DOI: 10.22034/ISJ.2024.387080.1977

International Studies Journal (ISJ)
Vol. 21, No. 1 (81), Summer 2024
Reseived Date: 2024/1/13
Accept Date: 2024/6/19
Article Type: Original Research
PP: 187-204

فصلنامه مطالعات بین‌المللی
سال ۲۱، شماره ۱ (۸۱)، تابستان ۱۴۰۳
تاریخ دریافت: ۱۴۰۲/۱۰/۲۳
تاریخ پذیرش: ۱۴۰۳/۳/۳۰
نوع مقاله: علمی- پژوهشی
صفحات: ۲۰۴-۱۸۷

بررسی نارسایی‌های دولت آمریکا در مواجهه با تروریسم صنعتی

دکتر داود جعفری* - دکتر مهران خلج** - دکتر پژمان صالحی***

چکیده

مطالعه شواهد و یافته‌های به دست آمده از تحقیقات صورت‌گرفته نشان می دهد یکی از وجوه تروریسم با حمله به زیرساخت‌های صنعتی، تأثیرات منفی و مخربی بر رونق اقتصادی یک کشور دارد. بنابراین هدف اصلی تحقیق حاضر بررسی میزان توفیق دولت آمریکا در کنترل اثرات تروریسم بر اقدامات صنعتی در مطالعه موردی شرکت راه‌آهن آمریکایی است و لذا مطالعه حاضر تروریسم را از منظر تأثیر بر فعالیت های صنعتی مورد بررسی قرار داده و می کوشد به صورت نظام مند به پاسخ این پرسش بپردازد که آیا دولت آمریکا در موجهه با تروریسم صنعتی موفق بوده است؟ فرضیه تحقیق حاضر به صورت شهودی بیان می دارد که دولت آمریکا در مواجهه با تروریسم صنعتی دارای نارسایی است و از این رو برای آزمون فرض بر شرکت «امترک » (شرکت راه‌آهن آمریکایی) تمرکز شده است. این پژوهش با استفاده از روش تحلیل محتوا ضمن بررسی نظام مند و تعمیم پذیر تروریسم صنعتی در آمریکا به تبیین نارسایی های دولت در مواجهه با تبعات آن پرداخته است. برخی نتایج این مطالعه نشان می دهد ارزش اقتصادی صنایع مادر و اقدامات کنترلی دولت آمریکا برای حفاظت از این صنایع ارتباط مستقیمی با تروریسم صنعتی دارد و در نهایت پیامدهای تروریسم صنعتی برای برخی صنایع مادر آمریکایی نظیر راه آهن به بی ثباتی سیاسی، کاهش سرمایه های اجتماعی و اعتماد عمومی منجر گردیده است.

کلیدواژگان

دولت آمریکا، تروریسم صنعتی، صنایع حیاتی و مادر

* استادیار عضو هیأت علمی گروه مهندسی صنایع آموزشی، دانشکده مهندسی صنایع، واحد پرند، دانشگاه آزاد اسلامی، پرند، ایران.

** استادیار عضو هیأت علمی گروه مهندسی صنایع آموزشی، دانشکده مهندسی صنایع، واحد پرند، دانشگاه آزاد اسلامی، پرند، ایران./ نویسنده مسئول/ ایمیل: mkhalaj@rkiau.ac

*** دانش‌آموخته دکتری تخصصی مهندسی صنایع، واحد پرند، دانشگاه آزاد اسلامی، پرند، ایران.

Article Link: https://www.isjq.ir/article_199871.html

مقدمه

دامنهٔ اقدامات و ارزیابی‌های امنیتی، حفاظت از زیرساخت‌های حیاتی و شریان‌های مهم اطلاعاتی یک کشور در برابر ریسک‌های طبیعی، حملات برنامه‌ریزی‌شده و تروریسم را برمی‌گیرد به‌طوری‌که از طریق مدیریت و نظارت بر تهدیدها، امکان مواجهه با حملات فیزیکی و سایبری در سطح صنایع مادر فراهم شود (Banks and Barclay, 2006). از منظر حاکمیتی، تروریسم صنعتی اصطلاحاً به انواع حملات و خشونت‌های برنامه‌ریزی‌شده توسط گروه‌های خاص با هدف تحت‌تأثیر قراردادن مقاصد صنعتی، تجاری و حیاتی صورت می‌گیرد که می‌تواند زیرساخت‌های حساس صنعتی یک کشور را دچار اشکال نماید (Vanderau and Haakinson, 2009). باتوجه‌به جذابیت سفرهای ریلی و مقرون‌به‌صرفه بودن آن از منظر هزینه و مصرف انرژی از یک‌سو، و روند فزایندهٔ تقاضا برای استفاده از خدمات شبکه ریلی؛ ازدحام ناوگان قطارها و ایستگاه‌ها اجتناب‌ناپذیر شده است و این خود مقصد وسوسه‌انگیزی برای گروه‌های تروریستی و نفوذگران صنعتی محسوب می‌شود (Bergen and Hoffman, 2015). باتوجه‌به افزایش ۱۰ درصدی تقاضا برای حمل بار و مسافر در شبکه ریلی سرتاسری آمریکا و نیز حفره‌های امنیتی متعدد آن، مانند قابلیت دسترسی آسان و آسیب‌پذیری ایستگاه‌ها و خطوط ریلی، انجام سرمایه‌گذاری‌های گسترده در شبکه ریلی برای دولت آمریکا به‌ویژه در حوزه فناوری‌های اخیر ریلی را از ضرورت بالایی برخوردار نموده و این در حالی است که علی‌رغم توصیه کارشناسان امنیتی، میزان سرمایه‌گذاری برای ارتقای امنیت‌بخش حمل‌ونقل ریلی در مقابل شبکه حمل‌ونقل هوایی این کشور بسیار ناچیز بوده و این خود نشان از ضعف سیاست‌های حمایتی دولت آمریکا برای حفظ امنیت زیرساخت‌های حیاتی این کشور است (Slovic, 2012).

حال باتوجه‌به آنکه اغلب حملات موفق تروریستی به زیرساخت‌های حیاتی توسط مهاجمان تقلید می‌شود؛ ازاین‌رو موفقیت‌های گذشتهٔ تروریست‌ها، احتمال انجام حملات آینده را افزایش می‌دهد؛ زیرا آنان می‌آموزند که از حفره‌های امنیتی و آسیب‌پذیری‌های زیرساخت‌های صنعتی چگونه برای رسیدن به مقاصد خود استفاده نمایند (Turégano et al., 2018). از منظر امنیت ملی بیش از ۳۰ هزار مایل از شبکه ریلی سرتاسری آمریکا دارای موقعیت استراتژیک بوده و تحت نظارت وزارت دفاع این کشور است؛ زیرا از آن برای جابه‌جایی و حمل مهمات، تسلیحات نظامی و سایر محموله‌های دفاعی استفاده می‌شود که مقدار آن بالغ‌بر ۱/۸ میلیون تُن کالاهای خطرناک (مواد منفجره، مواد شیمیایی سمی، گازها و مایعات مورداستفاده در کارخانجات مهمات‌سازی و غیره) در طول یک سال است و لذا در صورت بروز هر حادثه خرابکارانه، تبعات جدی و خطرناکی را برای محیط‌زیست و شهروندان ایجاد می‌شود و این خود نشان‌دهنده اهمیت و حساسیت شبکه راه‌آهن سرتاسری از منظر ژئوپلیتیک برای دولت آمریکا است (Strandh, 2020).

بنا بر آنچه در فوق ذکر گردید و باتوجه‌به پراکندگی جغرافیایی زیرساخت‌های ریلی آمریکا و سهولت دسترس‌پذیری آن توسط مهاجمان و آسیب‌پذیری آن را در برابر خرابکاری‌های برنامه‌ریزی‌شده، هدف اصلی تحقیق حاضر بررسی نارسایی‌های دولت آمریکا برای حفظ

زیرساخت‌های حیاتی در برابر بحران‌های امنیتی در مطالعه موردی شبکه ریلی سرتاسری آمریکا است. از این رو پرسش اصلی تحقیق حاضر آن است که چه نارسایی‌هایی برای مواجهه با تروریسم صنعتی فراروی دولت آمریکا است؟

۱- پیشینه تحقیق

در مطالعه‌ای که توسط استراند (۲۰۲۰) انجام‌شده، محقق ضمن بررسی میزان آسیب‌پذیری‌های امنیتی حوزه ترافیک در شبکه ریلی به ارزیابی میزان آمادگی زیرساخت‌های نرم‌افزاری و سخت‌افزاری شبکه ریلی در برابر حملات تروریستی پرداخته است. یافته‌های این مطالعه نشان می‌دهد ارزیابی امنیتی[1] و تست نفوذ[2] ضریب امنیت شبکه ریلی را در برابر تهاجمات احتمالی نفوذگران افزایش می‌دهد.

در پژوهشی که توسط اورتیز آلونسو و همکاران (۲۰۱۸) انجام‌شده، محققان در مطالعه موردی بمب‌گذاری تروریستی قطارهای مادرید، ضمن بیان تبیین جزئیات امنیتی این تهاجم، به ارزیابی میزان ترومای مسافری و ریشه‌یابی علل بروز فاجعه انسانی در این حادثه پرداخته‌اند. یافته‌های این مطالعه نشان می‌دهد در ازدحام مسافری بالا و سرفاصله پایین حرکت قطارها[3] احتمال مرگ‌ومیر عامل انسانی به‌شدت افزایش می‌یابد.

در تحقیقی که توسط استرندبرگ (۲۰۱۶) انجام‌شده، محقق با تبیین ابعاد و عوامل ساختاری ترافیک سیر و حرکت قطارها به بیان اهداف و مقاصد حملات تروریستی در شبکه ریلی پرداخته است. یافته‌های این مطالعه نشان می‌دهد اقدامات پیشگیرانه در مرحله مهندسی نیازها می‌تواند زیرساخت‌های شبکه حمل‌ونقل را در برابر حملات نفوذگران و مهاجمان مقاوم نماید.

در مطالعه‌ای که توسط کیسان (۲۰۱۷) با عنوان «وحشت در قطارهای پرسرعت فرانسه» انجام‌شده است، محقق ضمن بررسی جامع حادثه تروریستی قطار سریع‌السیر فرانسه به تبیین ابعاد تهدیدهای تروریستی در قطارهای پرسرعت پرداخته و با بیان چالش‌های امنیتی شبکه ریلی، روندهای آینده در حملات تروریستی را بررسی نموده است. در مطالعه‌ای که توسط مائوریلو (۲۰۱۵)

در مطالعه موردی راه‌آهن پرسرعت آمریکا انجام‌شده است محقق به تبیین جاذبه‌های مرتبط با قطارهای بین‌شهری آمریکا برای مهاجمان پرداخته است. یافته‌های این تحقیق نشان می‌دهد حمل‌ونقل انبوه مسافران و نبود نظارت‌های امنیتی از عوامل مهم ایجاد زمینه برای حملات تروریستی به شمار می‌رود.

در تحقیقی که توسط اورتیز و همکاران (۲۰۱۱) انجام شد محققان ضمن بررسی ایمنی و امنیت شبکه حمل‌ونقل ریلی بار و مسافر در ایالت پنسیلوانیا به بیان شیوه‌های بهبود و ارتقای سطح امنیت در برابر ریسک‌های احتمالی و حملات مهاجمان با تأکید بر استراتژی‌های امنیتی پرداخته‌اند.

---

[1]. Security Assessment

[2]. Penetration Test

[3]. Headway

یافته‌های این پژوهش نشان می‌دهد که تدوین نقشه‌های امنیتی و ایمنی می‌تواند نقش مؤثری در کاهش جرائم و حملات تروریستی داشته باشد.

در تحقیقی که توسط پلانت و همکاران (۲۰۱۰) در دانشگاه ایالتی پنسیلوانیا با عنوان امنیت و حفاظت از سامانه‌های ریلی در راه‌آهن سرتاسری آمریکا انجام‌شده، محققان در مطالعه موردی راه‌آهن ایالت هریسبورگ به تبیین تهدیدهای امنیتی و ریسک‌های تروریستی مرتبط با شبکه ریلی پرداخته‌اند. یافته‌های این مطالعه نشان می‌دهد رعایت اصول محرمانگی، جامعیت و یکپارچگی می‌تواند ضریب امنیت راه سرتاسری را افزایش دهد.

همان گونه که در بررسی پیشینه پژوهش مشاهده می‌شود مطالعات فوق‌الذکر ابعاد مختلف حملات تروریستی در شبکه ریلی را مورد بررسی قرار داده‌اند. بااین‌حال در هیچ‌یک از تحقیقات صورت‌گرفته، نارسایی‌های مرتبط با زیرساخت‌های حیاتی به طور خاص از منظر امنیتی موردمطالعه قرار نگرفته است؛ لذا ازاین‌جهت تحقیق حاضر می‌تواند دارای نوآوری باشد.

۲- چارچوب مفهومی

مطالعه حاضر براین‌اساس شکل‌گرفته که علی‌رغم آگاهی دولت آمریکا از میزان حساسیت شبکه ریلی و تأثیر تبعات ناامنی در آن بر اقتصاد این کشور و اقدامات وسیع دولت آمریکا برای حفاظت از حمل‌ونقل بار و مسافر در شبکه ریلی؛ دامنه این فعالیت‌ها برای کاهش ریسک‌ها به انجام مانورها و پیاده‌سازی برخی تکنولوژی‌های امنیتی محدود بوده که برای یک مهاجم مصمم باتوجه‌به شکاف‌های امنیتی و آسیب‌پذیری‌های موجود در شبکه ریلی آمریکا، فاقد اثربخشی کافی بوده و به‌راحتی می‌تواند آن را با تبعات سوء و فاجعه‌بار یک نفوذ جدی روبرو نماید (Berrick and Hecker,2006). نتایج مطالعات نشان می‌دهد که گستره آسیب‌پذیری‌های مرتبط با زیرساخت‌های ریلی در آمریکا تنها در دو بخش فیزیکی و ارتباطی خلاصه نمی‌شود، بلکه سرتاسر سیستم، کارکنان و مشتریانی که از آن استفاده می‌نمایند را در معرض سطح بالایی از ریسک‌های بالقوه قرار داده است (Vanderau and Haakinson ,2009).

۲-۱- زیرساخت‌های حیاتی

یکی از ارکان مهم در ایفای نقش و انجام کارکردهای اجتماعی و اقتصادی دولت‌ها به زیرساخت‌های حیاتی آن کشورها بازمی‌گردد. زیرساخت‌های حیاتی به آن دسته از تسهیلات حساس یک کشور اطلاق می‌گردد که تداوم خدمات عمومی را امکان‌پذیر می‌سازد (Turégano-Fuentes and et al., 2018). زیرساخت‌های حیاتی در یک کشور دارای ابعاد نرم‌افزاری و سخت‌افزاری است که ضمن ارائه مزایای عمومی دارای مخاطراتی نیز هست و می‌تواند در فضای عدم‌قطعیت جامعه را با تهدیدهای متعدد مواجه سازد. به‌عنوان‌مثال قطع راه‌های مواصلاتی در نظام حمل‌ونقل یک کشور از طریق حملات فیزیکی یا سایبری می‌تواند سبب ایجاد اختلال در جابه‌جایی بار و مسافر در بخش‌های مختلف یک کشور می‌گردد (Strandh, 2020).

۲-۲- بحران‌های امنیتی

امنیت یکی از اصول مهمی است که همواره در مطالعات بین‌الملل مدنظر سیاستمداران قرار می‌گیرد. از منظر لغت‌شناسی امنیت عبارت است از سطح آمادگی یک کشور برای رویارویی با مخاطراتی که زیرساخت‌های حیاتی آن کشور را در معرض خطر قرار می‌دهد. بحران‌های امنیتی در حوزه زیرساخت‌ها به وضعیت‌های مخاطره‌آمیز و ناپایداری اطلاق می‌گردد که می‌تواند سبب بروز تهدیدها و مخاطرات جدیدی برای تداوم کارکردهای این حوزه گردد که در نتیجه رفع آن به اقدامات فوق‌العاده و اساسی نیاز دارد (Chittester and Haimes, 2014).

۳- تاریخچه موضوع

شبکه راه‌آهن سرتاسری آمریکا به‌عنوان اصلی‌ترین زیرساخت در حمل‌ونقل بار و مسافر آمریکا در سال ۱۸۲۷ با افتتاح نخستین خط ریلی میان بالتیمور و اوهایو به طول ۱۳ مایل در امتداد رودخانه پاتاپسکو تا سواحل الیکات میلز برای ترابری بار و کالا به بهره‌برداری رسید و مسیر رشد و توسعه خود را پیمود. در سیر تاریخی توسعه راه‌آهن آمریکا، به‌روزآوری تجهیزات، استقرار تسهیلات فنی و رشد سرعت سیر و حرکت قطارها و افزایش ظرفیت متناسب با تقاضا مدنظر بوده است (Hartong and Wijesekera, 2016).

روند توسعه تکنولوژی‌های ریلی در این کشور تا آنجا بوده که امروزه لوکوموتیوهای الکتریکی مدرن قادرند تا بیش از ۱۰۰ واگن باری با وزن بالغ‌بر ۲۸۶۰۰۰ پوند را با سرعت ۶۰ مایل بر ساعت در فرازهای دشوار با مختصات بیش از ۶ در هر هزار متر بکشند. قطارهای مسافری مدرن نیز در این کشور می‌توانند به طور متوسط ۲۶۰ مسافر را با لحاظ پارامتر راحتی مسافر و مطلوبیت سفر جابه‌جا نمایند (Plant and Young, 2010).

بااین‌حال به اذعان مراجع حاکمیتی و نتایج مطالعات پیشین، توسعه مؤلفه‌های امنیتی برای حفظ زیرساخت‌های شبکه ریلی در برابر تهاجمات احتمالی نفوذگران، متوازن و متناسب با افزایش ظرفیت و سرعت و ارتقای فناوری نوین نبوده است؛ بنابراین مسئله امنیت زیرساخت‌ها، به‌دفعات شبکه ریلی سرتاسری آمریکا را با بحران جدی مواجه ساخته به‌طوری‌که علاوه بر ایجاد نارضایتی و موج گستردهٔ انتقادات رسانه‌ای از روش‌های فعلی مدیریت و پیشگیری بحران، تبعات قابل‌توجهی را در اقتصاد و حمل‌ونقل این کشور بر جای نهاده است (Markoff, 2013).

همان گونه که در تصویر شماره یک مشاهده می‌شود راه‌آهن سرتاسری، ترابری تمامی جنبه‌های مرتبط با صنایع حیاتی و مادر را در آمریکا پوشش می‌دهد. همچنین راه‌آهن سرتاسری آمریکا به طول یک‌صد و چهل هزار مایل تقریباً تمامی بخش‌های مختلف این کشور را به‌غیراز ایالت هاوایی به یکدیگر متصل می‌نماید. این مهم در تصویر شماره یک نشان‌داده‌شده است (Orr et al., 2011).

تصویر ۱- مسیرهای مواصلاتی شبکه ریلی سرتاسری آمریکا

Figure No 1. The Transportation Routes of the United States Rail Network

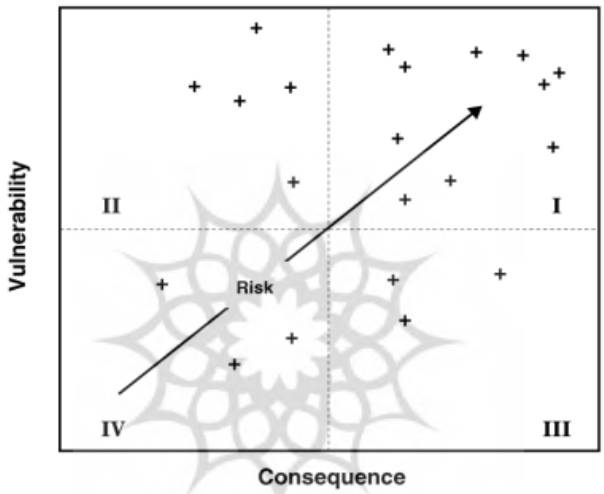
source: (Orr et al., 2011)

٤- روش‌شناسی پژوهش

تحقیق حاضر به روش تحلیل محتوا انجام‌شده است. در این پژوهش به‌منظور بررسی میزان تاب‌آوری زیرساخت‌های حیاتی آمریکا از منظر نقاط قوت و نارسایی‌ها، پنج مقوله کلی در نظر گرفته‌شده است. هر یک از این مقوله‌ها، یک بعد از کاربردهای امنیت در زیرساخت‌های حیاتی شبکه ریلی را مطرح می‌سازند. موارد مربوط به هر مقوله در مستندات و محتوای امنیتی مربوط به زیرساخت‌های ریلی آمریکا شمارش و به‌منظور مقایسه ثبت‌شده است. مقوله‌های مورد بررسی عبارت است از: ۱ ارائه دانش و اطلاعات در خصوص وضع موجود زیرساخت‌های ریلی آمریکا و به‌تصویرکشیدن واقعیت‌های غیرقابل‌رؤیت ۲ مطالعه نقاط ضعف و نارسایی‌های مرتبط با زیرساخت‌ها ۳ نمایش چگونگی کارکرد دفاعی سیستم و نفوذگران ۴ سازمان‌دهی، تلخیص و ترکیب اطلاعات ۵ جمع‌بندی تجارب.

جامعه آماری در این پژوهش عبارت بودند از اسناد، گزارش‌ها و متون امنیتی و دفاع سایبری ۱۵ سال اخیر آمریکا در حوزه زیرساخت‌های ریلی که به دلیل حجم زیاد اسناد و مدارک تنها بخش‌های مرتبط با امنیت زیرساخت‌ها (ناوگان، ایستگاه‌ها و خطوط ریلی) انتخاب شد؛ بنابراین مباحث امنیتی مطرح‌شده در اسناد، مدارک و گزارش‌ها تنها مربوط به بخش‌های ذکرشده می‌باشد. ازاین‌رو محققان برای بررسی دقیق یکی از مباحث مشترک امنیتی در اسناد و مدارک باتوجه‌به دردسترس‌بودن، منابع مرتبط را به‌عنوان نمونه انتخاب کردند؛ لذا نمونه آماری این تحقیق را مباحث امنیت تدافعی زیرساخت‌های ریلی در اسناد امنیتی آمریکا (جمعاً ۱۵۰ سند) تشکیل دادند. در این

اسناد وضعیت برنامه‌ریزی دولت آمریکا برای امنیت کریدورهای ریلی، پیشینه حملات صورت‌گرفته به سطوح مختلف حمل‌ونقل ریلی، انواع فرایندهای موجود امنیتی، روندهای مورد انتظار در حملات آینده و سایر مسائل مرتبط ذکر گردیده است. برخی از این ۱۵۰ سند شناسایی‌شده برای تحقیق حاضر نظیر مقالات خبری، تفسیرها و مقالات موجود در وبلاگ‌ها به‌طورکلی به مقوله امنیت در صنعت حمل‌ونقل ریلی آمریکا پرداخته و دربرگیرنده سیاست‌های امنیتی مربوطه نبوده است. تصویر شماره دو افزایش میزان آسیب‌پذیری زیرساخت‌های ریلی آمریکا باتوجه‌به افزایش وسعت و ازدحام شبکه ریلی در برابر حملات تروریستی را بر اساس تحلیل اسناد توسط محققان نشان می‌دهد.



تصویر ۲- افزایش میزان آسیب‌پذیری زیرساخت‌های ریلی آمریکا باتوجه‌به افزایش وسعت و ازدحام شبکه ریلی در برابر حملات تروریستی

Figure No 2. The Increase in the Vulnerability of the US Rail Infrastructure Due to the Rise in the Size and Congestion of the Rail Network Against Terrorist Attacks

Source: (Document Analysis by Authors, 2023)؛(منبع: تحلیل اسناد توسط نگارندگان، ۱۴۰۲)

۵- یافته‌ها

یکی از رویدادهای نامطلوب در بخش ارائه خدمات شبکه ریلی که می‌تواند دارای تبعات اقتصادی و اجتماعی قابل‌توجهی باشد؛ حملات فیزیکی و سایبری برنامه‌ریزی‌شده در بخش‌های ترافیکی و فیزیکی شبکه ریلی است. به‌عنوان یک نمونه می‌توان به اختلال برنامه‌ریزی‌شده سال ۱۹۹۸ که در اثر تهاجم نفوذگران سبب بروز اغتشاش گسترده در خدمات بخشی از شبکه ریلی منتهی به ایالت تگزاس گردید، اشاره نمود که خسارت مستقیم آن بالغ‌بر یک میلیارد دلار ارزیابی شد و علاوه بر خسارت مستقیم، خسارت غیرمستقیمی در حدود ۶۴۳ میلیون دلار برای ذی‌نفعان و مشتریان به همراه داشت (Hartong et al., 2013). نمونه دیگری از تهاجم خرابکارانه نفوذگران به

زیرساخت‌های ریلی آمریکا در ۲۱ اوت سال ۲۰۰۳ رخ داد که در اثر آن تمامی حرکت‌ها و اعزام‌های باری و مسافری در امتداد سواحل شرقی آمریکا به مدت ۲۴ ساعت لغو شد. گزارش‌های نهایی مرتبط با این حادثه نشان از ورود یک ویروس به سامانه‌های رایانه‌ای کنترل و اعزام قطارها داشت که توانسته بود همه آن‌ها را از کار بیندازد (Maurillo, 2015).

یافته‌های به‌دست‌آمده از مستندات نشان می‌دهد که تبعات ناشی از اختلالات عمدی در شبکه ریلی گاه می‌تواند فراتر از آثار اقتصادی باشد. به‌عنوان یک نمونه دیگر حمله به قطارهای حاوی محموله‌های نظامی می‌تواند سلامت شهروندان را از طریق انتشار مواد شیمیایی و خطرناک در محیط پیرامون خطوط ریلی در معرض خطر قرار دهد؛ لذا حمل کالاهای نظامی به طور بالقوه با نوعی ریسک بسیار بالا برای شهروندان توأم است (Jeong et al., 2016). به‌عنوان‌مثال دیگر می‌توان به عبور سالانه ۸۵۰۰ واگن حامل کلر و سایر مواد شیمیایی از طریق شبکه ریلی که در انحصار وزارت دفاع آمریکا است، اشاره نمود، این محموله‌ها از نزدیکی شهر واشنگتن‌دی‌سی عبور می‌کند و بر اساس یک سناریوی بدبینانه در صورت واژگون شدن واگن‌ها و خروج قطار از ریل، تنها در یک حرکت باری، محتویات یک قطار ۹۰ تنی حامل مواد شیمیایی می‌تواند تا مرکز شهر واشنگتن را آلوده نموده و بر اساس برآوردها می‌تواند تا حدود یک‌صد هزار کشته و مصدوم بجای گذارد (Chittester et al., 201).

۵-۱- نارسایی‌های امنیتی و آسیب‌پذیری زیرساخت‌های ریلی در شبکه ریلی آمریکا در برابر حملات خرابکارانه و تروریستی

همان گونه که پیش‌تر نیز ذکر گردید تعدد ریسک‌های امنیتی و آسیب‌پذیری‌های بالقوه در شبکه ریلی آمریکا ضرورت حفاظت از آن را به‌عنوان یک اقدام پیشگیرانه امنیتی ضروری می‌سازد. دراین‌بین تهدیدهای امنیتی و حملات مخرب عمدتاً زیرساخت‌های فیزیکی و شبکه‌های ارتباطی و نرم‌افزاری را در حمل‌ونقل ریلی هدف قرار می‌دهد (Wilson, 2017). در سال ۲۰۱۵ پایگاه‌داده RAND CORP، فهرستی از حوادث تروریستی را در جهان منتشر نمود. در این گزارش بیش از ۲۵۰ حمله تروریستی موفق علیه زیرساخت‌های ریلی آمریکا برای بازه زمانی ۱۹۹۵ تا ۲۰۱۵ به ثبت رسیده که گویای آسیب‌پذیری زیرساخت‌های ریلی آمریکا در برابر حملات تروریستی از منظر امنیتی است (Strandh, 2018). بنابراین باتوجه‌به ماهیت تهدیدهای امنیتی، مطالعه و بحث در خصوص نقاط آسیب‌پذیری برای زیرساخت‌های حیاتی یک کشور، مقوله‌ای کلی و جهان‌شمول است که از صنعتی به صنعت دیگر متفاوت می‌باشد؛ لذا ارائه یک الگوی دقیق که دربردارندهٔ تمامی جزئیات حفاظتی - امنیتی برای صنایع مادر در یک کشور باشد، قدری دور از دسترس به نظر می‌رسد. ازاین‌رو شناسایی تهدیدهای امنیتی برای آن دسته از صنایعی که در حوزه تهاجمات امنیتی دارای پیشینه‌ای از حادثه نیستند، انجام تحلیل‌های امنیتی دشوار است.

۵-۲- نارسایی‌های امنیتی و آسیب‌پذیری مسیر حرکتی قطارها در شبکه ریلی آمریکا در برابر اقدامات خرابکارانه و تروریستی

اتصالات سازه‌های مسیر ریلی به‌گونه‌ای طراحی‌شده تا بتواند بارهای استاتیک و دینامیک ناشی از

حرکت قطارها را به‌خوبی مهار نموده و درعین‌حال با زهکشی مسیر ریلی امکان خارج نمودن آب‌های اضافی زیرزمینی، سطحی و رواناب‌ها را میسر ساخته و شیب عرضی خطوط ریلی را در ارتفاع تراز و مناسب نگاه دارد. در این سازه تراورس‌ها نیز نیروهای عمودی را به طور همسان بین بالاست ها توزیع و میرا نموده و عرض خط دقیقی را برای حرکت قطار و جلوگیری از خروج آن از خط‌آهن فراهم می‌نماید (JenkinsM et al., 2010).

بااین‌حال هرگونه آسیب خرابکارانهٔ عمدی یا غیرعمدی به این تأسیسات و تسهیلات سبب خروج قطار از ریل شده و بازگرداندن آن به خط مستلزم صرف زمان و هزینه فراوان است که از آن جمله می‌توان به ایجاد وقفه در سیر و حرکت قطارهای شبکه ریلی، آسیب به فلنچ چرخ و یا تجهیزات لوکوموتیو و غیره... اشاره نمود. آنچه از بررسی روسازی و زیرسازی مسیر ریلی در راه‌آهن سرتاسری آمریکا به دست می‌آید آن است که حمله نفوذگران و آسیب به سازه‌های خط‌آهن با کمترین تلاش از سوی مهاجمان امکان‌پذیر می‌شود. ساده‌ترین نوع تهاجم به ساختار خطوط آهن آمریکا، باز کردن و برداشتن پیچ‌های پابند ریل حرکتی است که مهم‌ترین تبعه سوء آن برهم‌خوردن شیب عرضی خط و درنتیجه خروج قطار از ریل است. یک حمله ساده دیگر که معمولاً برای مهاجمان طعمه جذابی به شمار می‌آید، ایجاد اختلال در مکانیسم‌های ایمنی و منحرف‌کردن قطار از مسیر حرکتی آن در ریل اصلی است که گاه درنتیجه انحراف از برنامه زمان‌بندی از قبل تعیین‌شده و در اماکن خاص نظیر سوزن‌ها رخ می‌دهد. از دیگر ملزومات ریلی، سوئیچ‌های سوزن در خط‌آهن است که یکی دیگر از راه‌های نفوذ و حمله به شبکه ریلی می‌باشد. سوئیچ‌ها در شبکه ریلی آمریکا، غالباً دارای مکانیسم تغییر وضعیت دستی هستند که امکان تغییر مسیر حرکتی قطار را فراهم می‌نماید.

مکانیسم‌های حفاظتی در نظر گرفته‌شده توسط دپارتمان امنیت وزارت حمل‌ونقل آمریکا، استفاده از قفل‌های مستحکم برای سوئیچ‌های دستی است که بر اساس شواهد آماری و کتب سوانح منتشرشده توسط وزارت حمل‌ونقل، این قفل‌ها به‌راحتی توسط مهاجمان شکسته شده و درنتیجه با ورود قطار دارای سرعت به خط حرکتی دیگر امکان تصادف و یا خروج از ریل را به وجود می‌آورد. از طرفی حملات مهاجمان به شبکه ریلی در تونل‌ها، پل‌ها و یا تقاطع‌های غیرهمسطح و مرتفع، مستلزم صرف انرژی و کوشش مضاعفی از سوی مهاجم است و توفیق حمله مستلزم استفاده از مواد منفجره یا سوخت‌های آتش‌زا می‌باشد به‌استثنای حالتی که در آن مهاجمان عملیات تخریبی را هم‌زمان در قطار و پل و یا قطار و تونل انجام دهند، در این صورت علاوه بر انهدام قطار و آسیب جانی به مسافران و خدمه، سازه‌های پل و یا تونل نیز تخریب می‌گردد. مطالعه پیشینه حملات صورت‌گرفته به شبکه ریلی آمریکا نشان می‌دهد در تونل‌های ریلی، فروریختن بخشی از تونل توسط مهاجمان و یا تخریب قسمتی از سازه پل توسط آن‌ها می‌تواند به خطوط ریلی آسیب‌زده و مسیر اعزام قطار را مسدود نماید. همچنین استفاده از مواد قابل‌اشتعال در ساختمان پل‌های راه‌آهن آمریکا، سازه‌های پل را بسیار آسیب‌پذیر نموده تا آنجا که مهاجمان به‌راحتی، با کمترین هزینه و با استفاده از وسایل آتش‌زا، مقاصد خود را اجرایی می‌نمایند. بهره‌گیری از ضعف‌های موجود در

هندسه مسیر ریلی به‌خصوص در قوس‌ها که بار استاتیک و دینامیک قطار به بیشینه مقدار خود می‌رسد از دیگر نقاط آسیب‌زا برای تخریب مسیر ریلی این کشور است به‌طوری‌که مهاجمان با ایجاد حداقل تغییر در عرض شیب‌خط (دور) این مکان‌های هندسی، می‌توانند قطار را از خط خارج نموده و سبب اختلال در ترافیک سیر و حَرکت قطارها شود.

۵-۳- نارسایی‌های امنیتی و آسیب‌پذیری سامانه‌های سیگنالینگ در شبکه ریلی آمریکا در برابر اقدامات خرابکارانه و تروریستی

یکی از حساس‌ترین سامانه‌های راه‌آهن سرتاسری آمریکا که در برابر حملات مهاجمان و نفوذگران بسیار آسیب‌پذیر است، سامانه سیگنالینگ می‌باشد. هدف از استقرار سامانه سیگنالینگ انتقال دقیق و به هنگام داده‌های قابل‌اطمینان در خصوص وضعیت قطارها جلویی به راهبر قطار و کنترل سیر و حرکت آن برای حفظ فاصله ایمنی میان قطارها در خطوط شبکه ریلی است. در سامانه سیگنالینگ هر رنگ به‌عنوان یک علامت ویژه برای راهبر قطار و مجموعه کنترل خط ریلی محسوب می‌شود که می‌تواند دلیلی بر اشغال بودن مسیر پیش روی، مجوز حرکت و یا تغییر مسیر برای قطار محسوب گردد. در سامانه سیگنالینگ همچنین محدودیت‌های مربوط به حداکثر سرعت و سقف سرعت مجاز به راهبر قطار اعلام می‌گردد که این مهم شامل واگن‌های حاوی محموله‌های نظامی نمی‌شود. ابعاد سامانه سیگنالینگ از طریق زیرسیستم سیگنالینگ کابین مستقیماً به لوکوموتیوران نمایش داده می‌شود (Jeongg et al., 2011).

بااین‌حال اجرای تهاجم و نفوذ به سامانه‌های سیگنالینگ دشوارتر از اجرای حمله برای تخریب سایر زیرساخت‌های ریلی است. در یک تهاجم موفق، مهاجمان به‌طور عمده دو اقدام مخرب را در سامانه‌های سیگنالینگ پیاده‌سازی می‌نمایند. نخست: بر هم زدن منطق سیستم‌های سیگنالینگ از طریق پیکربندی مجدد نرم‌افزار به‌طوری امکان حضور دو قطار به‌طور هم‌زمان در یک بلاک ایجاد شود که در این صورت بروز تصادم میان دو قطار در بلاک یادشده حتمی خواهد بود. دوم: نفوذگران با پیکره‌بندی تنظیمات سامانه، سیگنال‌های کنترلی را طوری تغییر دهند که سرعت قطار با موقعیت آن در مسیر ریلی نظیر شیب، فراز، قوس و غیره ... تناسبی نداشته باشد، در این حالت احتمال تصادف و یا خروج قطار از خط‌آهن به‌ویژه در سوزن‌هایی که به‌اشتباه تنظیم‌شده باشند، بسیار بالا خواهد بود. اجرای هر یک از این حملات، مستلزم اشراف مهاجمان بر پیچیدگی‌های ساختاری سیستم سیگنالینگ و درک دقیق از مدار راه[1] و یاز و کارهای آن است، زیرا نفوذ موفق در این حالت باید بتواند طراحی ایمن و مقاوم در برابر خطای سامانه را بشکند. مهاجم می‌تواند از طریق کنترل سیگنال‌های بازخورد در حلقه‌های مثبت سیستم، زمینه ایجاد تصادف میان قطارها و یا خارج شدن قطار از ریل را ایجاد نماید.

بنابراین کافی است نفوذگر از طریق کنترل و هدایت تعداد مناسب سیگنال‌های مرتبط در یک مسیر خاص، زمینه حضور دو قطار به‌طور هم‌زمان در بلاک را فراهم سازد تا تصادم آن‌ها

[1]. Track Circuit

اجتناب‌ناپذیر شود. برای سیگنال‌هایی که در مسیرهای طولانی در مناطق جغرافیایی مختلف پراکند هستند، در این صورت ارتباط مهاجمان با کارکنان مرکز فرمان از طریق شیوه‌هایی نظیر مهندسی اجتماعی، ضروری می‌نماید تا بتواند سیگنال‌های متضاد در زمان صحیح را برای یک برخورد عمدی ارسال نمایند. همچنین از طرف دیگر یک تهاجم جامع و دقیق مستلزم داشتن اطلاعات کافی از جدول زمان‌بندی حرکت قطارها و محدودیت سرعت ناوگان در هر موقعیت جغرافیایی است تا از طریق بتوانند زمان مناسب برای کنترل جریان حرکت ناوگان قطارها را از پیش محاسبه نمایند. علاوه بر آن، برخورداری از دانش نفوذ گری و رخنه به سیستم‌ها در سطحی بالا برای مهاجمان ضروری است.

هرچند سیستم سیگنالینگ و کنترل آمریکا در برابر اختلالات غیرعمدی استوار نشان داده است، بااین‌حال ارسال سنگال‌های نادرست که منشأ آن نفوذ مهاجمان سایبری است، سبب می‌شود قطار به‌اشتباه وارد بلاک اشغال شود. نمونه‌ای از بروز چنین تهاجماتی را می‌توان در سال ۲۰۱۳ برای راه‌آهن کلاس یک آمریکا مشاهده نمود که در طول تنها یک سال بیش از ۴۳ حمله سایبری به سامانه‌های سیگنالینگ صورت گرفت که درنتیجه سبب اختلال در جابجایی ۱/۷ تریلیون تُن بار در مایل گردید.

۵-٤- نارسایی‌های امنیتی و آسیب‌پذیری مرتبط با تجهیزات ثابت و متحرک در شبکه ریلی آمریکا در برابر اقدامات خرابکارانه و تروریستی

سومین عنصر مهم از مجموعهٔ زیرساخت‌های فیزیکی در شبکه راه‌آهن سرتاسری آمریکا؛ شامل لکوموتیوها و تجهیزات آن است که از چندین شیوه مختلف می‌تواند در معرض تهاجم نفوذگران قرار گیرد. این شیوه ساده‌ترین راه برای دسترسی به دارایی‌های فیزیکی در شبکه ریلی است. دپوها و پایانه‌های راه‌آهن جایی است که در آن تعداد زیادی واگن و لوکوموتیو آرایش‌شده و برای اعزام و یا دریافت آماده می‌شوند. در این محوطه پرتردد، پیش از برنامه‌ریزی اعزام قطارها، واگن‌های نظامی حامل کالاهای خطرناک هستند که دسترسی و نفوذ به آن‌ها در این محوطه پرترافیک و شلوغ می‌تواند به‌منزله از دست رفتن کنترل ماشین‌های ریلی و درنتیجه رها شدن محموله‌های خطرناک در مراکز جمعیتی باشد که خود می‌تواند سلامت تعداد زیادی از شهروندان را متأثر می‌سازد. گزارش‌های ثبت‌شده در پایگاه داده‌های دپارتمان امنیتی آمریکا نشان می‌دهد که دسترسی نفوذگران به محوطه‌های ریلی به‌سادگی امکان‌پذیر است زیرا در راه‌آهن سرتاسری آمریکا، غالب پایانه‌ها فاقد حصار و یا فنس مستحکم بوده و موانع موجود در دیواره‌های فعلی محوطه نیز به‌سهولت توسط مهاجمان دور زده می‌شود.

در بسیاری از مناطق آمریکا، شبکه راه‌آهن از دوربین‌های مداربسته و یا سیستم‌های تشخیص نفوذ بهره نمی‌گیرد و در برخی پایانه‌های نسبتاً بزرگ‌تر که پلیس استقراریافته است، گشت‌های مأموران برای پوشش وسعت از کارایی لازم برخوردار نیست. در شبکه ریلی آمریکا، علاوه بر انبوه فراوان واگن‌ها که در محوطه‌های ریلی دپو شده‌اند، مجموعه‌های منفرد از واگن‌ها نیز در حاشیه‌ی بخش‌های صنعتی تحت پوشش شبکه ریلی در یک پرکندگی جغرافیایی، آرایش یافته‌اند که

نظارت اندکی بر امنیت آن‌ها صورت می‌گیرد و یا آنکه اصلاً در بُرد محافظتی[1] سامانه‌های امنیتی نیستند و لذا در معرض انواع تهاجمات سازمان‌یافته می‌باشند که هم خود واگن و هم کالاهای موجود در آن‌ها را تهدید می‌نماید. یکی از اقدامات پیشگیرانه، ملزم نمودن مدیریت پایانه‌های ریلی به نصب تابلوها و نشانه‌های هشداردهنده بر روی واگن‌های حاوی کالاهای خطرناک است که می‌تواند نوع و تبعات احتمالی آن‌ها را در یک منطقه خاص بر اساس آیین‌نامه‌های مدون و نیز مشخص نمودن انجام اقدامات پیشگیرانه و اصلاحی برای کاهش از شدت خسارت‌های احتمالی به افراد و محیط پیرامون در صورت بروز حادثه است.

یکی دیگر از تهدیدهای فراروی شبکه ریلی آمریکا، ربودن قطارهای حاوی کالاهای خطرناک توسط مهاجمان و انتقال آن به مناطق پرجمعیت است که درنتیجه پتانسیل‌های آسیب‌زای محیطی را به حداکثر می‌رساند و این خود بدان علت است که دسترسی به کابین لوکوموتیوران به‌سهولت امکان‌پذیر است. ازاین‌رو یکی از استراتژی‌های امنیتی در راه‌آهن سرتاسری آمریکا تقسیم قطار به یونیت‌های مستقل است که درنتیجه امکان ربودن کل قطار و جابجایی کالاهای خطرناک را دشوار می‌سازد. آمارهای منتشرشده از دپارتمان امنیتی آمریکا نشان می‌دهد که در سال ۲۰۱۰ تعداد ۴۹ فقره رهاسازی مواد خطرناک در محیط پیرامون شبکه ریلی در اثر رباییش قطار، ۱۹۷ مورد تصادف عمدی و ۱۸۴۹ مورد خروج از ریل رخ‌داده است که این خود نشان‌دهنده آسیب‌پذیری تجهیزات ثابت و متحرک شبکه ریلی در برابر تهاجمات نفوذگران و خرابکاری‌های عمدی است.

۵-۵- نارسایی‌های امنیتی و آسیب‌پذیری مرتبط با سامانه ارتباطات در شبکه ریلی آمریکا در برابر اقدامات خرابکارانه و تروریستی

ارتباطات در راه‌آهن سرتاسری آمریکا با گستره‌ای از امواج رادیوئی پیاده‌سازی شده است که در محدوده‌ای تا حدود ۱۶۰ مگاهرتزی عمل می‌نمایند. این سامانه‌های رادیوئی آسیب‌پذیری نسبتاً کمی را در برابر حملات سایبری از خود نشان داده است. بااین‌حال در صورت عدم کدگذاری و درنتیجه عملیات ناامن ارتباطات رادیوئی، خود زمینه‌ای برای نفوذ مهاجمان خواهد بود. اپراتورهای مرکز کنترل ترافیک و راهبران و سایر خدمه قطار معمولاً به‌صورت تیمی عمل می‌نمایند و پس از احراز هویت می‌توانند در یک بستر امن به تبادل اطلاعات بپردازند. در صورت نفوذ شخص ثالث و احتمال شنود مکالمات در ارتباطات شبکه‌ای می‌توان از گزینه‌های امنیتی جایگزین برای ارتقای قابلیت اطمینان شبکه و تأیید هویت طرفین استفاده نمود که گاهی طیفی از شیوه‌های مختلف نظیر مجوزهای کاغذی تا تماس‌های بی‌سیم و تلفنی را در برمی‌گیرد. در این صورت حتی اگر نفوذگر بتواند مسیر مبادلات رادیوئی را به طور کامل مسدود نماید می‌توان از بروز حوادث احتمالی جلوگیری نمود؛ زیرا حرکت قطار در مسیر ریلی، تنها تا حدودی معتبر است که مجوز حرکت بر اساس آن به راهبر دیده‌شده و تا دریافت مجوز بعدی امکان سیر وجود نخواهد داشت. در راه‌آهن سرتاسری آمریکا هر زیرسیستم عملکردی مجموعه‌ای از اجزای فیزیکی است که با استفاده از پایگاه‌داده‌های تهاجم مختلف، سامانه‌های ارتباط داده‌ها، تجهیزات پردازش اطلاعات و تنظیمات

[1]. Protective Board

سخت‌افزاری و نرم‌افزاری پیاده‌سازی شده است. تجهیزات ارتباطی سامانه‌های در شبکه ریلی دارای دو حالت سیمی و بدون سیم است که زمینه‌های بروز نفوذ در سیستم‌های بدون سیم از سیمی بیشتر است. در این حالت پنج دسته ممکن از انواع حملات برای سامانه‌های کنترل ترافیک مبتنی بر ارتباطات (CBTC[1]) قابل‌تصور است که عبارت‌اند از حملات فعال، غیرفعال، دسترسی، درونی و توزیع‌شده. انواع حملات مرتبط با سامانه‌های سیگنالینگ و تهدیدهای امنیت اطلاعات در سیستم‌های CBTC در جدول شماره یک نشان داده‌شده است.

چنانکه در این جدول مشاهده می‌شود اگرچه هیچ حمله سایبری مرسومی علیه زیرسیستم اسکادا در CBTC شبکه ریلی سرتاسری آمریکا گزارش نشده است، بااین‌حال در نتایج مطالعات شورای تحقیقات کمیته امنیت ملی دولت آمریکا (GAO) آورده شده است که حملات سایبری موفقیت‌آمیزی علیه سایر بخش‌های سامانه‌های کنترلی شبکه ریلی رخ‌داده است. در این تقسیم‌بندی هر یک از کلاس‌های پنج‌گانه حملات سایبری دارای دامنه تأثیراتی متفاوتی بر ایمنی سیر و حرکت قطارها هستند. از میان این پنج تهاجم، حملات فعال و غیرفعال دارای بالاترین درجه اهمیت هستند و سایر تهاجمات می‌توانند در دسته‌بندی حملات فعال و یا غیرفعال قرار گیرند که در این صورت اندازه درجه اثربخشی اقدامات امنیتی و توفیق مهاجمان در دسترسی به سیستم به‌سهولت اندازه‌گیری می‌شود. به‌استثنای هنگام تبادل احتمالی کلید رمزنگاری که از آن برای حفظ یکپارچگی سیستم و احراز هویت استفاده می‌شود، دامنه اثرگذاری حملات فعال بسیار وسیع‌تر از حملات غیرفعال است. همچنین در حالت کلی اطلاعات مبادله شده بین عناصر سیستم‌های کنترلی فاقد ارزش ذاتی است و تنها هنگامی برای نفوذگران جذابیت دارد که شخص ثالثِ غیرمجاز بتواند از طریق آن استنباط نماید که در این صورت یک تهدید بالقوه برای سیستم محسوب می‌شود، بااین‌حال دامنه تأثیر حملات فعال در مورد آن صدق نمی‌نماید.

نوع تهاجم	معرفی و بیان ابعاد در شبکه ریلی آمریکا
حملات غیرفعال	حملات غیرفعال می‌تواند شامل تجزیه‌وتحلیل اطلاعات ترافیکی خطوط ریلی، به‌دست‌آوردن اطلاعات نظارتی در خصوص دارایی‌های محافظت نشده در خطوط ریلی باشد. رخنه و دسترسی به کانال‌های ارتباطی، رمزگشایی از داده‌های ترافیک به دلیل مکانیسم رمزگذاری ضعیف و عدم پشتیبان‌گیری از داده‌های ثبت‌شده در پایگاه‌داده سامانه به‌دست‌آوردن اطلاعات احراز هویت و رهگیری جریان‌های غیرفعال در عملیات شبکه ریلی می‌تواند فرصت مناسبی را از طریق ارسال نشانه‌ها و اطلاعات اخباری برای مهاجمان به‌منظور شناسایی آسیب‌های سیستم و تدارک حمله بالقوه به دست دهد. حملات غیرفعال می‌تواند منجر به افشای اطلاعات یا فایل‌های داده‌ای برای مهاجمان شود. مهندسی اجتماعی و دسترسی غیرمجاز بدون اطلاع و یا بااطلاع کاربران سیستم‌های کنترلی شبکه ریلی.

[1]. Communications-Based Train Control

حملات فعال	حملات فعال شامل مجموعه تلاش‌های گسترده برای دورزدن یا شکستن حصار حفاظت از داده‌های حساس است. در این حملات نفوذگران مقاصد خود را از طریق شناسایی ویژگی‌های سیستم، استفاده از کدهای مخرب و یا دستبرد و نیز تغییر در اطلاعات و ازبین‌بردن یکپارچگی آن به دست می‌آورند. حملات فعال می‌تواند منجر به افشا یا انتشار فایل‌های داده‌ای محرمانه از طریق شخص ثالث غیرمجاز گردد. انکار سرویس‌های سامانه کنترلی قطار و یا ایجاد تغییر داده‌ها مرتبط
حملات مجاورت	حمله مجاورت از نوع تهاجم‌های منظم و ساختاریافته‌ای است که نفوذگران به‌منظور ایجاد مجاورت فیزیکی و یا نرم‌افزاری به شبکه‌ها انجام می‌دهند. در این حملات نفوذگران سیستم‌ها یا تجهیزات مرتبط با آن را به‌منظور تغییر و نقض یکپارچگی، جمع‌آوری داده‌های حیاتی و یا جلوگیری از دسترسی کاربران مجاز به اطلاعات به‌صورت فیزیکال سد می‌نمایند. حملات مجاورت از طریق ورود مخفیانه، دسترسی به پورت‌های باز یا هر دو صورت امکان‌پذیر می‌شود.
حملات داخلی سیستم	حملات داخلی و یا خودی می‌تواند برای سامانه‌های کنترل قطار مخرب یا غیرمخرب باشند. در این شیوه نفوذگران با تفکر مخرب از طریق شنود، سرقت اطلاعات یا آسیب رساندن عمدی به یکپارچگی داده‌ها، تغییر و استفاده از اطلاعات با روش‌هایی نظیر تقلب و یا ممانعت از دسترسی کاربران مجاز به اطلاعات، به مقاصد خود جامه تحقق می‌پوشانند. حملات غیرمخرب معمولاً ناشی از بی‌دقتی کاربران و عدم وجود مکانیسم‌های پیشگیرانه امنیتی در سامانه‌ها است. در این حملات نفوذگران از دانش لازم برای دورزدن امنیت اطلاعات برخوردارند.
حملات توزیعی	حملات توزیعی بر روی بدافزارهایی تمرکز می‌نمایند که در طول عملیات بهره‌برداری از سامانه‌های کنترلی شبکه ریلی می‌توانند از طریق نصب، امکان توزیع و تکثیر ویروس‌ها را با بهره‌گیری از باگ‌های سیستم و یا حفره‌های امنیتی در سخت‌افزار و یا نرم‌افزار شبکه میسر سازند. این حملات می‌توانند کدهای مخرب را وارد سامانه‌های ریلی نموده و همانند حملات «درب پشتی» دسترسی غیرمجاز به اطلاعات را میسر نموده و یا عملکرد سیستم در عملیات بعدی نظارت قطارها را مختل نمایند.

جدول شماره ۱- کلاس‌های طبقه‌بندی حملات برنامه‌ریزی‌شده به سامانه‌های سیگنالینگ و زیرسیستم CBTC در شبکه ریلی سرتاسری آمریکا

Table No 1. Classification classes of planned attacks on signaling systems and the CBTC subsystem in the American rail network

source: (GAO, 2023)

همان گونه که در جدول شماره یک مشاهده می‌شود طیف گسترده‌ای از حملات فعال برای راه‌آهن سرتاسری آمریکا وجود دارد که رخ‌دادن هر یک از آن‌ها می‌تواند تأثیرات منفی قابل‌ملاحظه‌ای بر عملیات کنترل ناوگان قطارها در شبکه ریلی داشته باشد. در زنجیرهٔ حملات به شبکه ریلی، در

یک انتهای زنجیره، حملات فعال قرار دارند که می‌توانند به‌سهولت با انسداد تمامی کانال ارتباطی شبکه، امکان هر مبادله اطلاعات میان موجودیت‌های کل سیستم را از بین ببرند. در یک انتهای دیگر از این زنجیره، حملات غیرفعالی قرار دارند که از درک دقیق نفوذگران از رخنه‌های امنیتی سیستم ریلی ناشی می‌شود. در این نوع حملات مهاجمان با سوءاستفاده از ضعف‌های موجود در پروتکل‌های ارتباطی و فرایند «انکار» کانال را مسدود نموده و آن را با داده‌های نامعتبر دچار اشکال می‌نمایند. سایر حملات فعال در شبکه ریلی به طور عمده از ضعف‌های امنیتی موجود در سامانه‌ها، نظیر حفره‌های امنیتی در سمت فرستنده، مانند: دستبرد به اطلاعات هویتی توسط کاربران غیرمجاز و یا ضعف رایانه سمت گیرنده، مانند: شبکه‌های ارتباطی مخرب و حفاظت نشده، مهندسی اجتماعی و یا جلب‌اعتماد کاربران برای برگزاری نشست با یک گیرنده به‌ظاهر معتبر و غیره... ناشی می‌شود. گاهی این ضعف‌ها به اشکالات مسیر ارتباطی بازمی‌گردد که شخص ثالث بین کامپیوتر گیرنده و فرستنده قرار گرفته و پس از شنود اطلاعات با تغییردادن آن و برهم‌زدن یکپارچگی از طریق تقلید اطلاعات هویتی هر یک از کاربران داده‌های تقلبی را برای طرفین ارسال می‌نماید.

نتیجه‌گیری

در این مطالعه کوشیده شد به‌صورت مروری نارسایی‌های دولت آمریکا در تأمین امنیت زیرساخت‌های حیاتی بر اساس اصول محرمانگی، جامعیت و دسترس‌پذیری در مطالعه موردی شبکه سرتاسری راه‌آهن آمریکا مورد بررسی قرار گیرد. نتایج بررسی و تحلیل مستندات نشان می‌دهد که صنعت حمل‌ونقل ریلی و دولت آمریکا گام‌های بسیار مهمی را برای افزایش ایمنی و امنیت شبکه ریلی برداشته‌اند که در این مطالعه به بخشی از آن‌ها اشاره گردید. بااین‌حال شبکه حمل‌ونقل ریلی این کشور به‌عنوان یک هدف وسوسه‌انگیز همچنان در برابر حملات و پیامدها بالقوه ناشی از آن آسیب‌پذیر است. برخی از این حملات به خسارات و تلفات سنگین انسانی منتهی می‌شود که از آن جمله می‌توان به بمب‌گذاری در حریم ریلی و واگن‌های راه‌آهن آمریکا اشاره نمود. افزایش تاب‌آوری شبکه ریلی آمریکا در برابر اشکال مختلف حملات احتمالی دربردارنده هزینه‌های زیادی است و لذا لازم است متکی به اطلاعات دقیق و جامع از حفاظت و ایمنی در برابر ریسک‌ها باشد تا بتواند درصد موفقیت حملات خرابکارانه در شبکه ریلی را کاهش دهد.

مسئله دیگر اعتماد افکار عمومی به ارزیابی سیستماتیک و مدیریت ریسک در صنعت حمل‌ونقل ریلی آمریکا است که ماهیت غیرخطی داشته و از تحلیل‌های کمی تبعیت نمی‌نماید و به‌این‌ترتیب تصور عموم شهروندان از احتمال وقوع حوادث و پیامدهای مرتبط با آن بسیار بیشتر از احتمال و پیامدهای واقعی آن است، ازاین‌رو اعتراضات عمومی می‌تواند به‌سهولت ریسک را از یک بخش جامعه به بخش دیگر منتقل نماید. مطالعات نشان می‌دهد که علی‌رغم وجود فرصت‌های بهبود تقریباً هیچ تلاشی از سوی دولت فدرال برای استفاده از سایر گزینه‌ها در حمل مواد شیمیایی و کاهش محموله خطرناک در راه‌آهن سرتاسری صورت نگرفته است. قوای مجریه و مقننه دولت آمریکا هیچ تلاش قابل‌توجهی را برای ملزم نمودن صنعت حمل‌ونقل ریلی به ارزیابی ریسک و استفاده از راهکردهای امن‌تر انجام نداده‌اند و در مقابل شرکت‌ها و صنایع مرتبط با حمل‌ونقل ریلی،

بعضاً به طور انفرادی اقدامات امنیتی را پیگیری نموده‌اند که با نتایج متفاوت مواجه شده‌اند.

صرف‌نظر از امنیت بخش بار همچنان مخاطرات مرتبط با خدمات مسافری در راه‌آهن سرتاسری آمریکا پابرجاست که یک راه‌حل کاهش تعداد مسافرانی است که با قطار جابه‌جا می‌شوند و تحقق این امر با افزایش هزینه و ترافیک بزرگراه‌ها توأم خواهد بود. هرچند برخی تلاش‌های دیگر توسط صنعت ریلی و دولت برای افزایش امنیت مسافری صورت‌گرفته است؛ اما به‌خوبی و در مقیاس وسیع اجرانشده است و یا به علت عدم استفاده از فناوری‌های نوین فاقد کارایی است. فقدان یک سیاست جامع، متمرکز و پایدار از دیگر مواردی است که امنیت شبکه ریلی در آمریکا را رنج می‌دهد. ناتوانی در تعیین برنامه‌های بلندمدت برای بخش مسافری و بار و عدم توسعه مطلوب زیرساخت‌های امنیتی و مشارکت ناقص بخش عمومی و خصوصی در توسعه این زیرساخت‌ها، مزید بر معضلات امنیتی شبکه ریلی آمریکا شده است. همچنین نبود مدل‌های تأمین منابع مالی برای ارتقای امنیت شبکه ریلی و اختلاف گسترده دیدگاه‌ها و نرسیدن به اجماع با محوریت منافع عمومی، راه‌آهن سرتاسری آمریکا را در برابر تهدیدات تروریستی آسیب‌پذیر نموده است.

English References

1. Banks, W. E., & Barclay, R. P. (2006). An Analysis of a Strategic Rail Corridor Network (STRACNET) for National Defense (No. MTMC-RND-76-1).
2. Bergen, P., & Hoffman, B. (2015). Assessing the terrorist threat. A report of the bipartisan policy center's national security preparedness group, 6.
3. Berrick, C. A., & Hecker, J. (2006). Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts. DIANE Publishing.
4. Chittester, C. G., & Haimes, Y. Y. (2014). Risks of terrorism to information technology and to critical interdependent infrastructures. Journal of Homeland Security and Emergency Management, 1.(4)
5. Hartong, M., Goel, R., & Wijesekera, D. (2016, May). Communications based positive train control systems architecture in the USA. In 2006 IEEE 63rd Vehicular Technology Conference (Vol. 6, pp. 2987-2991). IEEE.
6. Hartong, M., Goel, R., & Wijeskra, D. (2013). Secure Rail Interchange Routing.
7. Jenkins, B. M., Butterworth, B. R., & Shrum, K. S. (2010). Terrorist attacks on public bus transportation: A preliminary empirical analysis.
8. Jeong, D. Y., Tang, Y. H., & Perlman, A. B. (2011). Evaluation of semi-empirical analyses for railroad tank car puncture velocity, part 1: correlations with experimental data (No. DOT-VNTSC-FRA-99-9). United States. Federal Railroad Administration.
9. Jeong, D. Y., Tang, Y. H., Yu, H., & Perlman, A. B. (2016, January). Engineering analyses for railroad tank car head puncture resistance. In ASME International

Mechanical Engineering Congress and Exposition (Vol. 47780, pp. 1-7).

10. Kissane, D. (2017, June). Terror on the TGV? The Terrorist Threat to France's High Speed Train Network. In The Terrorist Threat to France's High Speed Train Network (June 20, 2007).'Contemporary Challenges and Future Trends in International Security'Conference, Paris, France.
11. Markoff, J. (2013). A silent attack, but not a subtle one. New York Times, 160(55176), 6.
12. Maurillo, D. R. (2015). High-speed rail in the us: will it be a more attractive terror target than inter-city rail? (Doctoral dissertation, Master's thesis, San Jose State University).
13. Orr, M. F., Kaye, W. E., Zeitz, P., Powers, M. E., & Rosenthal, L. (2011). Public health risks of railroad hazardous substance emergency events. Journal of occupational and environmental medicine, 94-100.
14. Ortiz, D. S., Weatherford, B. A., Greenberg, M. D., & Ecola, L. (2011). Improving the safety and security of freight and passenger rail in Pennsylvania.
15. Plant, J. F., & Young, R. R. (2010). Securing and protecting America's railroad system: US railroad and opportunities for terrorist threats. Harrisburg: Pennsylvania State University.
16. Role, C. F. (2019). HIGH SPEED PASSENGER RAIL.
17. Schweizerische, S. N. V. (2016). Information technology-Security techniques-Information security management systems-Requirements. ISO/IEC International Standards Organization.
18. Slovic, P. (2012). Terrorism as hazard: a new species of trouble. Risk analysis.
19. Strandberg, V. (2016). Rail bound traffic—a prime target for contemporary terrorist attacks?. *Journal of Transportation Security*, 6, 271-286.
20. Strandh, V. (2018). Preparing and responding to mass-casualty terrorist attacks: a comparative analysis of four terrorist attacks targeting rail bound traffic. *International Journal of Emergency Management*, 11(3), 262-281.
21. Strandh, V. (2020). Exploring vulnerabilities in preparedness–rail bound traffic and terrorist attacks. *Journal of Transportation Security*, 10(3-4), 45-62.
22. Turégano-Fuentes, F., Pérez-Díaz, D., Sanz-Sánchez, M., & Ortiz Alonso, J. (2018). Overall asessment of the response to terrorist bombings in trains, Madrid, 11 March 2004. *European Journal of Trauma and Emergency Surgery*. 34. 433-441.
23. Vanderau, J. M., & Haakinson, E. J. (2009). An Evaluation of the Proposed Railroad VHF Band Channel Plan. *US Department of Commerce, National Telecommunications and Information Administration*.

24. Wilson, J. M. (2017). Securing America's passenger-rail systems (Vol. 705). Rand Corporation.