazine/railway-digitalization-cybersecurity.

[30] Shift2rail report. *CYbersecurity in the RAILway sector D2.1 – Safety and Security requirements of Rail transport system in multi-stakeholder environments* [Online]. Available: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b678c2dc&appId=PPGMS.

[31] CSRC. *NIST Computer Security Resource Center * [Online]. Available: https://csrc.nist.gov/.

[32] ICS-CERT. *Industrial Control Systems Cyber Emergency Response Teams* [Online]. Available: https://ics-cert.us-cert.gov/.

[33] US-CERT. *Critical Infrastructure Cyber Community Voluntary Program* (C^3) [Online]. Available: https://www.us-cert.gov/ccubedvp.

[34] Anonymous (-02-10T15:19:26-05:00). *Information Sharing and Analysis Organizations (ISAOs)* [Online]. Available: https://www.dhs.gov/cisa/information-sharing-and-analysis-organizations-isaos.

[35] APTA. *American Public Transportation Association. Information Sharing & Analysis Center (PT-ISAC)* [Online]. Available: https://www.surfacetransportationisac.org/.

[36] CIS®. *Center for Internet Security* [Online]. Available: https://www.cisecurity.org/about-us/.

[37] Minimum Cyber Security Standard. *Version 1.0. UK* [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/719067/25062018_Minimum_Cyber_Security_Standard_gov.uk__3.pdf.

[38] W. Xu, Y. Tao, C. Yang and H. Chen, "MSICST: Multiple-scenario industrial control system testbed for security research,".

[39] H. Kim, H. Kwon and K.K. Kim, "Modified cyber kill chain model for multimedia service environments," *Multimedia Tools Appl*, vol. 78, no. 3, pp. 3153–3170, 2019.

[40] M. Mohsin and Z. Anwar, "Where to kill the cyber kill-chain: An ontology-driven framework for iot security analytics," in *2016 International Conference on Frontiers of Information Technology (FIT)*, 2016, pp. 23–28.

[41] B.D. Bryant and H. Saiedian, "A novel kill-chain framework for remote security log analysis with SIEM software," *Comput.Secur.*, vol. 67, pp. 198–210, 2017.

[42] A. Hahn, R.K. Thomas, I. Lozano and A. Cardenas, "A multi-layered and kill-chain based security analysis framework for cyber-physical systems," *International Journal of Critical Infrastructure Protection*, vol. 11, pp. 39–50, 2015.

[43] I. Mihai, S. Pruna and I. Barbu, "Cyber kill chain analysis," *Int'l J.Info.Sec.& Cybercrime*, vol. 3, pp. 37, 2014.

[44] S. Wen, N. He and H. Yan, "Detecting and Predicting APT Based on the Study of Cyber Kill Chain with Hierarchical Knowledge Reasoning," in *Proceedings of the 2017 VI International Conference on Network, Communication and Computing*, 2017, pp. 115–119.

[45] S. Wen, Y. Rao and H. Yan, "Information Protecting against APT Based on the Study of Cyber Kill Chain with Weighted Bayesian Classification with Correction Factor," in *Proceedings of the 7th International Conference on Informatics, Environment, Energy and Applications*, 2018, pp. 231–235.

[46] L. Ertaul and M. Mousa, "Applying the Kill Chain and Diamond Models to Microsoft Advanced Threat Analytics," in *Proceedings of the International Conference on Security and Management (SAM)*, 2018, pp. 252–258.

[47] Garba FA, Junaidu SB, Ahmad I, Tekanyi MS, "Proposed framework for effective detection and prediction of advanced persistent threats based on the cyber kill chain," 2018.

[48] I. Herwono and F.A. El-Moussa, "Automated Detection of the Early Stages of Cyber Kill Chain." in *ICISSP*, 2018, pp. 182–189.

[49] C. Velazquez, "Detecting and preventing attacks earlier in the kill chain," *SANS Institute Infosec Reading Room*, pp. 1–21 2015.

[50] Y. Ayrour, A. Raji and M. Nassar, "Modelling cyber-attacks: A survey study," *Network Security*, vol. 2018, no. 3, pp. 13–19, 2018.

[51] W. Wang, J. Bickford, I. Murynets, R. Subbaraman, A.G. Forte and G. Singaraju, "Detecting targeted attacks by multilayer deception," *Journal of Cyber Security and Mobility*, vol. 2, no. 2, pp. 175–199, 2013.

[52] R.A. Yadav T, "Technical aspects of cyber kill chain," in, 2015, pp. 438–452.

[53] K.E. Heckman, F.J. Stech, R.K. Thomas, B. Schmoker and A.W. Tsow, "Intrusions, Deception, and Campaigns," in *Cyber Denial, Deception and Counter Deception*, Anonymous: Springer, 2015, pp. 31–52.

[54] A. Marcella Jr and D. Menendez, *Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes*, Auerbach Publications, 2007.

[55] R. Kour, R. Karim and A. Thaduri, "Cybersecurity for railway – A maturity model," *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit (2019)*: 0954409719881849.

[56] D. Kuipers and M. Fabro, "No title," *Control systems cyber security: Defense in depth strategies* 2006.

[57] X. Fan, K. Fan, Y. Wang and R. Zhou, "Overview of cyber-security of industrial control system," in *2015 international conference on cyber security of smart cities, industrial control system and communications (SSIC)*, 2015, pp. 1–7.

[58] R. Radvanovsky and J. Brodsky, *Handbook of SCADA/control systems security*, CRC Press, 2013.

[59] K. Swearingen, W. Majkowski, B. Bruggeman, D. Gilbertson, J. Dunsdon and B. Sykes, "An open system architecture for condition based maintenance overview," in *2007 IEEE Aerospace Conference*, 2007, pp. 1–8.

[60] Kenneth Holmberg et al., "Information and Communication Technologies Within E-maintenance," in *Emaintenanc,* Anonymous: Springer Science & Business Media, 2010, pp. 39–60.

[61] A. Yokoyama, "Innovative changes for maintenance of railway by using ICT–to achieve "smart maintenance"," *Procedia CIRP*, vol. 38, pp. 24–29, 2015.

[62] R. Karim, J. Westerberg, D. Galar and U. Kumar, "Maintenance analytics–the new know in maintenance," *IFAC-PapersOnLine*, vol. 49, no. 28, pp. 214–219, 2016.

[63] J. Reason, E. Hollnagel and J. Paries, "Revisiting the swiss cheese model of accidents," *J.Clin.Eng.*, vol. 27, no. 4, pp. 110–115, 2006.

[64] R. Starrett. *How to protect data in an IP world* [Online]. Available: https://www.eetimes.com/document.asp?doc_id=1274286.

[65] NSA. *Defense in Depth. US National Security Agency* [Online]. Available: https://apps.nsa.gov/iaarchive/customcf/openAttachment.cfm?FilePath=/iad/library/ia-guidance/archive/assets/public/upload/

Defense-in-Depth.pdf&WpKes=aF6woL7fQp3dJimPuJLAvwxazbq3mDYX6mWmFe.
[66] IndustryWeek. *Proactive Protection Through Industrial Networks* [Online]. Available: https://www.industryweek.com/rockwell-automation-connected-industrial-enterprise/proactive-protection-through-industrial-networks.
[67] W. Knowles, J.M. Such, A. Gouglidis, G. Misra and A. Rashid, "Assurance techniques for industrial control systems (ics)," in *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy*, 2015, pp. 101–112.
[68] C.I.T. Force, "Operational levels of cyber intelligence," 2013.
[69] I. Tarnowski, "How to use cyber kill chain model to build cybersecurity?" *European Journal of Higher Education IT* [Online]. Available: http://www.eunis.org/download/TNC2017/TNC17-IreneuszTarnowski-cybersecurity.pdf 2017.
[70] S. Malone, "Using an expanded cyber kill chain model to increase attack resiliency," *Black Hat US* 2016.
[71] The Denver Post. *SamSam virus demands bitcoin from CDOT, state shuts down 2,000 computers* [Online]. Available: https://www.denverpost.com/2018/02/21/samsam-virus-ransomware-cdot/.
[72] P. Paganini. *For the second time in two weeks CDOT shut down computers after a ransomware infection* [Online]. Available: https://securityaffairs.co/wordpress/69946/cyber-crime/cdot-second-ransomware-attack.html.

Biographies

Ravdeep Kour is a Ph.D. student in the Division of Operation and Maintenance Engineering at Luleå University of Technology, Sweden. She received Bachelor's degree in Information Technology and Master's degree in Computer Science Engineering from Jammu University of India and Punjab

University of India, in 2004 and 2012 respectively. She worked as Assistant Professor in India from 2004 to 2012 and worked in Luleå Technical University, Lulea, Sweden as Research Engineer from 2012 to 2014. She worked on European Union and Swedish Railway Projects. Her total academic and research work experience is 15 years. Her research interests are machine learning, cybersecurity in the context of IT and OT technologies, security risk assessment, cloud computing, and big data analytics.

Adithya Thaduri is working as Associate Senior Lecturer in the Division of Operation and Maintenance Engineering at Luleå University of Technology. He has experience in coordination of four European projects (IN2RAIL, INFRALERT, IN2SMART and FR8RAIL) and three national projects (InfraSweden, Mindi and SKF) in the area of Railways and have worked in collaboration in other seven projects. He recently got funding for one European project for Railways (IN2SMART2) and two national projects; one from Vinnova to Railway and other from Coal India Limited to Mining. He is part of over 35 deliverables/reports within above mentioned projects. He has over 40 research publications (28 after PhD) in journals, book chapters and conference proceedings. He has been teaching Maintenance Engineering course for master's programme for two years. His areas of research are machine learning and context-aware maintenance decision making within the framework of Maintenance 4.0 in Railways, asset maintenance analytics, prognostics and degradation modelling of railway infrastructure, reliability predictions, maintenance planning and optimization, RAMS, LCC and Risk assessment, predictive analytics of mining machines, and cybersecurity.

Ramin Karim is PhD in the area of Operation and Maintenance Engineering with focus on eMaintenance and Industrial AI. Ramin has over 20 years of industry experiences in computer science and Information and Communication Technologies (ICT), with roles as software developer, systems architect, project manager, multi-project leader, process owner, product manager, responsible for standardization, model developer, and technology business developer. Ramin has over 60 publications in several research areas related to eMaintenance. Ramin is head of the eMaintenance Research Team, focusing on Industrial AI for Operation and Maintenance. He is also founder of a spin-off company from Luleå University of Technology, which develops analytics solutions based on Industrial AI and eMaintenance.