RAC Cybersecurity Committee Meeting

June 20, 2024

People. Goods.
Canada moves by rail.

Railway Association of Canada

Competition Law Compliance Policy

STATEMENT

The RAC is committed to compliance with all **competition laws** applicable in Canada, including Canada's *Competition Act*.

Under the leadership of its Board of Directors, the RAC carries out its activities in strict compliance with all **competition laws**, provides guidance to its committees and its employees on how to comply with these laws, and promotes with them the importance and value to the RAC of complying with them.

The RAC Corporate Secretary ensures that RAC, its committees and its staff are familiar and comply with this policy.

COMPETITION LAW

Competition laws are designed to maintain and encourage competition in the marketplace. Non-compliance with the **competition laws** relating to improper coordination among competitors could constitute a criminal offence to which significant fines and prison terms can be attached, and for which significant damages can be awarded in private lawsuits, including large class actions.

RAC is a forum for railway members to exchange information and views on the railway sector. Particularly because RAC is an association that represents most of the players in the rail sector in Canada, including many that compete with one another, any activity it conducts must be in strict accordance with the **competition laws**, and avoid even the perception of possible improper conduct.

PROHIBITED ACTIVITIES

Due to the presence of multiple competing entities in RAC, any activity, including discussions or agreements that relate, directly or indirectly, to the following "**Prohibited Topics**" are strictly prohibited:

- Prices (rates) charged to shippers for services provided by members of the RAC
- Prices (costs) paid to suppliers for services provided to members of the RAC
- Any other conditions associated with services provided to shippers or received from suppliers of RAC members, including discounts, rebates, etc. and level of service provisions
- Customer or territory allocation
- Limitation of supply of services provided by RAC members to their customers

GUIDANCE

Any activity, including discussions or agreements that could even remotely be construed as relating to the above Prohibited Topics, cannot take place at the RAC or any of its committees or any meeting organized or attended by RAC staff, or otherwise among RAC members.

To ensure compliance with these rules, when meeting, members of a RAC committee or of the Board of Directors must:

- Have a pre-set agenda and take minutes, recording resolutions adopted and summarizing the essentials of conversations that took place.
- Limit themselves to issues identified on the agenda, except if circumstances call for other issues to be addressed, in which case careful notes of the additional issues discussed must be recorded.
- If any participant believes that Prohibited Topics have been raised or discussed, they must advise all participants of their concern and any discussion relating to that issue be ceased immediately pending legal advice.
- Require legal advice if any issue to be discussed might cause the members to believe that **competition laws** could be infringed.
- Suspend or even postpone to a later date discussions on such issues if legal advice cannot be sought in a timely manner.

Staff of the RAC shall in their duties ensure the confidentiality of information brought to their attention by members, avoid conflict of interest or situations that would discredit the RAC, unless doing so could violate the **competition laws**.

Railway Association of Canada

RAC CYBERSECURITY COMMITTEE MEETING

June 20, 2024
12:00 – 13:00 (ET)

Microsoft Teams Meeting
Click here to join the meeting

AGENDA

	SCHEDULE	DISCUSSION LEADER	TIME
1.	Welcome, Call to Order and Roll Call	Vaughn Hazen (Chair)	12:00
1.1	Competition Law Compliance Policy – Forward Statement	Enzo De Benetti	12:05
2.	Approval of Meeting Minutes (April 11, 2024)	Vaughn Hazen	12:10»**D**
3.	TC presentation of the rail threat assessment	Chris Free	12:15
4.	General Discussion	All	12:55
5.	Miscellaneous / Adjournment	Vaughn Hazen	13:00

D **Decision Required**
» *Supporting material*

Railway Association of Canada

RAC CYBERSECURITY COMMITTEE MEETING
DRAFT MINUTES 24-02
Virtual Meeting
April 11, 2024; 13:00 HOURS (ET)

In Attendance	**Regrets**
Brianna Bowman (RAC)	Alex Borhani (CSX)
Enzo De Benetti (RAC)	Mike Chung (CPKC)
Jana Dewar (VIA)	Jessie Gill (WCE)
François Du Perron (VIA)	Biying He (WCE)
Vaughn Hazen (CN)	Malwinder Singh (CPKC)
Rick Hislop (Rocky Mountaineer)	Janet St. John (AAR)
Adrian McLeod (ONTC)	Fawad Sukhera (CN)
	Douglas Sul (CPKC)

1. **Welcome & Introductions**
   Mr. De Benetti called the meeting to order in accordance with the Railway Association of Canada (RAC) bylaws and read the Competition Law Compliance Policy – Forward statement.

2. **Approval of Minutes January 24, 2024**
   It was moved by Mr. Du Perron (VIA) and seconded by Mr. Hislop (Rocky Mountaineer) to approve the minutes of the January 24, 2024, meeting.

3. **Update from Cybersecurity Working Group**
   The working group held their first meeting on February 28, 2024, and are continuing to work towards their mission statement and vision.

   The working group discussed:
   - Bill C26 being too vague and not prescriptive enough.
   - They are concerned about the timing of the bill being unknown.
   - Lawmakers are still trying to determine thresholds of when and what to report.
   - Its still undetermined as to who would be subject to the bill itself.
   - An appendix is to be attached to the bill which would be populated by critical industries. This is yet to be completed.
   - Everyone agreed that the punitive measures defence to promote the regulatory compliance reviewed as too aggressive by all.

   Ms. Dewar will be reaching out to the Cybersecurity Center to set up regular meetings/touchpoints to find out their influence on the bill and get regular updates on what's happening. The working group also wants to find out what type of supports will be coming from the cyber center moving forward as they currently are unable to provide support outside of the current government.

4. **General Discussion**
   SECU completed clause-by-clause consideration of Bill C-26. While details were not shared regarding certain amendments, there were relevant amendments agreed to per the Blues. Two policy wins that came from this meeting were:

- Amendment to clarify that the due diligence defence **is** applicable under a strict liability framework (Parts I & II) – apparent policy win.
- Amendment to adjust duty to report period from “immediately” to “within a period not to exceed 72 hours” – policy win.

However, other asks – at least based on the Blues – remain undiscussed and unaddressed. These include the prioritization of supply chain risks over others, moving towards risk-based thresholds, and a reduction in AMP’s, among others.

Mr. De Benetti attended a meeting recently where he was asked by RAC members if the RAC would consider responding to regulations happening on the American side, should they negatively impact the Canadian railways. If the RAC were to respond, it would have to ensure that all railways are represented as well as require consensus from all its members.

Next meeting
The next meeting will be held on June 10, 2024, at 13:00.

The meeting was adjourned at 13:31 ET.

Action Items	Lead	Status
1. Circulate meeting minutes	Brianna Bowman	Completed
2. Create shared working folder for working group to start working on its mission statement and vision	RAC	

THREAT OVERVIEW - RAIL

TRANSPORT CANADA

REPORT: 7-2024
DATE: 2024-05-15

UNCLASSIFIED//FOR OFFICAL USE ONLY

2024 Threat Overview: Canadian Rail Transportation (U//FOUO)

EXECUTIVE SUMMARY (U//FOUO)

The Canadian rail system supports the movement of people and goods and is a cornerstone of national and continental security and supply chains. The rail system faces various cyber and physical threats from malicious actors, such as cybercriminals, hostile activities by state actors (HASA), and extremist groups, which has the potential to cause significant disruption, or damage to the rail system. (U//FOUO)

Threats to life remain the primary concern, but the threat environment is evolving and becoming more complex. (U//FOUO)

Religiously motivated violent extremism (RMVE), ideologically motivated violent extremism (IMVE), and politically motivated violent extremism (PMVE) actors aspire to target rail transportation, but likely have limited cyber capabilities, making other unsophisticated methods of attack more likely. (U//FOUO)

BOTTOM LINE FOR CANADA (U)

- Intermodal Surface Security and Emergency Preparedness (ISSEP) and the Integrated Terrorism Assessment Centre (ITAC) assess that the overall threat to Canada's passenger, freight, and trans-border rail systems is **LOW.** (U//FOUO)
- There has been an uptick in hostile rhetoric aimed at the railway industry. Consequently, it is assessed that the most probable threat scenario involves an unsophisticated attack, such as the use of bladed weapons or firearms, carried out by lone actors or small groups against rail transportation systems, including commuter trains and rail stations. The motivation for such an act could be equally attributed to ideological, religious, or political motivations. (U//FOUO)
- According to 2023 data, there has been significant instances of deliberate tampering and obstacles on railway tracks in Canada, which has impacted both passenger and commercial transport in several regions. Recent geopolitical developments in the Middle East have sparked numerous pro-Palestinian rallies throughout Canada, culminating in disruptions to rail operations. Although these actions adversely affect the economy and railway operations, they do not qualify as acts of terrorism. (U//FOUO)
- Critical infrastructure (CI), including transportation, can be exploited by cybercriminals and HASA leading to the collection of vast amounts of personal, business, and financial data, such as passenger travel data, detailed freight data, and intellectual property available online. (U//FOUO)
- Cyber threats involving attacks against information technology (IT) systems initiated by foreign state actors have reached critical levels globally. The probability of data theft, espionage and ransomware attacks occurring is assessed as **VERY HIGH**. (U//FOUO)
- The impact of climate change on Canada's railway infrastructure could be more severe than that of sabotage, intentional property damage, terrorism, and similar events. This is attributed to climate change being more pervasive, recurrent, and erratic in nature. (U//FOUO)

SCOPE NOTE (U//FOUO)

This assessment is an unclassified version of a classified report. It provides an overview of some malicious operations targeting rail systems worldwide, based on a variety of open-source research as of **31 March 2024**. The report also identifies key trends, challenges, and implications of these operations. (U//FOUO)

KEY POINTS (U//FOUO)

- While the overall incident trend impacting the rail industry for 2023 has been consistent on a year-to-year basis, the 12-month data reveals that violent extremist (VE) threats to Canada's rail networks remain **LOW**. (U/FOUO)
- Since late 2023, there have been increasing links between IMVE groups acting in solidarity with various causes, which will remain a prominent aspect of the VE threat landscape in Canada in early 2024. (U//FOUO)
- Globally, the rail systems experienced a surge of ransomware attacks in 2023, affecting both information technology (IT) and operational technology (OT) environments of rail operators and service providers. (U//FOUO)
- Foreign state actors will continue to attempt to participate in Canada's rail transportation sector directly or indirectly using various surreptitious methods. (U//FOUO)
- All foreign IT systems and foreign-made components integrated into locally manufactured IT systems used by Canadian transportation companies are vulnerable to malicious exploitation. (U//FOUO)

Excerpt from the Criminal Code of Canada on terrorism: (U//FOUO)

Clause 83.18(1) of the Canadian Criminal Code specifies that criminal liability is generally based on actions rather than beliefs.

VIOLENT EXTREMIST THREATS TO RAIL TRANSPORTATION SYSTEMS (U//FOUO)

- IMVEs, RMVEs, or PMVEs continue to perceive train stations and railway infrastructure as soft targets due to limited security measures in place or target remote locations that are not subject to ongoing monitoring. (U//FOUO)
    - In October 2022, an incident of sabotage against German railways occurred; communications cables were cut at two sites, causing disruptions. (U//FOUO)
    - In January 2023, an individual wielding a bladed weapon injured several people at a railway station in Paris, France, before being shot and arrested. The motive for the attack was not clear, and the attack was not considered terrorism. (U//FOUO)
    - In early February 2024, an individual injured three people with a knife and a hammer at a Lyon railway station in France. The motive of the attack was not clear, but the suspect appeared to have deliberately targeted French people, according to French authorities. (U//FOUO)
    - Also, in early February 2024, Swiss authorities reported a man with an axe and a knife held 15 hostages on a train in western Switzerland for four hours. Authorities noted that there was no indication of a terrorist motive. (U//FOUO)

POTENTIAL VIOLENT EXTREMIST THREATS TO RAIL TRANSPORTATION IN NORTH AMERICA (U//FOUO)

- Transport Canada statistics for 2023 show there has been notable incidents of tampering and obstacles on tracks. Although these disruptive actions are damaging to the economy and to rail network operations, they do not qualify as acts of terrorism. (U//FOUO)

- *Terrorgram*, a loose network of transnational IMVEs active on Telegram, has disseminated several publications promoting sabotage of CI since 2021, according to Department of Homeland Security (DHS) reporting. The Hard Reset, an IMVE publication issued in July 2021 that promotes accelerationist ideologies included extensive details on how to exploit the vulnerabilities of power grids and other CI, according to the same DHS report. (Accelerationism is a range of revolutionary and reactionary ideas in left-wing and right-wing ideologies that call for the drastic intensification of capitalist growth, technological change, infrastructure sabotage and other processes of social change to destabilize existing systems and create radical social transformations, otherwise referred to as "acceleration"). (U//FOUO)

Excerpt from the Criminal Code of Canada on terrorism: (U//FOUO)

Clause 83.01 (1) (b)ii (D) Advocacy and Protest exclusion: The law recognizes that significant property damage or disruption of essential services, while serious, does not constitute terrorist activity if it arises from advocacy, protest, dissent, stoppage of work not intended to cause death, serious bodily harm, or endangerment of life.

Clause 83.01 (1) (b)ii (E) Protection of Lawful Dissent: It is explicitly stated that interference with essential services resulting from lawful advocacy protest, dissent, or work stoppage, without the intent to cause grave harm as outlined in terrorism offences, is not considered a terrorist act, thus safeguarding legitimate civil activities.

- In November 2022, a group of anarchists claimed responsibility for sabotaging rail lines in eastern Ontario in solidarity with an indigenous group against a gas pipeline. They used nails, wires, and metal bars to interfere with the railway signals which caused delays and disruptions. (U//FOUO)

- According to a mid-July 2023 ITAC assessment, the most significant VE threat to Canada's domestic rail systems remains individuals or small groups inspired or incited online by IMVE. Although IMVE actors claimed responsibility for alleged attacks on Canadian rail infrastructure and incited further attacks, there were no confirmed VE attacks against Canada's rail networks, even though IMVEs have the capability to conduct unsophisticated attacks. Transport Canada observed an increase in rail security incidents, however, ITAC notes that although this increase coincides with certain ITAC threat indicators, the increase in security incidents does not appear to indicate a heightened threat of terrorism. (U//FOUO)

- In April 2023, according to a rail law enforcement agency, an anonymous post on X (Twitter) with the following message "*I have just purchased a train derailer [sic] and plan to use it in 4 days,*" follows the pattern of multiple posts referencing train derail devices. Railway authorities in the U.S. judge that these types of posts align with accelerationist ideologies. These ideologies suggest such devices could potentially be used to intentionally derail trains. Furthermore, there are claims that recent train derailments across the U.S. could be attributed to deliberate acts of sabotage. (U//FOUO)

  In addition, the same rail law enforcement agency noted that since a train derailment in East Palestine, Ohio, on 3 February 2023, there has been a significant increase in online posts relating to these rail incidents, along with some messages suggesting the subsequent derailments may have been intentional acts of sabotage targeting CI. (U//FOUO)

- On 21 July 2023, a communication posted to the anarchist website *Nameless* (*"Sansnom")*, which provides updates on anarchist activity in France and other Western countries, included a French-language pamphlet entitled "*Another End of the World is Possible: Indigenous Solidarity and Blocking Extractive Infrastructure in Canada.*" (U//FOUO)

CONFLICTS AND THEIR IMPACT ON RAIL (U//FOUO)

While global conflicts do not have a direct impact on rail operations in Canada, rail systems in Canada are targeted in support of or in reaction to those conflicts. Some examples include:

- On 20 November 2023, pro-Palestine supporters calling for a ceasefire blocked a Canadian National (CN) line in Winnipeg, MB for five hours. (U//FOUO)

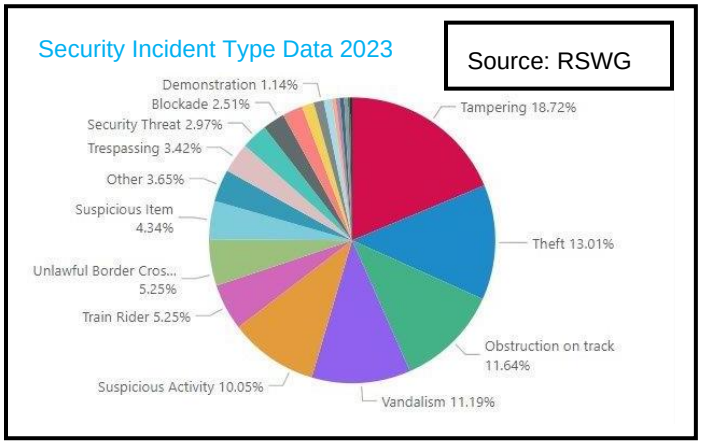
- In mid-January 2024, pro-Palestine protestors blocked CN rail lines near Halifax, NS without causing delays to trains. (U//FOUO)

- Between 27 and 31 January 2024, three shunting incidents occurred in Ontario, which caused a signal malfunction. It is unknown whether the suspects' intentions were to shunt the rail right before the train was proceeding through the area or if the act occurring before the train passed was coincidental.[15] A sign was later found at one of the locations (a piece of cardboard with black marker) placed between the rails of the track that read "*CN must end freight shipments for ZIM, ZIM supplies Genocide.*" (U//FOUO)

TAMPERING AND SHUNTING (U//FOUO)

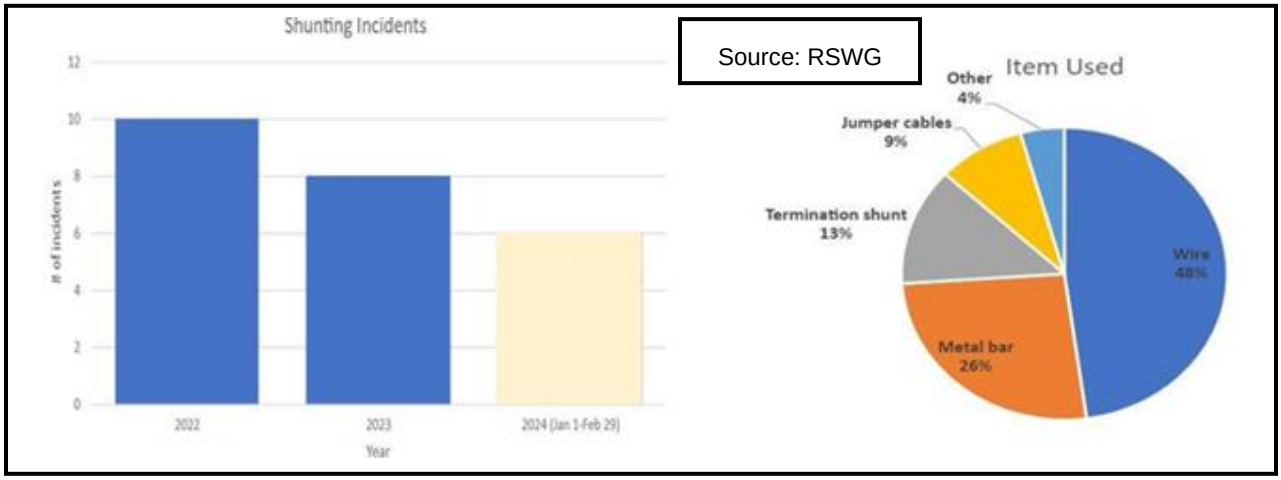
- Tampering with railway infrastructure, including tracks, and signalling equipment by unknown individuals and unknown motives has been impacting passenger and freight railway traffic in various parts of the country. (U//FOUO)

  According to Transport Canada's Rail Security Working Group (RSWG) March 2024 report, there has been an increase in shunting incidents on regulated railways in Canada in the first two months of 2024, compared to all of 2023. The intent of these incidents is unclear, other than those related to current and most likely pro-Palestinian activism. According to ITAC's mid-July 2023 assessment on VE threats to Canada's rail networks, although this increase coincides with certain ITAC threat indicators, the increase in security incidents does not appear to indicate a heightened threat of terrorism. (U//FOUO)



- Intelligence gaps exist in identifying threat actors that intend to carry out acts of violence without actively communicating this intent online. These entities are often radicalized individuals who passively consume extremist content and can remain under the radar of intelligence agencies and law enforcement. (U//FOUO)

- A threat actor with high intent but low capability poses a different level of threat compared to one with both high intent and high capability. (U//FOUO)



Source: RSWG

HOSTILE ACTIVITIES BY STATE ACTORS (U//FOUO)

- The PRC's 2017 Cybersecurity Law grants the PRC government full access to data held by PRC-owned enterprises and affiliated foreign firms. Thus, the PRC could collect personal, private, and commercial information from transportation systems that use technology, such as intelligent train systems and connected and automated vehicles. Moreover, the PRC national security laws, including the 2015 National Security Law and the 2021 National Intelligence Law, have increasingly formalized an obligation for all PRC nationals and all spheres of Chinese society, including business, financial, media and academic domains, to collaborate with PRC intelligence agencies. (U/FOUO)

- Hungary is proceeding with PRC's Huawei to build Europe's first 5G smart railway. After completion, it will become the largest intelligent multimodal railway hub in Europe, and the first railway in Europe to use a 5G dedicated network for internal communication and technical management. (U//FOUO)

- The PRC is intent on becoming a global leader in standard-setting, including through international technology that runs along the Belt and Road Initiative (BRI) routes. It does this by setting up de facto standards from the ground up through the export of its technologies. These exports could create path dependencies that essentially lock customers into using PRC technology by making it difficult and expensive to switch to an alternative product. Canadian companies face a disadvantage as the PRC's export of technology along BRI routes creates a market preference for PRC standards. This dominance can reduce market opportunities for Canadian products, hinder innovation, and force Canadian firms to adapt to PRC standards, which will impact their competitiveness and financial viability. (U//FOUO)

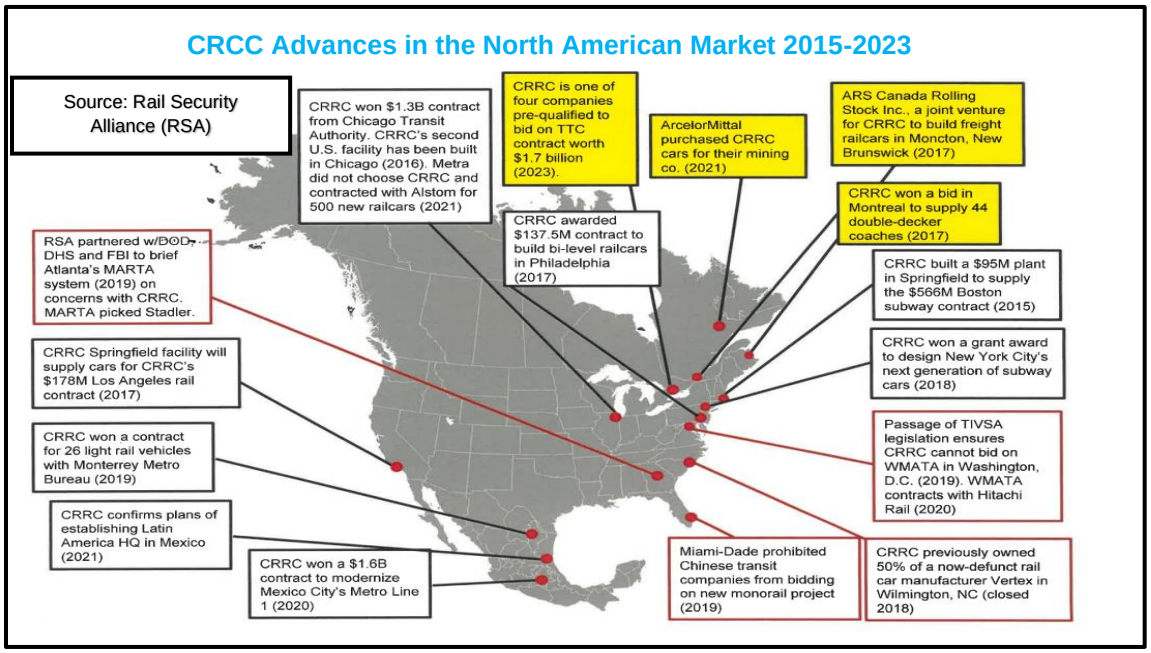
Made in China (MIC) 2025 is a China Communist Party (CCP) led industrial policy that seeks to make the PRC dominant player in global manufacturing. It identifies the rail manufacturing sector as a top target for international expansion. (U//FOUO)

The **Belt and Road Initiative (BRI)** is a global infrastructure development strategy for the PRC to invest in nearly 70 countries, focused on proliferating PRC rail technology and transport globally. (U//FOUO)

The **China Railway Construction Corporation (CRCC)** is a PRC state-controlled entity with nexus to the PRC military-industrial complex, and actively cooperates with Huawei, connecting the physical infrastructure of rail to Huawei's information technology networks. (U//FOUO)

- Some Canadian surface transportation infrastructure, including rolling stock, has been designed and constructed by foreign companies. There are risks that some of this infrastructure could be compromised by foreign threat actors during periodical maintenance work which can lead to unauthorized data collection and monitoring. This also raises concerns regarding the possibility or extent to which these systems could be vulnerable to direct control or interference by the same actors. (U//FOUO)

- The PRC also remains intent on being the dominant player in the international rail industry via the BRI. However, a growing number of nations are cancelling or suspending major projects with the PRC over fears of corruption, debt trap concerns, and overpricing. Additionally, in direct competition with the PRC's BRI, the U.S. led "Build Back Better World" initiative intends to spend hundreds of billions of dollars to develop infrastructure world-wide. In late 2020, the U.S. also took the step of blacklisting the (CRCC), amongst others. (U//FOUO)



CYBER THREATS (U//FOUO)

- ISSEP observed that malicious cyber activities in the rail sector carried out by cybercriminals and state-sponsored actors, mainly involves the theft of valuable data (e.g., corporate data, rail passenger and employee personally identifiable information (PII)). Additionally, these actors may hinder railway operations using ransomware and phishing schemes, aiming to infiltrate critical systems for future sabotage or wide scale disruption. (U//FOUO)

- A 2021 study on ransomware attacks found that the top six most targeted countries were: U.S., Canada, UK, France, Germany, and Italy, altogether accounting for 81 percent of ransomware attacks. The main state actors include the PRC, Russia, the Democratic People's Republic of Korea (DPRK) and Iran. Cybercriminals looking for financial gains will almost certainly continue to target businesses of all sizes, including those associated with rail transportation. (U//FOUO)

- The following examples illustrate incidents where ransomware attacks were used against railway systems:
    - In 2016, a ransomware attack on the San Francisco Municipal Transportation Agency disabled ticketing machines, attackers demanded $73,000 in bitcoins to restore the system (U//FOUO)
    - In 2017, a cyberattack on German Railways disrupted the passenger information systems, ticket machines, and website, as part of a global ransomware campaign known as *WannaCry*. (U//FOUO)
    - In 2020, a ransomware attack on the state-run railway company in Belarus aimed to prevent the transport of Russian troops and artillery to the country, in anticipation of an attack on Ukraine. (U//FOUO)
- Indirect cyber threats to the rail sector posed by targeting the supply chain:
    - Sophisticated state and non-state cyber actors will almost certainly continue to target third parties, such as managed service providers (MSPs) and other suppliers to reach high-value targets in the rail sector. (U//FOUO)
- Digital transformation of OT in the rail sector:
    - Intelligent, data-driven systems and digitally transformed OT are increasingly integrated in every major element of the rail industry. Research into the cyber security of supervisory control and data acquisition (SCADA) systems and industrial control systems (ICS) have demonstrated that the methods and approaches commonly used to breach information and computer security can be successfully employed to disrupt functional safety, reliability, and industrial process safety. (U//FOUO)
- The Canadian Centre for Cyber Security (CCCS) assesses, and ISSEP concurs, that it is unlikely that pro-Russia non-state actors, such as *Killnet*, will disrupt Canadian transportation infrastructure unless the context of the Ukrainian conflict were to change, such as if Canada would evolve its support to Ukraine. In the current context, significant long-term disruption or destruction in the Canadian transport sector by Russia-aligned groups is unlikely. (U//FOUO)
- Globally, observed malicious cyber activity in the rail/surface transportation sector in 2022 was primarily related to disruption of operations through distributed denial of service (DDoS) and ransomware attacks, and the theft of valuable data, such as PII. (U//FOUO)

The Internet of Things (IOT) and its implications in the rail transportation realm

IOT refers to the network of physical devices, sensors, and software that can collect and exchange data. IOT has many applications in railway operations, such as monitoring the condition of tracks, trains, and signals, optimizing the energy consumption and performance of trains, enhancing the passenger experience and information, and improving the safety and security of railways systems. (U//FOUO)

The IOT also introduces new challenges and risks for railway operations, especially in terms of cyber-physical security. Cyber-physical security refers to the protection of both the digital and physical aspects of critical infrastructure from malicious attacks.

Railway systems are vulnerable to cyber-physical attacks because they rely on wireless connectivity, have diverse mix of vendors and technologies, are widely dispersed across different regions, and are often under-funded by governments. Cyber-physical attacks could cause serious consequences, such as collisions, derailments, fires explosions, injuries, deaths, environmental damages, and economic losses. (U//FOUO)

- Several hostile states have highly sophisticated cyber capabilities and have successfully disrupted rail operations worldwide, for example in Europe, India and in Israel. Currently, ISSEP has not observed hostile states deliberately using cyber capabilities for the purpose of disrupting Canadian railway services as a form of retaliation or intimidation. (U//FOUO)

CLIMATE CHANGE (U//FOUO)

While not a threat, climate change poses significant challenges to the Canadian rail industry, impacting its safety, efficiency and infrastructure as extreme weather events occur more frequently and are of greater severity. There are no indications that climate change issues could be exploited by VE in the future. Impacts of climate change on the rail sector include: (U//FOUO)

- **Flooding and Landslides**: Increased precipitation and melting permafrost can lead to flooding and landslides, disrupting rail services and damaging tracks. In August 2021, Hurricane Ida caused widespread flooding and damage to the rail network in the U.S. Northeast, forcing Amtrak and other rail operators to cancel or modify service for several days. Hurricane Sandy which struck New York in late October 2012, had a devastating impact on the city's subway infrastructure, rail yards and maintenance facilities. (U//FOUO)

- **Forest Fires**: Rising temperatures and drier conditions contribute to a higher risk of forest fires, threatening safety and causing delays when near rail lines. In September 2021, a wildfire in BC destroyed a wooden trestle that was part of the CPKC Railway, disrupting freight and passenger service between Vancouver and Calgary. (U//FOUO)

- **Permafrost Degradation**: In northern regions, thawing permafrost can undermine the stability of rail infrastructure, requiring new engineering solutions. (U//FOUO)

- **Extreme Temperatures**: Rail operations face challenges from both extreme heat, which can warp tracks, and extreme cold, which can cause mechanical issues. In June 2021, a heat wave in the US Pacific Northwest caused several rail lines to suspend or reduce service, affecting both passenger and freight trains. (U//FOUO)

ASSESSMENT (U//FOUO)

- ISSEP concurs with ITAC that the overall threat to Canada's passenger, freight, and trans-border rail systems is **LOW.** (U//FOUO)

- ISSEP has observed an increase in IMVE rhetoric directed toward the rail sector. As a result, ISSEP assesses that a low-sophistication attack (e.g., using bladed weapons or firearms) by small cells or lone actors against rail transportation (e.g., onboard commuter rail and at rail stations) is the most likely threat scenario. There is an equal likelihood that the threat actor would be directed or inspired by ideology, religion, or political motivation. (U//FOUO)

- In 2022, ITAC assessed domestic extremists have the capability to carry out unsophisticated attacks against rail networks, and that an RMVE attack would likely target passengers on an urban passenger system, while an IMVE attack would likely target freight to destroy infrastructure and supply routes to force societal change. (U//FOUO)

- The interconnectedness between the rail networks in Canada and in the U.S. makes it very likely that a disruption of operations elsewhere in U.S. would have repercussions in Canada. (U//FOUO)

- ISSEP has not identified VE actors that possess capabilities and intent to target rail transportation through cyber means. (U//FOUO)

- Cybercriminals seeking financial gain will almost certainly continue to target organizations of all sizes whose IT systems remain vulnerable, including those in the rail industry. (U//FOUO)

- ISSEP assesses that climate change could have a more serious impact on the rail industry in Canada than sabotage, damaging rail property on purpose, terrorism, and other occurrences, as it is more widespread, frequent, and unpredictable. (U//FOUO)

Railway Association of Canada

The Railway Association of Canada
Cybersecurity Committee
Terms of Reference

Name

This committee shall be known as the RAC Cybersecurity Committee.

General Mandate

The general mandate for this committee is to provide RAC members a forum:

- For the identification and assessment of industry cybersecurity concerns.
- To monitor and advise on new or proposed changes to cybersecurity-related legislation or regulation and evaluating the impact of such changes on the industry.
- To identify and recommend opportunities for cybersecurity improvements within the industry.
- To facilitate and coordinate cybersecurity concerns and activities between freight and passenger members
- Collaborate with the federal and provincial governments to enhance the rail cybersecurity posture to prevent, mitigate, respond to and recover from potential terrorist or major cybersecurity incidents.

The Cybersecurity Committee will monitor, analyze, and provide reports and recommendations to the RAC Safety Committee on matters within the scope of its mandate. The Cybersecurity Committee will serve as a focal point for sharing of ideas, technology, best practices, and new initiatives that provide positive improvements in cybersecurity within the industry.

The Cybersecurity Committee may establish Working Groups to study specific cybersecurity incidents or issues and deliver on targeted project objectives.

Each Working Group will develop its own terms of reference and elect a Chair. Working Groups will report to and be governed by the decisions of the Cybersecurity Committee.

Committee Responsibilities & Guidelines

- Monitor, assess and report findings and recommendations to SOMC on issues emanating from within the committee's mandate.

- Research and report on issues assigned to the Committee by the membership.

- Foster an open environment of sharing cybersecurity program strategies and successes, new technologies and procedures, incidents and exercises, threat assessments where appropriate and generally spearhead ideas that enhance the development of all member company's cybersecurity initiatives.

- Ensure that regulators overseeing railway cybersecurity and other agencies with an interest in cybersecurity are made sufficiently aware of railway operations and

cybersecurity activities. The Cybersecurity Committee will promote voluntary approaches for cybersecurity management rather than prescriptive regulatory approaches.

- Review, assess, develop, and implement appropriate broad industry strategies that promote the cybersecurity interests of RAC members. These could include industry cybersecurity best practices and guidelines, cybersecurity training packages, presentations, and other activities.

- Act as the managing entity for the various cybersecurity-related activities in which RAC is engaged as well as assessing and reviewing proposed regulatory actions related to cybersecurity, including Bill C-26.

- Monitor industry cybersecurity intelligence (as appropriate and reasonable for this level of participation), trends, incidents and other related cybersecurity issues and identify improvement opportunities.

- Liaise as required with other organizations involved in the promotion of cybersecurity and threat assessment / risk management in the industry, including AAR.

Officers

There shall be a Chair and Vice-Chair, elected by the Cybersecurity Committee from its membership. Their terms of office shall normally be of two years, which can be renewed. It is recommended that these officers represent freight and passenger interests respectively.

An officer from the RAC will be appointed to the Cybersecurity Committee as a member and will assist in the management of the Cybersecurity Committee's activities and act as the Secretary.

Duties of Officers

The Chair shall be responsible for the general supervision of the affairs of the Cybersecurity Committee, preside at meetings and be empowered to call special meetings as conditions warrant. The Chair will act as the Cybersecurity Committee spokesperson to SOMC. The Vice-Chair shall perform duties of the Chair whenever the Chair is unable to perform the duties of his/her office.

The Secretary will record the events of the proceedings including but not limited to discussion topics, resolutions, action items and responsibilities. The Secretary will draft minutes of the meeting and forward them to the Chair for approval/distribution within 21 calendar days.

Membership

Membership is open to the RAC, RAC member companies, and the AAR. Persons shall be nominated by their respective companies and shall serve until the person notifies the Chair of his/her resignation. Membership will be of special interest to those with responsibilities in the function of corporate cybersecurity, regulatory affairs, railway operations and risk management.

A member who is unable to attend a meeting, should send a representative who shall be counted in determining a quorum and be permitted to vote in place of the regular member.

Decisions will be made on a consensus basis with recommendations being made to the Security Committee that reflect this consensus.

Meetings

The Cybersecurity Committee shall meet on an quarterly basis or on a schedule to be determined by the committee. Special meetings may be called in response to significant developments. Meetings may be held by telephone, video conference or any other means allowing people to communicate and make decisions on a real time basis, at the discretion of the members.

Quorum

The quorum at meetings of the Cybersecurity Committee is five members. One member should be from CN, and one from CPKC. The following three railway categories should also be represented: passenger (intercity, commuter or tourist), shortline and US carrier. A RAC or an AAR member can be considered as a railway member in the shortline or US carrier categories for quorum purposes.

Reporting Authority

The Cybersecurity Committee will report to the SOMC. The Cybersecurity Committee will liaise with other RAC committees and working groups on matters which are of mutual interest.

Railway Association of Canada

Cyber Security Committee

Hazen, Vaughn — **Chair**
Assistant Vice-President and Chief Information Security Officer
CN
(514) 399 4953
Vaughn.Hazen@cn.ca

Dewar, Janna — **Vice Chair**
Senior Manager, Cybersecurity
VIA Rail Canada Inc.
Janna_Dewar@viarail.ca

Borhani, Alex
Sr. Director and Deputy CISO
CSX Corporation
Alex_Borhani@csx.com

Chung, Mike
Managing Director, Enterprise Security
CPKC
(913) 449 9427
Michael.Chung@cpkcr.com

De Benetti, Enzo
Consultant, RAC Spectrum & Telecommunications
Railway Association of Canada
(438) 455 7236
edebenetti@railcan.ca

Gill, Jessie
Manager, Systems Technical Services
West Coast Express Ltd.
(778) 879 2107
JESSIE_GILL@BCRTC.BC.CA

He, Biying
Director - IT Security,Risk, Compliance & Resilience
West Coast Express Ltd.
Biying.He@translink.ca

Railway Association of Canada

Hislop, Rick
IT Security Manager
Great Canadian Railtour Company Ltd.
(604) 606 7200
rhislop@rockymountaineer.com

McLeod, Adrian
Senior Communication and Security Engineer
Ontario Northland Transportation Commission
(705) 472 4500
Adrian.McLeod@ontarionorthland.ca

Du Perron, François
Lead Advisor, Cybersecurity and Networks - CFR
VIA Rail Canada Inc.
(514) 871 6201
Francois_DuPerron@viarail.ca

Singh, Malwinder
Security Operations Specialist
CPKC
(403) 888 8388
Malwinder.Singh@cpkcr.com

St.John, Janet
Director, Cybersecurity
Association of American Railroads
(202) 639 2221
jstjohn@aar.org

Sukhera, Fawad
Security Analyst, Security Operation Center | I&T
CN
(514) 399 8245
Fawad.Sukhera@cn.ca

Sul, Douglas
Senior Manager, Operational Technology
CPKC
(204) 218 8826
Douglas.Sul@cpkcr.com