The Riot Act – Radio Monitoring

Thomas Withington

Radio monitoring technology could help enhance law enforcement during violent disturbances, provided the technology is used with forethought.

As these words were being written, the United States' House Select Committee on the 6th of January Attack was receiving evidence regarding the violent scenes witnessed at the US Congress in Washington DC in 2021. The committee is investigating the attack on the Congress by supporters of outgoing President Donald Trump. For Mr. Trump, the stakes are high. On 12th June, the committee announced it had sufficient evidence for him to be indicted by the US Justice Department. There is the possibility that Mr. Trump could face trial for obstructing electoral certification procedures. A conviction might not only bar him from public office, torpedoing any hope of running for president in November 2024, it could also see him sentenced to up to 20 years in jail.

Crowds of Mr. Trump's supporters began to gather in the early morning of 6th January in central Washington DC to hear a speech by the outgoing president. By 08.51 local time members of the US Secret Service, tasked with protecting the president and other political leaders, noted that over 10,000 people had gathered. They were close to the White House from where Mr. Trump would give his address. "Some members of the crowd are wearing ballistic helmets, body armour and carrying radio equipment and military grade backpacks," the service reported. Television viewers around the world will now be familiar with the sight of individuals involved in the disturbance wearing tactical-style clothing. The inclusion of radios is a small, yet not insignificant, detail.

Smartphones are usually seen as the preferred means of communications for the extremist groups supporting Mr. Trump. As for most of the population, these devices are useful for sharing information on social media and accessing social networks to coordinate any violent actions at a protest. The 'radio equipment' referred to by the Secret Service seems surprising. Why would protestors resort to such seemingly archaic technology?

Photo: TapTheForwardAssist / CC-BY SA 4.0

Protestors gather on the step of the US Congress ready to force entry into the building following claims by President Donald Trump that the presidential election had been rigged.

According to a report by the Cable News Network on 18th January 2021, the Facebook and Twitter social media platforms had removed several people using these networks to plan attacks, spread hate speech or conspiracies. Mr. Trump was himself was banned from Twitter on 8th January. The Parler social network used by neofascists was banned by Amazon, Apple, and Google. Such actions have progressively restricted the communications channels available to Mr. Trumps supporters to spread propaganda or plan violent actions.

Civilian Two-Way Radios

The fallback, it seems, for some has been to use civilian two-way radios. Although basic in comparison to today's smartphones, these radios are ideal for organising criminal actions. Nonetheless, they have limited use for spreading propaganda due to the comparatively limited audiences they reach compared to the online world. A report on 29th June 2022 by the Slate website said several civilian radio frequencies were identified as being used by neo-Nazis in the US. These include Citizens Band (CB), the Family Radio Service (FRS) and the Multi-Use Radio Service (MURS). The US Federal Communications Commission (FCC) allocates 40 ten kilohertz/KHz-wide channels at frequencies of between 26.965 megahertz/MHz and 27.405MHz for CB. For those intent on law breaking, CB is attractive. It is unlicenced by the FCC, meaning that "anyone, regardless of age, can operate a CB station – except a foreign government, a representative of a foreign government, a federal government agency or someone who has received an FCC a cease-and-desist order that is still in effect. Anyone who is eligible may operate a CB station for personal or business use, in accordance with the rules" in the commission's own words. The FRS is, as its name suggests, is intended for use by families for short-range communications. 22 channels

Author

Thomas Withington is an independent electronic warfare, radar and military communications specialist based in France.

12.5KHz wide are made available by the FCC on frequencies between 462MHz and 467MHz. Like CB, an individual can use an FRS radio without a licence, provided they are not a representative of a foreign government. Finally, MURS is used for short range communications with 'walkie-talkie' style handheld radios. Five channels between 11.25KHz and 20KHz wide are made available by the FCC across frequencies of 151.820MHz to 154.600MHz. As with FRS and CB, provided an individual is not working for a foreign government, they can use MURS sans licence.

While the Federal Communications Commission says CB, FRS and MURS can all be used without a licence it warns that these networks cannot be used to help break the law. In the wake of the Capitol Riots, the FCC's enforcement bureau said it had become aware "of discussions on social media platforms suggesting that certain radio services regulated by the Commission may be an alternative to social media platforms for groups to communicate and coordinate future activities." The bureau warned that "individuals using radios in … this manner may be subject to severe penalties, including significant fines, seizure of the offending equipment, and, in some cases, criminal prosecution."

Nonetheless, before any arrest or prosecution can take place, individuals using radios in this manner must be identified and located. The first step is ensuring it is legal for a country's law enforcement organisations to monitor these types of communications. Laws differ from nations to nation. "In some countries … verbatim transcription of intercepted communications requires a court order, although in most, passive monitoring is permissible and can be hugely successful" says a statement provided to the author by COMINT Consulting. Assuming it is legal for law enforcement to do so in certain situations, police and domestic intelligence agencies have several capabilities they can use to keep tabs on radio traffic moving between persons of interest.

Radio Monitoring

Using radio monitoring to locate and track potential troublemakers is not new. This technology has "long been used by law enforcement agencies for active prosecution and passive monitoring of extremists, militias, gangs, organised criminal groups, narcotraffickers, arms and human traffickers, protection of vital installations and other roles," says COMINT Consulting.

The first step is to use a radio which can be tuned to the wavebands used by these persons. Provided the latter radios are in physically in range, they should be easy to detect and listen to. Radios using the bands mentioned above transmit across Line-of-Sight (LOS) ranges. That means two radios must have an imaginary uninterrupted straight line stretching between them. Any obstructions such as buildings, terrain or even the horizon can degrade or stop transmissions altogether. Typically, a person who is 1.6 metres/m (5.2 feet) tall, with carrying a handheld radio with a one metre (three feet) antenna will have a height of 2.6m (8.5ft). This will give their radio a LOS range of 6.6 kilometres (four miles). If the person is standing on a building 20m (66ft) high, this increases to 18km (eleven miles). However, the same problem will exist for the person on the building wanting to talk to a person in the streets below if buildings or other obstructions are in their way.

One solution to is to have a radio monitor mounted on an aircraft flying above the area where the persons of interest either are, or are thought, to be. Radio transmissions radiate outwards from an antenna much like ripples from a pebble dropping into a pond. Unlike obstructions on the ground caused by buildings or terrain, radio waves will also move upwards into the air. A radio receiver on an aircraft flying at 10,000ft (3,048m) altitude should be able to detect radio transmissions across a 123 nautical mile (227km) range. One caveat to this is that the range a radio can achieve will depend on how much power is put behind the transmission. Generally speaking, a CB radio can generate between four and twelve watts of power, according to FCC regulations.

Law enforcement aircraft carrying radio monitors are already operating in the US. In September 2020 two Department of Homeland Security aircraft flew surveillance orbits Louisville, Kentucky. These Cessna C-206 aircraft were deployed during disturbances there. Angry scenes had followed the failure of a grand jury to indict three police officers accused of killing Breonna Taylor in her apartment that March. Sources said the C-206s were gathered communications intelligence during disturbances which accompanied the protests. These aircraft were thought to be collecting intelligence on cellphone traffic accompanying the disturbances. Platforms like these could easily accommodate radio monitoring equipment collecting intelligence from civilian radios. It may be possible to modify existing equipment carried by these aircraft with software that can demodulate these transmissions and appropriate antennas for capturing the signals. Demodulation is the process by which a radio signal is electronically discombobulated to tease out the relevant intelligence.

Photo: CIES Corp

The US Department of Homeland security flies light turboprop aircraft believed to perform cellphone monitoring during civil disturbances.

Considerations

Harnessing radio monitoring to enhance law enforcement is easier said that done. Firstly, the bad guys may understand how to use their radios to help evade monitoring. "Many criminal, terrorist, trafficking and other organisations are much more technologically-savvy than law enforcement," says COMINT Consulting. "Having awareness of the construction of networks" thus becomes essential for law enforcement radio monitoring. Put simply, you must know what you are looking for before you start, one spectrum expert shared. Let us suppose police are keen to identify potential troublemakers involved in a protest. First, they need to know that their persons of interest have radios and what type they are using. This could be done by having undercover officers mixing in the crowd. Alternatively, a signal scanner could betray the presence of these radios. Nonetheless, to know what abnormal looks like you need to recognise normal, the source continued. Officers maybe convinced they have dis-

Photo: COMINT Consulting

COMINT Consulting produces several systems that can be used by law enforcement for radio monitoring. These include the company's Krypto-1000 software, the user interface of which is shown here.

covered a group of potential troublemakers using CB radios on a street corner. A closer inspection reveals that this is a taxi company with several cabs parked near the office. Analysing radio traffic is all about patterns of life. Collecting traffic from the same part of the city over several days would have quickly eliminated the taxi office as this radio traffic would be regular and predictable. Conversely, the sudden burst of CB traffic around a closed kindergarten might be suspicious and worth investigating.

Traffic pattern-of-life recognition is further complicated for law enforcement by the random nature of civil disturbances. These might not always happen where you expect. They may happen sporadically, unpredictably and may quickly dissipate. Moreover, scanners would need to be in range of these radios, bearing in mind that transmissions could be blocked or distorted by large buildings and other obstacles. "Finding and locating handheld radios in a city is tough," the source advised.

They added that radio monitoring needs skilled practitioners. Such individuals are few and far between, and expensive to employ. In addition, law enforcement must ascertain an end state before it starts using radio monitoring for crime prevention during civil unrest. Do you want to simply hear what potential bad guys maybe planning? Do you want to follow where the bad guys going by locating and tracking their transmissions? Do you want to jam their communications if they announce they are going to do something illegal? Concerning the latter, is it legal to jam their communications, even if they are planning to commit a crime? To further complicate matters, they will certainly not discuss such action sans code, no matter how simple. A person of interest saying they are 'going to the store to buy a soda' could mean they are about to break the law. It could also mean they are thirsty. Are police monitoring professionals suitably acquainted with the persons of interests' modus operandi and chatter?

Exercising Your Rights

None of this is to say that traffic collection and exploitation has no role in helping stop crime during civil disturbances. It does however underscore the need to develop legal, precise, and workable concepts of operations if communications intelligence gathering is to yield results in such scenarios. Radio monitoring equipment, people and training is not cheap. It may also be necessary to overcome institutional resistance in some cases. "Overcoming an anti-technology/anti-intelligence mentality in some law enforcement agencies can be a greater impediment" than using the technology, COMINT Consulting's statement notes. At the same time, police services have a myriad of competing budget priorities. Meanwhile, politicians may like to keep a purse string on a tight leash. The right to protest is a legitimate and vital part of a vibrant democracy. No-one wants protests marred by violent, law-breaking thugs no matter what the cause. Radio monitoring has a role to play in helping keep lawful demonstrations and the general public safe. However, it must be harnessed in a practical, cost-effective, and efficient way. ■