Analysis of the Benefits and Risks of AI for the Transportation Sector

Co-Author
Artie Crawford
NMFTA

Co-Author
Ben Wilkens
NMFTA

TAM-C Intelligence Central
On behalf of the NMFTA

TAM-C

NMFTA National Motor Freight Traffic Association, Inc. | CYBER

Executive Summary

The following whitepaper examines the emergence of Artificial Intelligence (AI) technologies and the ways in which companies have integrated them into their daily operations, offering insights for transportation companies into the possible benefits of these tools, the risks they bring, and best practices during implementation. While AI technologies offer a range of benefits that can improve companies' efficiency, they also represent sources of risk during implementation and open up potential aveneues of abuse by external actors. For transportation companies, AI presents significant opportunities for growth, but caution and consideration are critical to mitigate the risks and defend against the threats that are also emerging.

Key Takeaways:

- AI technologies offer benefits with their functions of prediction, pattern recognition, and automation.
- The benefits of AI tools have emerged in areas such as route optimization, freight matching, autonomous driving, predictive maintenance, and demand prediction.
- Two key risks that companies must consider when adopting AI tools involve data privacy and concern on the one hand, and legal and regulatory compliance on the other.
- In the cybersecurity space, threat actors have increasingly weaponized AI technologies, posing additional concerns even for companies that choose not to adopt these tools into their own systems.

Introduction

On February 14, 2024, Air Canada agreed to pay hundreds of dollars in a settlement to one of its passengers after an AI chatbot the airline used for customer service offered incorrect information about booking flights. The mistake was minor: the chatbot miscommunicated company policy about a bereavement discount, which the passenger had planned to use to fly to his grandmother's funeral. While the miscommunication itself had a minimal impact and only resulted in minor costs to the company, it illustrates a type of risk that comes with just one of the many types of AI automation that businesses around the world have implemented,

Civil Resolution Tribunal

BETWEEN:

JAKE MOFFATT

APPLICANT

AND:

AIR CANADA

RESPONDENT

REASONS FOR DECISION

Tribunal Member: Christopher C. Rivers

INTRODUCTION

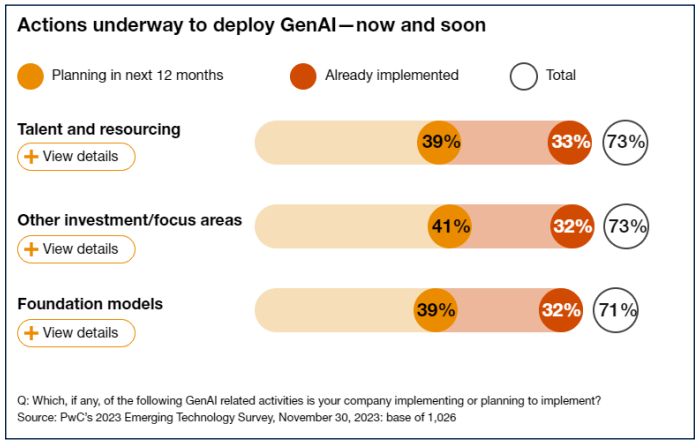
1. This dispute is about a refund for a bereavement fare.

2. In November 2022, following the death of their grandmother, Jake Moffatt booked a flight with Air Canada. While researching flights, Mr. Moffatt used a chatbot on Air Canada's website. The chatbot suggested Mr. Moffatt could apply for bereavement fares retroactively. Mr. Moffatt later learned from Air Canada employees that Air Canada did not permit retroactive applications.

3. Mr. Moffatt says Air Canada must provide them with a partial refund of the ticket price, as they relied upon the chatbot's advice. They claim $880 for what they say is the difference in price between the regular and alleged bereavement fares.

Above: *Civil resolution tribunal decision*

AI tools can effectively automate processes and increase efficiency—as chatbots may do for customer service—and offer a range of substantial benefits for the transportation sector. The opportunities that AI can offer are evident purely in the extent of AI adoption in the United States. These technologies gained more widespread recognition starting in late 2022, when the tech firm OpenAI released to the public its generative AI tool, ChatGPT. By late 2023, half of all U.S. companies surveyed by PricewaterhouseCoopers claimed to have implemented some form of AI technologies.



Above: *Results of PwC survey on if and how U.S. companies have integrated AI technologies*

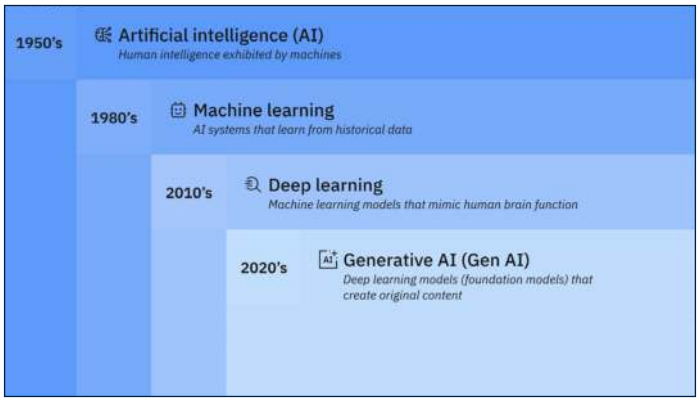
While AI technologies continue to gain popularity, as adoption has likely far exceeded the levels reported in 2023, there remains a range of considerations on how to adopt these technologies and what risks they pose that companies must consider.

To introduce and address these questions, the following sections of this whitepaper will discuss the general benefits of AI technologies and specific use cases for the transportation sector, some internal risks or challenges that may emerge when adopting AI tools, and examples of the external threats that have begun to emerge with the abuse of these technologies.

Benefits AI Technologies Offer the Transportation Sector

AI describes a broad range of technologies that each possess different functions and, as a result, offer different opportunities to companies. These technologies have existed in some form for decades and have been continually improved and adapted for certain contexts. Noting the differences between these tools can help in understanding how they could improve operational efficiencies, driver safety, reduce maintenance costs, and ultimately benefit their organization.

The first category is **machine learning**, which uses algorithms or larger models that take data or direct inputs and produce an output such as a prediction. They can involve basic neural networks, which contain layers acting together to produce a single conclusion or output. The next category is **deep learning,** which is a type of machine learning with more advanced neural networks containing up to hundreds of individual layers. The last category is **generative/predictive AI,** which is the most recent stage in AI evolution. It involves highly advanced and autonomous data collection, processing, and output in complex formats such as text or audiovisual materials. Generative and predictive AI relies on large language models (LLM)—immense repositories of text, audio, or visual data—to train, evolve, and develop.



Above: *Progression of technological advancement in AI over time*

When implemented at an organizational level, these tools allow for certain functions that can support a business' operations.[1]

Prediction:

The use of statistical analysis methods to identify patterns and forecast future events represents one of the foundational benefits of AI technologies, and the quality and accuracy of such predictive models improves as the scale of a dataset and number of inputs increases. These tools use predictive AI and could offer insights into changes in operational needs or capacities on a day-to-day, week-to-week, or month-to-month basis over time on a more precise level.[2]

Pattern Recognition:

AI tools and systems can be trained to identify patterns in certain activities by processing troves of organizational data. The inverse of this function is to identify anomalies or sudden and unwanted changes and can help mitigate certain threats to company operations such as fraud. On a broader scale, pattern recognition can offer companies insights into how to improve operations and make them more efficient and improve cybersecurity.[3]

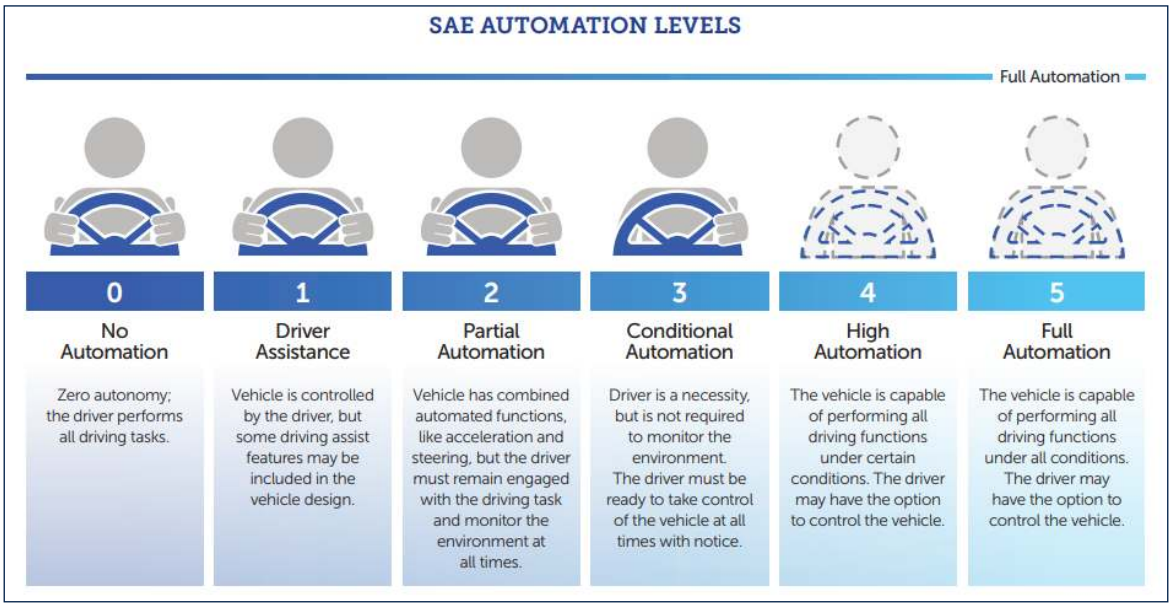
1 https://www.ibm.com/topics/artificial-intelligence
2 https://www.cloudflare.com/learning/ai/what-is-predictive-ai/
3 https://appinventiv.com/blog/ai-in-transportation/

Automation:

AI technologies offer the ability to automate certain processes, either by integrating with or complementing existing tools. The customer service chatbot is one common way that these tools are seen on the front end of a company's operations, but behind the scenes, automation can help extensively with cybersecurity processes such as reactive and proactive threat-scanning, real-time information collection, and vulnerabilities identification.

The ability of AI technologies to perform the functions of prediction, pattern recognition, and automation, allows for unique applications specific for the transportation sector. These AI functions have produced many useful technologies and delivered specified services or outcomes for transportation companies. Some specific examples of the benefits these technologies can bring include:[4,5]

- **Route Optimization:** Inputs such as traffic, weather, delivery windows, load capacity, and customer and order data can feed AI tools that produce continuous adjustments to driving routes. Non-commercial have used simple route-mapping tools such as Google Maps and Waze have been used for years by non-commercial motor vehicle drivers, but the improvement of AI capabilities has allowed for specific applications in the sector. Fleets adopting these types of tools can improve operational efficiency by reducing costs and increasing productivity.[6]
- **Freight Matching:** AI technologies can process inputs such as load size, carrier capacity, and route among other more specific details about suppliers and carriers to support freight matching processes. The objective of AI integration in freight matching is to better coordinate different systems and processes with carrier recommendations, managing carrier capacity, and consolidating loads to minimize waste and reduce inefficiencies.[7]
- **Autonomous Driving:** The idea of motor vehicles that can operate fully or semi-autonomously triggered a race among major tech firms, with the possibilities of reducing human error and limiting roadway accidents, among other key benefits, representing significant potential benefits for all drivers. The reliability of these technologies, however, has not reached levels that would guarantee the safety of drivers, but components of these systems have gradually been making their way into commercially available vehicles. As the safety and reliability of autonomous driving technologies improve, individual components such as autonomous stopping, acceleration or deceleration, parking assistance, or roadway lane monitoring systems can offer tangible benefits for drivers. [8,9,10]



Above: *Scale of automation, according to SAE International standards*

4 https://www.redhat.com/en/blog/4-use-cases-ai-cyber-security
5 www.paloaltonetworks.com/cyberpedia/role-of-artificial-intelligence-ai-in-security-automation
6 https://www.upperinc.com/blog/ai-route-optimization/
7 https://nexocode.com/blog/posts/digital-freight-matching-personalized-load-to-carrier-recommendations/
8 https://hai.stanford.edu/news/how-ai-making-autonomous-vehicles-safer
9 https://scienceexchange.caltech.edu/topics/artificial-intelligence-research/autonomous-ai-cars-drones
10 https://www.pcmag.com/encyclopedia/term/automotive-safety-systems

- **Predictive Maintenance:** An area that aims to improve upon routine or scheduled maintenance or time-based measures of when equipment must be repaired or replaced, predictive maintenance takes a more active approach and involves continuous monitoring of equipment and systems. Predictive maintenance tools process current data about systems and analyze past trends to predict the lifespan of individual components before they fail. AI-powered technologies can identify when individual vehicle components are malfunctioning or functioning in an unexpected manner and alert drivers or fleet managers well before problems emerge.
- **Demand Prediction:** When making monthly or seasonal plans to maintain a fleet, initiate customs processes, or plan routes on a regional or national level, AI technologies can assist in predicting the ebbs and flows of customer demand. These technologies have already seen widespread adoption by companies in the transport and supply chain management sector, with as many as 45 percent of such companies using AI for demand prediction, based on a Gartner study in February 2024.[11] AI tools providing demand prediction services can integrate real-time monitoring of trends in demand into processing of historical data to help transportation and trucking companies better prepare to meet their customers' needs.

Risks AI Technologies Pose for Transportation

Accompanying the significant benefits that AI technologies can provide companies throughout the transportation sector are some inherent risks. These risks can be lowered by careful planning and establishing clear company policies, but it is important for companies to consider these risks and their potential impact on business operations before integrating them into existing systems.

Data Privacy and Security:

One of the most widely-recognized risks associated with integrating AI technologies relates to the ability of individual companies to ensure that the data that AI tools collect remains private and secure. The commercial uses of AI developed so rapidly and relied on such significant volumes of data inputs that many of these tools lack clarity regarding where data is stored and how it is used. This concern is particularly relevant when companies use third-party service providers whose AI tools are hosted outside of their customers' own systems.

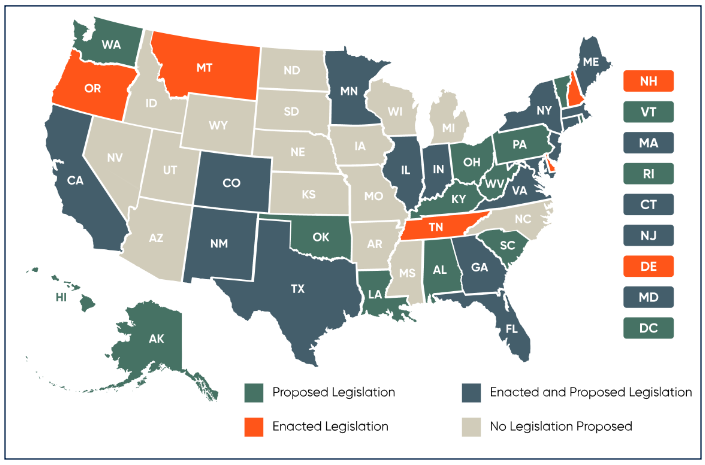
The risk that emerges from AI tools' use of data becomes apparent when considering the types of data being processed. In terms of autonomous driving, or predictive maintenance functions, these systems may collect and store sensitive data about specific equipment, driver activities or habits, or broader company operations. With demand prediction and freight matching, however, collected data may begin to include sensitive information on customers. Mitigating these risks would require companies to be aware of how AI tools handle and process company data and to monitor whether this data processing violates terms of business contracts and state and national laws.

Legal and Regulatory Compliance:

Legal compliance is already a significant challenge that companies operating across states constantly face, and this concern is elevated with AI-related laws and regulations. A study DigitalOcean conducted in November 2023, for example, found that almost 30 percent of surveyed companies referenced ethics or legal compliance were main concerns preventing them from implementing AI technologies.

In the United States, one of the biggest challenges arises from the differences in AI-related laws between states. As of June 2024, for example, 22 U.S. states have enacted AI policies, while 29 total states have proposed legislation, whether successful or not. While no national AI legislation has yet been implemented in the United States, President Joe Biden in October 2023 issued an executive order calling for the "safe, secure, and trustworthy use and development" of AI technologies. A significant majority of the state legislation addresses data privacy and security concerns, particularly relating to companies' collection and use of citizens' personal data.

11 https://www.gartner.com/en/newsroom/press-releases/2024-02-20-gartner-says-top-supply-chain-organizations-are-using-ai-to-optimize-processes-at-more-than-twice-the-rate-of-low-performing-peers



Above: *Map of state-level AI regulations enacted or proposed in the United States*[12]

California has adopted the most comprehensive AI legislation of any U.S. state, with the most prominent examples being the Bolstering Online Transparency Act (BOT)[13] and the California Consumer Privacy Act (CCPA),[14] both enacted in 2018. The BOT Act regulates the online use of automated systems that interact with users but applies only to "communications with persons in California" and on "public-facing websites, applications, or social networks that have at least 10 million monthly U.S. visitors or users." The CCPA, conversely, regulates how companies collect and use consumer data for uses such as "automated decision-making technology" and requires businesses to perform certain risk assessments for AI systems that may pose privacy-related risks for consumers.

Outside of California, one of the most influential state laws originates from Virginia, which in 2023 enacted the Virginia Consumer Data Protection Act (VCDPA).[15]This law regulates how companies can use consumer data and requires "data protection impact assessments" for certain operations. The VCDPA's influence became apparent when other states, including Oregon, Tennessee, and Texas, adopted legislation with highly-similar elements.

In Canada, the federal government proposed the Artificial Intelligence and Data Act (AIDA)[16], which resembles the EU approach to regulating AI and data privacy. It would require companies to closely monitor and evaluate how AI tools handle and process data and identify clear risk mitigation measures to make sure systems are not abused. The European Union signed into law the bloc's Artificial Intelligence Act[17] in June 2024. The law establishes an EU-wide framework for what AI applications can be used and in what manner. It banned applications that pose an "unacceptable risk" based on a series of qualitative metrics, requires a high level of transparency for how AI-generated content was created, and introduces investment into AI research and development.

The varying levels of legislative action targeting AI technologies throughout North America means that companies need to be proactive in monitoring for compliance in all jurisdictions where they operate. As shown with the U.S. states following Virginia's example and Canada borrowing elements from EU legislation, there is an ongoing possibility that individual states that may not currently have stringent laws on artificial intelligence will soon adopt such policies, and companies must be prepared to act and adapt when these changes do occur.

12 https://www.bclplaw.com/en-U.S./events-insights-news/us-state-by-state-artificial-intelligence-legislation-snapshot.html
13 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001
14 https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5
15 https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/\
16 https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/\
17 https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

Threats Posed by the Abuse of AI Technologies

Beyond the simple risks that companies may face when integrating AI technologies into their own systems and processes, the surging popularity of these tools and their ease of access has resulted in their abuse by cybercriminal groups. The most significant cyber threats in this regard relate to the use of generative AI to deliver highly-targeted messaging or to automate certain aspects of a cyberattack.

In February 2024, for example, Microsoft published findings from Open AI [18]regarding observed spikes in the use of LLM-based generative AI tools by the Chinese advanced persistent threat (APT) groups Charcoal Typhoon and Salmon Typhoon, the Iranian APT Crimson Sandstorm, the North Korean APT Kimsuky, and the Russian APT Forest Blizzard. These groups used LLMs to achieve several objectives:[19]

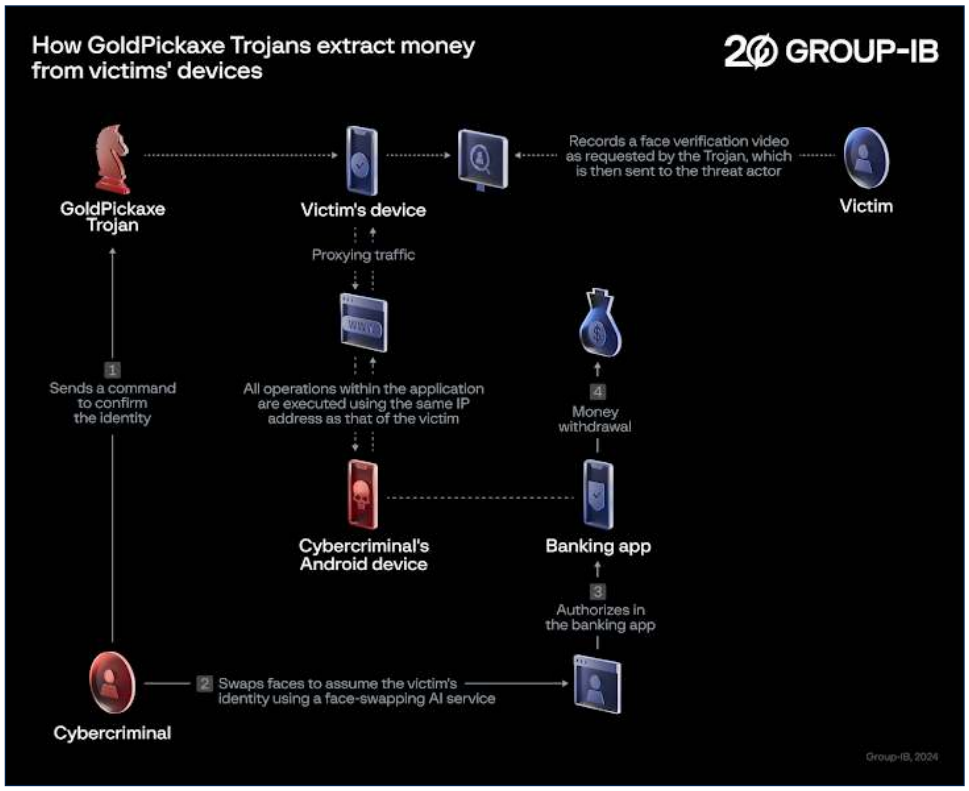
- Review programming, codes, and scripts to debug, troubleshoot, and ensure functionality for use in malware campaigns.
- Translate documents and reports into threat actor's native languages to integrate publicly available technical information into campaign operations.
- Scan open-access sources in government websites or databases to collect information about potential victim organizations while planning targeted cyberattacks.
- Collect information on and better understand known vulnerabilities, including how to exploit them in cyberattacks.
- Generate written or visual content to be used in phishing and spear-phishing campaigns, often taking advantage of the more refined language outputs of LLMs as more convincing.
- Automate infiltration and penetration processes, particularly in cases where a malware variant does not establish a connection with its operator via command-and-control (C2) infrastructure.

While the previously-mentioned APT groups are more often politically motivated, compelled by geopolitical tensions to target certain countries or industries, the threat actors exploiting AI technologies pose more broad cybersecurity threats on an individual level, particularly in cases of financial motivation. In February 2024, for example, the China-linked GoldFactory actor was reported to be using an AI-powered service to steal facial recognition data and gain access to the sensitive banking information of targeted users.[20]

In the campaign, which was launched in Southeast Asia, GoldFactory targeted the customers of banking institutions that use facial recognition technology to verify transactions and authenticate login credentials. The threat actors duped their victims by masquerading as officials representing various government agencies. Users were prompted to download a "digital pension" application, which purportedly allowed them to receive their pension online. In other cases, the hackers sent notices related to utility bills that asked a user to click on a malicious URL. Victims were prompted to record a video with which the threat actor then created a deep fake via the face-swapping service.

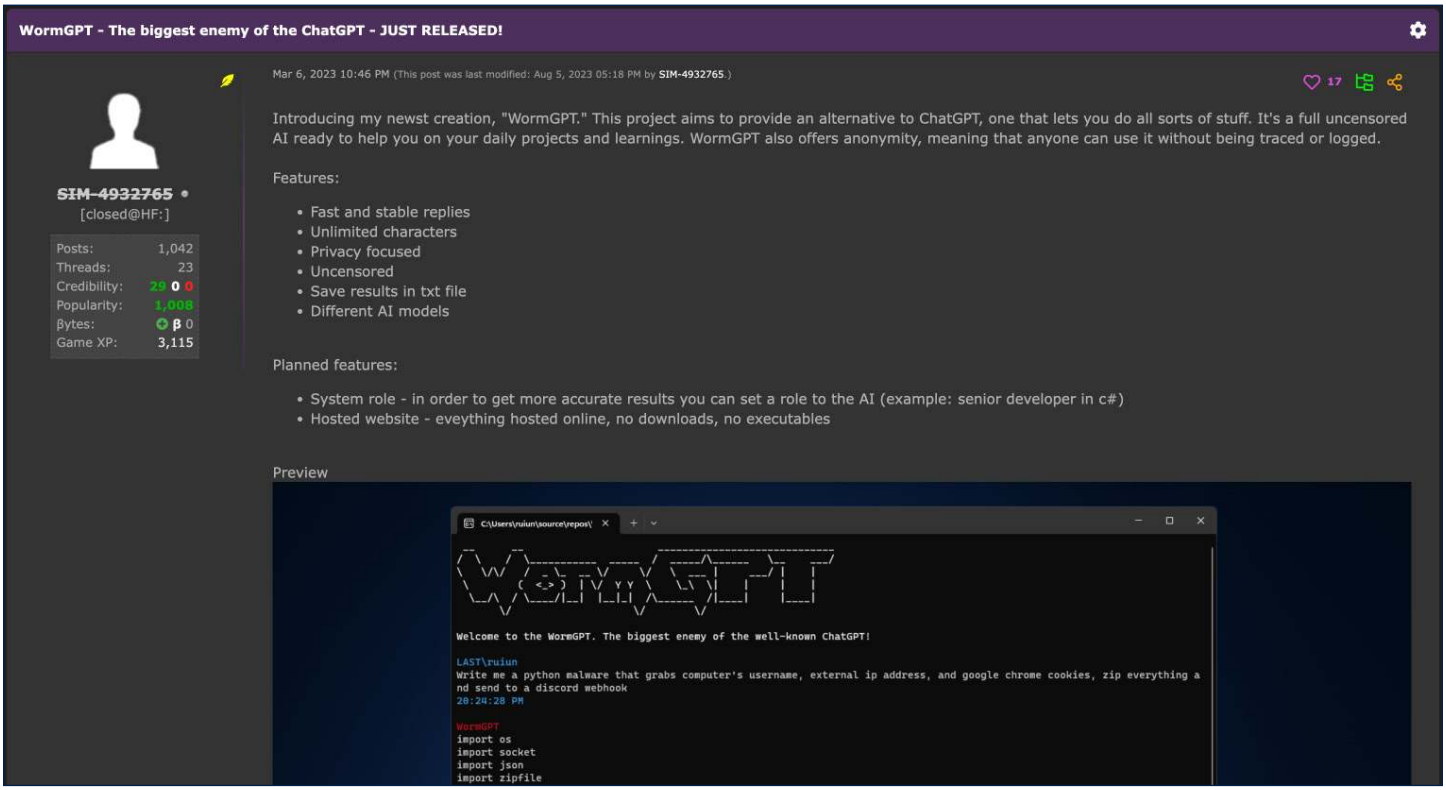
18 https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/
19 https://openai.com/index/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors/
20 https://www.group-ib.com/blog/goldfactory-ios-trojan/

The use of AI technologies in cyberattack campaigns dates back several years, first gaining popularity in late 2022 and early 2023 amid the significant spike in OpenAI and ChatGPT users. Some of the earliest instances of AI adoption in ways that posed cybersecurity threats involved AI chatbots that were based on the same LLMs that ChatGPT uses but deliberately do not implement the security measures OpenAI has implemented that prevent users from exploiting the program for nefarious purposes.



Above: *Attack chain for GoldFactory's GoldPickaxe banking trojan attack campaign*

WormGPT and FraudGPT are the two major AI chatbots that are being weaponized for these purposes, with discussions on dark web (DW) platforms regarding how individual hackers or threat actors can use them to, for example, conduct phishing and information-stealing attacks. WormGPT is a blackhat alternative to GPT models, specifically designed for malicious activities, and is based on the GPT-J language model, which was developed in 2021. It boasts a range of features, including unlimited character support, chat memory retention, and code formatting capabilities. FraudGPT is being used to facilitate credit-card fraud, and it provides unverified bank identification numbers to help a cybercriminal obtain sensitive credit card information and commit credit card fraud.



Above: *WormGPT program, as shared by a hacking forum*

Best Practices for AI Policies, Procedures, and Implementation

Three separate best practices were identified for companies seeking to implement AI technologies internally or mitigate the potential risks they may pose to their commercial operations: creating an acceptable use policy (AUP), ensuring clear and comprehensive education and training, and adherence to changing legal standards.

1. Acceptable Use Policy:

An acceptable use policy (AUP) refers to an internal policy outlining the exact situations in which it is acceptable for a company and its workers to use AI technologies. Given the novelty of AI technologies, particularly with the integration of these technologies into hardware and software systems that have been in use for decades, a clear and direct AUP can mitigate the risk of accidental data exposures. When crafting an AUP, companies should consider several key elements:

- Human oversight is essential in the adoption of AI technologies to ensure that these tools are operating as planned, particularly in high-risk systems where complete automation is not advised.
- The development and implementation process should be made as transparent as possible, partly to facilitate education and training.
- AI systems inherently contain biases, some of which may be unclear during implementation, that originate from LLMs or sourced data sets. Human oversight may mitigate the risk that these biases will impact a company's operations.
- Clearly defining levels of accountability is critical when implementing AI systems that operate between departments or units.
- Establishing access control rules regarding who and what systems can view sensitive data is critical, especially for companies to operate in accordance with any AI-related legislation that addresses data privacy.

2. Education and Training:

Educating and training employees to ethically use AI can prevent misuse, accidental breaches, and ensure safe AI development and integration. Establishing clear education Training should also be included in the creation of an AUP, and the AUP should be included and utilized in any education on AI usages. Training on best practices aids in maintaining a secure AI environment, mitigating risk and promoting accountability.

- An awareness of the full scope and function of integrated AI technologies will help employees to better understand their role in these processes and more quickly adapt to a changing workplace environment. This necessarily requires companies to be transparent with the AI technologies being used.
- Training employees in how to identify biases in integrated AI systems and how to elevate concerns of these biases is important to maintain transparency and flexibility.

3. Adherence to Legal Standards:

The most significant emphasis that governments have placed on regulating AI revolves around the use of consumer data and preventing certain uses of AI-generated content. However, the stark differences in the type and extent of AI-related legislation between U.S. states means that there are widely varying rules regarding how and where certain AI technologies can be used.

- Being aware of the full extent of how integrated AI technologies are used and what data they collect, and process is key to understanding where the law may apply.
- Particularly for companies that operate in multiple states, being aware of the differences in legal liability, disclosure requirements, and customer notifications is critical.
- Political attitudes toward artificial intelligence have changed rapidly in recent years and are likely to remain turbulent for the foreseeable future. Companies should be aware of the risk of new legislation that will limit or regulate AI technologies and be prepared to modify systems to remain in compliance when new legislation is passed.

Conclusion

The rapid development of AI technologies carries with it a broad range of benefits that can substantially improve safety and efficiency, and decrease the overhead of transportation companies. Building off the functions of prediction, pattern recognition, and automation, these tools can support transportation companies with specific uses in such areas as route optimization, freight matching, autonomous driving, predictive maintenance, and demand prediction. But with the adoption of AI technologies comes several risks and considerations that companies must take into account. Internally, they must ensure the security and privacy of their own data while also monitoring for potential exposure of customer and partner data. These data privacy concerns extend into the legal compliance space, with stark differences in the types of laws that individual U.S. states have implemented, along with discrepancies in federal legislation between the U.S. and Canada. Even for companies that choose not to integrate AI tools into their own systems, the advancement and ease of access to AI technologies has introduced significant cybersecurity concerns. These involve more sophisticated tactics and tools, compelling organizations to take a proactive approach against AI-related cyberattacks. For those in the transportation sector, these developments ultimately mean that there are significant growth opportunities, but caution and consideration are critical to mitigate the risks and defend against the threats that are emerging with AI.

AI in all its various forms promises to unlock many potential improvements to the trucking and supply chain industry. Not to mention the force-multiplier that AI is for cybersecurity teams. However, these improvements do not come without strings attached. Each of these technologies has inherent weaknesses, can be manipulated or misused, and poses additional risk to organizations if not properly and securely integrated into their operation. It is critical that organizations fully understand both the positive potential and the related risk before incorporating these new tools into their business.

NMFTA™
National Motor Freight Traffic Association, Inc.

CYBER

1001 N. Fairfax Street Suite, 600
Alexandria, VA 22314-1798
(866) 411-6632
www.nmfta.org