BUY AMERICAN ACT / BUY AMERICA CERTIFIED
MADE IN THE USA

Artificial Intelligence, Emergency Communications and Robots Enhancing Federal Security Programs

Security Enhancing Technology

The security and protection of Federal properties and buildings, the employees who work there and the public that visit them is of paramount importance to the government of the United States. Today, there are thousands of Federal buildings, including court houses, in all fifty states, territories and Washington, DC. To protect these buildings, Congress and the Executive Branch have created over twenty law enforcement agencies with a primary and sometimes secondary responsibility to protect these facilities.

Most of these protective security agencies employ sworn law enforcement officers who provide a myriad of traditional investigative, intelligence, and security guard services. And in most of these agencies the law enforcement personnel are augmented by private security guards who assist with screening people, mail, and other goods entering the federal buildings as well as patrolling building perimeters and parking lots and performing other duties. The security guards use their extensive training and observation skills to detect prohibited items, deter and prevent the entry of disruptive or dangerous people, and identifying suspicious persons and vehicles that could pose a threat to Federal property.

Over the last several decades as certain security enhancing technologies have emerged, agencies began using new tools to augment the trained skills of security officers and security guards. In the 1970s, magnetometers and x-ray machines were introduced to the security screening processes. As greater advancements in digital video management, intrusion detection, personnel access control systems and biometrics were developed, these technological tools were also introduced.

Adding these new technologies has helped the protective security community in detecting items they may have missed in years past. It has allowed them to capture intruders that may have otherwise absconded and has improved the process by which employees enter restricted areas. In 2015, the Interagency Security Committee (ISC) published a White Paper, Securing Government Assets through Combined Traditional Security and Information Technology, which aimed, "…to join the traditional security and information technology communities in a unified and coordinated effort to secure U.S. Government assets." The ISC clearly understood the need for a marriage of responsibilities that built upon the human capabilities with the new capabilities of information technology.

New Challenges – New Tools and Technologies Needed

With threats facing Federal buildings increasing every day, the costs of protecting them climbing, and security workforce shortages becoming a growing challenge, agencies must look at additional levels of cost-effective protective security technologies to enhance their Security Programs. Proven and cost-effective tools - such as artificial intelligence (“AI”), robots and wireless emergency communications - are immediately available to agencies seeking additional avenues to improve deterrence, detections, and actionable, evidentiary-quality data. These capabilities have already been proven successful in the private sector and provide powerful benefits, at a cost of $1-$11 per hour, that broaden an existing security force’s effectiveness.

Artificial Intelligence

AI improves and fortifies national security in the battle against crime. It is a compelling tool capable of processing enormous amounts of data to aid in making quick, sound, data-driven decisions. It digests information quickly, formulates diverse conclusions, creates strategies and multivariate scenarios, conducts numerous analyses, and alerts security teams to probable threats in record time. The application of AI increases the likelihood of crime discovery, prevention, and suppression.

Emergency Communications

Modern blue light emergency phones and call boxes are the key to curing an overconfident dependence on cell phones. Many people may not have (or simply may not be carrying) a cell phone, the cell phone’s battery may be down, or there may be no signal in the area. Similarly, it is possible that visitors who find themselves in need of assistance may not be familiar with the local geography and landmarks, thus being unable to give emergency responders an exact or accurate location over a cell phone. In extreme situations (e.g., a major terrorist event, campus shooting, and natural or man-made disasters such as hurricanes, tornadoes, earthquakes, floods, wildfire, hazardous materials spill, etc.) cell phone users may also experience overloaded networks from too many subscribers trying to access the system during emergent situations when emergency access is most needed.

Illuminated, fixed, reliable devices strategically located on federal properties can be very reassuring when emergency services are needed. Familiar blue light call towers and emergency phones provide highly visible points to establish reliable, one-touch communication with local security, police, fire or medical services. They work day and night in all weather and even when communications are most congested. Blue light emergency phone systems also always report one’s precise location reliably, ensuring the expedited arrival of the appropriate type of help.

Emergency communication systems are more sophisticated these days with features like wireless solar power, wireless phone connectivity, satellite communications, audio broadcast capabilities and self-monitoring software all built in. There are even retrofit kits that allow users to easily upgrade outdated blue-light-style phones and call boxes to function like modern products. System owners may access automated daily email reports on the operational status of their system rather than having to manually test each device in person as required by legacy products. They can even receive status updates via text messages and view their network of devices in real-time on a graphical map.

Robots

Fully autonomous security robots (meaning robots that operate with zero human intervention, including charging) were first introduced in the private sector in 2013 to augment security guard services. It was determined that placing robots in boring, routine and monotonous, or dirty, dull and dangerous roles was an ideal use case that freed up humans to utilize their strengths – strategic thinking, empathy and rendering aid. This made mobile robots particularly suited for patrol duties in parking lots, parking structures, campuses and large buildings, while stationary robots were placed at points of ingress/egress, in lobbies/reception areas and in hallways and stairwells.

Security robots in use today feature the following capabilities (which are rapidly evolving) that can be turned on or off, depending on an agency's needs or policies.

1. 24/7/365 Operational Coverage
2. Force Multiplying Physical Deterrence Roaming at 1 to 3 miles per hour
3. 360-Degree Ultra-High-Definition Streaming Video
4. People Detection
5. Facial Recognition
6. Thermal Anomaly Detection
7. Automatic Signal Detection (mobile, Wi-Fi enabled devices)
8. Automatic License Plate Recognition
9. Two-Way Intercom
10. Pre-Recorded Messages
11. Live Audio Broadcast
12. Analytics
13. Security Operations Center (SOC) Interface and Integration
14. Fed
15. RAMP Authorization/Authority to Operate

Robot Capabilities in Detail

This section provides an overview of the above features of today's security robots which clearly demonstrate the potential force multiplying effects for today's ever-challenging security environment.

1. 24/7/365 Operational Coverage

Security robots can operate in any weather condition and under a wide range of temperatures. They work twenty-four hours a day, seven days a week, 365 days a year, with just a few short breaks to self-charge. They do not get sick or take leave, and they have a perfect memory.

2. Force Multiplying Physical Deterrence

Security robots of today can be quite intimidating. Some stand close to 5'8" and weigh up to 420 pounds, making them a valuable and proven deterrent. The robots have a very similar effect to a police car on the side of the road - everyone slows down. A large, "uniformed" security robot creates a commanding presence that can help save a life and even help de-escalate a situation. Crime rates and 911 calls have gone down in communities and properties where security robots patrol for almost a decade already.

3. 360-Degree Ultra-High-Definition Streaming Video

Security robots have perfect vision. They stream video in 4K ultra-high-definition, 360-degrees around them and at eye-level. The video data can be viewed in real-time or uploaded to any storage device and used later for investigations. One of the questions posed regularly is, "What happens when someone attacks the security robot and knocks it over?" Several people have already been convicted of assaulting security robots because the robots recorded the whole event and were their own best witness. The robots typically have all the evidence needed to prosecute to the fullest extent of the law.

4. People Detection

Security robots recognize humans. A fundamental quality of a good law enforcement officer or security guard is knowing "what" you are dealing with. When the security robot sees a person where or when they should not be there, they can announce with a pre-recorded message, or the humans in a dispatch or security operations center can speak to the intruder directly or alert other authorities. The pre-recorded messages are contextual and vary according to time of day, day of week, or location. They may even be randomly generated or manually selected by an officer or guard.

5. Facial Recognition

If the policies of a protective security agency allow the use of facial recognition, the security robots can not only detect “what” they are dealing with but often times “who.” Individuals on a watch list, whether permitted or prohibited, are easily recognized and appropriate action can be taken. Applications may be at federal checkpoints or ports of entry, which sometimes can be unstaffed but where low-risk travelers need to access. This feature is currently only available on stationary models.

6. Thermal Anomaly Detection

The security and safety of federal employees and members of the public that visit federal buildings includes fire safety. Security robots can see and detect anomalous temperatures that may indicate or result in a fire. The security robot reports the incident and provides real time video. The data also aids in providing forensics as part of an investigation (e.g., a recently running vehicle).

7. Automatic Signal Detection (“ASD”)

Automatic Signal Detection alerts can range from a cell phone belonging to individuals previously believed to have committed a crime, to a bomb detonation device accessing Wi-Fi, to a rogue router placed in the trunk of a vehicle by a hacker to be used for cyber-intrusion. The ASD alert has the capacity for providing a photo of the individual along with reasoning for being placed on the watch list. It can also be used at a SCIF (“Sensitive Compartmented Information Facility”) to ensure compliance with policies and procedures.

8. Automatic License Plate Recognition (“ALPR”)

Mobile and stationary robots operating in or around a federal facility are able to recognize license plates on a watch list and run them through the agency’s connection to the National Law Enforcement Telecommunications System or the National Crime Information Center. Like facial recognition, this feature is contingent on agency policies and may be disabled for compliance.

9. Two-Way Intercom

The two-way intercom allows for real-time interaction with humans. Any designated user with the appropriately assigned permissions can speak with a possible intruder using the included, browser-based interface. A person in distress may activate the intercom directly from a push-to-talk button on a robot and speak with security or the local police department. At the low-risk Canadian border, a crosser can speak with a CBP officer through the security robot, if needed.

10. Pre-Recorded Messages

The pre-recorded message feature is a powerful one for protective security agencies. Protection includes prevention. Security robots can broadcast announcements to the general public standing in line before entering a federal building warning that certain items are prohibited from being brought into the facility. Similarly, the pre-recorded feature can be used at airport security checkpoints. In addition, security robots can broadcast alerts to federal employees.

11. Live Audio Broadcast

Live audio broadcast is a feature that incorporates Features 9 and 10 and allows for real-time broadcast to any affected employee or member of the public. It could include news alerts, warnings or announcements from an Emergency Alert System and effectively act like a mobile public address system. It may also be used to assist in evacuations or mustering exercises.

12. Analytics

Analytics is only possible with data, and security robots collect massive amounts of it – approximately 90 terabytes each year. With that data, protective security agencies can analyze past activities, plan for future events and increase their situational awareness and decision-making. This is another area where the security robots can have a force-multiplying effect on the role of the protective security force.

13. Security Operations Center Interface and Integration

A security operations center user interface brings the power of security robots to any command center or desktop computer. All the features above are accessible and controlled by authorized users anywhere in the world where there is an Internet connection, leading to enhanced situational awareness and decision making. The cloud-based software provides officers and guards with extra eyes, ears, and voice on the ground 24/7 in multiple locations at the same time, creating a significant force multiplying effect.

14. FedRAMP Authorization/Authority to Operate

Companies offering security robot technologies must comply with the rigid cybersecurity policies and procedures enforced by the Federal government, including requirements for FedRAMP Authorization and Authority to Operate in the agencies they serve.

Technologies Coming Soon

Other security robot functions on the horizon include:

Integrating Existing Video Surveillance Systems

The federal government has deployed thousands of cameras in and around federal buildings. Many of those cameras are not fully integrated nor are they viewable in command centers or on desktop computers. Because many of these cameras are IP based, the security robots can receive the cameras' outputs and act as repeaters through which to stream existing CCTV and other video feeds. With the integrated data feeds, sharing across geographic locations and across agencies becomes possible, and leads to enhanced situational awareness and decision making.

Navigating Multi-Floor Buildings by Accessing Elevators

Improvements to have security robots navigate elevators is underway. Many any elevators in federal buildings are an integral part of the federal building's Industrial Control Systems (ICS) and have an IP address which allows security robots to be programmed to communicate with the ICS for elevator access and control.

Developing the Five Senses

The security robots of today use three of the five senses extremely well: Sight (4K/360 video), Sound (hearing and speaking), and Touch (thermal detection and LIDAR to avoid objects). On the horizon is the ability to also develop the senses of Smell and Taste. Integrating hazardous material and potentially bomb sniffing technologies into the existing security robots is a foreseeable capability.

Taking to the Air

Fully integrating drone technology with security robots and emergency communications will form a unified autonomous offering committed to reimagining public safety. Drones equip the autonomous security ecosystem with the best of both worlds, creating a comprehensive suite of autonomous public safety solutions that integrate ground-based robots, stationary emergency communication devices and advanced aerial platforms. End users can expect a synergy that enhances their security programs, providing a seamless and comprehensive approach to safety, threat detection, and emergency response.

Light Off-Road Duty

A security robot for more rugged, multi-terrain applications will broaden the spectrum of automated, ground-based devices. Military bases, border operations and federal prisons are among the types of properties that would benefit from a larger, more capable security robot with an extended range. And dirt, gravel, rocks and grass will soon be on the approved list of surfaces to traverse.

Federal Use Cases

Artificial intelligence, security robots and emergency communications are all being used by the private sector to fight crime and enhance security and safety in places such as airports, corporate buildings and campuses, hospitals, parks, neighborhoods, shopping malls, parking structures and casinos – to name only a few. The private sector is turning to these technologies for several reasons, and it's now time for the federal government to start leveraging them, too.
The mission for many Federal agencies makes them ideal candidates for integrating AI, security robots and emergency communication devices into a multi-layered, robust safety program. In particular, those agencies (FPS, GPO, Mint Police) charged with protecting the security and safety of federal buildings, the employees who work there and the general public who visit those buildings are the most obvious. There are other agencies whose mission includes national defense (DOD), border control (CBP), airport security (TSA), disaster recovery (FEMA), securing courts and prisons (DOJ/USMS), Veteran's hospitals (VA), and even agencies (CISA) that oversee our critical infrastructure like chemical plants, dams, and power plants.

A few use cases critical to the U.S. and Federal mission where this tech will enhance existing security programs, include:

- Federal Facilities
- Airports
- Border
- Capitol
- Critical Infrastructure
- Data Centers
- High Value Targets
- Immigration Facilities
- Military Bases
- Parking Facilities
- Ports
- Postal Service
- Rail
- Roads
- Special Events
- Warehouses

In all of these use cases AI, security robots and emergency communications can....

- Deter bad actors from nefarious activities.
- Provide a cost-effective tool to augment contract security staff to provide more expanded and less expensive security coverage.
- Provide high quality 365/24/7 360-degree 4K video as they patrol the interior and exterior of Federal buildings and parking structures.
- Provide pre-recorded instructions to the people waiting in line to enter Federal buildings as to what items are not permitted in the buildings.
- Listen for distress signals or other anomalies where the public is gathering.
- Provide reliable, one-touch communication and access to emergency services.
- Recognize and alert security officials about individuals banned from federal buildings based on prior documented illegal activity.
- Identify and alert security officials to suspicious vehicles based on license plate recognition.
- Using integrated command and control technology, gather video feeds from security robots and cameras installed at federal facilities and display them in real time in agency Command Centers and on the desktops of federal security officials.

Privacy Concerns Addressed

An important step agencies can take before deploying new technologies at Federal facilities is to consider privacy concerns. AI and robots, in particular, can conjure up fear among employees and the public. That fear must be addressed. Although it can be argued that these fears are almost entirely due to how robots have been portrayed in science fiction novels or Hollywood films. Now that robots are becoming an increased presence in our lives, we can evaluate the real robots. What they can do and what they are not capable of doing. Today we can see, touch, and even talk to robots. We also have existing technology that serves a similar purpose that can be relied on to help address privacy concerns. Today's security robots use many of the technologies already in use in public spaces. Closed circuit television, or CCTV, is a technology that has been around for decades. CCTV is already used in Federal buildings and Privacy Impact Assessments (PIA) have already been conducted and published for their use. The CCTV cameras are used to both deter and detect crime and video footage has been used in courts of law to convict many criminals. The video capabilities of security robots are both fixed and mobile. License plate readers are already used by several law enforcement components of the Federal government, and so too is facial recognition. Again, capabilities that today's security robots can do. So, the privacy experts in the Department of Homeland Security, DOJ and other departments can be guided by the existing PIA structures to ensure robots meet the standards for privacy.

Conclusion

AI, security robots and emergency communication devices can be viewed by Federal agencies as a way of augmenting, enhancing and increasing the productivity of existing security programs. Security robots utilizing AI, at rates of $1 - $11 per hour, are a cost-reducing way to relieve security guards of repetitive and routine responsibilities, and do so without time off, without getting sick, and without risking their health from exposure to contagious diseases. Security robots can record incidents and capture data for use by law enforcement to be used as evidence in a court of law to better guarantee conviction. Existing Privacy Impact Assessments for similar technology can be relied upon or updated as appropriate to ensure security robots meet the standards for privacy.

Blue light emergency communication devices are conspicuous and familiar beacons of safety that provide reliable, one-touch access to first responders and security operators. They enable invaluable security when one is in distress or in need of assistance.

There are too many criminals and criminal acts to be prevented by the number of law enforcement personnel employed in the U.S. today. Law enforcement and security professionals are in critical need of assistance that these new advancements in technology can provide. FedRAMP authorized providers can help us continue the technological progress that has allowed us to effectively join traditional security with information technology, and now cyber security and Artificial Intelligence to help protect the security and safety of Federal buildings, the employees who work there and the public that visit them.