AI Poses New Cyber Threats, While Physical Ones Persist

Artificial intelligence is helping hackers spy better on networks and build faster, more efficient and more convincing tools for attacking them.

Rail operators, suppliers and regulators around the world face key policy, security and operational challenges in the coming year.

These include fortifying industrial bases against intense competition from China's state-owned rail car manufacturer, as well as warding off security threats from the operational technology and information technology (IT) in its products.

Another concern centers on cybersecurity risks intensifying as attackers tap the capabilities of readily available artificial intelligence (AI) tools and techniques. An underlying element is ongoing weaknesses in cyber resilience efforts of enterprises across the globe.

Also, in the face of ongoing criminal and terrorist threats, rail must maintain physical security for its customers, tracks, facilities and far-flung wayside infrastructure.

Concerning China's influence, U.S. efforts started 2025 with a boost. Effective January 21, the Federal Railroad Administration (FRA) put in place new freight car safety standards that target Chinese products.

A key change to the Code of Federal Regulations, Title 49, Part 215 says new freight cars "must be manufactured, assembled, and substantially transformed in a qualified facility by a qualified manufacturer" and restricts components "from countries of concern and state-owned enterprises."

The changes were championed by American rail car makers, suppliers and unions, as well as the Canadian Association of Rail Car Suppliers.

"Protecting the constant movement of critical goods and supplies on the U.S. freight rail interchange is not optional," said Erik Olson, executive director of the Rail Security Alliance, a lobbying outfit that also backed the changes. "Freight rail touches every state and economy in the U.S." Olson expressed confidence that President Donald Trump, who took office Jan. 20, would back the new standards.

CRRC is a key state-owned enterprise

By James T. McKenna

targeted by them. It is considered the world's largest rail car manufacturer, with contracts in more than 110 countries.

"The safety and security of our nation's freight rail system are of the highest importance," said FRA administrator Amit Bose prior to his departure at the end of President Joe Biden's administration. Required by 2021's bipartisan infrastructure investment law, the rule is "aimed at preventing the exploitation of freight cars for illicit purposes and the potential compromise of sensitive technologies within the industry" by stringently controlling "where freight car technology and materials originate."

In October 2022, the U.S. Defense Department included CRRC in a list of 60 "Chinese military companies" operating in the U.S. to support China's military-civil fusion strategy. It aims to modernize China's military, the Pentagon said, by having Chinese companies, universities and research programs "that appear to be civilian entities" acquire and develop "access to advanced technologies and expertise." (That followed a 2020 finding that also included CRRC. In 2021, then-President Trump banned Americans from investing in companies on that list.)

An October 2024 congressional report declared that the Chinese Communist Party "is engaging in warfare tactics against the [U.S.] with increasing efficacy." Published by the Republican majority staff of the U.S. House of Representatives' oversight and accountability committee, the report, "CCP Political Warfare: Federal Agencies Urgently Need a

The U.S. Department of Homeland Security (DHS) said it expects domestic and foreign adversaries "will continue to threaten the integrity of critical infrastructure with disruptive, destructive attacks."

Government-Wide Strategy," made several points. Among them: Chinese state-owned entities "manufacture over 95 percent of containers in the world's market, including U.S. domestic train and truck intermodal containers." Also, they are "the sole manufacturers" of 53-foot containers used by U.S. intermodal rail and trucking companies.

Despite past warnings, the report said, "CRRC has made aggressive and dangerous inroads" in American rail, including CRRC's 2015 opening of a Springfield, Mass. factory and a second in Chicago in 2017. From 2015 through 2020, the report said, CRRC won four U.S. passenger rail projects, in Boston, Chicago, Philadelphia and Los Angeles "by significantly undercutting the competition through below-market bids" with Chinese state-backed financing.

The U.S. is not alone in its concerns over industrial base harm.

Early last year, the European Commission (EC) launched an investigation into whether CRRC's Qingdao Sifang Locomotive Co., Ltd. used a market-distorting foreign subsidy to give it an unfair advantage in bidding for a Bulgarian government tender for 20 push-pull locomotive sets and related services. That was the EC's first use of new foreign subsidiaries regulation powers.

Weeks after the investigation started, CRRC withdrew its Bulgarian bid. (Siemens and Alstom had cited growing, subsidized competition from CRRC as a justification of their 2017 plan for Siemens to acquire Alstom. The EC blocked that plan.)

Questions have also been raised about CRRC's practices during bidding in Bolivia, Chile, Mexico and Peru.

Homeland Threat Assessment in U.S.

Regarding American rail security, the U.S. Department of Homeland Security (DHS) said it expects "domestic and foreign adversaries … will continue to threaten the integrity of our critical infrastructure" with disruptive, destructive attacks because they believe "targeting these sectors will have cascading impacts on U.S. industries and our standard of living."

Its 2025 Homeland Threat Assessment sees China, Russia and Iran as the most pressing foreign threats, with China continuing to pre-position itself on U.S. networks "for potential cyberattacks in the event of a conflict" with America. (Last March, the U.S. Department of Justice indicted seven Chinese nationals based in China as members of a hacking group backed by that nation that targeted US-based critics, businesses and political officials. The group reportedly has been active for about 14 years.)

DHS said state actors will join criminal hacktivists (attackers infiltrating systems to achieve political aims) and financially motivated criminals in honing their techniques to disrupt services or spy for vulnerabilities in U.S. networks.

Europe Attempts to Prioritize Cyber

In Europe, the latest threat landscape report from the European Union Agency for Cybersecurity (ENISA) said "transport is the second most targeted sector." Executive director Juhan Lepassaar said, "The recent emergence of cybersecurity attacks in railways, along with geopolitical tensions, indicate that it is crucial to prioritize cybersecurity to safeguard critical infrastructure."

Achieving prioritization is a cybersecurity challenge in itself. A survey of 2,600 IT cybersecurity leaders across the globe is among the latest reports on the gap between corporate statements of concern about cyber vulnerability and actual spending on efforts to build cyber resilience.

Commissioned by the global cyber security software company Trend Micro, Sapio Research interviewed the leaders from organizations of all sizes and various activities and prepared the report, "The CISO Credibility Gap: A Global Trend Micro Study."

Many CISOs (chief information security officers) "struggle to be heard by their boards," the report found. "That creates a fundamental credibility gap which many are finding difficult to close."

Those interviewed were aware of the close link between cyber and business risk but cannot convince top executives and boards of directors, the report said. That jeopardizes their organization's cyber resilience of the organization.

Over a third of leaders interviewed said cybersecurity is still treated in their organization as part of IT rather than a business risk. Eighty percent said their board of directors would only be incentivized to act decisively on business risk if a cyber breach occurred.

Nearly 80 percent said they have felt pressure from the top "to downplay the severity of cyber risks facing their organizations," the report said. "Of those, 43 percent said it was because they are seen as being repetitive or nagging, while 42 percent said they are viewed as overly negative. A third claimed that they had been dismissed out of hand."

Cyberattacks Doubling Annually

Trends suggest cyberattacks on railways are doubling annually, according to analysts for the engineering consultancy Ricardo. The firm's global managing director for rail, Michael Newman, and its leader for independent security assessment (Cyber), Tony Gao, operators and others in Belgium, Denmark, France, Germany, Italy, India, Poland, the United Kingdom and the U.S. have all reported malicious network assaults recently.

"Rail systems are undergoing a profound digital evolution, integrating advanced technologies like the Internet of Things, the Cloud, AI, and connected control systems to deliver day-to-day efficiencies," Newman said. "However, these advances have also brought increased exposure to cyber threats."

One force behind the rising threat against railroads is Russian interest in disrupting European countries' ability to support Ukrainian efforts in fighting the ongoing Russian invasion there. For instance, in late 2023 hackers infiltrated the VHF radio system of Poland's rail network, sending emergency stop messages throughout the network and causing widespread disruption. Last September, Poland deputy prime minister, Krzysztof Gawkowski, told Reuters cyberattacks had doubled since then, particularly targeting Polish organizations that run military deliveries to Ukraine.

"Cybersecurity is an arms race between attackers and defenders," American Association of Railroads president and CEO Ian Jeffries told the U.S. House Homeland Security Committee Nov. 19, 2024. He said the industry taps highly skilled, well-trained employees to "guard against cyberattacks that threaten the safety and integrity of our operations."

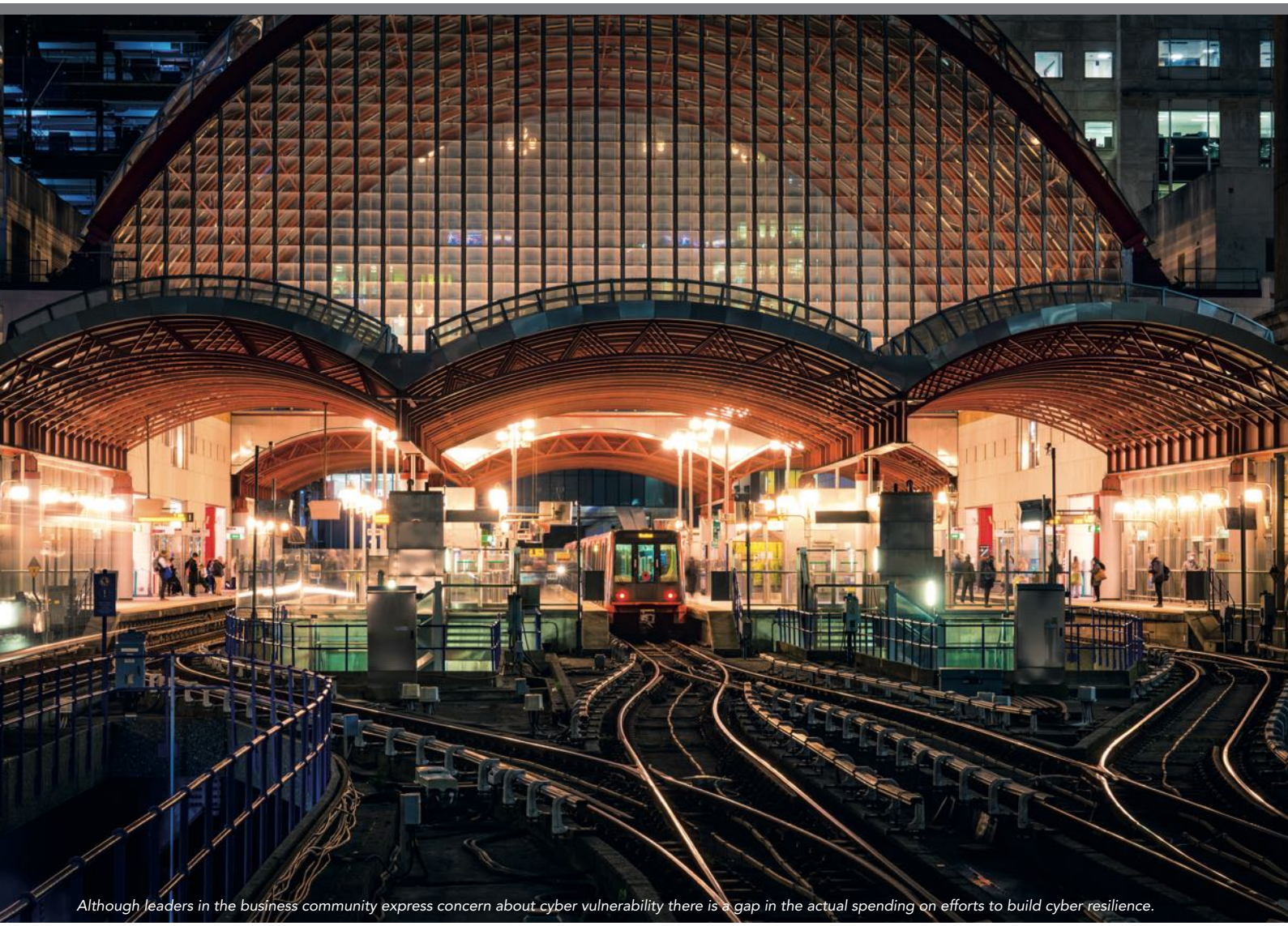
The battlefront in that arms race is continually expanding as cybercriminals as well as agencies and accomplices of national governments refine their techniques and exploit new "attack vectors."

"The threat surface is getting bigger all the time," said Daryl Plummer, managing vice president and chief of research for Gartner, Inc. last October in Orlando, Fla. at that technological research and consulting firm's annual information technology symposium, Xpo.

Cyber threats must be countered while rail operators also guard against physical attacks on their infrastructure. That was highlighted on July 26, when saboteurs torched signal lines along tracks connecting Paris with Lille, Bordeaux and Strasbourg in the north, west and east, respectively. (An attack on the line south to Lyon and Marseille was foiled.) The attack came on the opening day of the Summer Olympics. Based in Paris, the Games held events elsewhere, including the four other cities. The attack disrupted service for approximately 800,000 people.

Further proof of rail's physical vulnerability came the following week in Germany when fires damaged signaling on Deutsche Bahn lines between Bremen and Hamburg and, days later, between Berlin's main station and Spandau to its west.

In Pakistan on the morning of Nov. 9, a suicide attacker blew himself up in a crowded station in Quetta, the capital of the western province of Baluchistan.



Although leaders in the business community express concern about cyber vulnerability there is a gap in the actual spending on efforts to build cyber resilience.

The blast, responsibility for which was attributed to a provincial separatist group, killed 32 and injured 65.

AI To Play A Role in Cyber Threats

A big part of the growing cyber threat surface that Plummer cited is the already-evident rapid increase in attackers' application of artificial intelligence (AI) to their efforts.

More and more malicious actors will adopt AI tools to aid online operations throughout attack life cycles, numerous analysts said. They foresee more convincing phishing efforts as well as "vishing" — phishing attacks using convincing phone calls relying on faked but familiar voices — and other social engineering attacks to steal identities and commit other fraud.

AI-based attacks can be particularly effective at bypassing customer-identification and due-diligence elements of know-your-customer (KYC) security safeguards through their greater capability to develop deep-fake avatars of real people. AI also provides actors with greater, faster capability to do reconnaissance on a target company and test the vulnerability of its employees and systems.

That AI aspect will worsen as business enterprises expand their replacement of workers with AI agents (systems or programs designed to autonomously perform tasks currently done by humans). Boston Consulting Group's latest AI Radar report, released in January, surveyed 1,800 executives worldwide on their companies' plans. Three in four said AI is a top-three strategic priority for their companies. Two-thirds of companies are exploring the use of AI agents, respondents said. The consultancy noted "2025 could mark a turning point for their adoption."

By 2028, Gartner analysts predict, one in four cyber assaults will exploit AI agents. Humans can't respond to the speed and efficiency of AI-based attacks, Plummer said, so enterprises must invest in more mature security environments.

AAR's Jeffries said the American rail industry's cyber challenges include a lack of analysis of cyber incidents by the federal government, which can leave operators unaware of developing threats and how to reduce susceptibility to them. "Further analysis of an attack or other incidents by the government can inform railroads' decisions about strengthening our network," he said.

Another challenge, Jeffries said, is the U.S. government's focus on transportation company cybersecurity risks that overlooks ensuring the security of industry suppliers. "Suppliers play a critical role in various aspects of railroad operations," he said. "The government should consider how best to directly address their vulnerability to cyber incidents." TSI