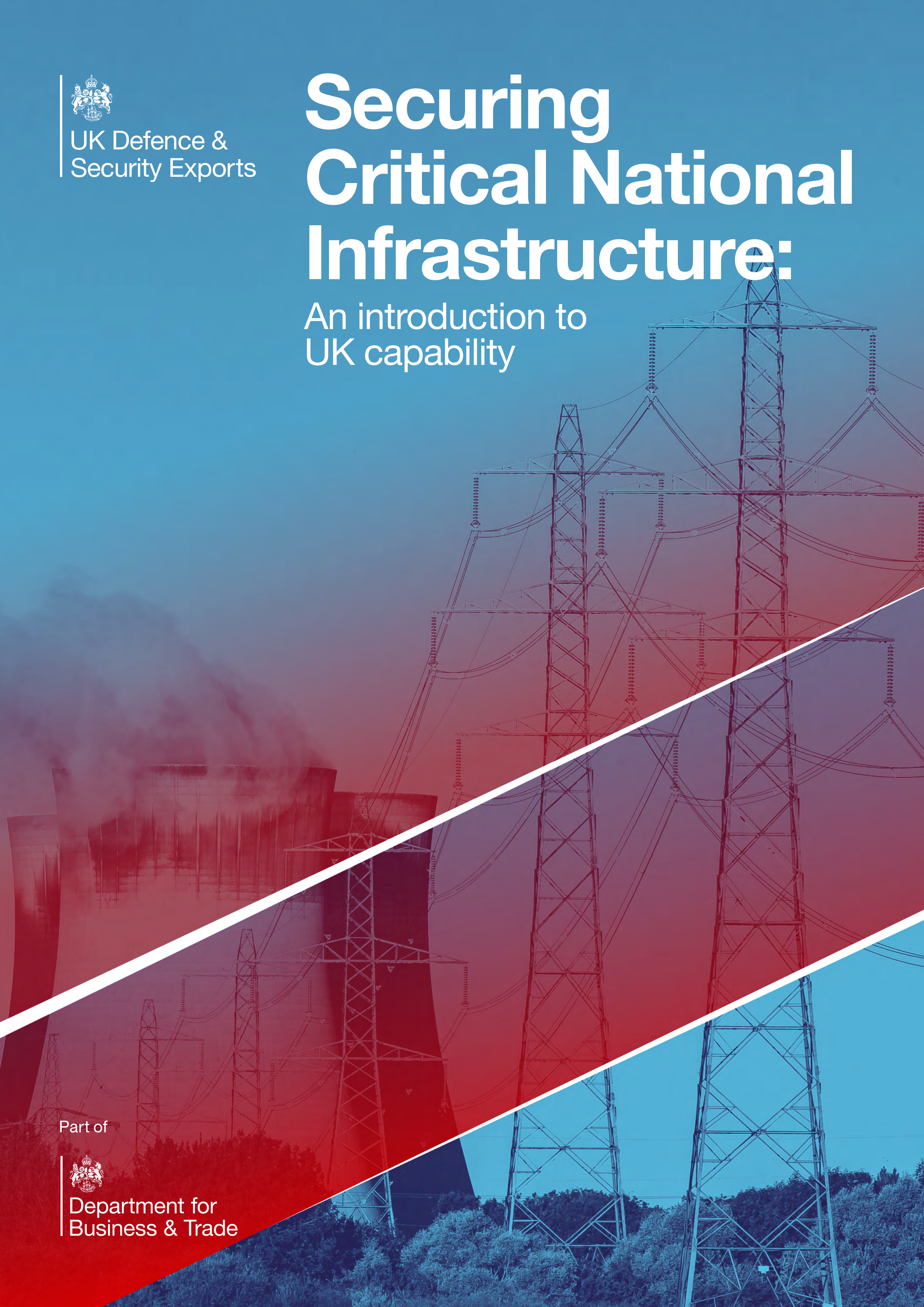
UK Defence &
Security Exports

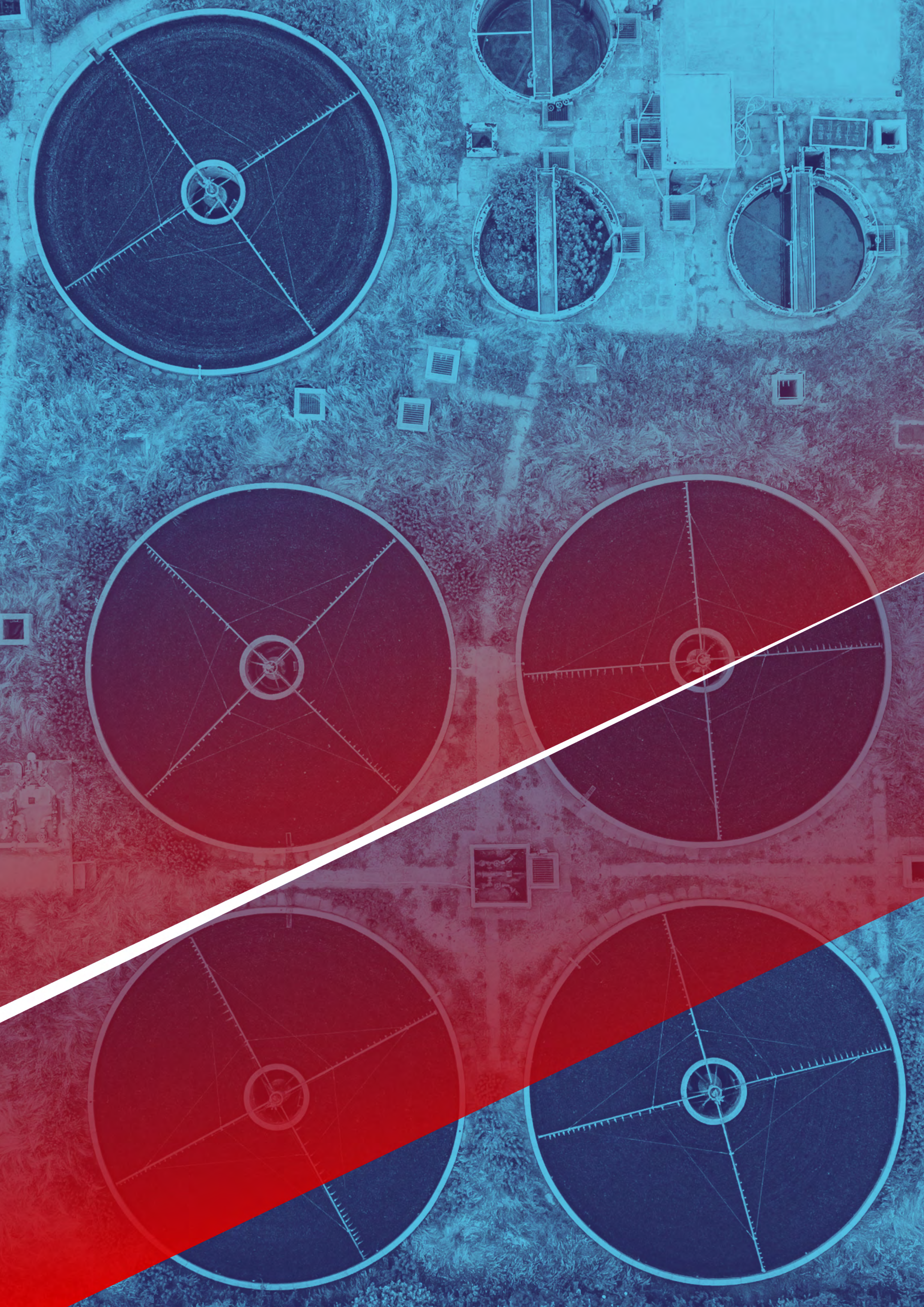
Securing Critical National Infrastructure:

An introduction to UK capability



Part of

Department for
Business & Trade



Contents

Executive Summary

Protecting Critical National Infrastructure Sites is essential for several reasons:

- Any disruption to these systems can have serious consequences for citizens, for example a cyber-attack on a power grid or water supply network can result in the widespread disruption of essential services, potentially putting people's lives in danger. Such disruptions also impact negatively on public confidence and citizens' views on the competence of suppliers.
- Protecting these facilities is important economically as interruptions can result in substantial financial losses and cause interference with the supply chain and business operations. Such sites are also heavily interdependent, and a disruption in one sector can ripple across others to cause significant issues across the wider economy.
- The uninterrupted operation of these facilities contributes to national security. As a target for malicious actors as well as hostile nation states, attacks can result in damage to essential systems, information theft and even physical harm, so protecting Critical National Infrastructure sites is crucial for maintaining national security and preventing large-scale disruption.
- As critical infrastructure systems become more interconnected the risk of cyber-attacks increase. Protecting these systems from intrusion is crucial in maintaining their integrity and preventing unauthorised access.

UK industry can help overseas customers, both public and private, in addressing all these concerns, and the aim of this brochure is to introduce you to the broad range of solutions to ensure the security of sites of Critical National Infrastructure, including power facilities, water plants and the communications network, as follows:

- Perimeter Security – physical and electronic barriers that deter and detect unauthorised access to a site
- Access Control – ensuring that only authorised personnel can access a site, and only those areas dictated by their role and responsibilities
- Incident Response – tools and equipment to deal with incidents that take place on a site
- Redundancy & Mitigation – ways of ensuring that facilities are less vulnerable and can be brought back into service rapidly should an incident occur
- Command, Control & Communications – ensuring that staff have a complete overview of a site and have robust communications to support their activities
- Cyber Security – protecting sites against electronic intrusion and attack
- Training & Capacity Building – ensuring that staff have the skills they need to effectively manage the security elements of a site and can mount an efficient response
- Planning & Consultancy – developing sites with security at the forefront and support services available to implement improvements

Each capability area is matched with case studies that give an indication of the range of products and services that can be utilised to address site security. At the end of this brochure, you will find further information on how UK Defence & Security Exports can link you to appropriate UK expertise, including resources and contact details.

A Forward Look – The Industry Perspective

Simon Banks is Chairman of the British Security Industry Association) (BSIA), the trade association which represents companies who supply more than 70% of UK security products and services, and of Skills for Security, the UK's largest fire and security apprenticeship provider. He is also the founder of CSL Group, a technology company focused on critical communications.

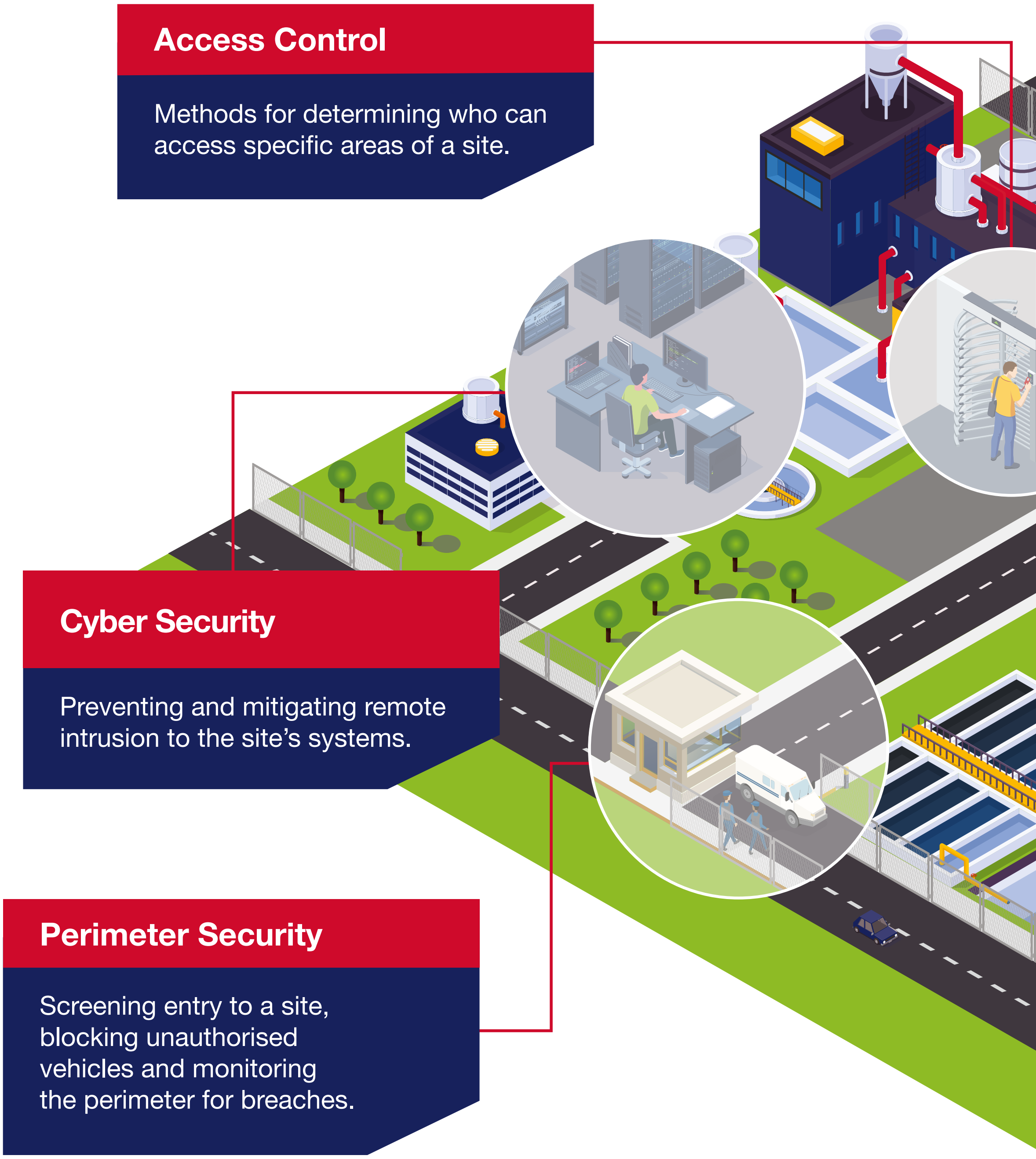
The UK Security Sector has a rich heritage of protecting lives and property. The development and production of automated alarm systems and protection devices in the UK dates all the way back to the 1960s for example. However, the world is now a very different place, and one of the key challenges for industry is to ensure that we are always one step ahead of those with criminal intent. One vital element of this is technology, where improvements due to the proliferation of Internet of Things (IoT) devices and machine-to-machine (M2M) technology have served the sector extremely well. As an illustration, these developments have enabled Artificial Intelligence and deep learning environments to be integrated into CCTV systems and associated security technologies, helping staff in control rooms to identify developing incidents and deploy resources more effectively.

As with any situation which may negatively affect people and property, deterrence and early warning are key to successfully mitigating the worst impacts. Many lessons have been learned from incidents that have taken place in the UK, such as the tragic Manchester Arena terrorist attack which took place in 2017. This and other events have resulted in the adoption of more robust procedures by operators, and in 'Martyn's Law,' which seeks to legislate stronger requirements on venues and locations to protect citizens from potential terrorist attacks. More comprehensive use of existing technologies as well as the introduction of new and innovative solutions have also taken place as a consequence of these incidents.

In the world of Critical National Infrastructure, in recent years technology has transformed the security capabilities of the industry and enabled a more proactive approach rather than a reactive one. These important facilities underpin the everyday functioning of society, and so the ability to deter threats and to have appropriate mitigation measures if incidents do take place is absolutely key, and it is UK companies and the robust products and services they provide that protect these sites.

Products and Services however are not enough on their own to provide the necessary protection needed. Competency can only be borne out of a sustainable skills pipeline and incremental training. The Security Industry Authority (SIA) has recently mandated that all 375,000 licenced Security Officers employed in the UK have top-up training every three years. Security Inspectorates, such as the National Security Inspectorate (NSI), British Approvals for Fire Equipment (BAFE) and the Security Systems Alarms Inspection Board (SSAIB) also mandate British Standards and Codes of Practice to ensure that all professionally installed Fire and Security Systems are the best they can be, whether being installed on business premises or in homes..

Securing Critical National Infrastructure



Access Control

Methods for determining who can access specific areas of a site.

Cyber Security

Preventing and mitigating remote intrusion to the site's systems.

Perimeter Security

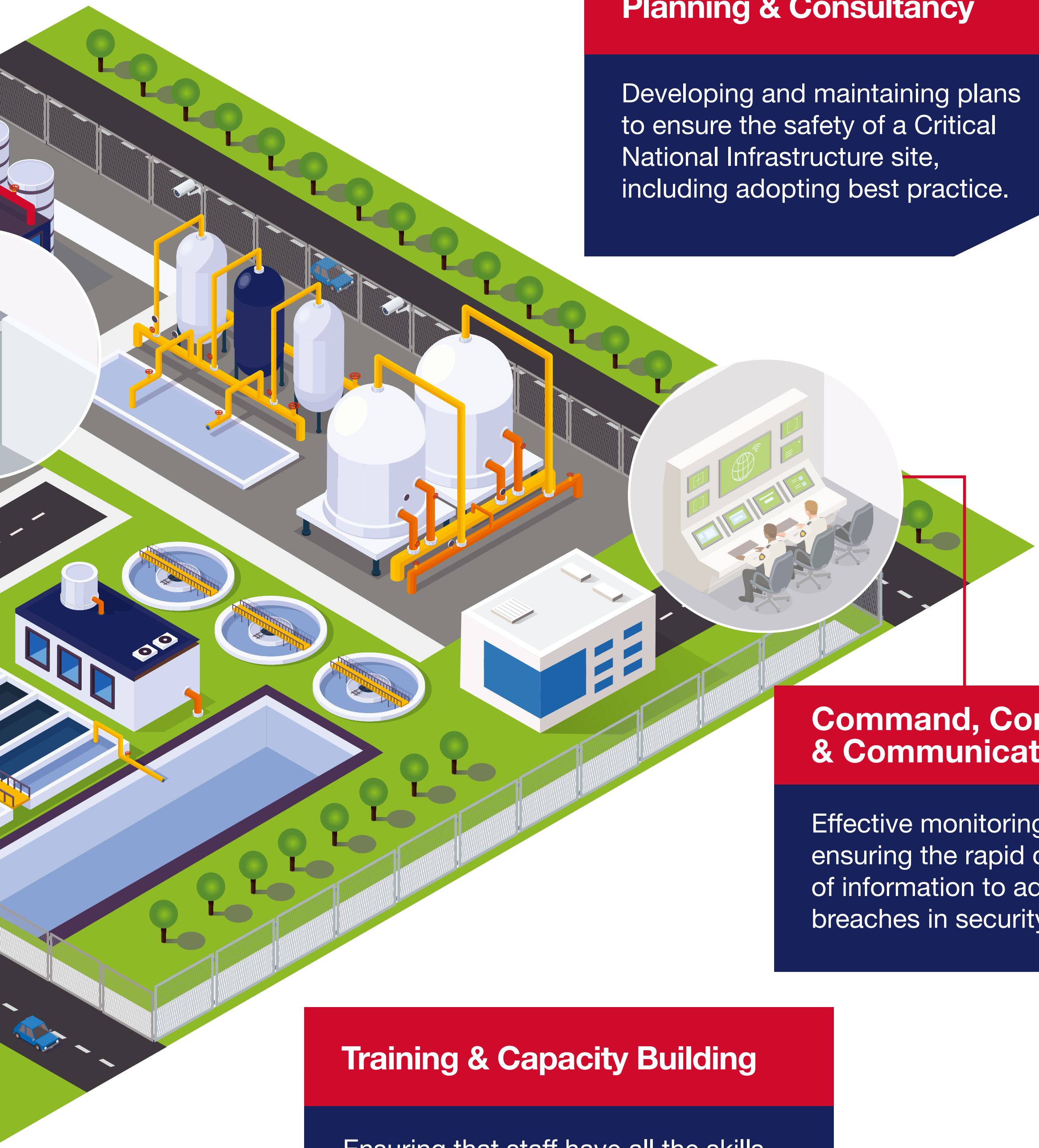
Screening entry to a site, blocking unauthorised vehicles and monitoring the perimeter for breaches.

Resilience & Mitigation

Ensuring that plans, procedures and backups are in place to quickly rectify any damage.

Planning & Consultancy

Developing and maintaining plans to ensure the safety of a Critical National Infrastructure site, including adopting best practice.

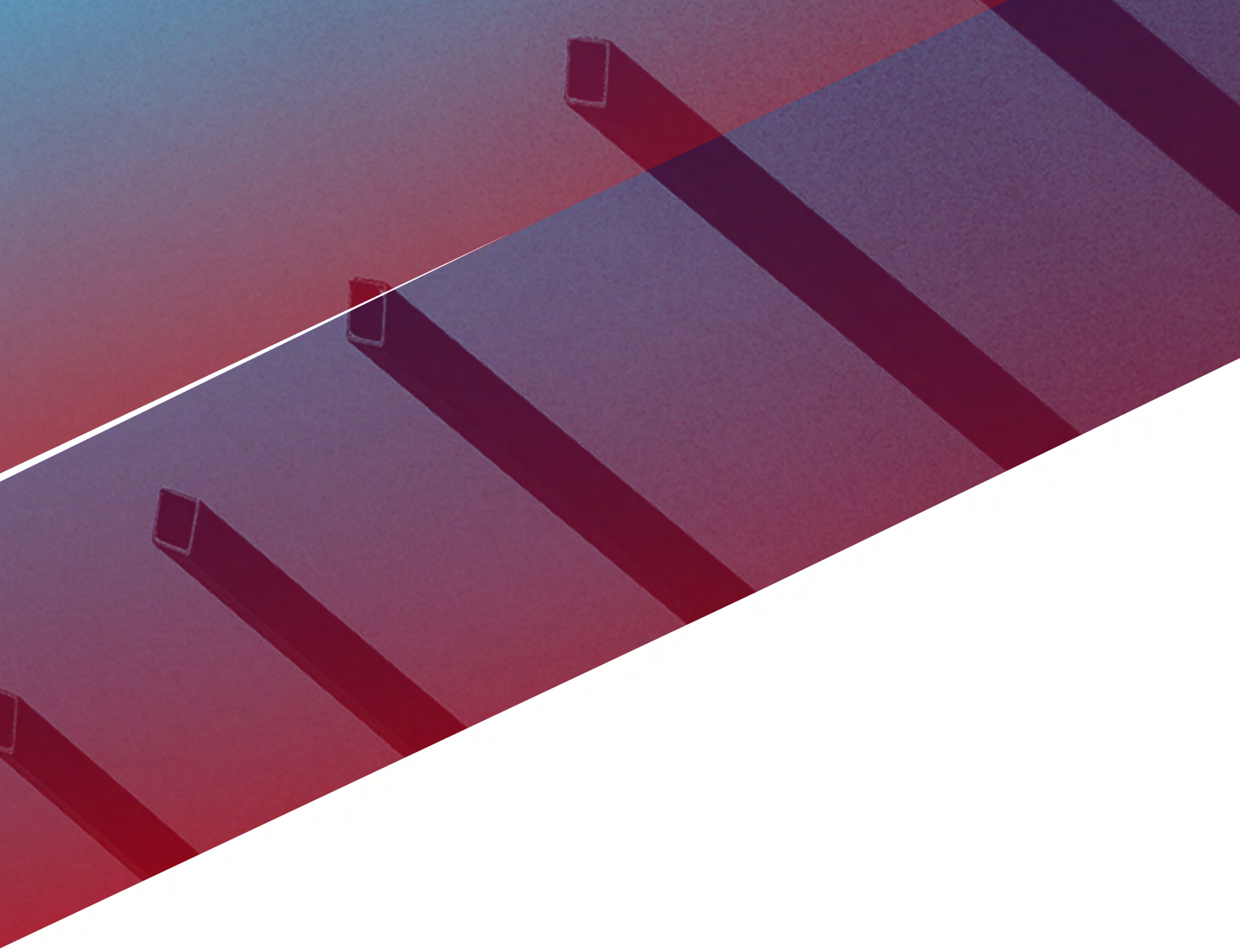


Command, Control & Communications

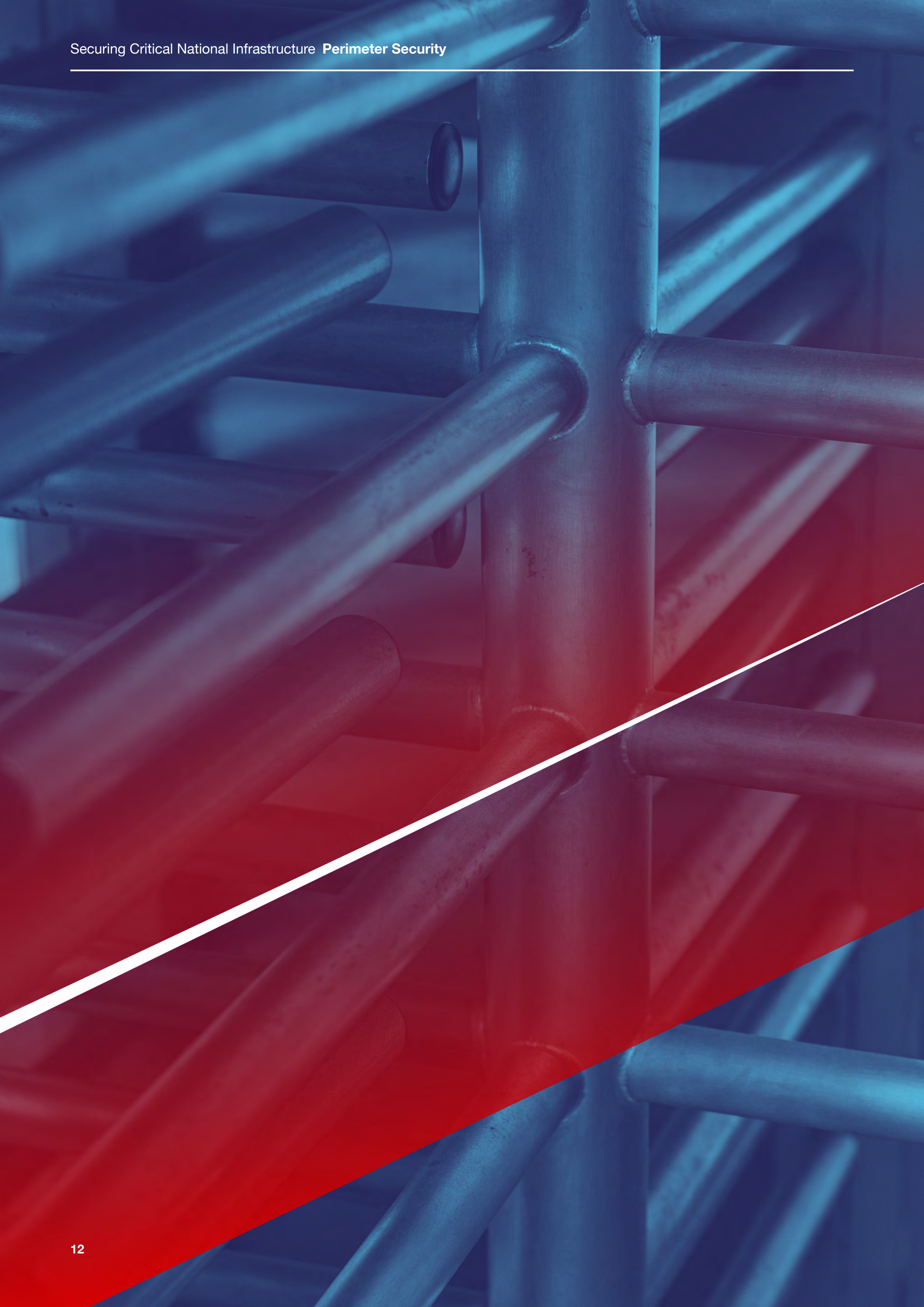
Effective monitoring of a site and ensuring the rapid dissemination of information to address breaches in security.

Training & Capacity Building

Ensuring that staff have all the skills necessary to tackle any threats to the safety of personnel and the site.



Perimeter Security



Perimeter Security

Critical National Infrastructure sites can become the targets of physical threats and so it is vital that effective perimeter security is in place, which is the first line of defence in their protection. These threats can consist of acts of sabotage that seek to damage sites in order to put them out of action or to cause collateral damage to the surrounding area, or from theft where valuable equipment and materials are removed from the site.

The most widely used methods to deter such activity include security-rated fences and gates, often with anti-climb features, that are frequently combined with CCTV that monitors the entire perimeter and, on larger sites, security patrols and other methods including specially trained dogs. Fences and access points are now being supplemented by hostile vehicle mitigation which protect sites against ramming attacks, with the latest systems being able to disable the largest vehicles before they can physically connect with the perimeter itself.

Sophisticated solutions available from the UK also include software tied to infrared CCTV feeds that can track an identified individual both outside and inside the site, even at night-time, as well as perimeter intrusion detection systems that utilise ground radar and vibration monitoring to detect when an intruder has crossed the perimeter. The physical threats to sites posed by chemical, biological, radiological and nuclear (CBRN) materials can also be addressed by companies who offer high-resolution imaging systems, capable of scanning for threats present in hand luggage up to large cargo containers, and trace detection equipment that can quickly identify hazardous substances.

In recent times, drones, or unmanned aerial vehicles (UAVs) have seen increased use as they become more affordable and capable. They are a particularly effective toll in protecting sites that cover large areas or pose hazards to the wider population if they suffer damage. The latest systems available from the UK can now remain over an area for extended periods and can be operated by security personnel with minimal training, integrated directly into existing control room systems and security procedures. The UK is also expert in counter-drone systems, which might be employed where bad actors are using drone technology to conduct hostile surveillance and gather intelligence on the vulnerabilities of site perimeters.

Package Scanning Case Study

Modern business environments rely on the delivery of letters and parcels, with this in mind the mail route into any organisation remains the preferred method for anonymously targeting a business or an individual. We are seeing an increase in reports of both hoax and genuine postal attacks, with hazardous powder threats being sent to several facilities across the UK in the recent years. Whether a hoax, or a genuine threat – both can be equally as damaging to a business and its personnel.

Winning the 2022 Queens Award for Innovation, the Todd Research TR15 cabinet scanner meets the demands of almost all busy mail room situations while taking up minimal operating space. Due to the compact size of the TR15, it can be used as a security scanner in a variety of areas within a building. The unit also comes equipped with the EPD™ (Enhanced Powder Detection) feature, providing a heightened ability to detect threats conveyed via powder-based elements.

Founded in 1950, Todd Research has a proud history of designing, manufacturing and supplying X-ray scanners, metal detectors and blast suppression equipment across a diverse range of public and private market channels. The company has distribution partners situated in key locations around the world, and are actively growing their export opportunities.

Radiation Detection Case Study

It is widely accepted that Nuclear CNI sites need to establish and maintain security measures to address the risk posed by "insiders" who have both malicious intent and authorised access to nuclear assets. To maintain nuclear security these measures need to be highly capable, deliver reliable detection and accurate identification. This is particularly important because insiders typically have knowledge, access and authority to bypass and defeat many of the traditional elements of physical and other security systems.

UK provider Symetrica provides high performance Vehicle and Personnel Radiation Portal Monitors that are linked to a secure, central facility that integrates with access control systems and, where used, small- and large-scale x-ray screening systems. This enables a whole-organisation-approach to security during high volume egress and makes sure that it is not just gate-house security personnel who are taking responsibility for site security.

Their systems are used in the UK and by Customs Organisation to secure ports and borders around the world including in the USA and EU.

Perimeter Monitoring Case Study

Small sites such as electrical substations or communications installations can present challenges for surveillance given the limited footprint available for the installation of monitoring equipment.

Crime and Fire Defence Systems Ltd, innovated a product to address this security and asset protection problem, and its solution allowed for the maintaining of security at the perimeter and beyond but with limited use of asset land to assign CCTV, lighting and detection security.

The Campost© solution is adaptable to accept any CNI security products of choice from Physical Barriers to CCTV and Technology and offers an operational requirement to meet most of today's risks. Campost© offers low-cost project delivery and the safe maintenance of an operational security system by its ability for the Camera and Lighting system to be lowered and raised by a single operator in limited safe areas without needing to work at height. Campost© technology design also means time saving and quick operational recovery as the system does not need any resetting positions after any maintenance so full security can resume instantly.

With restricted space or the need for asset space Campost© replaces the need for separate camera columns as it is located within the perimeter barrier of choice as a component of the perimeter solution. This means exceptional savings on land space for expansion or restricted areas where security surveillance is not always achieved. This has an impact on reducing carbon footprint at the time of installation and environmental aesthetic, coupled with a more efficient project delivery time.

Crime and Fire Defence Systems Ltd offers the full turnkey solution of Campost© for CNI Security protection across energy and utility sites, and are also employed in border security and transport network installations, from the initial design stage through to regular programmes of maintenance.

Securing Large Sites Case Study

Securing the perimeter of a larger Critical National Infrastructure site, particularly one located in a remote area, can be challenging due to the topography and natural features found around its edges.

Vaylia Integrated Security recently secured a UK water utility site with over 2km of high security fencing topped with razor coils, access gates for both pedestrians and vehicles and several other security enhancements. The solution provided perimeter fencing that met the UK standards set by the national organisation tasked with providing guidance on securing critical national infrastructure sites, CPNI, and also included security-rated bar sets, doors, bottle clamps and cages.

The site had a large perimeter which adjoined wetland marshes, water courses, railway infrastructure and was also impacted by overhead power lines. Vaylia's security risk assessment plotted the new fence line and also considered potential vulnerabilities of the site given its large size, identifying those locations around the perimeter where the fence line could be breached unobserved. As part of the subsequent programme of works trial holes and trenches were also employed to establish the local ground conditions so the perimeter could be constructed without the risk of future physical failure.

The installation also had to take into account the ecological impacts of construction as the perimeter was immediately adjacent to habitats used by migratory birds and small mammals such as otters, water voles and badgers. A detailed plan addressing the ecological considerations was provided to the client for consideration, and throughout the planning and construction process Vaylia worked with the clients' project management team to ensure early buy-in to the company's proposals.

Vaylia Integrated Security are experts in high-security projects and have a wealth of experience, its employees having worked on the most sensitive and high-profile sites. They offer a full package of services from advice and specification to final delivery, installation, testing and sign-off. They are a UK-based company that operates globally, with experience working in export markets across the world, notably in the Middle East.

Access Control

Access Control

The purpose of any access control system is to manage who goes where and when, whether they are an employee, contractor or a visitor. The level of access can and will vary depending on their status and access requirements and the sensitivity of the location they are entering.

The implementation of a suitably sophisticated access control system is one of the most effective ways of mitigating the risks to a Critical National Infrastructure site, and technological advancements have enabled a wide range of different methods to be employed to control access.

There are several key methods that can be utilised, all of which can be supplied by the UK. Traditional access control involves security personnel being stationed at entry points who check IDs, Passes and Tickets. Staff also fulfil a role in surveillance and monitoring, however today this traditional approach is being supplemented by more sophisticated systems that offer automated access and monitoring.

Automated access control systems provide a predefined set of rules which dictate who has access to sensitive sites, when they can access them and which areas of a building they can enter in accordance with their role. Typically, these systems use passes to scan entry systems, PIN code entry for locks and Automatic Number Plate Recognition (ANPR) for Vehicles, with entry logs and connections to alert systems that sound when unauthorised access is detected.

Several UK companies also offer smart key management systems which regulate access to the physical keys and passes needed on a site, using secure cabinets that log removals and returns and which are administered from a control centre in a central location. Particularly useful on remote sites which are not typically staffed, these systems negate the need for engineers to routinely carry several sets of passes and keys thus increasing site security, and only allow personnel to access specific areas of a site at defined times.

The most sophisticated solutions for access control that are available today involve the use of biometrics, which identity specific individuals according to their physical characteristics. Some of the sophisticated systems can combine fingerprint readers alongside face and eye recognition. Following the increase in terrorist attacks in the early 2000s such systems have seen widespread adoption in airports and in the most secure locations. They offer additional security measures over and above the magnetic stripe ID card systems that many locations have relied upon in the past, which can be vulnerable to cloning in certain circumstances. Several UK companies offer solutions to clients in this area.

Secure Entry Door Case Study

Attack resistant doorsets are vital in keeping occupants and property safe by delaying forced entry from intruders and protecting vulnerable assets. Sunray Engineering take a consultative approach to their customer's needs by providing bespoke design solutions

A leading energy utility company approached Sunray to assist with the design and specification of a range of attack and blast resistant steel doorsets to form a secure boundary around the perimeter of an exposed site of strategic importance whilst providing controlled access for authorised personnel. This resulted in the supply and installation of a complete range of fully certified security and blast resistant steel doorsets, which operated seamlessly with the required access control and intruder detection systems whilst maintaining high levels of attack resistance to potential adversaries. The multi-point locking systems fitted to each doorset also featured panic escape devices which permitted a quick and easy means of egress should an emergency evacuation situation arise.

Sunray Engineering are the UK's leading steel door, timber door and louvre system manufacturer, specialising in the design, manufacture and installation of high security, fire, blast and ballistic rated products for critical national infrastructure applications. For over 40 years they have been safeguarding HM Government's personnel and estate from physical attack and collateral damage. The company's bespoke product ranges have been tested and certified to the most demanding British, European and global standards, resulting in a formidable range of protective perimeter solutions.

Visitor & Staff Scanning Case Study

Traditional entrance security has relied on security guards using walk-through or hand-held metal detectors to check visitors for weapons or prohibited items hidden in clothing. With metal detectors likely to false alarm on zips, wired underwear and replacement hips amongst others, physical "pat-downs" by guards are all too common. So, metal detectors are a slow and intrusive way to check visitors and, of course, they do not detect non-metallic items.

Originally developed in the British Government's prestigious Rutherford Appleton Space Laboratory, Thruvision people security screening technology overcomes all of these problems. Using patented AI-enhanced Terahertz imaging technology, Thruvision allows security staff to see items concealed by clothing. Pat-downs are no longer necessary, and all types of material are reliably detected.

Having successfully passed UK and US Government testing, Oxford-based Thruvision technology is now widely deployed, and screens thousands of people at hundreds of locations in more than twenty countries every day. Farnborough International Airshow, a flagship British Government event, uses Thruvision for its "fast-track" visitor-friendly security. US Customs and Border Protection has deployed Thruvision along its Southern Border with Mexico and uses Thruvision to detect drugs, cash and other contraband. Major retailers, such as Tesco, Next, Saks Fifth Avenue and Clarins use Thruvision to check staff for stolen items.

Around the world, CNI security leadership teams are constantly looking for better ways to protect their facilities against a worsening threat environment. Thruvision offers proven detection capabilities for all types of threat, and a faster, more visitor-friendly security experience.

Response

Response

CPNI, the UK Government body that provides protective security advice to operators of the UK's national infrastructure, emphasises the importance of putting comprehensive plans in place to respond to any incidents, to keep these under review and to ensure that staff are adequately trained in implementing them.

With vast experience in supporting our domestic operators, UK industry is well placed to support overseas organisations in developing their own plans to protect vulnerable sites. In addition, the UK can help with practical solutions across a range of areas.

For example, should a fire take place in a facility there is a strong domestic industry in the UK which can supply the entire range of fire detection and suppression systems, fire doors and so on, and many of these solutions can be retrofitted into existing structures without major modifications being required. Additionally, as well as building full-sized fire appliances the UK's two domestic manufacturers also offer a range of small mobile units suitable for use in space-restricted locations which can be equipped with the latest fire-fighting equipment.

Protective equipment for staff operating in challenging environments is manufactured in the UK, as is decontamination and clean-up equipment and the latest remotely controlled robotic units that can drastically reduce personal risk. Specialist tools, including hand-held units, that can detect hazardous substances across the entire chemical, biological, radiological, nuclear and explosive (CBRNe) spectrum are also available.

Innovative electronic tags that map the locations of all staff within and around the facility in real time are also a useful tool when an incident occurs, so that staff can be directed towards an area to respond or away from an area to prevent injury.

Secure Response Case Study

For the most sensitive of Critical National Infrastructure sites, a rapid response to any incidents is absolutely essential to limit potential impacts on the safe, continued operation of the site.

Mitie Security began working with Sellafield in late 2012. Sellafield covers more than two square miles, and is home to more than 200 nuclear facilities and the largest inventory of untreated nuclear waste in the world. Sellafield is the only nuclear site in the country that can safely manage all three forms of radioactive waste; low, intermediate and high. Due to the nature of work on site, having highly effective security solutions is vital, to ensure only approved personnel and vehicles are allowed to access the site, and hazardous materials are protected.

Initially, the company was tasked with providing security at the 10-mile-long outer perimeter, conducting thorough vehicle and personnel checks, managing access and egress at the site. However, since the initial contract award, Mitie's solution has grown to now encompass a much more holistic security solution, with over 380 colleagues on the contract now forming the Civilian Guard Force (CGF).

This has enabled the Civil Nuclear Constabulary (CNC) to manage other operations more efficiently on site, and having partnered with Sellafield for 9 years the CGF is now seen as integral to the overall security solution, delivering a range of services. In addition to the outer perimeter access and egress control, the CGF are also responsible for internal security, including escorting vehicles across the site, and managing access for high security areas and vulnerable areas of a site. With numerous hazardous materials on site, it is imperative that access and egress is tightly controlled, making the work the CGF do an essential part of protecting the site.

Throughout the contract, Mitie have built strong relationships with Sellafield Fire and Rescue, the CNC, and Cumbria Constabulary to ensure effective and efficient security is delivered across the site. In addition, they also work closely with the Ministry of Defence (MOD) to cordon and control areas as and when necessary, for the safe removal of hazardous materials. The CGF team have also been an integral part of the recently formed "Joint Intelligence Cell" (JIC), a collaborative group including Mitie CGF, Sellafield, Cumbria Constabulary and the CNC, with the aim of better sharing of intelligence across the groups working on site to ensure all security solutions are optimised and as effective and efficient as possible.

Employing 77,500 people, Mitie works across a diverse range of environments including central & local government, critical national infrastructure, data centres, healthcare, corporate & iconic buildings, financial services, pharmaceuticals, telecoms & media, and retail. They take care of their clients' people, assets and environments, by delivering the basics brilliantly and deploying advanced technology.

Strengthening Cyber Threat Response Case Study

Research by the UK Government shows that more than half of domestic businesses are experiencing a digital skills gap, where staff responsible for cyber security lack the confidence to complete the basic tasks outlined in the National Cyber Security Centre's Cyber Essentials Scheme. This issue is not limited to the UK, as businesses around the world face similar challenges.

Building the capability to combat cyber-attacks, a now ever-present risk across almost every sector, must be a top priority for Defence, Government and private enterprise such that attacks can be responded to effectively and in a time-sensitive manner. Improving cyber resilience demands a collective effort, and one that deliberately seeks out and utilises untapped talent.

Veteran-led SaaS company WithYouWithMe (WYWM) is working alongside the Ministry of Defence and some of the UK's largest private employers to train diverse individuals with a proven aptitude for technology to learn critical skills for cyber security analysis, security operations and IT.

The software platform, dubbed 'Potential', uses AI-led psychometric testing to match individuals with tech-based roles using a series of personality, base intelligence and aptitude insights. WYWM then facilitates targeted training to build individuals' skills in under 200 hours through tailored learning pathways accredited by the UK Government's GCHQ and the internationally-developed Skills Framework for the Information Age (SFIA).

A program currently underway with the British Army's Royal Lancers aims to establish a sophisticated data analytics capability by identifying and training soldiers with an aptitude for information technology and cyber security. Captain Guy Parker, Regimental Signals Officer and Officer Commanding Perseus Troop at the Royal Lancers, said the pilot exercise would equip the force with the agility to react to the future requirements of the modern battlefield and to day-to-day work in barracks.

"To ensure we're strongly placed to take advantage of emerging digital technologies, we must adopt a forward-looking approach to capability building," said Captain Parker. "With the changing character of the modern battlefield, soldiers need to analyse more information than ever to provide intelligence... The Army that adjusts fastest will ultimately have the fighting edge over adversaries and the enemy."

Resilience & Mitigation

Resilience & Mitigation

To mitigate against incidents that might occur on a key site, a comprehensive approach is required that takes into account all likely scenarios and vulnerabilities of the site and involves conducting a thorough risk assessment that is regularly reviewed, establishing a robust incident response plan and implementing continuous monitoring and testing. Taking these steps minimises the risk of disruption, allowing for critical operations to be maintained even in the face of unexpected challenges.

Threats can be mitigated by ensuring that all the security components of the site are robust and carry the highest security ratings, from the perimeter and access control elements through to the IT systems. For example, disaster recovery services and solutions allow organisations to maintain business continuity when incidents occur, by helping to restore data and critical systems in the event of a software or hardware failure, as a result of a natural disaster or due to a cyber-attack that results in data loss.

For critical operational systems and data, cloud-based and physical solutions can be utilised which carry complete off-site backups. Once the data is stored it is typically secured with encryption and access controls to protect against unauthorised access. These off-site backups can also be stored in multiple locations to provide additional redundancy and protection against data loss.

To ensure the resilience of other elements of the site, backup power supplies should also be considered alongside communications systems that offer redundancy. UK companies can offer solutions that cover all aspects of the resilience of sites and mitigation should incidents occur.

Risk Management Case Study

As risks to CNI sites continue to grow with technology developments and potential terrorist threats, it becomes challenging to manage the unexpected. Therefore, the best way to manage these threats is to mitigate their impacts and most commonly this is achieved by risk assessments and detailed mitigation plans for the failure of any part of security be it physical or cyber.

For businesses operating in the energy sector the equipment and machinery often kept on-site will be extremely valuable and/or dangerous if accessed unlawfully. These resources are vulnerable to theft, vandalism, and fire damage, all of which will cause significant financial losses to the business in addition to their inability to trade, which will ultimately deprive citizens of essential services. The energy sector, encompassing oil and gas producers, electricity generators and energy distribution networks is recognised as being at high risk of fire due to the fact that raw energy components are often highly flammable and highly combustible.

In addition, due to the turbulent socio-political climate in many countries energy providers and distributors are particularly at risk of becoming victims of environmental terrorism or ‘eco-terrorism’. Although not always violent or destructive in nature this activity is frequently highly disruptive to business.

To mitigate these risks Kings Secure Technologies combines their solutions and expertise in several key areas:

- Carrying out comprehensive, evidence-based fire risk assessments to proactively managing the risks inherent to operation in certain sectors, particularly in the energy sector. Effectively managing fire risk is about both protecting staff from harm whilst at work and protecting equipment and raw energy components they process from damage and/or destruction in a fire.
- Assessing the effectiveness of access control systems to ensure that only competent and thoroughly vetted members of staff can access the machinery on-site.
- Surveying installed CCTV systems to ensure that they are comprehensive and properly positioned to provide security staff with a complete overview of the largest sites whilst minimising blind spots and areas of low visibility.

Founded in 1971, Kings Secure Technologies is one of the largest independent security, fire and risk management businesses in the UK. With over 50 years of successful trading history and an enviable client portfolio that spans a very wide range of domestic sectors, the company has the size, scale and infrastructure to meet their clients’ challenging needs.

Monitoring Case Study

Utility services are vital for customers across the country and their continued supply is the key challenge for the security industry. Utility companies have adopted a whole range of the latest technologies to allow them to better supply services to their customers. This has enabled them to adopt a proactive approach to managing their assets to minimise disruption to services and to reduce their carbon footprint by avoiding unnecessary site visits.

CSL has worked with Water Utility companies in ensuring that water stations can be monitored in real-time, through their cyber-secure, fully managed, connectivity solution. The solution is a managed industrial router, which supplies multiple paths of connectivity within a secure private network infrastructure. It is fully managed and proactively monitored to ensure Utility companies always have access to data from all their sites, in real-time.

Previously, a Utility company would have to send a team of engineers to investigate a problem on a site first, then decide who and what tools to send in to resolve the issue. CSL's solution allows remote diagnosis so that an effective solution can be implemented more quickly and unnecessary site visits are removed. This system employs a private broadband connection, backed up by a 4G-enabled global roaming connection for the highest resilience. The broadband and 4G connection paths are delivered via fixed private links from the communications network operator into CSL's fully redundant core network. A secure encrypted link is then established between CSL and each of the Water Utilities company's facilities. These services are constantly monitored by CSL to ensure that they are always active, which makes it simple for the Water Utilities company to manage its assets effectively and focus its resources on the rapid resolution of issues.

CSL has been a Critical Connectivity Provider for over 25 years. They supply many industries with secure, managed, resilient connectivity including Critical National Infrastructure operators, retailers, defence organisations, emergency services, the finance sector, local and national government, and transport operators

Their solutions have been widely accredited by many security-led trade experts, including the British Security Industry Association (BSIA) and the Fire Industry Association (FIA).

Command, Control & Communications

Command, Control & Communications

To manage the security of Critical National Infrastructure sites effectively, and to deal promptly and capably with any incidents that might arise, effective command, control and communications systems are essential.

Given the multiple sources of data that feed into a control room monitoring a sensitive site, such as systems operations, CCTV, sensor feeds and access logs, information technology used in this environment needs to be sophisticated, and UK industry offers complete solutions in this area. Management software solutions can combine operational data, surveillance, analysis and reporting of camera feeds and communications and deliver this information to operators both on and off-site in real time, on traditional desktop platforms as well as mobile devices and tablets. Combined with data visualisation tools to make information readily accessible, this can aid in rapid and robust decision-making if a crisis occurs.

Highly secure communications networks capable of connecting staff on-site, as well as with remote locations and the emergency services are also key. Many facilities are also located in relatively remote areas, where solutions to resolve this problem combine satellite communications with mobile data networks to ensure that communications remain reliable. The UK offers clients resilient and innovate radio systems to ensure staff are connected, including innovative mesh communications networks, which allow multiple devices to be connected to each other without having to rely on the traditional method of using a central point to manage the connections.

UK domestic companies can also provide comprehensive design and build services that comprise all the elements needed for highly secure command and control rooms, from secure entry doors to server systems and sophisticated video walls. Many companies also offer short-term temporary structures as well as mobile solutions should primary facilities become unavailable for any reason.

Video Processing Case Study

When a breach takes place on a Critical National Infrastructure site, comprehensive real-time video feeds are necessary in order to aid decision-making and to support an effective response to threats.

Videosoft's highly experienced team of developers are specialists in the compression and transmission of live video, providing software and hardware solutions designed for bandwidth-efficient video streaming applications within the IoT and CCTV markets.

The company's solutions provide efficient and adaptive video compression features. Bespoke real-time transmission protocols ensure the most reliable and low latency delivery of streams, even across low bitrate and unreliable networks in inaccessible geographical locations. This ensures that operators have an uninterrupted overview of a remote and potentially unattended, site in real time using less bandwidth, less data consumption and with lower latency.

The Ultra-low Bandwidth video product range includes easy to use components and complete units for the setup and operation of secure real-time video, audio and data streams for viewing, control, and processing. The Edge Gateway software is the main video and data processing component, the powerhouse of the system, and is supplied in all of the company's products or separately for integration into systems of systems.

Video, audio and data can be recorded locally in full quality or delivering on demand (or activated by an alarm or sensor) in a live stream to a remote operator or video management system for later review. The Videosoft two-way communication protocol means that the operator has full command, control and re-configure functionality either within the company's software or via the client's own video management system. Multiple streams can be transmitted simultaneously with their own configurable bandwidth level, and the Edge Gateway adapts the video encoding dynamically in response to network bandwidth conditions ensuring reliable and real-time video delivery.

An area of interest can be selected to provide more detail then transmitted as a separate stream, and it has the capability to recall an exact frame of video if the encoded live stream does not provide the level of detail required. All streams can be controlled remotely by Videosoft software for multiple platforms such as Windows, Android and iOS, or alternatively passed through to a third-party solution.

Managed Service Case Study

Securitas

To remove complexity and improve cost and operational efficiencies a managed service model for deploying security solutions is seen as vital by many organisations in helping to secure the Critical Infrastructure Sites that they operate, and the UK has access to some of the world' s leading suppliers who are able to deliver a holistic security solution that delivers the best protection with a simple and compliant management wrapper.

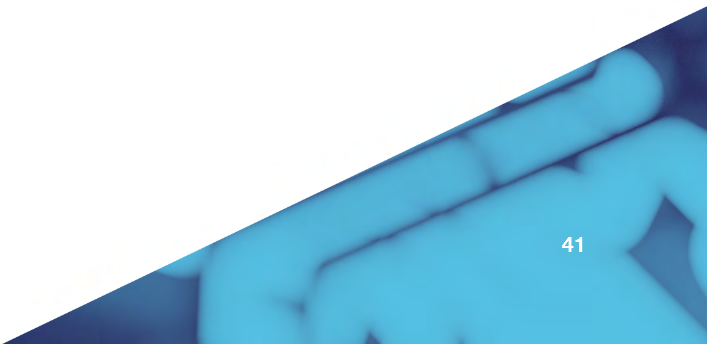
Securitas were given a brief to identify a combination of protective services that would meet a facility's unique risk profile, whilst delivering exceptional value for money. Applying a solutions-led approach, they recommended a risk-based package of protective services. This package combined manpower and technology to provide a smarter, efficient service that includes on-site physical security, car park management, surveillance control room management, cash in transit services, and reception services.

Soon after the start of the contract the company identified additional areas for improvement. One of these was the introduction of a comprehensive on-site First Response service to deal with emergencies. On-site 'Protective Service Officers' are on call 24/7 and able to respond to a wide range of events such as small fires, lift failures, environmental spillages, vehicle collisions and fire alarm activations. In addition, these staff provide specialist training so that their teams can act as Fire Wardens and First Aiders too, and a First Response vehicle (supplied and equipped by Securitas) ensures that the team are able to manage incidents quickly and efficiently. Their First Response service significantly reduces any risk to property, whilst also protecting business continuity. It also reassures staff and visitors that all the necessary safety and security measures are in place in the event of an incident.

Through the success of this working model Securitas has been given full responsibility for the maintenance of the site's CCTV, Access Control and Intruder Alarms with Securitas engineers permanently on site. Their enhanced solution, combining their First Response service with the highly visible presence of their officers, emphasises how seriously the site takes security. This unique offering and approach is available from Securitas for any CNI sites which require a more holistic approach to security.

Securitas are leading the transformation of the security industry by putting clients at the heart of their business. Supporting 15,300 clients in 47 Markets with over 80 years of experience. Securitas serves a wide range of customers in a variety of industries and customer segments. Their protective services, developed together with customers, are designed to incorporate a high degree of technology content. While manned guarding still represents the cornerstone of Securitas, they continuously work to develop their offering.

Cyber Security



Cyber Security

In the past critical national infrastructure sites were more secure as exploiting them required gaining physical access. However power stations, water facilities and other sites are now connected over the communications network so that they can be monitored and managed remotely. While this has reduced costs and increased flexibility for operators it has opened these sites to threats from cyber-attacks.

Whether used to deny service, damage equipment, steal intellectual property or impose ransomware demands, cyber-attacks perpetrated by hostile nation states or criminal networks are becoming increasingly frequent and more sophisticated. Therefore, over and above physically protecting a site it is essential that comprehensive protection and mitigation is in place in order to protect hardware and software, and that planning to prevent and mitigate cyber threats forms a key part of any site's security plan.

Recognising the significant impact that cyber-attacks can have, the UK Government supports operators and the public through advice, guidance and tools provided by the National Cyber Security Centre (NCSC) plus legislation contained in the Network & Information Systems Regulations (NIS). UK companies who provide solutions to help our domestic operators comply with these robust rules can also support operators overseas.

As a leader in global cyber security the UK offers comprehensive solutions that can counter all forms of threat. These include staff training and awareness raising to prevent data breaches and malicious entry to essential systems, endpoint protection software so that computers and smartphones cannot be compromised, next-generation firewalls to defend against attacks, end-point protection. Systems that can detect and alert operators to attempted breaches or unusual activity on IT systems can also be employed. Services offered include vulnerability assessments and penetration testing, as well as fully managed service packages that cover all aspects of an organisation's cyber security needs.

Malware Protection Case Study

In addition to protecting against remote attacks and intrusion it is also essential that IT systems are hardened in situations where a bad actor might have physical access to systems.

Platinum High Integrity Technologies' ABATIS product has been used by the Swiss Federal Office for Defence Procurement (Armasuisse) since 2006. ABATIS is employed to ensure that any personnel servicing high value air-gapped radar systems are not able to inject zero-day malware into systems, including via USB when they have direct access to sensitive equipment. This was the infamous methodology used in Stuxnet malware against the Natanz nuclear enrichment facility in Iran in 2010. The ABATIS solution also protects Armasuisse against supply chain attacks, and problematic or badly timed enforced updates which are a substantial risk on the battlefield or in Forward Deployment Bases in war zones.

The ABATIS solution is entirely preventative and completely self-contained, making it mission critical for the defence sector. Each ABATIS endpoint is autonomous, a fit and forget solution that is well suited to battlefield communications including air-gapped endpoints based upon either Microsoft or Linux operating systems. ABATIS stops cyber-attacks by preventing the ability of the attacker to write to disk, denying the attacker from co-opting legitimate tools such as PowerShell and preventing temporary infections of memory. PlatinumHIT is now bringing this technology commercially available for the first time.

Platinum High Integrity Technologies' solution has protected thousands of endpoints in Critical National Infrastructure systems for over 10 years. The company also offers managed service solutions from its office in Bristol alongside its portfolio of cyber security products. Utilised worldwide, the ABATIS software is used across CNI and transport systems and endorsed by prominent defence luminaries, including Lockheed Martin.

System Hardening Case Study

Most devices and networks on Critical National Infrastructure sites are permanently connected, despite this being in breach of rules established by several government regulators which state that network ports and services must only be opened if required for a particular device to function. In Singapore for example, this limited-connectivity requirement has been put into place, and the UK's Ministry of Defence has also set a goal of limiting the connectivity of its systems in order to "reduce the cyber-attack surface". However, with the explosive growth of Internet of Things (IoT) and network-connected devices in many working environments this potential attack surface is becoming a larger and larger target for bad actors.

Goldilock manufactures and develops an appliance which allows remote disconnection and connection of any device or network, anywhere in the world, without using the internet. Networks are segmented and either left offline until they are needed, have scheduled connection times or are left on at all times, with the capability of isolating areas so that they can be immediately isolated by a kill switch. The patent that makes Goldilock's technology is unique in that it does not use the internet and is the only product available that has this capability – it is a full, physical disconnect for vulnerable systems and provides the ultimate protection against adversaries in a heightened geopolitical climate of cyber threat. The company's vision is to have Goldilock embedded in every connected device, and eventually to provide it as a product to protect home users.

Founded by two ex-military serial entrepreneurs, Goldilock has developed its core patented technology over more than five years and is committed to only working with the UK and its allies. Its new ruggedised devices have been developed in conjunction with the DASA & Dstl UK Government agencies and complement the company's existing Enterprise IT rack-mountable 12-port Drawbridge unit. Goldilock has exported to Ukraine's CyberCommand, Etihad Airlines in the UAE, various EU government entities, Defence Digital, Cisco in the USA as well as to channel partners in Singapore serving the APAC region. Goldilock has the privilege of having passed through the UK's National Cyber Security Centre's Startups program and has received a number of awards, including the Barclays Startup Award.

Securing Connected Devices Case Study

ANGOKA

The connectivity of operational technology, the Internet of Things, is being driven into every aspect of Critical National Infrastructure at an ever-increasing pace. The challenge of connecting systems securely is also compounded by the mix of legacy and modern systems that are involved, which can result in operators having to deal with systems that offer multiple attack vectors to hostile actors.

Angoka offer a solution for securing connected devices which represents a paradigm shift in the market. Their unique and patented Device Private Network technology provides an Identity and Key Management platform tailored to connected devices, without the need for Public Key Infrastructure. Their solution generates tamper proof, hardware based identities combined with an automatic, decentralised and dynamic key management system. This allows for secure communications between systems to be maintained even over untrusted networks.

Angoka's technology can be retrofitted to legacy equipment as well as being built into products that are secure by design. Their monitoring system provides real time threat information with appropriate alerts and the ability to remotely administer the system allowing administrators to add and remove devices, or move devices between Device Private Networks.

The company's innovative solution offers operators of critical national infrastructure the ability to secure their connected devices from a range of cyber-attacks, whatever the network connection and without the need to rely on a Public Key Infrastructure.

Angoka was founded in 2019 to ensure the safety and resilience of connected devices, protecting their communication, through superior cybersecurity solutions. An Alumnus of the prestigious UK National Cyber Security Centre (NCSC) Cyber Accelerator Programme, they are a multiple award-winning company with a track record of delivery in connected and autonomous systems.

Managed Detection & Response Case Study

tmc3

In 2022, amid the continuing global surge in cyber threats a UK Government Department recognised a business-critical need for a 24 hour a day cyber managed detection and response (MDR) across their digital estate. Challenged with a complex IT estate of over 5000 users across new and legacy systems, and a lack of defined requirements. tmc3 was engaged to accelerate scoping, procurement, and deployment of an MDR solution.

The tmc3 Cyber Team swiftly mobilised to identify and assess current tools, technology, data feeds, and monitoring resources against industry best practice. Through a series of workshops, crucial "Must have, Should have, Could have, Won't have" (or MoSCoW) requirements were captured, and a comprehensive Statement of Requirements was produced. Working closely with the Department's procurement team, tmc3 enabled the diligent evaluation and scoring of potential providers, taking into account technical capabilities and financial budgets to determine the best fit for the Department's requirements.

tmc3 expedited the deployment of the capability by over 6 months, delivering a cost effective, fully operational MDR service by mid-2022. The MDR service was assessed against the National Cyber Security Centre's (NCSC) Cyber Assurance Framework, using fine-tuned policies and alerts to detect any previous compromise and to evidence compliance. The accelerated programme provided assurance to the Department that cyber threats were being effectively managed and provided added value through operational cost savings.

Trusted by central government, enterprise organisations and Critical National Infrastructure companies, tmc3 offer in-depth cyber security consultancy and products which enables secure business operations and peace of mind. They are specialists in cyber transformation, cyber security and data protection consultancy, secure software development lifecycle, supplier due diligence and assurance, security testing and assurance and cloud security.

Cyber Security Maturity Case Study

BAE SYSTEMS

Critical national infrastructure (CNI) organisations are targeted by some of the most advanced and persistent threat actors in the world. However, the services CNI organisations provide are critical to consumers and government, and so it is essential to understand the maturity of an organisation's security against relevant threats that their infrastructure faces.

BAE Systems supported a European and Asia based telecommunications provider that was being targeted by an advanced threat group. Our UK NCSC certified cyber incident response team supported the provider in dealing with a suspected cyber-attack by an advanced threat group. Their Security Operations Center Maturity Assessment (SOCMA) and Attack Simulation Assessment (ASA) services were then delivered to improve the maturity of the provider's security. The SOCMA first helped the organisation understand weaknesses in its security operations capability and put in place a set of prioritised, targeted and actionable recommendations aligned to strategic security maturity targets. The ASA then allowed the new capabilities to be tested through execution of various offensive and defensive techniques to test the organisation's security detection and response.

The purpose of an ASA is to identify risk across multiple attack vectors including but not limited to, exposed infrastructure / applications, social engineering, or even physical access, depending on the prior agreed scope. The main aim of an attack simulation is to ascertain a security operations centre's ability to detect, detain and mitigate an active threat actor within the target network, or respond to an attack carried out within the environment.

BAE Systems is one of the premier leading global suppliers of Enterprise cyber services, solutions, consultancy and expertise to government organisations, CNI, and large national corporates.

Training & Capacity Building

Training & Capacity Building

Threats to critical national infrastructure sites have increased over time, and the emergence of sophisticated technological threats has added a new dimension of risk. It is key, therefore, that staff who manage the security of sites have sufficient skills to understand and respond to threats, both familiar and novel.

The UK has the highest levels of expertise in this area and offers training and capacity building on all aspects of site security. Training providers work with our domestic security forces and academia to ensure that their programmes and courses are up to date and take into account emerging forms of threat. UK companies can offer training and capacity building to employees across organisations responsible for critical national infrastructure, including site managers, security guards, Human Resources staff and others in a range of disciplines including:

- Basic security and safety awareness
- Development of security procedures
- Man guarding
- Emergency response
- Risk management
- Vetting processes for incoming staff
- Cyber security

The UK has several large-scale training facilities, which in addition to classroom training also offer facilities for mock exercises and incident scenarios and can accommodate visiting staff. UK companies also have a long track record of successfully delivering training programmes around the world.

Building Skills, Knowledge & Competence Case Study

The eight principles of the integrated crisis management (ICM) cycle are anticipate, assess, prevent, prepare, validate, respond, recover and learn. These well-established and widely recognised principles are key in building more resilient systems, organisations and infrastructures.

Businesses, especially those that run essential services and Critical National Infrastructure, are a crucial partner in building our collective resilience.

The challenging context of increasing volatility and the interconnectedness of risks, generated by geopolitical and geoeconomic shifts, advancement in technology, and the significant impacts from climate change, means the risk picture we face is not just more complex, but is also evolving at a faster pace. The line between domestic and international is more blurred and events that originate abroad have a greater impact on the UK.

The Emergency Planning College (EPC) is the Cabinet Office college delivering training, exercising, advisory services and learning and development against all of the eight principles of integrated emergency management.

As the UK's national centre for increasing the skills, knowledge and competencies for building resilience, we offer our services, and have supported many of the most significant industries and organisations both in the UK and around the world.

The EPC specialises in the resilience disciplines of business continuity, organisational resilience, crowd and event safety, crisis communications, risk, planning and preparedness, emergency response and recovery and cyber resilience. Any public or private organisation, based domestically or overseas, can access the EPC's services.

Improving Cyber Awareness & Behaviours Case Study

In addition to unpatched and vulnerable hardware and software, people are also a key vulnerability to cyber-attacks as they can be tricked into clicking on malicious links, opening infected attachments, or giving away their personal information that allow attackers to gain access to systems and networks, steal data, or cause other damage.

UK startup ThinkCyber was engaged by a UK defence and security-focused professional services organisation seeking a cutting-edge solution to drive higher engagement with security awareness training and embed secure behaviours. The client had realised that traditional security awareness training was not delivering the behaviour change required to reduce the risk of cyber-attacks targeting their people. Whilst also feeling that phishing simulations left staff feeling tricked and embarrassed, damaging the security culture they were seeking. “Existing tools were OK, but OK isn’t good enough when 85% of cyber-attacks target people”.

ThinkCyber’s unique offering, Redflags® Real-time Security Awareness, delivered real-time interventions to staff at points of risk, guiding staff and embedding secure behaviours. For example, delivering campaigns to steer behaviours when staff plugged in a USB, tried to upload data in their browser, clicked a link and were about to give away their credentials, worked with attachments etc. These real-time interventions were tracked, allowing measurement of change from an initial baseline. In addition, the Redflags® drip fed content saw engagement levels up to 92% without the need to use negative incentives or trick staff with phishing simulations.

Beyond this case study, ThinkCyber has been carrying out research and development in the security and awareness field for six years, working with behavioural science academics at leading UK Universities, and on research projects, including with the UK Cabinet Office to hone their approach. They are engaged with automotive firms in Europe, energy and utilities firms in the US and defence, global financial services firms and security professional services firms in the UK and Canada.

Planning & Consultancy

Planning & Consultancy

Planning is an essential element in the building and later modification of critical national infrastructure sites to ensure that sufficient security features are built into the design. Expertise is available from the UK across a wide range of areas.

Where the necessary expertise is unavailable in-house, UK companies can provide comprehensive advice, whether at the initial design and build stage or during modifications where new technology is being introduced. Through the Register of Security Engineers and Specialists, supported by the UK Government's National Protective Security Authority, buyers can also access specialists who can provide advice and guidance to operators of critical national infrastructure in eleven key areas:

- Protection against the effects of weapons
- Protection against the effects of blast
- Electronic security systems
- Chemical, biological, radiological and nuclear (CBRN)
- Hostile vehicle mitigation
- Protection against forced entry
- Explosives and weapons search detection
- Force protection engineering
- Digital built environment
- Personnel security (insider threat)
- Personnel security (human factor)

Consultants can also help site operators to understand their level of risk by identifying the threat landscape present in the country and conducting impartial threat assessments.

The UK also has a healthy ecosystem of trade associations who can help buyers to identify member companies who can address their needs. These include ADS, the British Security Industry Association (BSIA), the Perimeter Security Suppliers Association (PSSA) and the Fire Industry Association (FIA).

Risk Consultancy Case Study

Securing CNI sites requires a wealth of understanding and expertise. To best plan and deploy the correct solutions its vital risks are assessed and planned for correctly. The UK has access to some of the best consultants to manage this for CNI sites.

G4S Risk Consulting supports clients to evaluate and understand the risks they and their organisations may face, acting to mitigate these risks wherever possible, and providing the tools to fully prepare clients to react successfully to a crisis should it occur. Their team of 24/7 analysts provide insight and intelligence into the threats that clients face. By understanding the threat they use their expertise, global resources and intelligence to work with clients to develop a solution which matches their exact requirements, with the aim of not only protecting people and assets but improving business efficiency.

The company offers trusted security advice, risk mitigation strategies, secure support and integrated solutions for strategic clients or those operating in complex or sensitive environments and can address threats that come from crime or terrorism, or simply from entering new ventures markets or territories. They work to design and implement effective measures to mitigate or manage these risks so that, should the unexpected happen, they can support clients in times of emergency or crisis.

They enable clients to develop resilience to business risk by providing:

- Proactive intelligence gathering, analysis and research, using the latest techniques and processes
- World class risk advisory and mitigation services
- Outstanding crisis management and response capability
- Expert advice on risk management technologies.
- Specialist training and capacity building programmes

G4S is a leading security and facility services company that provides proactive security services and cutting-edge smart technology to deliver tailored, integrated security solutions that allow clients to focus on their core business. Through a global workforce of approximately 800,000 people, they leverage best practices in communities all over the world. With revenues at approximately $20 billion, they are supported by efficient processes and systems that can only come with scale to help deliver their promise locally: keeping people safe so our communities can thrive.

Design & Build Case Study

While the design and build process for a new development is an extensive and complex process, ensuring that a site is secure by design requires an additional level of capability and sophistication.

Atkins Global were engaged by Vantage to design the security elements of a new hyperscale 80 megawatt data centre on an existing site in Newport, Wales. This required detailed designs for the implementation of CCTV, electronic access control systems, intrusion detection systems and a dedicated secure network, with the aim of making the site one of Europe’s leading data hubs. The nature of this high-profile build, and the sensitive nature of the site, reinforced the importance of the security requirements to be deployed at this location.

Working with Faithful and Gould, Atkins Global won the contract due to their expertise in delivering high technology builds, with their consultancy team providing the specialist security knowledge required for implementing such a high security installation. The customer also required centralised monitoring systems which were designed by Atkins to ensure interoperability and resilience in order to accommodate future expansion of the site.

Founded in 1938, Atkins Global is a British-Canadian engineering, design, planning, architectural design, project management and consulting services company headquartered in London. Employing approximately 18,000 staff based in 300 offices across 29 countries and having undertaken projects in over 150 countries, the company is now a subsidiary of SNC-Lavalin, having been acquired in a £2.1 billion deal in 2017.

About Us

As part of the Department for Business & Trade, UK Defence & Security Exports' role is to help UK companies to export, and to provide the specialist advice and practical help that overseas buyers need.

We do this by building close relationships with industry and with overseas governments as well as working closely with other UK Government departments including the Home Office, the Ministry of Defence, the Foreign, Commonwealth and Development Office.

In addition to the military, security, fire and resilience specialists in the Department we also work through a network of over 3,000 trade staff based in our Embassies and Consulates around the world. We also support the major trade shows for the defence, security and cyber security sectors that take place in the UK and overseas.

Next Steps

This brochure, which focuses on UK industry's expertise in providing support for operators of Critical National Infrastructure sites, represents the combined expertise of companies from across the sector. It contains case studies that give a snapshot of the world-class solutions the UK can offer, but the list is not exhaustive.

If you are interested in any of the capabilities presented here, our security industry stands ready to help. The depth of knowledge and expertise that companies in the UK provide can help you to keep your next major event safe and secure from threats.

For further information please contact the UK Defence & Security Exports staff locally or the domestic team based in London, Cardiff and Darlington.

UK Defence &
Security Exports

London address:

Old Admiralty Building
Admiralty Place
London
SW1A 2DY

https://www.gov.uk/government/organisations/uk-defence-and-security-exports

securityexports@businessandtrade.gov.uk

About Our Contributors

Simon Banks is the Chairman of the British Security Industry Association (BSIA) and Skills for Security, the largest provider for apprenticeships in the security industry. He is also the Founder and Director of CSL Group, a UK technology company that focuses on the provision of critical communications solutions.

Simon is also a Director of the National Security Inspectorate (NSI) and was formally a board member of BAFE.

The Department for Business & Trade would also like to thank CSL Group Ltd, the UK Security & Resilience Industry Suppliers Community (RISC) and its constituent trade associations, including ADS and the British Security Industry Association, for their support in the production of this brochure.

Whereas every effort has been made to ensure that the information in this document is accurate, UK Defence & Security Exports and the Department for Business & Trade do not accept liability for any errors, omissions or misleading statements, and no warranty is given, or responsibility accepted as to the standing of any individual, firm, company or other organisation mentioned.

This document is also available on our website at:

https://www.gov.uk/government/organisations/uk-defence-and-security-exports

Not all of the equipment listed in this brochure is necessarily in UK operational service. The inclusion in this brochure should not in any way be considered as HMG approval or endorsement of the products concerned. Interested parties should note that in all cases it is advisable for them to undertake their own research to ensure that any UK equipment being displayed meets their particular operational requirements.

UK Defence &
Security Exports

Department for
Business & Trade