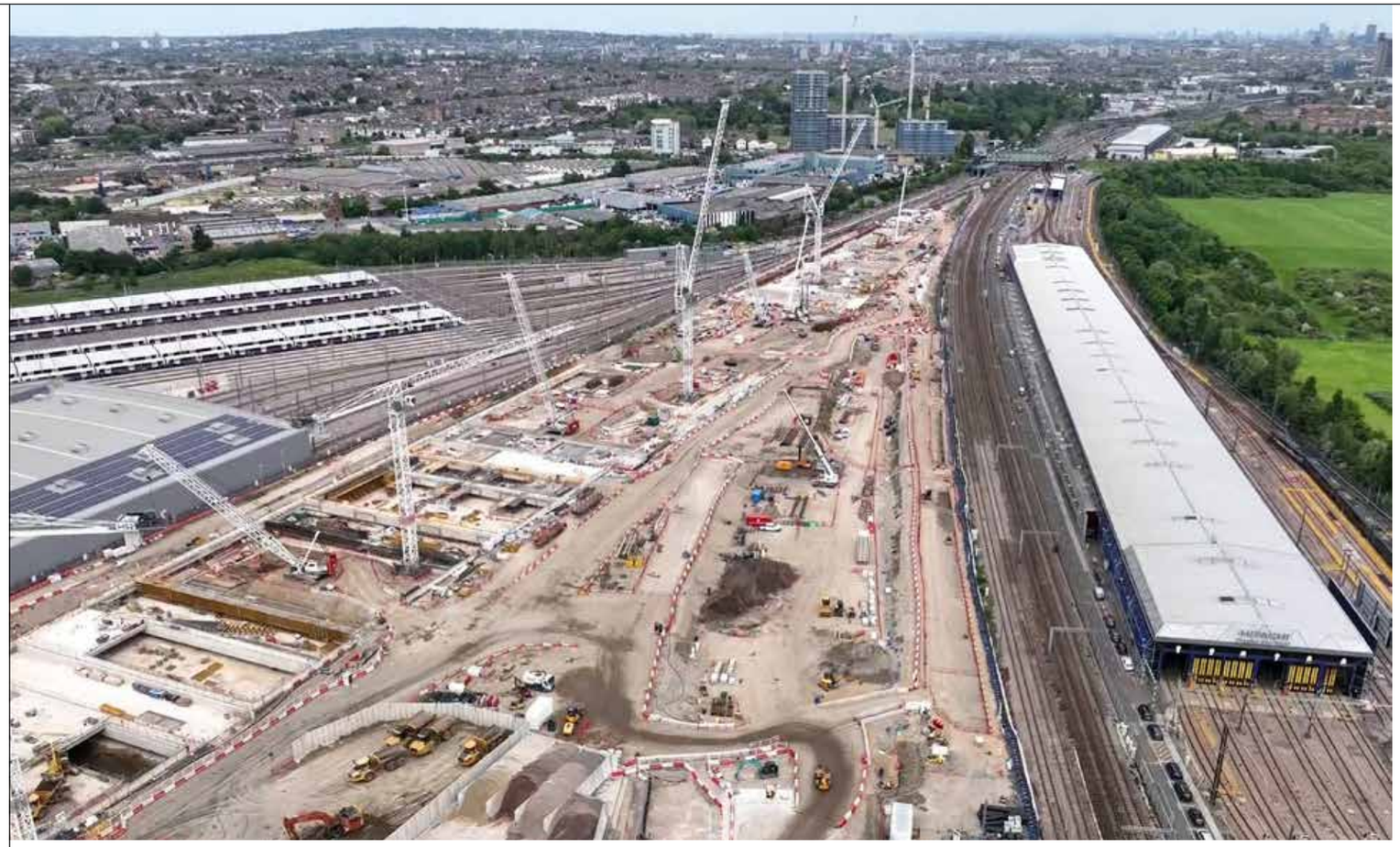

Picture credit: HS2

SYSTEMS DOWN!

Simon Alderson *believes vigilance in protection of UK infrastructure has never been more important*

Criminal activity involving UK infrastructure can have serious national implications, placing a crucial emphasis on rigorous monitoring and security every minute of the year. Facilities categorised as being 'critical national infrastructure' (CNI) are those whose loss of function have far-reaching consequences, being essential for the continuous smooth functioning of society. These include, for example, those associated with energy or water supply, transportation, or health and telecommunications.

At a practical level, crime or malign activity in these areas might mean trains, public transport or highways being seriously impacted, or telecommunications being severed including emergency services suffering prolonged outage. And there are many other elements to the CNI map besides these, including banking, nuclear, food distribution, data centres and a range of facilities the disruption of which would impact upon literally millions of lives. The Centre for the Protection of National Infrastructure (CPNI) judges that national infrastructure sectors represent core strategic interests for foreign intelligence services, whose targeting against the sectors is likely to include espionage for economic, political, military or commercial gain.

Even in times of comparative 'peace', elements of national Infrastructure will be targeted by hostile states daily, as well as by cyber criminals and terrorist organisations for the purposes of gaining some sort of advantage, be that testing infrastructure resilience, espionage or extortion for example.

While CNI security rests ultimately with government, MOD and the police, there is often an overlap with facilities which operationally fall under the day-to-day aegis of independent security companies. Examples include national construction sites for railways and highways, port facilities and distribution centres, the loss or damage of which still have strategic ramifications. This includes the protection of assets belonging to or being used at these facilities, some of which can be expensive to replace and highly attractive to the professional or opportunity criminal. In other instances of infrastructure crime, whether directly or indirectly, schools and hospitals can be affected, or sporting and music events interrupted or even cancelled. The impact of security breaches has many knock-on consequences.

Several agencies provide central government, regulators and Infrastructure owners and operators with advice on infrastructure risks and mitigation. For example, the CPNI provides protective security advice to businesses and organisations across the UK's National Infrastructure. Working in tandem with independent security firms contracted to public places, as well as with government security agencies, they will advise on security, aimed at reducing vulnerability to terrorism, espionage and other national level threats.

As technology advances and criminals get savvier, organisations must stay a step ahead, physically and technologically. Encompassing both physical and digital activity, crime against infrastructure warrants constant threat assessment and re-evaluation of working practices.

A conventional construction site is an area or piece of land where building or civil engineering work is taking place, but of course not all of these are the same, particularly where infrastructure is concerned, such as a major highway or bridge construction, or a huge engineering project such as the Crossrail development or the creation of a new power station.

The HS2 site stretches across 140 miles and presents highly complex challenges, particularly when it comes to cordoning off a large expanse of real estate

One of the biggest challenges facing security professionals in this arena is the sheer scale of operations. The HS2 site for instance stretches across 140 miles of English countryside, which in itself presents highly complex logistics and planning challenges, particularly at the start of a project in order to cordon off a large expanse of real estate.

Albeit in a different segment of infrastructure, one such example was the £20-million upgrade to build Europe's largest Tertiary Treatment Facility at the Water Recycling Centre in Chalton, near Luton, being managed by The Anglian Water @one Alliance. Here, the first major obstacle was to secure the 1.7-mile semi-rural site perimeter from trespasser threats, which themselves posed serious health and safety risks, faced with the additional complications of limited power availability at the multiple work sites to support the in-situ time-lapse CCTV systems. All of this was compounded by high volumes of large modular deliveries to the site which, if mishandled, had serious potential to cause major disruption to Chalton.

These are typical challenges for infrastructure security operators. Having won the contract to deliver a range of integrated site solutions over the 52-week project lifecycle, FRG assessed the requirement from beginning to expected completion, and among other suggested activity, deployed CCTV at three key positions to provide full site coverage. The CCTV guaranteed 24/7 self-powered monitoring and imagery delivering ultra-detail video analytics, all being monitored offsite at the FRG Central Control Room

THE UKRAINE WAR HAS GREATLY ELEVATED THE RISK FROM STATE-RELATED THREAT ACTORS

with audiovisual alarms alerting detected threats to permitter security. Indeed, trespassing is a key issue, particularly when there are already large teams of contractors from myriad different organisations each accessing the site at different times, with their own plant and vehicles, making it hard to distinguish between authorised and unauthorised personnel, relying all the more therefore on robust systems and processes being in put in place and rigorously followed through, including a full audit trail for compliance and detection.

The security of sites of this scale and complexity goes beyond criminal activity, including health and safety procedures and checks to ensure that workers and visitors to the site are at no stage exposed to undue levels of risk.

The UK's transport sector comprises the road, aviation, rail and maritime sub-sectors, the lion's share of transport operating on a commercial basis, with responsibility for resilience being devolved to owners and operators. Under the Department for Transport (DfT) all of the industry stakeholders are involved in the process of developing a common assessment of risks to ensure that proportionate and cost-effective measures and policies are in place.

Alongside aviation, perhaps rail is the most vulnerable to hostile or dangerous criminal activity, although our motorway and waterways are not far behind in terms of their own threats and challenges.

With its 2,750 stations and nearly 10,000 miles of track, the UK's rail network is the oldest in the world and although much reduced from its pre-Beeching glory days, is still evolving, including the construction of the UK's first high speed network – HS2.

With large infrastructure projects such as these, FRG has had to adapt to requirements, particularly in terms of upskilling staff with specific training, especially where emergency service response times can be up to an hour. For a rail project, members of the team completed the First Person on Scene (International) course, meeting the pre-hospital emergency medicine skills framework at descriptor level C or above. Further staff also completed FREC level 3, with the possibility of aiming for progression within emergency care.

The most recent example of a rail project however, has been taking place in Scotland. Since April, FRG has offered its full range of technological services helping to secure the Glenfinnan Viaduct renewal project in collaboration with principal contractor,

Amco Giffen. Before operations could get underway, two security risks had to be prepared for and mitigated against. The first was to protect the site compound from potential theft and vandalism, which had included temporary offices, staff welfare facilities, storage of plant and materials (including fuel and diesel). Secondly, given that the viaduct is a Scottish icon attracting over 300,000 visitors annually, there are elevated public health and safety considerations. The site's proximity to a popular tourist walk only increased the risks with the very real possibility of members of the public accidentally straying into the compound.

THE IMPACT OF CNI SECURITY BREACHES HAS MANY KNOCK-ON CONSEQUENCES

More generally across the rail network, access control is always a high priority, acting in support of British Transport Police, although monitoring every metre of the network is simply not possible. A key danger is route crimes, such as the placing of obstructions on tracks, and the sad reality of people taking their own lives, which tragically, even in 2022/23 still numbered two per week. Notwithstanding this, the UK rail network has probably never been in better hands when it comes to crime, particularly when it comes to major centres and the network's construction, and yet with so much development still ongoing on the network, the risks, dangers and threats of crime rely upon experienced operators to ensure it stays that way.

The electricity grid and gas transmission pipelines are impressive feats of engineering on a national scale and some of the most important systems in infrastructure. Cyber security is one of the biggest challenges for the energy sector, with the NCSC annual review 2023 naming ransomware as the top threat to the UK's critical infrastructure. The Ukraine war has elevated the risk from state-related threat actors, with the goal to disrupt operations. While resilience planning and emergency procedures are in place for critical sites such as hospitals and government buildings, they are not immune, as recent news bears testament to. Needless to say, the public are less equipped to prevent its impact on them.

I referenced distribution centres and data centres earlier, and in both segments FRG has developed tried and tested policies and systems to cater for the particular needs and special characteristics of these new facilities and centres, including work with a data centre in Leeds on the one hand and iPort, the enormous warehouse and logistics facility near the wetlands in Doncaster, on the other.

Data centres are often built away from towns and cities to prevent interference of the workings of the site, both physical and virtual. The geography of the data centre is important, in terms of the risks of weather, power outages and other natural phenomena, and each facility comes with its own unique challenges. Climate control within these buildings is one of these, making the protection of these assets a priority, along with access control and the security of its facilities, not least power.

The UK Security Sector has a rich heritage of protecting lives and property going back many decades, augmented today by the introduction of technologies, including biometrics, facial recognition and AI. The world is now a very different place, and one of the key challenges for industry is to ensure that we are several steps ahead of those with hostile or criminal intent, that's why organisations such as TINYg (anti-terrorism network) and regional groups such as the City Security Council – of which FRG is a member – help keep the industry informed. No segment is more important than our infrastructure ●

Simon Alderson is CEO of infrastructure security specialist First Response Group.

Motorways present their own unique security threats and challenges

Picture credit: AdobeStock