Image representation/VRT

During a military-related event on Aug 4, Venezuelan President Nicolás Maduro was nearly assassinated by a pair of drones. While Maduro escaped unscathed, the attack managed to injure seven soldiers. Various media outlets noted that this was the first known drone assassination attempt on a president. This development was however long in the offing.

The type of drone used in the Venezuelan attack was reportedly a DJI M600 model that can be ordered for $5,000 online. Each drone carried 1 kg of C-4 plastic explosives which itself can be confected from online DIY tutorials – if one knew where and how to look for it. Imagine what would happen if a few C-4 laden drones crashed into an oil tanker truck at a congested traffic stop or an oil refinery? Or even a crowded children's playground?

This incident came right on the heels of an alleged drone attack on Abu Dhabi's international airport last month by Yemen's Houthi rebels. According to rebel sources, the domestically-built Sammad-3 drones were launched and guided through 1,500km of mostly Saudi and UAE airspace before reaching the airport. This incredulous feat leaves many questions unanswered. Do Houthi rebels really possess such technology and navigation support to execute this feat? Or were they aided by a state actor? It is also within the realm of possibility for a few rebels to slip quietly across the porous Saudi-Yemeni border and assemble a weaponized drone from smuggled kits near the airport.

This ominous form of remote-terrorism is compounded by the relative anonymity enjoyed by perpetrators. While the study of remote killings had up till now focused on cyberattacks in hospital ICU units or nuclear power plants, weaponized drones have finally crossed the boundaries of fictional best sellers and movies into an ominous emerging threat.

Drones can be used for any variety of nefarious activities. Some drones can see through walls and generate high-resolution 3D images of targeted structures or record passwords clacked on a keyboard in a secure high rise office. It can be used for transport contraband, particularly narcotics, munitions and small arms across the US-Mexico border or be adjusted to make a special delivery all the way to the Trump Tower. US President Donald J. Trump should seriously rethink the projected height of his fabled wall.

Net-centric devices, including drones, will emerge as a major social disruptor in the coming years unless new regulations are drawn up to add extra layers of security to prevent its misuse. Otherwise, hackers may find a way to crash planes into skyscrapers or get a robot sex doll to administer a terminal climax. The possibilities are endless. Here is where the Internet of Things (IoT), Industry 4.0, cryptology and psychopathology may meet at the confluence of a terrifyingly complex new reality.

There will be increasing calls to restrict the sale of drones that can operate beyond a maximum 200 to 500 metre radius. However, there are many ways to circumvent future restrictions. The advent of 3D-printed drones, just like 3D-printed guns, will pose new challenges to law enforcement agencies worldwide.

Eventually, the ongoing drone revolution may lead to renewed calls for greater Internet surveillance, and a raft of drone-specific laws that will include mandatory licensing regimes. Drone enthusiasts may be required to attend drone piloting schools as a prelude to obtaining a license. Similar to vehicular driving licenses, drone permits can be revoked if users indulge in risky or anti-social activities.

But how does one prevent the transmission of a variety 3D-printable drone designs through cryptographic channels? If secure blockchain transmissions are good enough for Bitcoin, they will do equally well in an underground, cyber-facilitated illegal weapons industry.

The drone security solutions market may be worth up to $2 billion by 2024. To tap this lucrative market, several companies are already developing technologies that can detect and commandeer unauthorized drones in private or restricted airspace using radio frequency jamming and denial-of-service attacks.

However, basic levels of swarm intelligence – among other methods – can be used to “jam the jammers” and neutralize anti-drone solutions. Technologically-savvy subversives will always be a step ahead in any future drone war. Countermeasures developed will be protracted, expensive and based on hindsight. Security specifications will likely be designed to prevent a repeat of the last drone attack while hackers and terrorists work on new ways to breach drone defences that are still at the theoretical stages.

This calls for a new paradigm in risk foresight where analysts can think ahead and out-think perpetrators of future drone attacks. This is the real tricky part. The prevalent global talent identification regime is incapable of spotting those endowed with anticipatory or “metic intelligence”. The open source domain – the fertile data mining ground for malcontents – is equally disappointing. It is increasingly pandering to psychologically fragile snowflakes and ideological pansies whose flaccid viewpoints are prioritized in search engine results.

Google search, for instance, is no longer as effective, accurate and speedy as its previous iterations. There are ways to circumvent the prevalent “data smog” but this will entail either strong political will or tacit consent to securitize our future airspace.

Otherwise, cyber-mediated anti-social activities, including newer forms of harmful drone usage, will inevitably outpace our collective capacity to contain them.

**Mathew Maavak is a doctoral candidate in risk foresight at Universiti Teknologi Malaysia*

The views and opinions expressed in this article are those of the author and do not necessarily reflect the views of The Kootneeti Team

Facebook Comments