THE FUTURE OF PUBLIC SECURITY

Martin Cronin *reflects on technologies we can expect to see over the coming years to give us the advantage over terrorists*

If you're a follower of security theatre, you know that the American stage in 2018 has had a compelling season so far. Police in several American cities wore riot gear while white supremacists and counter protestors marched in the streets. Schools, shaken by two consecutive shootings, poured state and federal money into security capabilities previously reserved for prisons. And New York City, which welcomed 61.8 million tourists in 2017, installed 1,500 bollards after a 2017 vehicle ramming killed eight.

Politicians, compelled to act by an anxious public, are right to overcorrect when bad actors expose and exploit vulnerabilities. The measures that guard against repeat incidents do more to reassure the public than protect them. If New York City Mayor Bill DeBlasio wants to ensure the $4 billion in tourism returns next year, the bollards are a good investment to ensure visiting and native pedestrians feel safer.

However, if the goal is to prevent future attacks, fortifications are unlikely to help. The next perpetrator will simply choose a new target or employ new methods in their bid for chaos. In an era where a lone actor with a gun can shred the social contract in seconds, governments must move beyond over fortification and embrace a new way to protect their citizens.

LIFE BEFORE 9/11

Those of us who remember the world before 9/11 recall life free from the lingering shadow of sudden, unpredictable and devastating violence. After a small cadre of terrorists killed thousands on US soil, the shaken super power took measures to protect itself that have reshaped Western expectations of what safety looks like.

Almost overnight, assault rifle-toting police and soldiers appeared at major transportation hubs. Pilots barricaded cockpit doors. Airline passengers submitted themselves to what was now considered a necessarily long and invasive gauntlet: jackets off, water bottles jettisoned, tweezers – tweezers! – banned.

The high-profile efforts seem to have worked. In 2009, when a would-be bomber was caught attempting to smuggle explosives onboard in his underwear, Janet Napolitano declared airline security a success. In fact, there has not been a successful mid-air attack on a US aircraft since the events of 9/11.

Deterrence works, to a point. Despite investigations showing American airline security to be full of holes, airplanes themselves appear to be too hard a target. Shortly after abandoning planes, terror networks killed scores in train bombings in London and Madrid. Even airports are not entirely safe. Gunmen at the Brussels International Airport in 2016 and Fort Lauderdale International Airport in 2017 evaded detection by levelling attacks just outside of security perimeters.

Today, the world remains in the midst of a crisis. Violence can be unleashed at any time, in any place, by any radicalised, rejected or disenfranchised person. The measures we've put in place to protect us, the bollards, the guns, the metal detectors, the CCTV systems, serve to subtly remind us of that persistent, oppressive danger. "Don't get too comfortable," they whisper. "Fight or flight?" they ask. The fortress we have built in the West is a study in contradiction, at once necessary and imperfect, comforting and unsettling. What's worse, it's no match for the next clever attack.

If security theatre comforts the public but tips our hand to bad actors, why not turn to technologies that run undercover? This year, law enforcement and security organisations fought public relations battles over covert operations and technologies uncovered by the press.

When the American Civil Liberties Union discovered that Amazon was testing in-video facial recognition software, the internet lit up. Facial recognition software is unreliable and biased against people of colour, said critics. The technology could be used to track protestors or immigrants, said others. Even security experts said it could put departments in violation of the Fourth Amendment's guarantee against unlawful search.

When adopting new technologies, transparency and proper legislation are key to unlocking public trust. Robyn Greene, policy counsel and public affairs lead for New America's Open Technology Institute, wrote in *Slate* that cities are pushing back against police technology by requiring them to draft policies and procedures to preserve civil liberties. Even where strides aren't being made, cities are holding public hearings on the tech.

Highlighting these technologies puts their future use in question. Shortly after it was uncovered, Orlando Police Department dropped the facial recognition programme, even though it was only being used in a handful of cameras.

Citizens are willing to give up some measure of comfort and privacy in the name of safety, but only with consent. Could there be a middle ground? The US Transportation Safety Administration could point the way.

Earlier this year, *The Boston Globe* reported on Quiet Skies, a covert TSA operation that asks federal air marshals to watch and report on ordinary citizens as they move about public airports. According to the report, air marshals have trailed a South-West Airlines flight attendant, a businesswoman passing through the Middle East, and other unremarkable travellers. The previously undisclosed programme, in place for years, caused mild uproar.

QUIET SKIES CREATES A NOISE

TSA Administrator David Petroske defended the program in *USA Today*: "I would say to the American public: Ordinary citizens don't need to worry about Quiet Skies. They don't. Actually, ordinary citizens should be very happy that a program like Quiet Skies is in place because I think everybody expects us to do everything that we can do that protects the privacy and constitutional rights of our citizens to ensure that there is not an incident in an aircraft in flight."

This did nothing to discourage a week's worth of headlines in national print and digital publications.

But the TSA also earned praise this summer for its decisions to put body scanners in subways, install 3D scanners at airports and keep baggage inspection in place at 150 small airports. They weren't damned as search violations, instead, they were called wise decisions and groundbreaking new measures to safeguard the public. It's exactly this kind of asset detection that is forecast to be the future of public security. The world needs a security measure that is both proactive and reactive, visible, but not a threat to a person's privacy or civil rights. We believe that a citizenry already accustomed to body scanning at transportation hubs would not only accept, but welcome protection from a multi-sensor platform system that is capable of safeguarding a wide variety of places.

> THERE HAS NOT BEEN A SUCCESSFUL MID-AIR ATTACK ON A US AIRCRAFT SINCE THE EVENTS OF 9/11

Threat detection expert Patriot One offers this complete fleet of technologies in its PATSCAN product family. Imagine, for a moment, that a bad actor passes into a casino. He may or may not be scanned at the doors. He may or may not catch the notice of the security team on duty. But a low-profile, integrated system would provide several points for threat detection.

3D scanners offer an unobtrusive way to protect the public

Picture credit: Patriot One Technologies

Video recognition systems exist that could screen patrons before they even enter the casino. Enhanced by AI-powered object recognition software, the camera system identifies and flags forbidden objects like open-carry handguns, as well as potentially detecting rifles being put into large duffel bags at the trunk of a car in a parking lot.

CONCEALED PROTECTION

As the patron approaches the building from the car park, targeted magnetic sensors, concealed in planter boxes, scan the individual and duffle bag for large mass casualty threat objects, such as rifles and bombs. While passing through the entrance, cognitive microwave radar screens for concealed weapons, explosive vests and other catalogued threat items.

Finally, a personal electronic device and bottle liquid explosives scanners sit at the registration desk, ensuring no such threats exist in everyday objects, like laptop computers, tablets, mobile phones or bottled beverages. All these technologies are then integrated into a complete platform monitoring system that connects all threat solutions and is operated by security headquarters.

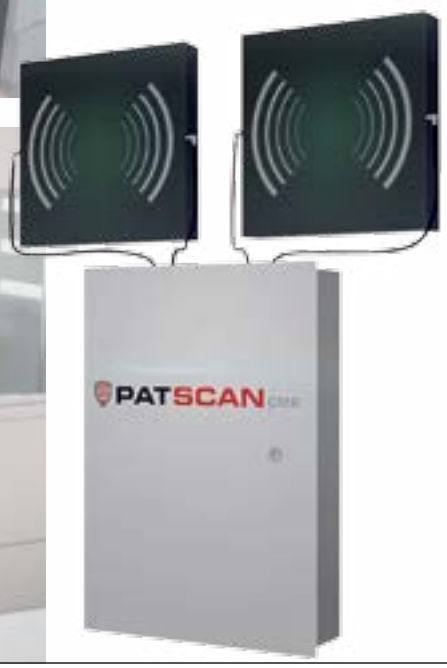
Integrated threat detection systems, like these are not silver bullets. Security staff must still be hired and trained to operate these new technologies. Signs should be posted for transparency and, when activated in public places, approved by the appropriate civic bodies. They must also be properly introduced to a public that wants to be able to move around freely and safely in open spaces.

The omnipresent possibility of spontaneous violence has pushed governments to militarise police forces, turn schools into fortresses and use unlegislated technologies to covertly identify and track private citizens. This is not the world we want to live in.

Low-profile asset scanning systems offer a middle ground. By deploying them in public parks, college campuses, in office buildings and other high-traffic areas, police and security forces can detect weapons as soon as they cross the perimeter. Adequate public hearings, socialisation and publicity would both inform the public and deter bad actors that might never be exactly sure where scanners are installed. And integrated systems that notify call centres could hasten the emergency workers that defend our citizenry. Deter. Detect. Defend. That's the future of public security ●

VIOLENCE CAN BE UNLEASHED AT ANY TIME, IN ANY PLACE, BY ANY RADICALISED PERSON

Martin Cronin, CEO Patriot One Technologies, is an expert in counter-terrorism, conflict resolution and government/corporate interface. He has extensive experience in high-intensity conflict environments, including 20 years in international diplomacy with the British Government.



Low-key undercover security measures can be just as successful at rooting out potential terrorist threats

Picture credit: Patriot One Technologies