مطالعه تاب آوری زیرساخت‌های حیاتی در ایالات‌متحده آمریکا در برابر ریسک‌های امنیتی

(مورد کاوی : بحران‌های امنیتی در زیرساخت‌های شبکه راه‌آهن سرتاسری آمریکا)

مقاله علمی – پژوهشی

پژمان صالحی*، استادیار، دانشکده مهندسی صنایع دانشگاه آزاد اسلامی واحد پرند، تهران، ایران
مهران خلج، استادیار، دانشکده مهندسی صنایع دانشگاه آزاد اسلامی واحد پرند، تهران، ایران
*پست الکترونیکی نویسنده مسئول: pejmansalehi.metro@gmail.com

دریافت: ۱۴۰۳/۰۳/۲۰– پذیرش: ۱۴۰۳/۰۹/۲۰
صفحه ۴۸۲-۴۶۳

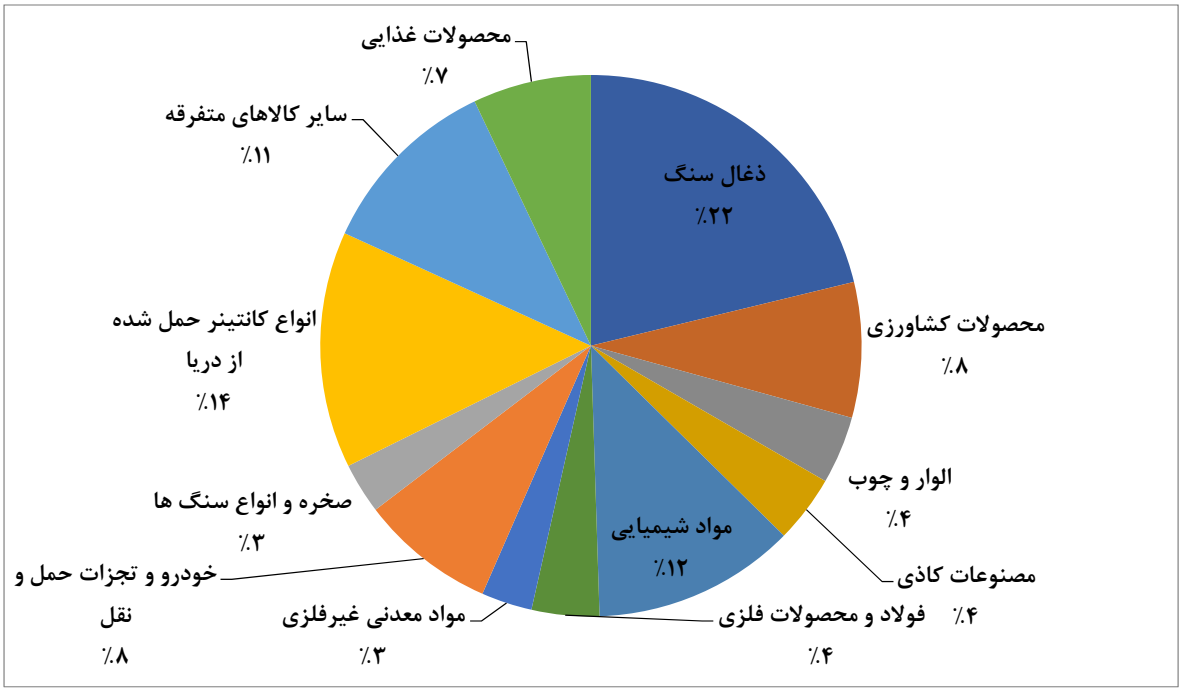
چکیده

صنعت حمل‌ونقل ریلی به‌عنوان یک زیرساخت حیاتی نقش مهمی در اقتصاد کشورهای توسعه‌یافته ایفا می‌نماید. این صنعت می‌تواند حجم انبوهی از محصولات، کالاها و یا مسافران را در طول یک جغرافیای گسترده، پراکنده و متنوع که درعین‌حال قابل‌دسترس و رخنه توسط نفوذ گران و مهاجمان بوده و نیز در برابر انواع حملات فیزیکی و سایبری آسیب‌پذیر می‌باشد؛جابجا نماید. بنابراین ایجاد استحکام و ارتقای سطح امنیت در این شبکه وسیع در مقابل انواع حملات و نفوذهای متنوع به سهولت امکان‌پذیر نیست و با موانع و چالش‌های عدیده‌ای روبروست. در این مطالعه کوشیده شده است به‌صورت موردی با بررسی جایگاه و اهمیت راهبردی راه‌آهن سرتاسری برای حمل‌ونقل بار و مسافر در آمریکا به بررسی مجموعه طبقه‌بندی‌شده از حملات به‌ظاهر ساده که دارای اثرات مخرب و پیچیده بر ترافیک شبکه راه‌آهن و سلامت شهروندان در ایالات‌متحده بوده‌اند، پرداخته شود. همچنین دامنه اقدامات امنیتی صنعت حمل‌ونقل ریلی و دولت آمریکا و نیز تصمیم گیران و کنشگران فعال این عرصه برای کاهش ضریب ریسک‌ها و مدیریت بحران در موقعیت‌های پیچیده، مبهم و نامطمئن و هنگام بروز نفوذ و حملات ساخت‌یافته به شبکه ریلی این کشور مورد تحلیل قرار گیرد. در این مورد کاوی، همچنین پیامدهای برخی حملات موفق و نیز ضعف‌ها و کاستی‌های نظام حکمرانی آمریکا برای تأمین امنیت و ایمنی شبکه حمل‌ونقل ریلی در پیاده‌سازی برنامه‌ها و تدابیر امنیتی به‌منظور مقابله با حملات احتمالی و حراست از زیرساخت‌های حیاتی موردبحث قرارگرفته و کوشیده شده است نتایج و آموزه‌های به‌دست‌آمده از آن را برای ارتقای امنیت بهره‌برداری از صنعت حمل‌ونقل ریلی و زیرساخت‌های حیاتی کشور در برابر حملات خرابکارانه در قالب تجاربی ساده تشریح نماید.

واژه‌های کلیدی: امنیت، ایمنی، مدیریت بحران، آسیب‌پذیری، بهترین تجارب، زیرساخت‌های حیاتی، راه‌آهن

۱- مقدمه

صنعت حمل‌ونقل ریلی یک دارایی بسیار حیاتی و راهبردی برای همه کشورها محسوب می‌شود. تصویر شماره یک فراوانی انواع مختلف محصولات حمل شده توسط صنعت حمل‌ونقل ریلی را در امریکای شمالی نشان می‌دهد. همان‌گونه که در تصویر شماره یک مشاهده می‌شود راه‌آهن ترابری تمامی جنبه‌های مرتبط با صنایع حیاتی و مادر را در ایالات‌متحده 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 ۲ نشان داده‌شده است (اطلس پایگاه داده های حمل و نقل ملی آمریکا، ۲۰۰۸).



شکل ۱. میزان کالای حمل شده توسط راه‌آهن سرتاسری آمریکا (منبع: ARR)

شکل ۲. مسیرهای مواصلاتی شبکه ریلی در سرتاسر ایالات‌متحده (منبع: USCGS)

چنانکه در تصویر شماره دو نیز مشاهده می‌شود، مقیاس عملیات در شبکه ریلی آمریکا بسیار گسترده بوده و تقریباً تمامی نواحی کشور را پوشش می‌دهد. شبکه ریلی در آمریکا دارای هفت کلاس مختلف است که تنها در کلاس یک از شبکه ریلی این کشور، یک‌صد و شصت‌وهفت هزار نفر (با میانگین حقوق ۹۴ هزار دلار در سال) اشتغال به کار دارند. تنها در این کلاس به‌طور

متوسط سالانه بیش از ۱/۷ تریلیون تُن بار در هر مایل جابجا می‌شود و درآمد این شبکه عظیم از راه ترانزیت کالا و بار برای سال مالی مشرف‌به ۲۰۱۱ به بیش از ٥٤ میلیارد دلار رسید (دپارتمان سیاست و اقتصاد راه آهن آمریکا، ۲۰۱۷). این رقم بالغبر ۲۵ درصد کل باری است که برحسب تُناژ در شبکه ریلی بین‌شهری ایالات‌متحده جابجا می‌شود و نیز دربرگیرنده ٤١ درصد از کل کالا برحسب تُن در مایل و تقریباً ۱۲ درصد کل درآمد حمل‌ونقل در ایالات‌متحده برحسب تُن در مایل است (بانکز و همکاران، ۲۰۰٦). همچنین از منظر امنیت ملی بیش از ۳۰ هزار مایل از شبکه ریلی ایالات‌متحده دارای ابعاد استراتژیک بوده و در اختیار وزارت دفاع این کشور است که از آن برای جابجایی و حمل مهمات و تسلیحات نظامی و نیز سایر محموله‌های دفاعی مرتبط با ارتش آمریکا استفاده می‌شود که مقدار آن به بالغبر ۱/۸ میلیون تُن کالاهای خطرناک در طول سال می‌رسد و قلمرو شمول این کالاها مواد منفجره، مواد شیمیایی سمی، گازها و مایعات مورداستفاده در کارخانه‌های مهمات‌سازی و غیره ... را دربرمی‌گیرد که با فرض بروز هر اغتشاش در جابجایی بار و نشت به محیط پیرامون، می‌تواند تبعات جدی و خطرناکی را برای سلامتی شهروندان ایجاد نمایند و این خود نشان‌دهنده اهمیت و حساسیت شبکه راه‌آهن از منظر ژئوپلیتیک برای دولت ایالات‌متحده است.بنا بر آنچه در فوق ذکر گردید بروز اختلالات عمدی یا غیرعمدی در ارائه خدمات شبکه ریلی می‌تواند تأثیر بسیار نامطلوبی بر اقتصاد آمریکا و همچنین دارایی‌های نظامی این کشور داشته باشد.

شکل ۳. سانحه ریلی عمدی برای حمل‌ونقل کالاهای نظامی در منطقه گرانیتویل (منبع:NTSB)

از سوی دیگر طیف پراکندگی جغرافیاییِ زیرساخت‌های ریلی در ایالات‌متحده و سهولت دسترس‌پذیری آن برای مهاجمان، به‌گونه‌ای مخاطره‌آمیز آن را در برابر خرابکاری‌های عمدی، بسیار آسیب‌پذیر نموده است و رخدادهایی نظیر اختلالات شبکه ریلی و نارضایتی مسافران حکایت از فقدان جامعیت و یکپارچگی آن برای ایجاد آستانه‌ای از امنیت مطلق دارد. بااین‌حال آگاهی از میزان حساسیت شبکه ریلی و تأثیر تبعات ناامنی در آن بر اقتصاد کشور، دولت امریکا را بر آن داشته است تا اقدامات وسیعی را

برای حفاظت از حمل‌ونقل بار و مسافر در شبکه ریلی انجام دهند و این در حالی است که دامنه این اقدامات برای کاهش ریسک به انجام مانورها و پیاده‌سازی برخی تکنولوژی‌های امنیتی محدود بوده که برای یک مهاجم مصمم با توجه به شکاف‌های امنیتی و آسیب‌پذیری‌های موجود در شبکه ریلی، فاقد اثربخشی کافی بوده و به‌راحتی می‌تواند آن را با تبعات سوء و فاجعه‌بار یک تهاجم جدی روبرو نماید (دپارتمان سیاست و اقتصاد راه آهن آمریکا، ۲۰۱۷). مطالعات نشان می‌دهد گستره آسیب‌پذیری‌های 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 می‌دهد (دپارتمان سیاست و اقتصاد راه آهن آمریکا، ۲۰۱۲). همان‌گونه که در تصویر شماره ۳ مشاهده می‌شود تبعات خرابکاری عمدی توسط مهاجمان در تاریخ ٦ ژانویه سال ۲۰۰۵ در منطقه گرانیتویلاز ایالت کارولینای جنوبی علاوه بر تخریب کامل واگن‌های قطار و بخش‌هایی از زیرساخت ریلی، سبب نشت گسترده مایعات شیمیایی واگن‌های واژگون شده که مورداستفاده در تسلیحات نظامی بود گردید و اختلال کل شبکه ریلی و نقض یکپارچگی آن را سبب شد. درنتیجه این بحران دست‌ساز نفوذ گران؛ ۹ نفر کشته و ٥٥٤ نفر مجروح شدند که علاوه بر خسارت‌های مستقیم ٤٠ میلیون دلاری به صنعت نظامی امریکا، می‌توان به تبعات دیگر آن نظیر رها شدن گسترده مواد سمی و مشتقات شیمیایی آمونیاک در محیط‌زیست پیرامون منطقه بحران‌زده نیز اشاره کرد که خود سبب کشته شدن یک نفر و مسمومیت بیش از ۳۳۳ نفر از ساکنین گردید که درنتیجه دولت برای جمع‌آوری و پاک‌سازی کامل منطقه، ناگزیر از تخلیه اضطراری ۱۱٦۰۰ محل تجاری و مسکونی و اسکان آن‌ها در محل امن شد (دفتر مدیریت و عملیات باربری راه آهن آمریکا، ۲۰۲۱).

با ذکر مقدمات فوق در تحقیق حاضر، کوشش محققان بر آن است که آسیب‌پذیری‌های بالقوه‌ی زیرساخت‌های ریلی آمریکا در برابر تهاجمات خرابکارانه و استراتژی‌های دولت برای ایجاد امنیت و کاهش ریسک‌ها در این زیرساخت حیاتی را موردمطالعه قرار داده و از این مجرا بتواند با استفاده از نتایج تجارب به‌دست‌آمده، توصیه‌هایی را برای مدیریت بحران در شرایط مشابه به سیاست‌گذاران و تصمیم گیران راه‌آهن جمهوری اسلامی ایران ارائه نماید.

۲- پشینه تحقیق

۲-۱- شکاف امنیتی در زیرساخت‌های ریلی بر اساس پیشینه راه‌آهن سرتاسری در ایالات‌متحده آمریکا

شبکه راه‌آهن سرتاسری 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 فرآیند توسعه راه‌آهن آمریکا،به‌روزآوری تجهیزات، استقرار تسهیلات فنی و رشد سرعت سیر و حرکت قطارها و افزایش ظرفیت متناسب با تقاضا مدنظر بوده است (انجمن حمل و نقل عمومی آمریکا، ۲۰۱۷). روند توسعه تکنولوژی‌های ریلی در این کشور تا آنجا بوده که امروزه لکوالکتریک های مدرن قادرند تا بیش از ۱۰۰ واگن باری با وزن بالغبر ۲۸٦۰۰۰ پوند را با سرعت ٦۰ مایل بر ساعت در فرازهای دشوار با مختصات بیش از ٦ در هزار متر بکشند. قطارهای مسافری مدرن نیز در این کشور می‌توانند به‌طور متوسط ۲٦۰ مسافر را با لحاظ پارامتر راحتی مسافر و مطلوبیت سفر جابجا نمایند (واینستین و کلوور، ۲۰۱۲). بااین‌حال به اذعان مراجع دولتی و نتایج مطالعات پیشین، توسعه مؤلفه‌های امنیتی برای حفظ زیرساخت‌های شبکه ریلی در برابر تهاجمات احتمالی نفوذ گران، متوازن و متناسب با افزایش ظرفیت و سرعت و ارتقای فن‌آوری نوین نبوده است (اور، ۲۰۱۱). بنابراین مسئله امنیت زیرساخت‌ها، به‌دفعات شبکه ریلی سرتاسری آمریکا را با بحران جدی مواجه ساخته به‌طوری‌که علاوه بر ایجاد نارضایتی و موج گسترده‌ی انتقادات رسانه‌ای از روش‌های فعلی مدیریت و پیشگیری بحران، تبعات قابل‌توجهی را در اقتصاد و حمل‌ونقل این کشور بر جای نهاده است (کمیسیون ملی برنامه ریزی سرمایه ای آمریکا، ۲۰۱۷).

۲-۲- طبقه‌بندی تسهیلات ریلی از منظر حساسیت‌های امنیتی

در شبکه ریلی ایالات‌متحده ٦۰۰ قطار باری مستمراً به‌صورت اعزام‌های نظیر به نظیر (میان ایستگاه‌های تشکیلاتی طول مسیر) و سوئیچینگ از پایانه‌ها و دپوها در خطوط سرتاسری سرویس‌دهی می‌نمایند. اعزام‌های نظیر به نظیر عمدتاً حمل‌ونقل بین‌شهری را پوشش می‌دهند و خطوط ریلی پایانه‌ای و سوئیچینگ امکان حمل بار و کالا میان باراندازها، انبارهای کارخانه جات، مراکز تولیدی، صنعتی و نظایر آن را فراهم می‌آورد. اهمیت حیاتی هر بخش از موارد ذکرشده بر اساس

ارزش و درآمد ناخالص سالانه؛ توسط وزارت حمل‌ونقل تعیین می‌شود. طبق قوانین بالادستی ارزش حیاتی تسهیلات ریلی بر اساس میزان سهم آن‌ها در درآمد ناخالص ملی در هرسال با توجه به سال پایه‌ی اولیه (۱۹۹۱) تعیین می‌گردد (دپارتمان ملی ارتش آمریکا، ۲۰۰۶). بر این اساس اهمیت حیاتی و ارزش پایه برای خطوط کلاس یک؛ مقادیر درآمدی بالغبر ۲۵۰ میلیون دلار تا ۳۴۷ میلیون دلار با توجه به ارزش فعلی دارایی‌هاست. کلاس دو نیز شامل آن دسته از تسهیلات خطوط ریلی است که دارای درآمدی بیشتر از ۴۰ میلیون دلار تا کمتر از ۲۵۰ میلیون دلار در سال هستند. در کلاس سه نیز آن دسته از تسهیلات و تجهیزات ریلی قرار می‌گیرند که دارای میانگین درآمد کمتر از ۴۰ میلیون دلار در سال هستند.برای طبقه‌بندی تسهیلات ریلی مسافری از منظر اهمیت و میزان حیاتی بودن شاخص و معیار سنجش ارزش برای دسته‌بندی امنیتی، مقدار مسافتی است که در آن عملیات مسافری توسط سیستم صورت می‌گیرد (مسافر بر مایل). در این قبیل سامانه‌ها، خدمات مسافری بین‌شهری، مسافت‌های نسبتاً طولانی‌تری را پوشش می‌دهند. شرکت هولدینگ AMTRAKارائه‌دهنده اصلی خدمات مسافری بین‌شهری توسط راه‌آهن آمریکا است که خود دارای ۲۲ شرکت زیرمجموعه در سرتاسر ایالات‌متحده است و وظیفه مدیریت ترافیک این شبکه ریلی بزرگ را نیز عهده‌دار است، اکثر مسافران کشور از ایالت‌های توسط این شبکه ترابری می‌شوند (دفتر حسابداری عمومی آمریکا، ۲۰۱۴). اقبال گسترده شهروندان به استفاده از شبکه ریلی برای جابجایی‌های بین‌شهری، از منظر تقسیم‌بندی‌های امنیتی آن را به یکی از مهم‌ترین گلوگاه‌های این کشور بدل نموده است.

۳-۲- بروز اختلال‌های برنامه‌ریزی‌شده توسط مهاجمان در سیستم‌های ریلی آمریکا

یکی از وقایع ناخوشایند در بخش ارائه خدمات شبکه ریلی که می‌تواند دارای تبعات اقتصادی و اجتماعی قابل‌ملاحظه‌ای باشد؛ نویزها (اختلالات) ترافیکی و فیزیکی شبکه ریلی است (دفتر امنیت سایبری سیستم های اطلاعات حمل و نقل آمریکا، ۲۰۱۳). به‌عنوان یک نمونه می‌توان به اختلال برنامه‌ریزی‌شده سال ۱۹۹۸ که در اثر تهاجم نفوذ گران سبب بروز اختلال 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 (چیتر، ۲۰۱۴). نمونه دیگری از تهاجم خرابکارانه نفوذ گران 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 ایالات‌متحده 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 (دفتر خدمات پژوهشی کتابخانه کنگره آمریکا، ۲۰۱۵). نتایج مطالعات نشان می‌دهد که تبعات ناشی از اختلالات عمدی در شبکه ریلی گاه می‌تواند فراتر از آثار اقتصادی ناشی از آن باشد. به‌عنوان نمونه 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 به‌طور بالقوه با نوعی ریسک بسیار بالا برای شهروندان توأم است (دفتر مدیریت ایمنی راه آهن آمریکا، ۲۰۱۲). به‌عنوان‌مثالی دیگر می‌توان به عبور سالانه ۸۵۰۰ واگن حامل کلر و سایر مواد شیمیایی از طریق شبکه ریلی که در انحصار وزارت دفاع است، اشاره نمود که از نزدیکی شهر واشنگتن دی سی 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 (واندراو و هاکیسون، ۲۰۰۹).

۳-۳- ضعف امنیتی و آسیب‌پذیری زیرساخت‌های ریلی ایالات در برابر حملات خرابکارانه

همان‌گونه که پیش‌تر نیز ذکر گردید تعدد ریسک‌های امنیتی و آسیب‌پذیری‌های بالقوه در شبکه ریلی ایالات‌متحده 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 (دفتر اداره ارتباطات و کنترل راه آهن فدرال آمریکا، ۲۰۰۹). در سال ۲۰۱۰پایگاه داده RAND CORP، فهرستی از حوادث تروریستی را در جهان منتشر نمود. در این گزارش بیش از ۲۵۰ حمله تروریستی موفق علیه زیرساخت‌های ریلی ایالات‌متحده برای بازه زمانی ۱۹۹۵ تا

۲۰۰۵ به ثبت رسیده است، که این خود گویای آسیب‌پذیری زیرساخت‌های ریلی آمریکا در برابر حملات تروریستی از منظر امنیتی است (هارتانگ و ویجسکرا، ۲۰۱۶). از سوی دیگر با توجه به 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 دربردارنده‌ی تمامی جزئیات حفاظت امنیتی برای صنایع مادر یک کشور باشد، قدری دور از دسترس به نظر می‌رسد، ازاین‌رو شناسایی تهدیدهای امنیتی برای آن دسته از صنایعی که در خصوص تهاجمات امنیتی دارای پیشینه‌ای از حادثه نیستند، انجام تحلیل‌های امنیتی دشوار است (دفتر کمیته مشورتی مخابرات امنیت ملی ریاست جمهوری آمریکا، ۲۰۱۳).

۳- زیرساخت‌های فیزیکی مهم در شبکه ریلی آمریکا از منظر میزان آسیب‌پذیری در برابر تهدیدهای امنیتی

در راه‌آهن آمریکا مهم‌ترین اجزاء فیزیکی که دارای ارزش حیاتی برای ارائه خدمات به شهروندان و صنایع مختلف است از منظر حفاظت امنیتی به سه دسته کلی تقسیم می‌شود: نخست: مسیر و خطوط ریلی که راه‌آهنی حرکت ادوات نقلیه را تشکیل می‌دهند؛ دوم: سامانه سیگنالینگ که ایمنی سیر و حرکت قطارها در مسیر ریلی را تضمین می‌نماید و سوم: تجهیزات ثابت و متحرک که خود مکمل دو بخش قبلی برای سیر و اعزام قطار و انجام خدمات مطلوب است (دفتر اداره امنیت حمل و نقل آمریکا، ۲۰۱٤).

تهدیدهای امنیتی و آسیب‌پذیری مرتبط با مسیر حرکتی قطارها در شبکه ریلی ایالات‌متحده

زیرساخت‌های ریلی به هر آنچه از تأسیسات راه‌آهن گفته می‌شود که قطار و سایر وسایل نقلیه ریلی بر روی آن به سیر و حرکت خود طبق برنامه زمان‌بندی از قبل تعیین‌شده، ادامه می‌دهند. این مسیر از تونل، ریل حرکتی، پل و زیرساخت‌های پایه نظیر بالاست، تراورس و غیره ... تشکیل‌شده است که می‌تواند علاوه بر ایجاد امکان سیر و حرکت قطارها از خطوط متقاطع نیز پشتیبانی نماید. این مهم در تصویر شماره ٤ نشان داده شده است.

شکل ٤. زیرساخت‌های ریلی شامل، بالاست، پابند و خط آهن (منبع: FRA)

همان‌گونه که در تصویر شماره ٤ مشاهده می‌شود 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 تراورس ها نیز نیروهای عمودی را به‌طور همسان بین بالاست ها توزیع و میرا نموده و عرض خط دقیقی را برای حرکت قطار و جلوگیری از خروج آن از خط آهن فراهم می‌نماید (انجمن حمل و نقل عمومی آمریکا، ۲۰۱٦). بااین‌حال هرگونه آسیب خرابکارانه‌ی 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 لکوموتیو و غیره ... اشاره نمود. آنچه از بررسی روسازی و زیرسازی مسیر ریلی به دست می‌آید آن است که حمله نفوذ گران و آسیب به سازه‌های خط آهن 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 بر هم خوردن شیب عرضی خط و درنتیجه خروج قطار از ریل است (اداره آمار حمل و نقل آمریکا، ۲۰۱۷). یک حمله ساده دیگر که معمولاً برای مهاجمان طعمه جذابی به شمار می‌آید، ایجاد اختلال در مکانیسم‌های ایمنی و منحرف کردن 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 خط آهن 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. این مهم در تصویر شماره پنج نشان داده‌شده است. 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 (دفتر مدیریت و بودجه ریاست جمهوری آمریکا، ۲۰۱٤).

شکل ۵. سوئیچ دستی سوزن‌ها در شبکه ریلی آمریکا

از طرفی حملات مهاجمان به شبکه ریلی در تونل‌ها، پل‌ها و یا تقاطع‌های غیره مسطح 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 که 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 صورت گرفته 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 (دفتر کمک‌های مالی آموزش آمریکا، ۲۰۰۶). همچنین استفاده از مواد قابل اشتعال 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 (دِور) این مکان‌های هندسی، می‌توانند قطار را از خط خارج نموده و سبب اختلال در ترافیک سیر و حرکت قطارها شود (انجمن بزرگراه و حمل و نقل ایالتی آمریکا، ۲۰۱۲).

تهدیدهای امنیتی و آسیب‌پذیری مرتبط با سامانه‌های سیگنالینگ در شبکه ریلی ایالات‌متحده

یکی از حساس‌ترین سامانه‌های راه‌آهن سرتاسری ایالات‌متحده که در برابر حملات مهاجمان و نفوذ گران 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 (بنیاد تحقیقات ملی راه آهن آمریکا، ۲۰۱۸). این سامانه‌ها در راه‌آهن شامل مجموعه ایاز چراغ‌ها بارنگ‌های هشداردهنده هستند که در بالای خطوط ریلی و زیر پل‌ها و یا در کنار خط آهن در موقعیت دید راهبر نصب‌شده‌اند و از طریق یک واحد کنترل به مرکز فرمان متصل می‌باشند، طیف ارائه و تنظیمات نورها به‌گونه‌ای است که راهبر قطار با مشاهده آن می‌تواند به جنبه‌ای از ابعاد سیگنال پی برده و عکس‌العمل مناسب را نشان دهد (همان منبع، ۲۰۱۸). تصویر شماره ٦ گویای این مطلب است.

شکل ٦. سیگنال‌های کنار راه در شبکه ریلی آمریکا

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 رو، 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. مدار راه کلیدی‌ترین عنصر سامانه سیگنالینگ است که هرچند ازنظر مفهومی، پیاده‌سازی آن ساده به نظر می‌رسد اما می‌تواند سیگنال‌های حیاتی کنترلی را از طریق جریان الکتریکی و تجهیزات رله‌ای متصل به ریل حرکتی برای قطار ارسال نموده و یا به‌عکس از آن دریافت نماید؛ همچنین مدار راه قادر است بلاک‌های طول مسیر ریلی را از هم تفکیک نموده و با استفاده از اینترلاکینگ رله‌ای، اشغال بودن مسیر ریلی پیش رو را برای حرکت بدون ریسک ناوگان قطارها نشان دهد. برای این منظور لازم است سامانه مزبور در برابر خرابی ایمن (مقاوم) باشد. 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: نفوذ گران 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 خط آهن به‌ویژه در سوزن‌هایی که به‌اشتباه تنظیم‌شده باشند، بسیار بالا خواهد بود (جونگ و تانگ، ۲۰۱۱). اجرای هر یک از این حملات، مستلزم اشراف مهاجمان بر پیچیدگی‌های ساختاری سیستم سیگنالینگ و درک دقیق از مدار راه و مکانیسم‌های 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 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. تصویر شماره ۷ محوطه پایانه و آرایش تجهیزات سیگنالینگ در راه‌آهن منطقه‌ای شیکاگو را در تلویزیون‌های مداربسته مرکز فرمان نشان می‌دهد.

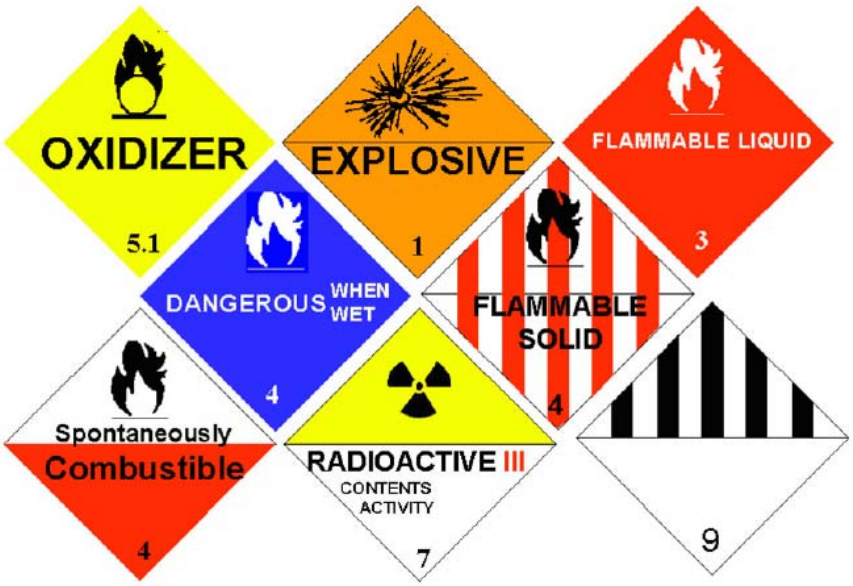
هرچند سیستم سیگنالینگ و کنترل در برابر اختلالات غیرعمدی استوار نشان داده است، بااین‌حال ارسال سنگال‌های نادرست که منشأ آن نفوذ مهاجمان سایبری است، سبب می‌شود قطار به‌اشتباه وارد بلاک اشغال شود. نمونه‌ای از بروز چنین تهاجماتی را می‌توان در سال ۲۰۰۷ برای راه‌آهن کلاس یک ایالات‌متحده مشاهده نمود که در طول 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 (جونگ و همکاران، ۲۰۱۱).

شکل ۷. محوطه پایانه و آرایش تجهیزات سیگنالینگ در راه‌آهن منطقه‌ای شیکاگو

تهدیدهای امنیتی و آسیب‌پذیری مرتبط با تجهیزات در شبکه ریلی ایالات‌متحده

سومین عنصر مهم از مجموعه‌ی زیرساخت‌های فیزیکی؛ شامل لکوموتیوها و تجهیزات است که از چندین شیوه مختلف می‌تواند در معرض تهاجم نفوذ گران 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 لکوموتیو 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. تصویر شماره ۷ گویای این نکته است (دپارتمان سیاست و اقتصاد راه آهن آمریکا، ۲۰۱۷). گزارش‌های ثبت‌شده در پایگاه داده‌های دپارتمان امنیتی در ایالات‌متحده نشان می‌دهد که دسترسی نفوذ گران به محوطه‌های ریلی به‌سادگی امکان‌پذیر است زیرا در راه‌آهن آمریکا، غالب پایانه‌ها فاقد حصار و یا فنس مستحکم بوده و موانع موجود در دیواره‌های فعلی محوطه نیز به سهولت توسط مهاجمان دور زده می‌شود. در بسیاری از مناطق ایالات‌متحده، 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 ایالات‌متحده، 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 سامانه‌های امنیتی نیستند و لذا در معرض انواع تهاجمات سازمان‌یافته می‌باشند که هم خود واگن و هم کالاهای موجود در آن‌ها را

تهدید می‌نماید (همان منبع، ۲۰۱۷). 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 ایالات‌متحده، 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 به سهولت امکان‌پذیر است (بانکز و همکاران، ۲۰۰۶). ازاین‌رو یکی از استراتژی‌های امنیتی در راه‌آهن سرتاسری ایالات‌متحده تقسیم قطار به یونیت‌های مستقل است که درنتیجه امکان ربودن کل قطار و جابجایی کالاهای خطرناک را دشوار می‌سازد. آمارهای منتشرشده از دپارتمان امنیتی ایالات‌متحده 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 شبکه ریلی در برابر تهاجمات نفوذ گران و خرابکاری‌های عمدی است (دپارتمان سیاست و اقتصاد راه آهن آمریکا، ۲۰۱۲).



شکل ۸. علائم، نشانه‌ها و تابلوهای مرتبط با کالاهای خطرناک در شبکه ریلی آمریکا (منبع:US DOT)

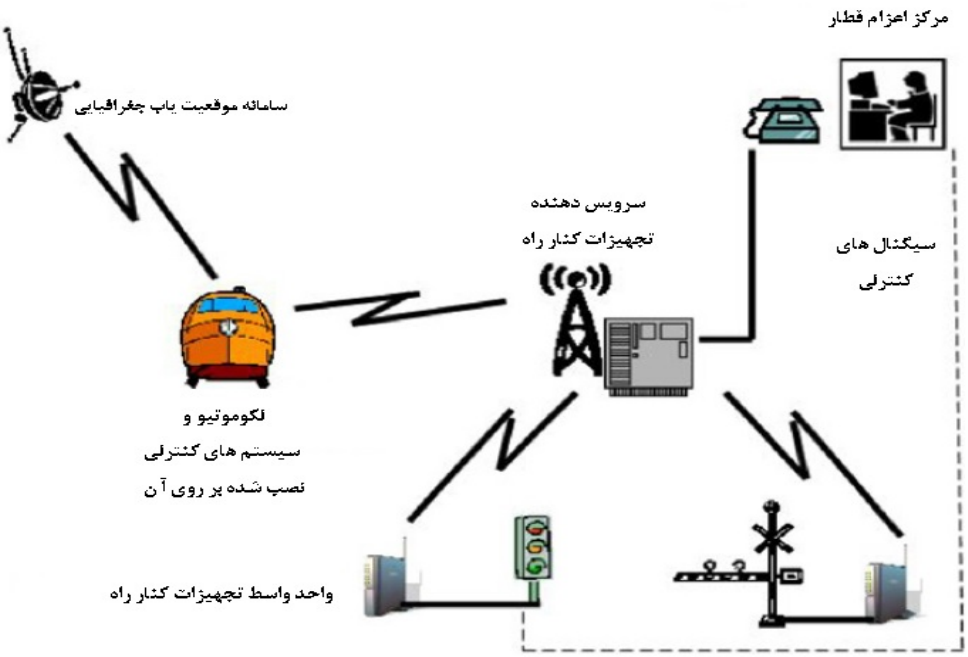
تهدیدهای امنیتی و آسیب‌پذیری مرتبط با ارتباطات در شبکه ریلی ایالات‌متحده

ارتباطات در راه‌آهن سرتاسری ایالات‌متحده 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 (دفتر مدیریت و عملیات باربری راه آهن آمریکا، ۲۰۲۱). در صورت نفوذ شخص ثالث و احتمال شنود مکالمات در ارتباطات شبکه‌ای می‌توان از آلترناتیوهای 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 به‌طور 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 داده‌شده و تا دریافت مجوز بعدی امکان سیر وجود نخواهد داشت. سیستم‌های کنترل قطار

مبتنی بر ارتباطات که به سیستم‌های کنترل قطار مثبت نیز معروف هستند امکان مبادله الکترونیکی داده‌ها در شبکه ریلی را فراهم می‌نمایند که این حالت چالش‌های امنیتی بیشتری نسبت به ارتباطات آکوستیک ایجاد می‌کند. برخی ویژگی‌های اساسی سامانه CBTC به این شرح است (همان منبع، ۲۰۲۱). تعیین مکان دقیق قطار با دقت بسیار بالا که مستقل از مدار راه است. شیوه‌های ارتباط پیوسته با تجهیزات کنار راه با پهنای باند بالا برای امکان صدور مجوز انتقال داده‌ها و کنترل صحت داده‌ها و دقت انتقال آن‌ها با پهنای باند بالا.همچنین کامپیوترهای کنار راه و نصب‌شده داخل قطار برای پردازش شرایط و وضعیت فعلی قطار و کنترل صحت داده‌ها و انجام کنترل‌های مداوم سیر و حرکت قطار از طریق تحلیل داده‌های دریافتی در صورت لزوم مورداستفاده قرار می‌گیرد. همچنین CBTC دارای برخی مزایای عملیاتی نیز هست که از آن جمله می‌توان به استفاده کارآمد از زیرساخت‌های کنار خط، بهبود قابلیت اطمینان، کاهش هزینه‌های نت از طریق کاهش در میزان تجهیزات کنار خط و توسعه عملیات سیگنالینگ در قلمرویی که در پوشش سامانه‌های سیگنالینگ نیست، اشاره نمود.سامانه‌های اصلی CBTC از سه زیرسیستم مهم عملکردی تشکیل‌شده است که ارتباط میان بخش‌های مختلف سامانه سیگنالینگ را فراهم می‌نمایند و عبارت‌اند از: تجهیزات کنار خط، تجهیزات متحرک و سامانه‌های مکان‌یابی قطار و درنهایت واحد اعزام و کنترل (انجمن حمل و نقل عمومی آمریکا، ۲۰۱۷). هر زیرسیستم عملکردی مجموعه‌ای از اجزای فیزیکی است که با استفاده از پایگاه داده‌های مختلف، سامانه‌های ارتباط داده‌ها، تجهیزات پردازش اطلاعات و تنظیمات 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 CBTC قابل‌تصور است که عبارت‌اند از حملات فعال، غیرفعال، دسترسی، درونی و توزیع‌شده (همان منبع، ۲۰۱۷).

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 گزارش نشده است، بااین‌حال در نتایج مطالعات شورای تحقیقات کمیته امنیت ملی دولت آمریکا آورده شده است که حملات سایبری موفقیت‌آمیزی علیه سایر بخش‌های سامانه‌های کنترلی شبکه ریلی رخ‌داده است (واینستین و کلوور، ۲۰۱۲). 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 به سهولت اندازه‌گیری می‌شود (اور، ۲۰۱۱). 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 نفوذ گران 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.

همان‌گونه که در جدول شماره یک مشاهده می‌شود طیف گسترده‌ای از حملات فعال وجود دارد که رخ دادن هر یک از آن‌ها می‌تواند تأثیرات منفی قابل‌ملاحظه‌ای بر عملیات کنترل ناوگان قطارها در شبکه ریلی داشته باشد. در زنجیره‌ی حملات به شبکه ریلی، در یک انتهای زنجیره، حملات فعال قرار دارند که می‌توانند به سهولت 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 نفوذ گران 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 (همان منبع، ۲۰۱۱). سایر حملات فعال در شبکه ریلی به‌طور 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 جلب اعتماد 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 قرارگرفته و پس از شنود اطلاعات با تغییر دادن آن و بر هم زدن یکپارچگی از طریق تقلید اطلاعات هویتی هر یک از کاربران داده‌های تقلبی را برای طرفین ارسال می‌نماید.



شکل۹. مدل مفهومی معماری سامانه CBTC در شبکه ریلی ایالات‌متحده

جدول ۱. کلاس‌های طبقه‌بندی حملات برنامه‌ریزی‌شده به سامانه‌های سیگنالینگ و زیرسیستم CBTC در شبکه ریلی آمریکا (منبع: GAO)

نوع حمله	معرفی و بیان ابعاد در شبکه ریلی آمریکا
حملات غیرفعال	حملات غیرفعال می‌تواند شامل تجزیه‌وتحلیل اطلاعات ترافیکی خطوط ریلی،به دست آوردن 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 پشتیبان گیری از داده‌های ثبت‌شده در پایگاه داده سامانه به دست آوردن اطلاعات احراز هویت و ره‌گیری جریان های 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
حملات فعال	حملات فعال شامل مجموعه تلاش‌های گسترده برای دور زدن یا شکستن حصار حفاظت از داده‌های حساس است. در این حملات نفوذ گران مقاصد خود را از طریق شناسایی ویژگی‌های سیستم، استفاده از کدهای مخرب و یا دستبرد و نیز تغییر در اطلاعات و از بین بردن 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 نفوذ گران به‌منظور ایجاد مجاورت فیزیکی و یا نرم‌افزاری به شبکه‌ها انجام می‌دهند. در این حملات نفوذ گران 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.

نوع حمله	معرفی و بیان ابعاد در شبکه ریلی آمریکا
حملات داخلی سیستم	حملات داخلی و یا خودی می‌تواند برای سامانه‌های کنترل قطار مخرب یا غیر مخرب باشند. در این شیوه نفوذ گران 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 غیر مخرب معمولاً ناشی از بی‌دقتی کاربران و عدم وجود مکانیسم‌های پیشگیرانه امنیتی در سامانه‌ها است در این حملات نفوذ گران از دانش لازم برای دور زدن 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.

٤- اقدامات دولت و راه‌آهن سرتاسری آمریکا برای کاهش آسیب‌پذیری‌های امنیتی شبکه ریلی

طی سال‌های اخیر دولت و راه‌آهن سرتاسری ایالات‌متحده به‌صورت مشترک به انجام اقدامات امنیتی پیشگیرانه و اصلاحی پرداخته‌اند تا از این طریق بتوانند میزان آسیب‌پذیری شبکه ریلی را در برابر تهاجمات کاهش دهند.

٤-١- اقدامات امنیتی صورت گرفته توسط راه‌آهن سرتاسری برای ارتقای امنیتی صنعت حمل‌ونقل ریلی

سیاست‌گذاران در صنعت حمل‌ونقل ریلی آمریکا به تدوین برنامه‌های جامعی برای کاهش ریسک‌های امنیتی بر اساس تجزیه‌وتحلیل جامع زیرساخت‌ها، قطارها، محموله‌های قابل‌حمل توسط واگن‌ها و غیره ... و با لحاظ نوع حملات نفوذ گران پرداخته‌اند. دراین‌بین مرکز تجزیه‌وتحلیل اطلاعات حمل‌ونقل جاده‌ای و عمومی آمریکا به‌عنوان فرمانده و کانون هماهنگی برای در نظر گرفتن اقدامات تأمینی و امنیتی در صنعت حمل‌ونقل ریلی به درخواست وزارت حمل‌ونقل و بر اساس دستورالعمل ابلاغی بخش امنیت ریاست جمهوری آمریکا به‌توسط انجمن راه‌آهن آمریکا و انجمن حمل‌ونقل عمومی آمریکا مشغول به فعالیت گردید. بر این اساس ISAC موظف است با بخش‌هایی اجرایی دولت، آژانس‌های اطلاعاتی و امنیتی، تیم‌های واکنش اضطراری برای مقابله با حملات و تهدیدهای رایانه‌ای و آسیب‌پذیری اطلاعات در سطوح فوق سری امنیتی، هماهنگی و همکاری نماید. نتایج به‌دست‌آمده از این اقدامات به بهره‌برداران مستقل راه‌آهن سرتاسری آمریکا ارائه‌شده و آن‌ها را قادر می‌سازد تا از طریق بالا بردن امنیت فیزیکی و سایبری، سطح آمادگی خود را برای مواجهه با حملات محتمل نفوذ گران افزایش دهند.

راه‌آهن سرتاسری آمریکا دارای دو دسته از پتانسیل‌های ارزشمند و عمده برای ارتقای سطح امنیت زیرساخت‌هاست که عبارت‌اند از نخست: نیروهای پلیس راه‌آهن و دوم: کارکنان و خدمه آموزش‌دیده. نیروهای پلیس راه‌آهن شامل افسران دانش‌آموخته، مجری قانون و کاملاً مسلح هستند که از اختیارات قانونی کامل برخوردار بوده و بسته به حوزه نظارتی و استحفاظی می‌تواند مرجع مهم حفظ دارایی‌های ریلی باشند. همچنین خدمه راه‌آهن و لوکوموتیوران‌ها نیز می‌توانند با استفاده از ارتباطات رادیوئی مجهز به VHF هر رفتاری مشکوکی را به مرکز کنترل ترافیک گزارش دهند تا در صورت لزوم مأموران پلیس به محل اعزام شوند. افسران راه‌آهن می‌توانند از اختیارات خود استفاده نموده و در صورت لزوم با آژانس‌های امنیتی و پلیس فدرال در هر منطقه برای مواجهه قاطع با مخاطرات هماهنگ شوند. همچنین در راستای ارتقای سطح امنیت زیرساخت‌ها، مدیران ارشد کلاس یک‌راه‌آهن و نیز بخش مرکزی راه‌آهن سرتاسری به‌صورت داوطلبانه تیم‌هایی را برای ارزیابی منظم مخاطرات مرتبط با جابجایی مواد خطرناک و کالاهای نظامی و یافتن شیوه‌های عملیاتی برای کاهش آسیب‌پذیری زیرساخت‌های فیزیکال، فن‌آوری اطلاعات و هوشمند نمودن شبکه‌های ریلی ایجاد کرده‌اند که به ارائه بهترین شیوه‌های مدیریت ریسک در سرتاسر راه‌آهن می‌پردازد (دفتر حسابداری عمومی آمریکا، ٢٠١٤). این تیم‌ها تمامی دارایی‌های مهم، آسیب‌پذیری‌ها و تهدیدهای شبکه ریلی را برای اتخاذ اقدامات متقابل امنیتی در سرتاسر راه‌آهن بررسی و اولویت‌بندی می‌نمایند. به‌عنوان بخشی از فعالیت‌های این تیم‌ها می‌توان به ایجاد مراکز شبانه‌روزی واکنش به مخاطرات امنیتی اشاره کرد که از طریق هماهنگی با آژانس اطلاعاتی دولت،

اقدامات امنیتی را اجرایی می‌نماید. دیگر طرح امنیتی صنعت راه‌آهن اقدام به سطح‌بندی تهدیدهای امنیتی بر اساس دستورالعمل‌های وزارت امنیت داخلی برای واکنش مؤثر به تهدیدهای امنیتی است. در این مدل مقیاس شناسایی تهدیدهای امنیتی شامل چهار سطح است؛ که این سطوح از سطح اول (عملیات روزانه تردد قطارها) تا سطح چهارم (مواجهه با تهدیدهای بالفعل در شبکه راه‌آهن) بخش‌بندی شده‌اند. در این حالت واکنش‌های امنیتی تابع سطح و نوع تهدید است که می‌تواند از بازرسی‌های تصادفی ساده و ردیابی تسلیحات نظامی تا بررسی اجزای فیزیکی شبکه نظیر پل‌ها، تونل‌ها و مسیر ریلی باشد. این طرح به‌عنوان یک مدل پویا دربرگیرنده تمامی مستندات امنیتی به‌روز است که مستمراً موردبازنگری قرار می‌گیرد (همان منبع، ۲۰۱٤). برنامه‌ریزی دقیق قطارهای حامل محموله‌های خطرناک و کالاهای نظامی با توجه به ریسک‌ها و تبعات نامطلوب محیطی، همواره به‌دقت برنامه‌ریزی می‌شود و برای کنترل پیامدهای احتمالی ناشی از آن دستورالعمل‌های خاصی توسط صنعت حمل‌ونقل ریلی ایجادشده است. دراین‌بین رعایت الزامات فنی برای جابجایی مواد و تعیین مسیرهای ریلی کلیدی و امکانات حمل‌ونقل و ردیابی مستمر محموله‌ها برای حصول اطمینان از دریافت آن در مقصد بر اساس دستورالعمل‌های امنیتی از آن جمله است. راه‌آهن ایالات‌متحده روزانه ۱/٤۰۰ میلیون مسافر را جابجا می‌نماید. بنابراین کنترل دسترسی و بازرسی کامل مسافران در تمامی ورودی‌های ایستگاه ازجمله اقداماتی است که برای ارتقای امنیت عملیات سیر و حرکت قطارها مسافری تعریف‌شده است که درنتیجه دسترسی نفوذ گران برای انجام حملات را با دشواری و مانع روبرو می‌سازد. بهره‌گیری از فن‌آوری‌های نوین هرچند هزینه زا است اما می‌تواند مکمل سایر اقدامات تأمینی باشد (دفتر مدیریت ایمنی راه آهن آمریکا، ۲۰۱۲). برآوردهای صورت گرفته توسط دپارتمان مالی راه‌آهن سرتاسری آمریکا نشان می‌دهد که انجام اقدامات تأمینی صرفاً در حوزه مسافری در سال مالی مشرف‌به ۲۰۱۱ بالغ بر ٤/۳ میلیارد دلار هزینه داشته است.

٤-۲- اقدامات امنیتی صورت گرفته توسط دولت آمریکا برای ارتقای امنیتی صنعت حمل‌ونقل ریلی

دولت آمریکا برای تأمین امنیت شبکه ریلی با کمبود نیروی انسانی متخصص در این حوزه روبروست. در سال ۲۰۰٤ بودجه تعیین‌شده توسط دولت فدرال برای تأمین امنیت خطوط هوایی ٤/۵ میلیارد دلار در نظر گرفته شد و این در حالی است که این مبلغ برای راه‌آهن سرتاسری تنها ٦۵۰ میلیون دلار بوده است. در سال ۲۰۰٦ وزارت امنیت داخلی تنها دو درصد از تمامی بودجه مرتبط با زیرساخت‌های حیاتی کشور ایالات‌متحده را برای ارتقای امنیت راه‌آهن سرتاسری تعیین کرد (واندراو و هاکیسون، ۲۰۰۹). از طرفی با لحاظ این تفاوت در نیروی انسانی و بودجه و اهمیت راه‌آهن در جابجایی بار و مسافر، مشاهده می‌شود که فقدان حمایت دولت از امنیت بخش ریلی نمی‌تواند توسط بخش خصوصی جبران شود. صنعت حمل‌ونقل ریلی در ایالات‌متحده به‌شدت سرمایه‌بر است به‌عنوان‌مثال راه‌آهن کلاس یک در ایالات‌متحده در سال ۲۰۰۵ به میزان ۱۷/۸ درصد از درآمد کل خود را برای بهبود زیرساخت‌ها سرمایه‌گذاری نمود که نتیجه آن استقراض قابل‌توجهی برای سرمایه‌گذاری به‌منظور نگهداری و توسعه زیرساخت‌های موجود است. اختلاف میان مخارج سرمایه‌ای و میزانی که راه‌آهن سرتاسری می‌تواند از درآمد خود سرمایه‌گذاری نماید سالانه بالغبر ۲ میلیارد دلار است که درنتیجه استفاده از فن‌آوری‌های نوین به‌منظور حمایت از زیرساخت‌های امنیتی را در راه‌آهن امریکا را دشوار نموده است (دفتر اداره ارتباطات و کنترل راه آهن فدرال آمریکا، ۲۰۰۹). از سال ۱۹۹۸ به بعد هزینه‌های ایالتی و فدرال برای بهبود و توسعه بزرگراه‌ها بیش از ۳۳ برابر بیشتر از هزینه نت خطوط ریلی باری و مسافری بوده است. بااین‌حال از مجموع بودجه عمومی مصوب در سال قبل ۱۰۸ میلیارد دلار به بزرگراه‌ها، ۱۱ میلیارد دلار حمل‌ونقل جاده‌ای، ۹ میلیارد دلار حمل‌ونقل هوائی و تنها ۳ میلیارد دلار به راه‌آهن سرتاسری تخصیص یافت (همان منبع، ۲۰۰۹). بااین‌حال وزارت امنیت داخلی از طریق ابلاغ دستورالعمل‌های امنیتی، بهره‌برداران را ملزم نموده برخی از سیستم‌های خود را برای بهبود امنیت ارتقا دهند به‌عنوان‌مثال می‌توان به حذف سطل زباله در کلیه ایستگاه‌های ریلی اشاره نمود تا از آن طریق پوشش امنیتی این اماکن توسط سگ‌های کشف مواد منفجره برای تمامی بهره‌برداران ریلی بین‌شهری و درون‌شهری از قبلی مترو، تراموا و راه‌آهن سبک میسر گردد که این اقدام درواقع مکمل تلاش‌های امنیتی تیم‌های ارتقای سطح امنیتی شبکه ریلی است. دولت همچنین برای جابجایی مواد خطرناک و کالاهای نظامی توسط راه‌آهن محدودیت‌هایی را وضع نموده است که از آن جمله می‌توان به افزایش استحکام مسیرهای توأم با ریسک برای کاهش دغدغه‌های امنیتی به‌منظور حمل کالاهای خطرناک از مسیرهای دارای سطح ایمنی بالاتر اشاره نمود.

شکل ۱۰. نمونه‌ای از انفجار واگن‌های مخزن در راه‌آهن سرتاسری ایالات‌متحده (منبع: US EPA)

برخی از مقررات دولت فدرال برای ارتقای سطح امنیت شبکه ریلی ازاین‌قرار است: لزوم گردآوری و ثبت داده‌های امنیتی و ارسال آن به‌صورت سالانه به وزارت امنیت داخلی، تجزیه‌وتحلیل ریسک‌های ایمنی و امنیتی در مسیرهای حمل و مواد خطرناک و کالاهای نظامی و ارائه آلترناتیوهای مسیریابی بهینه و کم‌خطر، اخذ تصمیم بر اساس ارزیابی‌های امنیتی، استفاده از الگوهای مسیریابی ایمن که مبتنی بر سیستم‌های پیشرفته کنترل ریسک باشد (هارتانگ و ویجسکرا، ۲۰۱۶). از سوی دیگر دولت فدرال راه‌آهن سرتاسری را ملزم نموده است تا از طریق ارتقای یکپارچگی ساختاری در واگن‌های راه‌آهن، مقاومت آن‌ها را در برابر تخریب و انتشار مواد خطرناک در محیط پیرامون افزایش داده و به‌طور غیرمستقیم امنیت آن‌ها را بهبود بخشد. در سال ۲۰۰۴ دپارتمان ملی ایمنی حمل‌ونقل با بررسی ساختار قطارها در شبکه ریلی آمریکا دریافت که بیش از ۶۰۰۰۰ واگن مخزن که از آن به‌منظور حمل‌ونقل مواد خطرناک و شیمیایی استفاده می‌شود، با استانداردهای ایمنی انطباق نداشته و در صورت بروز هرگونه تصادف، در برابر حملات مهاجمان کاملاً آسیب‌پذیر هستند. این دپارتمان همچنین تأکید نمود که رعایت الزامات سال ۱۹۸۹ و استفاده از فولاد سخت، واگن‌های مخزن را ایمن‌تر نموده است بااین‌حال در حدود ۶۰٪ از واگن‌های مخزن برای حمل‌ونقل مواد شیمیایی و خطرناک قبل از سال ۱۹۸۹ ساخته‌شده‌اند (همان منبع، ۲۰۱۶). مطالعات قبلی در مورد یکپارچگی واگن‌ها، مبنایی برای ابتکارات نظارتی فعلی توسط FRA به‌منظور رفع نگرانی‌های دپارتمان ملی ایمنی حمل‌ونقل آمریکا گردید که درنتیجه به طراحی مجدد و ارتقای کل ناوگان قطارها تا سال ۲۰۱۷ منجر شد. همچنین به‌منظور حمایت از اقدامات نظارتی، مؤسسات تحقیقات صنعتی در حال کار بر روی توسعه نسخه جدید استانداردهای مرتبط با حمل‌ونقل مواد خطرناک هستند که شامل طراحی مجدد واگن‌های مخزن و افزایش امنیت و ایمنی سیر و حرکت قطارهای حامل مواد خطرناک در یک مقیاس کامل است. برخی نکات ایمنی که در پروژه توسعه‌ی واگن‌های مخزن بهبود مدنظر قرارگرفته است، عبارت‌اند از: دوجداره کردن دیواره‌های واگن‌های مخزن، نصب دریچه‌های متحرک در واگن‌ها، بهبود کوپلرهای واگن برای از بین بردن احتمال هر نوع اصطکاک اضافی، استفاده از زره‌های واکنشی برای افزایش مقاومت در برابر سلاح‌های سنگین، استفاده از فولادهای قوی‌تر که امروزه در صنعت ساخت تانک‌های جنگی استفاده می‌شود، افزایش تاب‌آوری واگن در مقابل حریق، نصب ترمزهای پنوماتیک الکترونیکی برای بهبود سامانه کشش قطار و غیره ... که سبب می‌شود واگن‌های مخزن

تا حدود ۱۰ برابر در مقابل اقدامات خرابکارانه ایمن‌تر شوند.همچنین وزارت امنیت داخلی ایالات‌متحده در بخش تهدیدهای سایبری شبکه ریلی اقدامات مرتبط با تقویت سیستم‌های کنترل نظارتی و جمع‌آوری داده‌ها در شبکه ریلی (اسکادا) را از طریق استقرار سامانه‌های ملی واکنش فضای مجازی و تشکیل تیم‌های اضطراری واکنش به تهدیدهای رایانه‌ای برای افزایش آمادگی در مقابل حملات و تجزیه‌وتحلیل آسیب‌ها و ارسال هشدارهای مرتبط با تهدیدهای سایبری، آموزش و ارزیابی‌های امنیتی را مدنظر قرار داده است. بااین‌حال تمامی این اقدامات تنها دربردارنده کمتر از ۲ درصد بودجه‌های امنیتی و معادل ۸۹ میلیون دلار است (دفتر اداره امنیت حمل و نقل آمریکا ، ۲۰۱٤).

۵-نتیجه‌گیری

صنعت حمل‌ونقل ریلی و دولت ایالات‌متحده 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 نرم، همچنان در برابر حملات و پیامدها بالقوه ناشی از آن آسیب‌پذیر است. برخی از این حملات به جراحات و تلفات سنگین انسانی منتهی می‌شود که از آن جمله می‌توان به بمب‌گذاری در حریم ریلی و واگن‌ها اشاره نمود. افزایش تاب‌آوری شبکه ریلی 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 این کشور است که غیرخطی بوده 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 به سهولت 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 آلترناتیوها در حمل مواد شیمیایی و کاهش محموله خطرناک در راه‌آهن صورت نگرفته است. قوای مجریه و مقننه دولت امریکا هیچ تلاش قابل‌توجهی را برای ملزم نمودن صنعت حمل‌ونقل ریلی به ارزیابی ریسک و استفاده از آلترناتیوهای امن‌تر انجام نداده‌اند و در عوض شرکت‌ها و صنایع مرتبط با حمل‌ونقل ریلی، بعضاً به‌طور انفرادی اقدام نموده‌اند که با نتایج متفاوت مواجه شده‌اند. صرف‌نظر از امنیت بخش بار همچنان مخاطرات مرتبط با خدمات مسافری در راه‌آهن سرتاسری این کشور پابرجاست که یک‌راه حل کاهش تعداد مسافرانی است که با قطار جابجا 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 صورت گرفته است اما به‌خوبی و در مقیاس وسیع اجرانشده است و یا به علت عدم استفاده از فن‌آوری‌های نوین فاقد کارایی است. فقدان یک سیاست جامع، متمرکز و پایدار از دیگر مواردی است که امنیت شبکه ریلی در ایالات‌متحده 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 ایالات‌متحده را در برابر تهدیدات تروریستی آسیب‌پذیر نموده است.

٦-مراجع

- AAR Circular OT-55-I Recommended Rail Operating Practicesfor Transportation of Hazardous Materials, August (2015).
- American Association of State Highway andTransportation Officials, (2012). Transportation-Invest inAmerica. *Freight-Rail Bottom Line Report.*
- 108th Congress 2d Session, (2014). Senate Report 108-278 CalendarNo. 536, *Rail Security Act Of 2014 Report of The Committeeon Commerce, Science, and Transportation*, on S.2273.
- 49 Code of Federal Regulations Part 172 Subpart 1.

- American Public Transportation Association, (2016). *Commuter RailPublic Transportation Ridership Report*, Fourth Quarter.
- American Public Transportation Association, (2017). PublicTransportation Fact Book, *American Public TransportationAssociation*, Washington, DC, May.
- Bureau of Transportation Statistics, (2015). Air Carrier Statistics-Form 41 Traffic-All Carriers, *US Department of Transportation*, Washington, DC.
- Chittester, Haines, (2014). Risks of terrorism to information tech-nology and to critical interdependent infrastructure. *Journalof Homeland Security and Emergency Management*, 1 (4).
- D.Y. Jeong, Y.H. Tang, A.B. Perlman, (2011). Evaluation of Semi-Empirical Analyses for Railroad Tank Car Puncture Velocity, Part I: *Correlations with Experimental Data*, Final Report,DOT/FRA/ORD-01/21.I.
- Department of Homeland Security, Budget in Brief- FY (2014).Office of Management and Budget.
-Federal Railroad Administration, (2009). Railroad Communicationsand Train Control, *Report to Congress*, July.
- Federal Railroad Administration, Office of Safety Analysis.
- Federal Railroad Administration, Report of the RailroadSafety Advisory Committee to the Federal Railroad Admin-istrator, *Implementation of Positive Train Control Systems*.
-Hartong Goel, Wijesekera, (2016). Communications Based PositiveTrain Control Systems Architecture in the USA, *in: Proceed-ings 63rd IEEE International Vehicle Technology Conference, Melbourne.* Australia, 7-10 May.
- Information Assurance Technical Framework (IATF), Release3.1, Sept. (2007). Information Assurance Solutions, *US NationalSecurity Agency Fort Meade*, MD.
- J. Vanderau, E. Haakison, (2009). An Evaluation of the ProposedRailroad VHF Band Channel Plan, US Department ofCommerce, Washington, DC, September.
- Jeong, et al., (2011). Engineering analyses for railroad tankcar head puncture resistance, *in: Proceedings of 2011 ASME International Mechanical Engineering Congress andExposition November 5-10*, Chicago, IL, USA.
- Letter from Major General H. Steven Blum, USA, (2012). HQ NorthAmerican Aerospace Defense Command and United StatesNorthern Command to Edward K. Hamberger, President andChief Executive Officer, Association of American Railroadsdated 2 December.
- M. Orr, (2011). Public health risks of railroad hazardous substanceemergency events. *Journal of Occupational and Environmen-tal Medicine 43*.
- National Transportation Atlas Databases (NTAD) (2008). Federal Railroad Administration (FRA) National Rail Network1:100,000 (line) 2008 ed., *Bureau of Transportation Statistics(BTS)*, Washington, DC.
- National Transportation Safety Board, (2005). Collision of NorfolkSouthern Freight Train 192 with Standing Norfolk SouthernLocal Train P22 with Subsequent Hazardous Material Releaseat Graniteville, SC January 6, 2020, NTSB # RAR-05/04, November.
- National Transportation Safety Board, (2009). *Derailment of Cana-dian Pacific Railway Freight Train 292-16 and Subsequent Re-lease of Anhydrous Ammonia Near Minot ND, Jan.* 2012, NTSB# RAR-04-01, March.
-Office of Freight Management and Operations, (2021). FederalHighway Administration Freight Facts and Figures 2021, *USDepartment of Transportation*, Washington, DC.
- Office of Grants and Training, (2016). FY 2006 InfrastructureProtection Program; Intercity Passenger rail Security ProgramGuidelines and Application Kit, *US Department of HomelandSecurity*, Washington, DC, October.
- Office of Management and Budget, Presidents (2014). *Budget-Department of Homeland Security*.
- Pipeline and Hazardous Material Safety Administration, (2016). Notice of Proposed Rule Making, Hazardous Material, *Enhancing Rail transportation Safety and Security forHazardous Materials Shipments, Federal Register*, Dec. 21, Vol. 71, No. 245.
-Policy and Economics Department, (2012). Association of AmericanRailroads Hazmat Transportation by Rail, *Association ofAmerican Railroads*, Washington, DC, Feb.
-Policy and Economics Department, (2017). Association of AmericanRailroads, Railroad Facts, 2007 ed., *Association of AmericanRailroads*, Washington, DC, November.
-Policy and Economics Department, (2017). Association of AmericanRailroads Mandatory Hazmat Rerouting, *Association of American Railroads*, Washington, DC, April.
-President George W. Bush, (2013). Critical Infrastructure Identifi-cation, Prioritization, and Protection (HSPD-7), Washington(DC), December 17.
-Public law 101-615 (Hazardous Materials TransportationUniform Safety Act)-Nov. 2001 Codified 49 USC 56101-5127General) amended Homeland Security Act of 2002 PL

107-296 and PL 109-592005 Safe, Accountable, *Flexible EfficientTransportation Equity Act- A Legacy for Users*.
- Public Law 101-647 (Crime Control Act of 2006) Section 1704.
- Statement of Edward K. Hamberger, (2017). President and Chief Ex-ecutive Officer, Association of American Railroads beforethe US House of Representatives Committee on Transporta-tion and Infrastructure, *Subcommittee on Highways and RailTransit and Subcommittee on Railroads, Pipelines, and Haz-ardous Materials Hearing on Transit and Rail Security*, Wash-ington, DC, March 7.
- Title 49 Code of Federal Regulations Part 172 Subpart F.
- Title 49 US Code of Federal Regulations Part 171.8.
- W. Banks, R. Barclay, (2006). An Analysis of a Strategic Rail CorridorNetwork (STRACNET) for National Defense. *Military Trafficmanagement Command*, Washington, DC, Nov.
-49 CFR Part 1201 General Instruction 1-1.
-Academy of Sciences,Washington, DC (2013).
-Accident Incident Overview (2012), US Department of Trans-portation, Washington, DC.
-American Public Transportation Association, (2017). Washington,DC, May
-Car Puncture Velocity,Part II: (2011). Correlations with Engineering Analyses, Final Report,DOT/FRA/ORD-01/21.II.
-Chemical Agents, (2006). FieldManual Army FM-285, *Department of the Army,*Washington,DC, Feb.
-Congressional Research Service of the Library of Congress, (2013). *Cyber Attacks and Cyber Terrorism-Vulnerabilities and PolicyIssues for Congress,* Report RL32114, Washington, DC,October 17.
-Congressional Research Service of the Library of Congress,Terrorist Capabilities for Cyber Attack-Overview and PolicyIssues, (2015). *Report RL33123,* Washington, DC, October 20.
-Federal Railroad Administration, (2009). Washington, DC, August.
http://freight.transportation.org/doc/FreightRailReport.pdf.
-National Capital Planning Commission, (2017). Rail RealignmentFeasibility Study Securing Freight *Transportation in theNational Capital Region*, NCPC Washington, DC, April.
-Notice Of Proposed Rule Making, (2018). Improving the Safety ofRailroad Tank Car Transportation of Hazardous Materials;Proposed Rule. *US Department of Transportation*, FederalRegister April 14.
-Railroad Research Foundation, (2018). Freight Rail Security ProgramGrant, *Department of Homeland Security*, March 31.
-Statement of Nancy Wilson, Vice President-Security, (2017). Association of American Railroads before the US Houseof Representatives Committee on Homeland Security,Subcommittee on Transportation Security and InfrastructureProtection, *Hearing on Railroad and Public transportationSecurity Efforts*, February 13, Washington, DC.
-Technology Information Policy, (2014). In-tergovernmental Relations and the Census, House Commit-tee on Government Reform, *Critical Infrastructure ProtectionChallenges and Efforts to Secure Control Systems*, Tuesday, March 30.
-The President's National Security Telecommunications Advisory Committee Wireless Task Force Report, (2013). *WirelessSecurity*, January.
-Transportation Security Administration, (2014).TSA Launches NewPassenger Rail Security Project, *Department of HomelandSecurity Press Release*, May 3.
-United States General Accountability Office, (2017). Testimony be-fore the Committee on Commerce, Science, and Transporta-tion, US Senate-Passenger Rail Security, *Enhanced Federalleadership needed to Prioritize and Guide Security Efforts*, Jan.
-United States General Accounting Office, (2014). Critical Infrastruc-ture Protection Challenges and Efforts to Secure Control Sys-tems, GAO Testimony Before the Subcommittee on Technol-ogy Information Policy, Intergovernmental Relations and theCensus, *House Committee on Government Reform*, Tuesday, March 30.
-Weinstein and Clower, (2006).The Impact of the Union PacificService Disruptions on the Texas and National Economies:An Unfinished Story, *Railroad Commission of Texas,* February.

Security Crises in the Infrastructure of the American Railway Network

Pejman Salehi, Assistant Professor, Faculty of Industrial Engineering,
Islamic Azad University, Parand Branch, Tehran, Iran.
Mehran Khalaj, Assistant Professor, Faculty of Industrial Engineering,
Islamic Azad University, Parand Branch, Tehran, Iran.

E-mail: pejmansalehi.metro@gmail.com

Received: August 2024- Accepted: December 2024

ABSTRACT
Rail transport industry an handle a large amount of products, goods or passengers during a wide, scattered and diverse geography, which is accessible and penetrated by intruders and attackers and is also vulnerable to all kinds of physical and cyber attacks, move Therefore, it is not possible to strengthen and improve the level of security in this vast network against various types of attacks and intrusions, and it faces many obstacles and challenges. In this study, an attempt has been made to investigate the position and strategic importance of cross-border railways for the transportation of goods and passengers in the United States and investigate an unclassified set of seemingly simple attacks that have had destructive and complex effects on the traffic of the railway network and the health of citizens in the United States. be paid Also, the range of security measures of the rail transport industry and the American government, as well as the decision-makers and active activists in this field, were analyzed to reduce the risk factor and manage the crisis in complex, ambiguous and uncertain situations and when there are intrusions and structured attacks on the rail network of this country. Take In this case study, the consequences of some successful attacks as well as the weaknesses and shortcomings of the American government system to ensure the security and safety of the rail transportation network in the implementation of programs and protective measures.

Keywords: Security, Safety, Crisis Management, Vulnerability