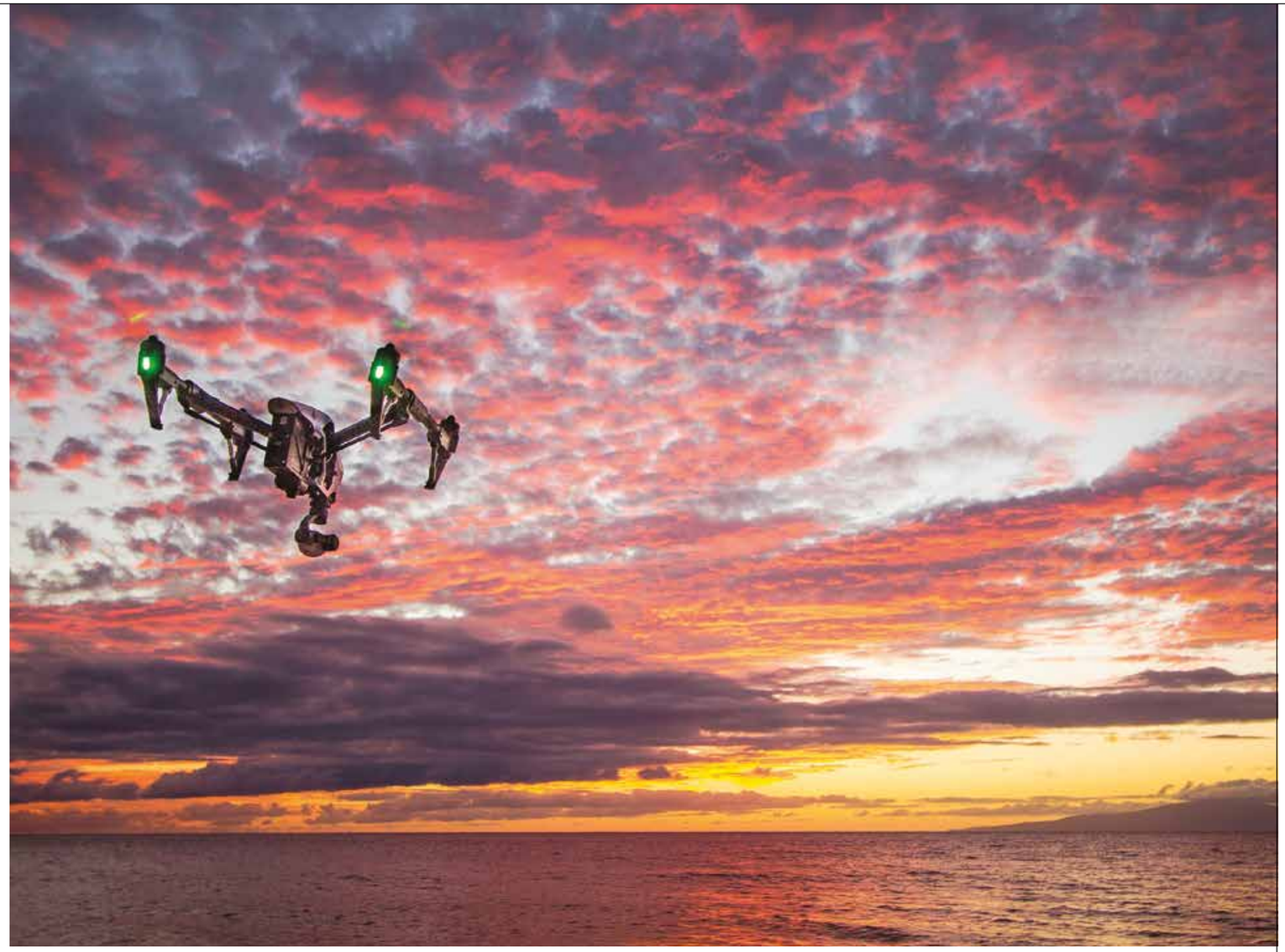
WATCH THE SKIES

Paul Hicks *explains what can be done to protect authorities – and the public – from the risk of drone attacks on the UK's critical national infrastructure*



Drones can move in excess of 60km per hour, carrying payloads that can be delivered in under a second

Imagine a Britain with no gas, electricity, water or other vital services – where modern life as we know it grinds to a halt. Sounds like an apocalyptic scene from a blockbuster movie, but if the latest Cyber Security Survey by the Department for Digital, Culture, Media and Sport is anything to go by, this isn't far off from becoming a devastating reality – with around a third (32 percent) of businesses and two in 10 charities (22 percent) reporting that they have experienced a cyber security breach or attack in the last 12 months.

It's not the first stark warning for the institutions and authorities behind our infrastructure. In October 2018, the National Cyber Security Centre (NCSC) warned that it is only a matter of time before the UK faces a cyber attack that threatens loss of life and other major social consequences.

The global WannaCry ransomware outbreak, which took down large portions of the National Health Service in 2017, is arguably the most prominent cyber attack the UK has ever had. But with the lessons from the incident still being implemented, UK-based airline British Airways faced a significant data breach, which resulted in around 500,000 customers' information being stolen by the attackers – landing the airline with a hefty £183-million fine from the Information Commissioner's Office.

LEARNING PROCESS

If we should learn anything from these unprecedented attacks, it is that critical infrastructure needs to be protected at all costs. This means that all of the systems, networks and assets that make up our infrastructure need to be secured. Otherwise, the institutions and authorities using them won't be able to function continually or safely.

Communication networks, for example, are a vital part of the UK's critical infrastructure. The availability of voice, data and internet infrastructure underpins much of the economic and social activity in the UK. In fact, there is hardly a sector that does not depend in some shape or form on the connectivity provided by telecoms, the services it enables and the activities it supports.

These networks, however, especially when connected to the internet, are increasingly vulnerable to a range of malicious cyber threats which include: denial of service attacks – malicious attempts to damage a service, sometimes by traffic overload, sometimes by the transmission of malware; malware such as viruses, worms and Trojans; and hacking, including attempts to subvert the proper operation of the billing system in networks. When assessing these risks, it is no longer a case of when an organisation will be attacked, but when.

Cyber threats aside, these networks also face a number of external physical threats – putting an authority's daily operations and business continuity at major risk of disruption. The consequences could be devastating from disgruntled customers and lost business through to damaged reputation. Such threats include: inappropriate signals injected by malicious users, either too high power or at the wrong frequency; similar signal pickup problems caused by radio interference, eg from unauthorised radio transmissions; traffic overloads, often stimulated by advertising campaigns and TV-based promotions

DETECTING DRONES AT DISTANCE IS CRITICAL TO ENABLING AUTHORITIES THE TIME TO RESPOND

and the transmission of specifically crafted signalling messages, designed to cause mis-operation of the network. Abnormalities in signal activity from drones, mobile phones and other satellite-enabled devices are increasingly threatening both asset security and public protection. As such, institutions and authorities are under pressure to detect and report on abnormal signal activity in real-time. In our inter-connected world, network security has never been so important.

For some, the potential of disruption from drones near airports was not unforeseeable. But for Gatwick Airport this was certainly not the case, leaving it and the authorities totally unprepared for a possible attack.

Following sights of unauthorised drone activity, the world's busiest runway came to a halt for 33 hours. Gatwick had no choice but to cancel more than 140,000 of its passengers' journeys at what was its busiest time of year, leaving them stranded at its airport. What's more, the financial implications of the incident had a significant impact not only on Gatwick, but also on the airlines operating from its airport – costing both a total of £50-million.

The drone incident triggered a chain reaction across multiple sectors, highlighting that there is significant room for growth when it comes to protecting critical infrastructures from potential attacks. To combat the rise in unexpected drone and cyber criminal attacks, many organisations are turning to technology.

Radio Frequency (RF) perimeter monitoring is emerging as an answer, providing an additional layer of protection that authorities desperately need. Using advanced analytics, it is able to warn of potential threats to the UK's critical systems, networks and assets early on – making it ideal for telecoms, transport, utilities, public safety, Government and defence organisations.

Advanced systems exist too. DGS Clearsky, for example, provides security monitoring at remote sites where physical attacks and sabotage may be more likely. Unlike existing systems it combines automated wide band RF spectrum analysis and drone threat management to provide authorities with real-time detection of unauthorised and unexpected communications activity and unauthorised drones. Unique in its approach, DGS Clearsky can go beyond the regular frequency bands, which drones are licenced to operate in – allowing it to identify potential threats operating in new and uncommon frequency bands.

In light of the recent increase in drone-related incidents – such as those at Gatwick and Heathrow Airport – telent and DGS Clearsky have combined their expertise to create a new Drone Threat Management System with the power to protect airports, borders, utilities, stadiums and large public venues, from the unpredictable threat of unauthorised and malicious drone usage. The solution is also able to operate in noisy areas, making it ideal for highly populated areas. Thanks to its flexible, simple-to-use system, which includes an app for smartphones and tablets, drones from distances of more than 2km can be detected, accurately identified by type and the location of the drone operator confirmed. Crucially, by identifying the type of drone, police and security services can

differentiate between a military-grade drone, which can indicate a potential terrorist attack or a commercial or hobbyist drone, allowing them to make an appropriate response. Also, by locating the position of the drone operator, a small team of officers can be deployed to directly deal with the situation, avoiding the need for larger scale search operations with many teams of officers.

Drones can move in excess of 60km per hour, carrying payloads that can be delivered in under a second, meaning detecting the presence of a drone without affording time to react is of little consequence. Therefore, detecting drones at significant distance is critical to enabling guarding agencies, the police and relevant authorities time to react and respond.

ALL SYSTEMS, NETWORKS AND ASSETS THAT MAKE UP OUR INFRASTRUCTURE NEED TO BE SECURED

This allows them to be fully informed and take the most appropriate course of action to manage the situation. Additionally, the solution overcomes the need to provide the extra training often associated with alternative, heavy-duty, military systems, ensuring that any authorised personnel have access to the solution as and when they need it.

Furthermore, the patented technology automatically captures, interprets, locates, and alerts on rogue wireless signals, such as the use of two-way radios or mobile phones in areas where there are no legitimate teams working. This information can be used to detect intruders and unauthorised personnel at locations beyond the reach of physical security staff and in areas not protected by CCTV, preventing unauthorised access, theft of key information and physical damage to infrastructure. By being able to capture and store threat data quickly, the authorities can also use it effectively as evidence for any legal proceedings that may arise.

Looking beyond airports, the Clearsky solution has applications at power generator plants and other public utilities such as water treatment plants, detecting drone usage and unauthorised physical access. Drones have also been known to be deployed at major sporting venues and events such as music festivals to live stream content to the internet, posing a significant threat to performing rights. Furthermore, this is content that legitimate fans and media organisations have purchased.

However, managing complex ICT solutions is not always easy, which is why many institutions and authorities choose to work with a managed services provider such as telent with experience of delivering 24/7 reliable monitoring and management of critical infrastructure protection.

While it is no surprise that the risks of unauthorised cyber attacks have never been greater, one thing that we can take from the Gatwick drone attack is the fact that the stakes have never been higher. It only took a single drone to tarnish the company's business operations, reputation and revenue. But it's a threat that can be managed – quickly, easily and cost effectively.

With the right solution in place, operators are able to detect rogue drones while enhancing usability at the same time. This can enable them to experience a faster, more accurate way to respond to unauthorised drone attacks. And be confident that a cataclysmic scene will stay where it belongs – on the big screen ●

Paul Hicks joined telent technology services as Wireless Head of Sales in 2012 and is responsible for developing new business within the wireless sector. As part of this, Paul leads business development, commercial, sales and strategy for the Wireless market.

Police officers use equipment on the rooftop of a building as the runway is reopened at London Gatwick Airport after closure due to a drone in 2018

Picture credit: Getty