CRITICAL INFRASTRUCTURE PROTECTION

Tony Kingham *explores CPI tech designed to protect and detect*

In February this year, the UN Security Council (UNSC) urged joint measures to protect 'critical infrastructure' from terrorist attacks. Given the importance of critical infrastructure for a country's prosperity and security and against the backdrop of increasingly diverse physical and cyber threats from terrorist groups, the United Nations Security Council underlined the need for international collaboration, both domestically and across borders to ensure their protection.

In a resolution adopted unanimously, the 15-member Council reiterated "the need to strengthen efforts to improve security and protection of particularly vulnerable targets, such as infrastructure and public places". Attacks against objects and sectors such as banking and finance, telecommunications, emergency services, air, maritime and rail transportation, and energy and water supply – perceived as attractive targets for terrorist groups, can result not only in civilian casualties, but also damage property on a large scale, disrupt proper functioning of public services and create chaos in societies. Such attacks may also cause widespread environmental damage, as well as significantly undermining national defence capabilities.

> ONE OF THE KEY CHALLENGES FACING US IS THE SHEER NUMBER OF POTENTIAL TARGETS

It called upon UN Member States "to share information… to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks on critical infrastructure facilities, including through joint training and use or establishment of relevant communication or emergency warning networks". The UNSC also highlighted INTERPOL's global role in providing capacity-building and technical assistance to protect critical infrastructure from terrorists.

INTERPOL Secretary General Jürgen Stock said the interdependence of infrastructure across sectors and industries – between cyber and physical areas and across national boundaries – means that the consequences of an attack could be far reaching.

"One attack on a single point of failure could disrupt or destroy multiple vital systems in the country directly affected, causing a ripple effect worldwide. This creates an appealing target to those intending to harm us. As our cities and infrastructure evolve, so do the weapons of terrorists," he said.

"Conflict zone tactics – such as simultaneous active shooter events, armoured vehicle-borne improvised explosive devices (VBIEDs) or portable Unmanned Aerial Systems (drones) with explosive payloads – can be honed for use in our city streets and against key facilities.

"Law enforcement is keenly aware of a tragic paradox: a terrorist incident is often among the best opportunity for learning and improving. Sharing these lessons across borders means reaping the benefits, without paying that cost. It's a win-win scenario," concluded the INTERPOL chief.

Subsequently, the issue hit the headlines again when the UK Government issued a warning to Britain's airports and nuclear power stations to tighten their defences against terrorist attacks in the face of increased threats.

SOFT TARGETS

So why, when ISIS and al-Qaeda are increasingly mounting and calling for low-tech attacks on soft targets such as we have seen at public gatherings in Paris, Nice, Berlin, London and elsewhere, should we be concerned about attacks on critical national infrastructure (CNI)? After all, low-tech attacks on soft targets are difficult to detect and stop, can be carried out by so-called lone wolf attackers, require little or no technical skill or support from an established terrorist network. And it would seem attract just as much publicity as attacks on airports and other CNI. So it would seem like a winning formula for terrorists.

The simple answer is that while low-tech attacks attract publicity and cause terror, the effects are largely localised and don't cause the widespread disruption to the normal everyday lives of the vast majority of citizens.

ISIS and al-Qaeda especially, still hanker after that world changing 'spectacular' like 9/11 that will, they believe, show that they are still able to strike the sort of massive blow that can cause mass casualties, disrupt economies and lives in a way that only an attack on critical infrastructure is likely to produce.

AUDS (Anti-UAV Defence System) with DJI Phantom Drone

So how do we protect our CNI? One of the key challenges facing us is the sheer number of potential targets and the fact that most are not operated by government bodies, but by commercial organisations. Many of these organisations also operate across national borders, which further complicates managing national jurisdictions and legislative governance. Which is why the sort of co-operative PPP approach led by organisations like INTERPOL is so important.

So, what are the threats and how do we counter them? One of the most worrying developments in recent years from a security perspective is the proliferation of drones. They are everywhere and are set to become a part of everyday life. Highly capable drones can already be bought through retail outlets and specialist models with much greater capability can be bought direct from manufacturers, but still very easily and usually unlicensed.

The capability of drones is also growing rapidly. Drones like the Freefly Alta 8 has a payload of up to 9kg, a control range of 2km and a flight duration time of 16 minutes and can be bought on Amazon. The DJI Agras MG-1 has a payload of 10kg, a control range of 1km and flight duration of 24 minutes. The Amazon delivery drone, currently under development, is planned to carry a payload of 25kg.

It is inevitable that civilian drones will be used as precision guided bombs to attack CNI targets at some point in the future, and in this scenario the fences, ground sensors and guards around our CNI are effectively rendered useless.

Single drones or even swarms of drones may be used to strategically place explosives in attacks on fuel facilities, power generation and chemical manufacturing or storage facilities, causing damage and devastation massively disproportionate to the size of the explosive employed.

More frightening still is the potential for an attack on a nuclear plant. Nuclear facilities are built to withstand a direct hit from a commercial jetliner, but it is not inconceivable that single or multiple drones could target the cooling or power systems that keep the facility functioning safely. So how to stop them?

COUNTERING THE THREAT

Where there is a problem there is a solution and industry has been working hard to develop technologies to counter the threat. One of the first operational systems on the market was the Blighter AUDS Counter-drone System becoming the first to achieve TRL-9 status following successful deployment with US forces.

AUDS uses electronic scanning radar to detect a

Picture credit: Blighter Surveillance Systems

drone six miles (10km) away, track it using infrared and daylight cameras and advanced video tracking software before disrupting the flight using a non-kinetic inhibitor to block the radio signals that control it.

Another technology approach is by DroneTech in Australia. Its DroneShield uses patent-pending acoustic detection tech that can sense drones invisible to radar or that lack radio-frequency links. Sensors recognise unique sound properties of common UAS types. They listen to surrounding activity and take a sound sample when they sense drone activity nearby. If it finds a match, the system issues an alert and records identifying information about the aircraft.

Once detected, for interdiction they offer a tactical drone jammer called the DroneGun, which is rifle shaped equipment with a back pack claimed to have a range of 2km, allowing the operator to perform a controlled vertical landing of the drone.

Probably more interesting for the CNI environment, DroneSentry combines DroneShield Long Range Sensing and RF and/or GPS jamming technologies to create a combined effective detection and counter measure. The DroneSentry system is programmed to detect and respond to drone threats autonomously. The unit has an effective range of up to 1km across a 90° arc so four units would be needed to defend a 360° perimeter with a 1km radius.

One of the other threats highlighted by Secretary General Stock is the Vehicle Borne Improvised Explosive Device (VBIED) or truck bomb.

This is still a favourite weapon of the terrorist because you can move large quantities of explosives direct to the target undetected, and once there, they are very difficult to stop.

It doesn't take much imagination to envisage the damage one of these weapons could do to a nuclear power station or an oil refinery like Buncefield in the UK or chemical plant like Bhopal in India. Pick the right target and in effect you create a dirty bomb. So, what's the answer?

One solution is offered by UK company e2v, which produces the RF Safe Stop. Activated when a vehicle fails to stop or triggered by security staff, it uses similar technology to the AUDS system. It transmits a non-lethal microwave energy pulsed beam, which couples into the vehicle's electronic systems to confuse the engine management system, temporarily deactivating the engine. It works on cars, trucks, motorbikes and even boats. RF Safe Stop is already operationally deployed at a number of CNI sites.

However, solve one problem and you create another. How do you integrate multiple systems from multiple manufacturers, including CCTV, thermal image cameras, advanced electro-optics, motion sensors, IR sensors, microwave sensors, radar, sonar, acoustic, the list goes on… into one effective security system? To address this problem Monaco-based company, MARSS has developed the NiDAR system.

360° PROTECTION

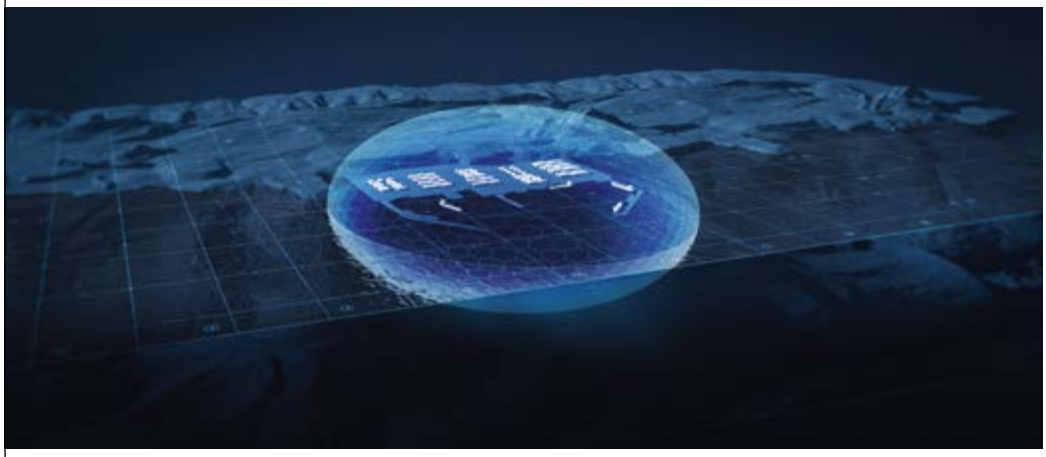
Developed over 10 years of collaboration with the European Union, European defence agencies, NATO and academia, NiDAR is a non-platform specific command and control system for protecting high-value maritime and land-based assets such as critical infrastructure. Through the integration of multiple sensor and data feeds it will generate a 360° perimeter security shield around any asset.

Rob Balloch, Strategy, Sales and Marketing Director at MARSS said: "We talk to customers, almost on a daily basis, who believed they had bought an integrated system but in-fact they find themselves with radars that don't talk to the cameras, cameras that don't talk to the sensors and they end up with a command and control system with multiple displays and multiple functionality that they don't understand and they haven't been properly trained on. NiDAR is platform agnostic, it can handle an almost unlimited number of sensors working on virtually any known operating platform made by any manufacturer.

"The real beauty of NiDAR is that anyone that can operate an iPad or an iPhone can run their entire system from a single tablet via a user-friendly touch screen experience. It provides total integration of all their sensors generating a single tactical picture on a single display. Using an advanced algorithm, the system will automatically build alarm and warning zones, intelligently detect, classify and respond to multiple air, surface and underwater objects determining potential threat levels while allowing for the legitimate movement of regular traffic. Enabling the user to sit back and monitor the system and it can even be operated and monitored remotely."

What is clear is that we are locked in a perpetual technological battle to protect ourselves from a relentless and ruthless enemy. There will be attacks on our CNI, how and when we can't say. But where there is a discernible threat we must do everything we can to be ready for it, because when it comes to CNI, the cost of failure could be catastrophic ●

Tony Kingham is a freelance journalist and publisher of www.WorldSecurity-index.com, specialising in information and public relations within the defence and security markets.



Picture credit: MARSS

NiDAR Protective Zone around a port facility