MAKING AI COUNT IN THE ECC

The technology transforming public safety communications carries risks and rewards.

By the APCO Cybersecurity Committee

Today, as we settle in behind a console or near a service monitor, we find ourselves at the forefront of fast-changing technologies. How we react to those changes and what we choose to do with them will shape our futures as emergency communications professionals. Adaptability will improve service, and one area ripe for adaptation is artificial intelligence (AI) — for call taking, dispatch or technical roles.

This raises the question of what AI deployment looks like in the emergency communications center (ECC) call processing environment. Addressing key areas such as call triage, call diversion, geo-fenced hotspots (based on a sudden uptick in call volume), transcription, multi-language transcription and multi-language interpretation would have to be near the top of the list. If we factor in just a few of these few changes, we've significantly lowered the public safety telecommunicator (PST) workload. For example, routing routine calls to a more precise department means no more garbage pick-up or fireworks schedule calls. In a 9-1-1 call that includes a language barrier between the telecommunicator and the caller, AI can mean quicker interpretation, potentially transcribing the text of the conversation on the CAD call screen.[1]

WHAT IS ARTIFICIAL INTELLIGENCE (AI)

AI is a branch of computer science that focuses on creating systems capable of performing tasks that typically require human intelligence. These tasks include understanding natural language, recognizing patterns, solving problems and making decisions. At its core, AI combines algorithms and data to learn, adapt and respond autonomously or semi-autonomously to different situations. It encompasses a wide range of techniques, including machine learning, natural language processing and computer vision, which together enable machines to interpret and interact with the world around them.

HOW AI IS CURRENTLY BEING USED IN ECCS

In ECCs, AI is transforming operations by enhancing efficiency, accuracy and responsiveness. AI-powered tools streamline call handling, improve data processing and support decision-making. Key applications include:

- Automated call triage and routing: AI systems can analyze incoming calls to prioritize emergencies and route them

JD8/SHUTTERSTOCK.COM

to the appropriate responders or departments. This ensures critical calls receive immediate attention.

- Natural language processing (NLP): AI-powered speech recognition helps transcribe and analyze 9-1-1 calls in real time, identifying key details like location, type of emergency and urgency. This reduces the workload on PSTs.
- Predictive analytics: AI models analyze historical data to predict patterns in emergency incidents, such as peak times or locations, enabling better resource allocation and staffing.
- Real-time translation: For non-English-speaking callers, AI can assist with instant language translation, bridging communication gaps and ensuring no critical details are lost during an emergency.
- Incident analysis and insights: AI tools can analyze data collected during incidents to uncover trends, optimize response strategies and improve long-term planning.
- Monitoring and alerting: AI systems can monitor social media, internet of things (IoT) devices and other data sources to detect emergencies early, providing an additional layer of situational awareness for ECCs.

By integrating AI into their workflows, ECCs are improving their operational efficiency and ensuring a faster, more accurate response to emergencies. This adoption of AI is paving the way for smarter, safer and more connected public safety systems.

One of the contributors to this article, Charles Vitale, 9-1-1 Shift Supervisor, Emergency Communications Department, Rochester, New York, describes how his department used AI to dramatically reduce the time needed to create standard evaluation guidelines (SEGs) for its daily observation reports (DORs).

The department had implemented new software that required SEGs for three different sets of DORs (call taking, police dispatch and fire dispatch). Each DOR contains approximately 15 categories and a seven-number rating scale. Manually creating over 300 individual SEG ratings was a daunting task that would have significantly delayed the program's launch. Recognizing the potential bottleneck, the department turned to AI for assistance. Providing well-worded prompts to a commercial AI program generated the wording for each number on the rating scale for every category across all DORs. AI saved over 120 hours of work, reducing the time to complete a task that could have taken several weeks to just a few days. It proved instrumental in expediting the implementation of the new software, ensuring a timely program startup.

IS ARTIFICIAL INTELLIGENCE SAFE AND SECURE IN PUBLIC SAFETY?

AI has the potential to enhance public safety by improving emergency response times significantly. However, its use also comes with risks such as cybersecurity challenges, accuracy and fairness. These areas are critical when lives are on the line. AI systems must be thoroughly tested and constantly monitored to prevent errors, cyberattacks or biases that could impact decisions. An example of this challenge is cyber threat actors subtly altering data to bias the AI's response to situations. This can lead to misclassification, false positives or false negatives, potentially causing security breaches. Mitigation strategies include using diverse datasets, conducting regular audits and combining AI with human oversight. Methods by which AI can be manipulated include:

1. **Data poisoning attacks.** According to the National Institute of Standards and Technology (NIST), a data poisoning attack involves an adversary deliberately injecting malicious data into the training dataset of a machine learning model. This manipulation aims to alter the model's behavior and degrade its performance, leading to incorrect predictions or classifications.[2]
2. **Prompt injection attacks.** These are one of the most widely reported weaknesses in large language models (LLMs). A prompt injection attack involves manipulating the input prompts given to LLM to cause unintended or unauthorized actions. There are two types: direct prompt injection when a user enters a malicious prompt directly, and indirect prompt injection when an attacker poisons the data sources that the LLM relies on.[3]
3. **Data privacy and leakage.** Data privacy and the risk of data leakage are major concerns for public safety agencies, which handle highly sensitive information. It's essential that AI tools used in these environments meet strict cybersecurity standards to prevent breaches. Data leakage refers to the unintended exposure of confidential or sensitive information, which can occur when an AI model inadvertently reveals such data through its outputs, training data or interactions. This can compromise investigations, personal privacy or public trust.

AI AND TECHNICAL SERVICES

What does AI bring to the service bench and transceivers used in a given jurisdiction? One of the greatest benefits would be AI's ability to analyze patterns of radio usage to ensure seamless communication and prevent interference. Technical services managers, directors and the agency FCC license holders stand to gain the most, especially when looking for additional frequencies to expand the reach of existing radio systems. More importantly, deep learning-based education models facilitate awareness of the operational environment and promise to offer end-to-end learning for creating an optimal radio system.[4]

ONBOARDING AND ONGOING EDUCATION

When we train new hires starting their career in the ECC, there is much to cover. Onboarding is the first real look at what the future holds for new employees. When it comes to AI, education should focus on how it works and what it does for the employee. They should understand how it can affect the center's workflow. Ongoing education is also critical as the ECC landscape will be different five years from now. A briefing on what the future holds can mold an employee's mindset by describing what is out there, what are the center's plans for AI and what role each employee plays in that future implementation. Education about appropriate ethical and legal use of AI in the ECC should be discussed with new and veteran ECC employees.

BEST PRACTICES FOR AI IN PUBLIC SAFETY

To safely and effectively integrate AI, public safety agencies should follow industry best practices. First, transparency is key. AI systems should be explainable, allowing users to understand how decisions are made. Regular audits help catch errors or biases early. Second, data quality matters. AI should be trained on accurate, diverse and unbiased data to avoid flawed outcomes. Third, strong cybersecurity measures, like encryption and continuous monitoring, are essential to protect AI systems from potential attacks. Fourth, keeping humans involved in the process (known as human-in-the-loop) ensures that AI recommendations are reviewed by experienced professionals before action is taken. Finally, ongoing education for staff is crucial. Ensuring that public safety teams understand both the capabilities and limitations of AI helps them use it effectively and responsibly. By following these practices, agencies can harness AI's power while maintaining safety, fairness and trust.

PERSONAL RESPONSIBILITY

AI can provide all of us with better work and personal tools to make our jobs more efficient. But with every new layer of technology comes an added layer of personal responsibility. AI tools are not perfect and can provide inaccurate or incomplete information. Someone must verify that the information is correct. To ensure that AI is optimally supporting staff workflows, open and consistent communication must flow among the staff doing the work, the technical staff and decision-makers. Each staff member in an ECC has a personal responsibility to take ownership of the center's work. At the same time, we must guard against complacency. We cannot fall into a mindset that technology is doing our jobs for us and lose sight of the need for attention to details. For now, a human must be "in the loop," meaning that a human must double-check AI's answers. In future scenarios, a human can be "on the loop," meaning that a human must provide supervision and oversight to AI without being directly involved in decision-making or execution.

THE FUTURE IS NOW

As we strive to improve public safety communications, AI must be reckoned with, and that starts with ECC employees understanding how to interact with it. We must get the hardware or software infrastructure in place that functions with AI before seeing its benefits.

Ultimately, AI should support, not replace, human decision-making. Keeping people at the center ensures accountability and reduces the risk of overreliance on automated systems. ●

This article was written by members of APCO's Cybersecurity Committee: ***Christine Giglio, ENP, RPL,*** *Director of Emergency Communications, Bedford County (Virginia) Emergency Communications;* ***Nathan Jackson,*** *Technical Services Specialist, Guilford Metro 911 Greensboro, North Carolina;* ***George Long, MA, RPL,*** *Lecturer, Central Washington University; Paresh Patel, VP of Information Security, Carbyne;* ***Denny Stortz,*** *Communications Specialist, St. Charles City (Missouri) Police Department-911 Dispatch — Cybersecurity Committee Goal Leader;* ***Charles Vitale, RPL, ENP, CPE,*** *9-1-1 Shift Supervisor, Emergency Communications Department, Rochester, New York.*

REFERENCES

1. Brandon Epstein, James Emerson and ChatGPT, “Navigating the Future of Policing: Artificial Intelligence (AI) Use, Pitfalls, and Considerations for Executives,” Police Chief Online, April 3, 2024.
2. Oprea, A., Singhal, A. and Vassilev, A. (2022). “Poisoning Attacks Against Machine Learning: Can Machine Learning Be Trustworthy?” National Institute of Standards and Technology. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934932
3. Vassilev, A., Oprea, A., Fordyce, A., Anderson, H., Davies, X. and Hamin, M. (2025). “Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations.” National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-2e2025
4. Carter, Scott. “The Future of Radio Communications: How AI Is Transforming the Field.” December 17 2024, https://c-at.com/blog/the-future-of-radio-communications-how-ai-is-transforming-the-field.

CDE EXAM #73787

1. In what ways could the role of AI in the ECC expand over the next five to ten years?
   a. By taking over all emergency call handling tasks and fully replace human telecommunicators.
   b. By improving real-time language translation, predictive resource deployment, automated call triage and scenario-based training development.
   c. By eliminating the need for human oversight in public safety decisions and reducing the ECC workforce by 90%.
   d. By focusing solely on analyzing social media trends without integration into daily ECC operations.

2. AI can be used as an adjunct, not a replacement, for minor tasks in the ECC?
   a. True
   b. False

3. What challenges can be foreseen in integrating AI into legacy ECC systems, and how might agencies overcome them?
   a. Compatibility and integration.
   b. Data quality and availability.
   c. Cybersecurity and privacy concerns.
   d. All of the above.

4. You can upload anything to any of the AI services without worrying about confidentiality due to the privacy policies they all follow.
   a. True
   b. False

5. What factors help determine balance of human oversight and automation in public safety AI systems?
   a. Humans can provide empathy, critical thinking and context that AI may not fully understand.
   b. AI is always accurate.
   c. Removing humans from the process increases public confidence in emergency systems.
   d. Full automation reduces the need for communication between departments.

6. AI can assist the PSTs to be more efficient in their work.
   a. True
   b. False

7. PSTs are at risk of losing jobs to AI.
   a. True
   b. False

8. What are some key best practices public safety agencies should follow to ensure AI systems remain secure and reliable?
   a. Regular audits, strong cybersecurity, and training staff on AI capabilities and limitations.
   b. Limiting AI access to supervisors only and avoiding feedback from line-level staff.
   c. Relying solely on private vendors for AI security without internal oversight.
   d. Using AI tools without audits to maximize efficiency and reduce human error.

9. AI can assist with real-time language translation during 9-1-1 calls, helping bridge communication gaps with non-English-speaking callers.
   a. True
   b. False

10. Which of the following is not mentioned in the article as a current or potential use of AI in ECCs?
   a. Real-time translation for non-English-speaking callers.
   b. Creating call scenarios for training purposes.
   c. Replacing all human telecommunicators with fully autonomous AI systems.
   d. Predicting patterns in emergency incidents using historical data.

FOR CREDIT TOWARD APCO RECERTIFICATION(S)

Each CDE article is equal to one credit hour of continuing education

1. Study the CDE article in this issue.
2. Answer the test questions online (see below for online exam instructions) or on the exam page from the magazine article (photocopies are not required).
3. Add/upload your CDE article information and certificate of achievement in the “My Classes Taken” section of APCO’s Training Central at www.apcointl.org/trainingcentral.

Questions? Call us at (386) 322-2500.

You can access the CDE exam online! To receive a complimentary certificate of completion, you may take the CDE exam online. Go to https://www.training-apcointl.org/ to create your username and password. Enter CDE in the search box, and click on the **“AI,”** then click on “enroll me” and choose **“AI (73787)”** to begin the exam. Upon successful completion of the quiz, a certificate of achievement will be available for download/printing.