QINETIQ

Countering the threat from emerging technologies

A new range of disruptive technologies, collectively labelled The Fourth Industrial Revolution (4iR) are transforming the way we live and work by fusing the physical, digital and natural worlds together.

Incorporating machine learning, artificial intelligence; synthetics; autonomous systems; connected devices; and data analytics, 4iR technologies are all distinct areas of innovation. The characteristic they all share is an ability to transform industries, economies and processes.

The potential changes offered by 4iR technologies is apparent. They include the promise of greater efficiency and productivity and improvements in service personalisation. But they also offer significant challenges for any organisation that needs to protect users, information, systems and processes because many could equally present a significant threat to our safety and security.

This is particularly the case for those organisations that manage the infrastructure on which society runs. The consequences of malicious attacks or innocent errors rise substantially in their operating environments. That makes them obvious targets for those who want to cause disruption or harm.

Their risk is further exacerbated by two fundamental truths. First, the complexity of the environments in which they operate make the number of potential vulnerabilities high. They are, in effect, a highly complex mesh of different elements, all working together in harmony. Facilities, vehicles, processes, equipment, technology platforms, and people - the smooth running our infrastructure depends on the effective interoperability of these component parts. At any point where one component interacts with another, gaps in the system can emerge and be exploited.

Secondly, the sheer variety of the technologies in question intensifies the challenge. Critical infrastructure organisations cannot be across all the emerging technologies with sufficient depth to identify the greatest areas of risk. Decisions around which technologies need to be considered potential threats is therefore not simple. Getting it wrong could have significant consequences.

Transport, finance, utilities, and telecommunications organisations all recognise why they must get in front of the problem and increase their understanding of, and countermeasures to, the 4iR threat. They understand the shifting threat vectors and are aware of the knowledge gap that exists around emerging technologies. This report is designed to provide them with insight into some of the most prevalent as a starting point.

Based on our experience of helping critical organisations mitigate the risk of complex and emerging threats, we have outlined what we believe to be five of the most prevalent 4iR technologies and the risks they could present to critical infrastructure organisations. For each one we provide an overview of the current technology; an outline of the potential threats; an example of that threat presenting itself in the real world where available; and a clear set of recommendations to mitigate its impact in the future. By doing, s so we hope that the organisations responsible for maintaining our infrastructure can move towards the front foot when countering the risks of 4iR technology today, and reduce the chances of being caught out by unexpected situations in the future.

Fifth Generation (5G) networks represent a revolution in mobile technology that connects people, machines and services. The potential to change the way we use mobile devices is considerable, but the infrastructure developments that enable 5G means greater potential risk to data and security and a need for greater focus on network assurance.

The technology

5G is an entirely new mobile network built to enable a new way of using mobile devices, applications (apps) and services. It delivers very fast mobile broadband speeds and its new infrastructure provides incredibly resilient and powerful new capabilities that make it far better suited to business users.

Network resilience

5G delivers us a truly software-definable network offering ultra-low latency and vastly increased reliability. This enables critical services such as remote healthcare video monitoring systems to rely more heavily on mobile connectivity - moving from fixed to mobile infrastructure with a very low risk.

Mass connectivity

5G is designed to natively support the Internet of Things (IoT), allowing up to a million devices to be connected per square kilometre. This unlocks massive potential for having IoT sensors in a whole host of applications where it was previously impractical, allowing organisations to offer much richer services than ever before.

Network slicing

Because 5G networks will be software-controlled, operators can define a 'slice' of the network tailored to particular requirements, which can be sold exclusively to a particular company, or for a specific service. If a large event is taking place and the organisers want to offer 4k live video streaming to attendees' mobile devices, 5G connectivity will give them the uninterrupted bandwidth and signal resilience to do so without the risk of service interruption.

Pay as you use models

The increased capabilities of 5G networks will underpin new business models that rely on charging for use rather than ownership. Heating equipment companies could use 5G connectivity to smart boilers to charge customers for the amount of time they use the boiler each year rather than for the one off cost of the boiler itself. The reliability of the network, along with its ability to support IoT sensors, will make that a low risk model and an easy way to maintain a longer customer relationship.


5G

Threats

The benefits of 5G for businesses, organisations and consumers are considerable. But new advantages do not come without new risks. These are the four main risks organisations need to be aware of as they plan their 5G exploitation strategies.

More hardware, more risk

Delivering 5G's benefits requires an entirely new mobile infrastructure to be built. High data rates come, in part, from higher frequency signals sent over short distances; whilst low latencies are achieved by placing computing power closer to the network edge and end users. This means more pieces of equipment, placed over shorter distances in lower service locations – including within business user premises. The result is a 5G network infrastructure that is bigger, more diverse and which offers more places where unintentional vulnerabilities or malicious attack could emerge.

Data dispersal through complex applications

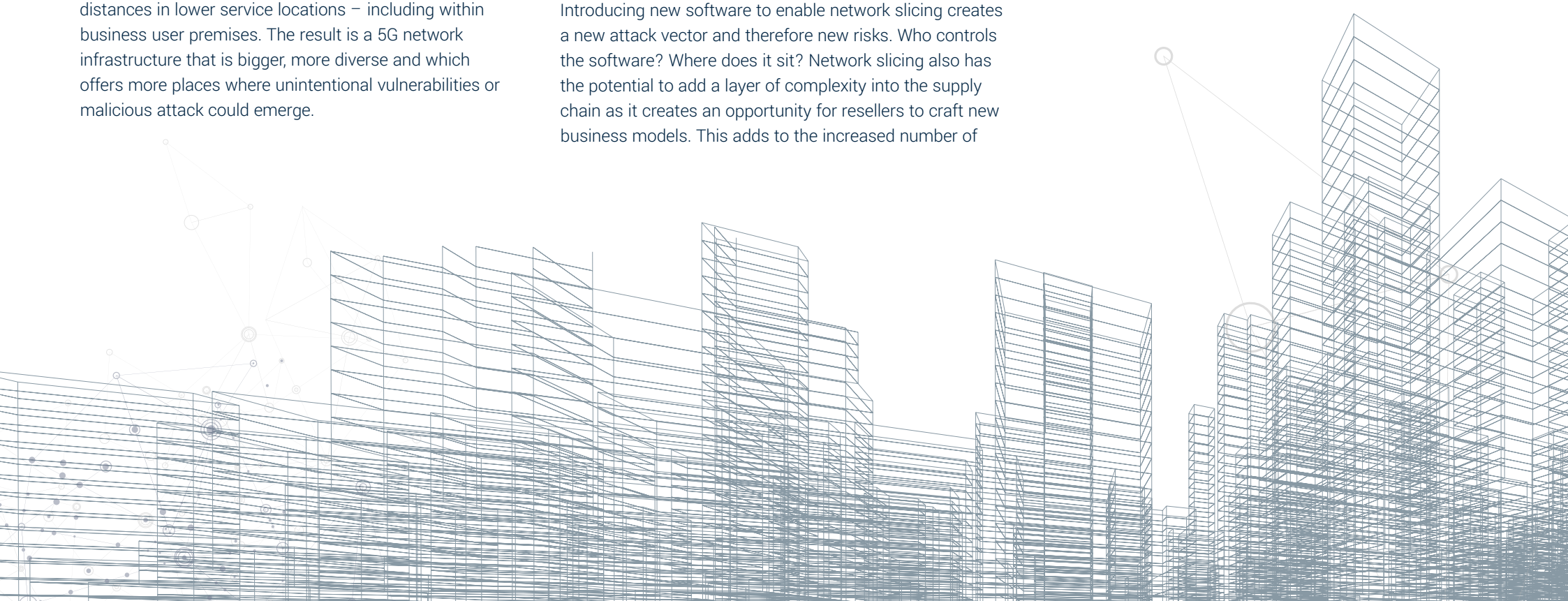
A larger, more complex infrastructure increases the size of the attack surface making it far harder to assure data as it moves through the network. How apps will access, use and share data will change radically in 5G environments, making it more difficult to substantiate and assure data location, provenance, and information security. It also means that valuable customer and industrial data will be 'at rest' in different locations to current company computing repositories or iron-clad data centres. This risk will be exacerbated when the power of 5G networks begins to stimulate the development of more powerful and data-hungry business applications for critical services.

Network slicing

Introducing new software to enable network slicing creates a new attack vector and therefore new risks. Who controls the software? Where does it sit? Network slicing also has the potential to add a layer of complexity into the supply chain as it creates an opportunity for resellers to craft new business models. This adds to the increased number of organisations and technologies involved, creating more gaps in the network architecture and therefore more potential vulnerabilities

Dynamic Network

As 5G networks mature they will become more dynamic, adapting and responding to traffic levels, as well as the applications running over them. For example if the number of users in a particular vicinity increases the level of traffic, network functions can be moved closer to that location to reduce latency and loading on the backhaul network. Or network slicing applications could influence and change the network configuration – for example changing how traffic is routed to reduce latency in particular instances. Such capabilities could be exploited for malicious purposes.



Recommendations for risk mitigation

With 5G still emerging, the reality of the risks involved and therefore a clear view of the ways to mitigate them is not yet available. But there are some ways in which organisations can build security, assurance, and risk reduction into their planning today to give them a headstart:

Use industry standards at the design phase

Industry guidance and standards for security should be incorporated at the design phase of any 5G application or network. For example the National Cyber Security Centre (NCSC) in the UK issue guidance on how to protect Internet of Things devices. It is important to ensure that the standards and guidance are tailored to the industry in question – for example the 5G Automotive Association is the industry body for 5G for vehicles.

Design in Security upfront

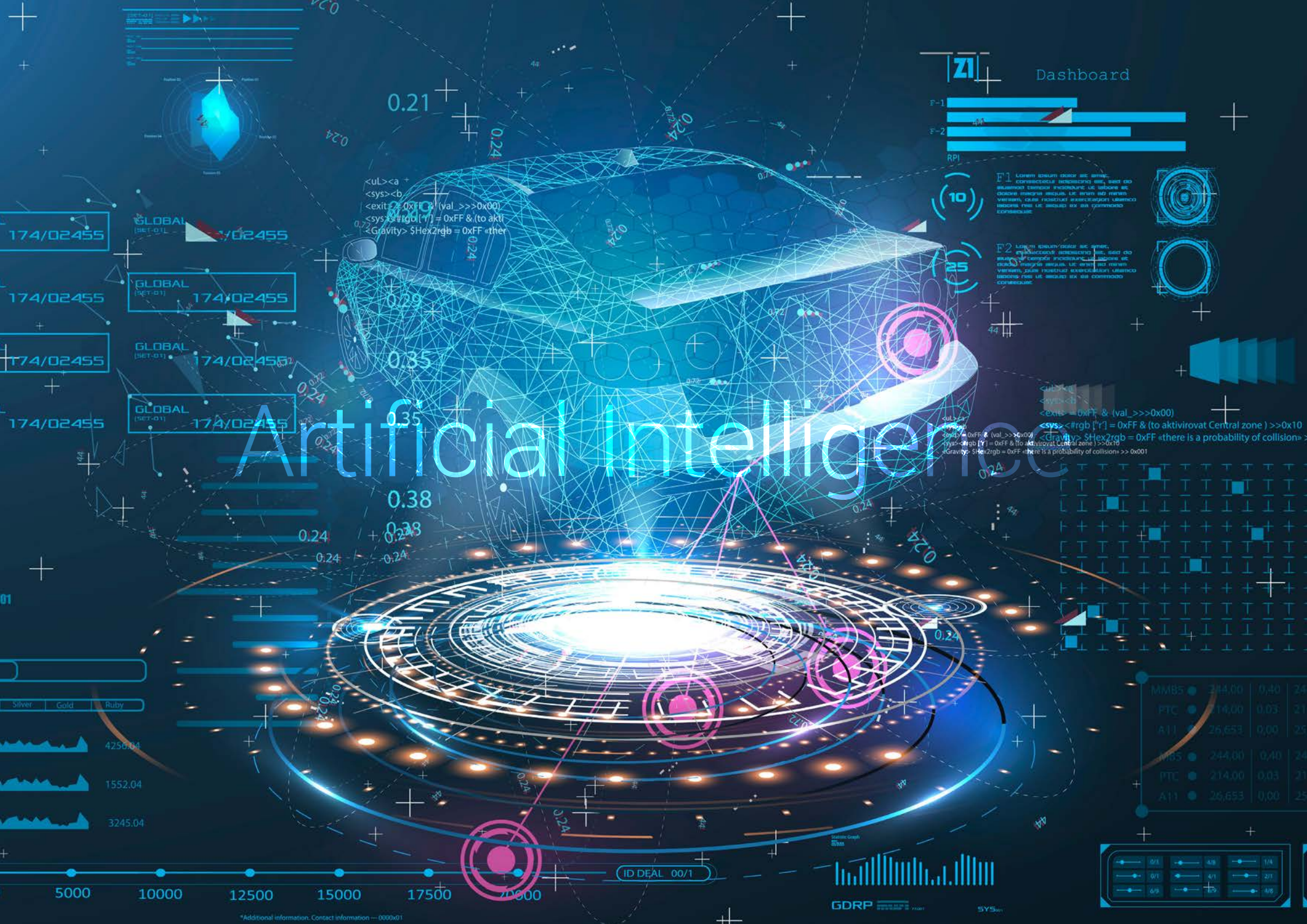
When designing a 5G network, application or service, security should be considered alongside other constraints such as cost, performance, and safety. This approach balances security risks against benefits based on an organisation's requirements.

Get it tested

5G networks, applications or services must be independently tested after they have been built to check that the security measures are working as designed, and that no unintentional vulnerabilities have been introduced. This testing needs to support the commercial model of continuous deployment 'DevOps' so it must include some automated testing as well. It is essential that this testing considers the radio interface as it will be used for business critical services when more and higher frequencies begin being used in complex environments where unintentional or malicious interference can cause issues for vital infrastructure.

Continuous analysis of mobile data traffic

Using emerging test technologies to analyse new 5G services and mobile applications for data leakage as part of the development cycle will make them more robust at first delivery. As these services become live the ongoing use of such test technologies to constantly monitor data traffic will maintain a low risk of data breaches through the service lifecycle.


Artificial Intelligence
Dashboard
GLOBAL
174/02455
Silver
Gold
Ruby
4256.04
1552.04
3245.04
5000
10000
12500
15000
17500
ID DEAL 00/1
GDRP

Artificial Intelligence (AI) and machine learning are already informing decisions and automating processes in the commercial world. As these technologies spread into critical infrastructure, questions need to be answered about how we build sufficient trust in intelligent systems to reap the rewards without increasing risk.

The technology

AI and machine learning involve computers crunching vast quantities of data to find patterns and make predictions without being explicitly programmed to do so. Larger quantities of data, more sophisticated algorithms and sheer computing power have given AI greater force and capability.

The outcomes are now similar to what an army of statisticians with unlimited time and resources might have come up with, but they are achieved far more quickly, cheaply and efficiently. This has led to a dramatic drop in the cost of making predictions.

From the impact of weather changes on agriculture, to forecasting demand for electricity, organisations outside of the technology sector are beginning to benefit in a myriad of ways.

A major development has been the expansion of data inputs that can power AI. Computers have been able to read text and numbers for decades, but have only recently learned to see, hear and speak to a sufficiently advanced level.

Many industries are becoming increasingly automated and the systems which power automated tasks often use machine vision to help them identify something or someone as part of their decision making. Similarly, AI's use of speech recognition now underpins voice assistants on phones and home speakers, allowing algorithms to listen to calls and take in the speaker's tone to define its response.

Threats

As AI moves beyond the technology sector and into more regulated industries that deliver complex and critical services, organisations will find an increasing number of applications for intelligent systems and automation. But as they explore the possibilities they need to balance the risks that come with such advanced technologies. There are three main risks organisations need to be aware of as they plan their AI strategy.

Old established infrastructure

Many of the industries responsible for maintaining and improving our national infrastructure are more than 100 years old. So are some of the facilities and the systems

they use, and many of the processes and policies that define their ways of working. The level of change AI and automation brings is substantial and if that change is not sympathetic to the operating environments in question it will create problems and risk. Many AI platforms are trained to look for modern answers to modern problems. In a well-established environment that could lead to missing important issues, resulting in downtime, loss of compliance, and exposure to malicious attack.

Hacking

AI-driven automation requires an increase in the scale and complexity of the technology embedded in our society's infrastructure. In many instances it will require improvements in connectivity, software, and hardware. Like any other connected system it will be vulnerable to malicious attacks from any number and type of activists. The more complex computing systems we use to automate our infrastructure, the larger the attack surface becomes. This is particularly important for utility services where any outage has an exponential effect. If a single power distribution point is taken down, the impact could affect tens of thousands of users.

Electronic interference

Electronic interference is all around us. It can be caused by mobile phones, wireless hardware, faulty wiring, or malicious attack. It has the potential to prevent AI systems performing as required; but it is incredibly difficult to measure and leaves no trace, making it impossible to identify with any real accuracy after the fact. The increase in process automation that AI can enable in our critical infrastructure means more elements of the critical services on which we rely exposed to this vulnerability. Finding new ways to measure, predict and pre-empt the threat is paramount.

Examples of AI threats in action

AI and machine learning are being used by criminals to exploit the vulnerabilities of companies. The first reported case of this was in November 2017 when a new type of cyberattack was found at a company in India, using early indicators of AI-driven software. Using AI, hackers infiltrated IT infrastructure and stayed there unnoticed for extended periods of time. Hiding in the shadows, the hackers then learn about the environments they had entered and blended in with daily network activity. Using a sustained, unnoticed presence in this way, hackers' knowledge of a network and its users grow stronger, to the point where they can control entire systems.

In 2016 Microsoft launched its experimental AI chatbot, Tay, onto Twitter. The intention was for Tay to mimic the language patterns of a millennial female using Natural Language Understanding (NLU) and adaptive algorithms in a bid to learn more about conversational understanding and AI design. After just 16 hours, Tay was removed from the internet after her jovial exchange turned into an A-Z of insults, sexism and racism after being corrupted by twitter trolls. Knowing that AI is only as intelligent as the data it is fed, they taught Tay all the wrong things.

Recommendations for risk mitigation

As AI becomes a critical part of the way we operate, infrastructure organisations need to take certain steps to get in front of the threat. There are three main considerations that can help them set out on the journey with security and assurance built into their approach:

Continuous monitoring

The most effective way to mitigate the risks outlined above is to continuously monitor the activity of intelligent systems. This is particularly relevant to electronic interference, both accidental and malicious. Early warning of electronic disruption enables rapid diversion of services, and reduced downtime, as well as protecting vital assets. Putting in place a system that allows for the continuous real time evaluation of electromagnetic threats is a recommended step for any organisation seeking to increase automation in critical environments.

Human in the loop

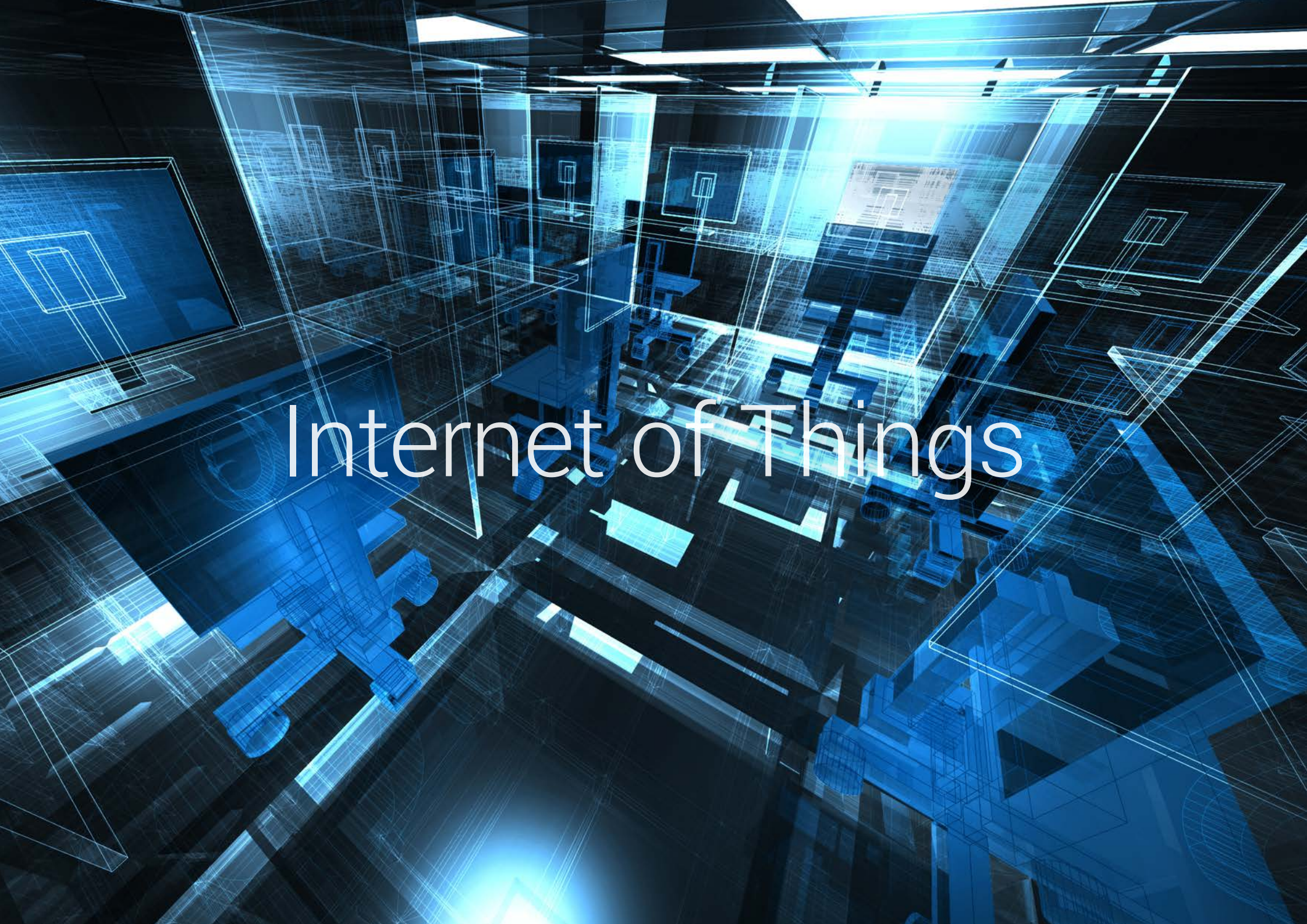
Fully automating new and existing systems can increase risk. Whilst AI systems can process far more data much faster than human beings, our creativity, curiosity and ability to make quality judgements with less learned data are key. Even the best machine learning algorithms are unable to see the potential of something in the same way a human can. It means that the 'sweet spot' for harnessing the value of AI at low risk is human-machine teaming where people and AI work together to employ the best of both assets. These are the design parameters critical infrastructure organisations should aim for when introducing automation.

Use your AI to monitor your own environment/ systems

Whist enabling a more automated environment, the implementation of the AI technology underpinning that increased automation also provides a way to monitor the same environment for anomalies. It is important to recognise the dual role this technology can play and implement it in a way which allows it to serve both purposes, maximising its value whilst reducing any associated risk.

Develop trust

Just like we do with humans we have to learn to trust what AI does and says. We also need to recognise that like humans, it will make mistakes. Any automated systems underpinned by AI and machine learning should be developed in a way that appreciates these challenges and therefore engender trust over time. Recognising the limitations of AI as much as its potential, and managing expectations accordingly, is critical to achieving this trust.


Internet of Things

Internet of Things (IoT), AI and machine learning are already informing decisions and automating processes in the commercial world. As these technologies spread into critical infrastructure, questions need to be answered about how we build sufficient trust in intelligent systems to reap the rewards without increasing risk.

The trend towards connected machines and objects has extended far beyond the consumer environment. It now permeates deep into the industrial and commercial devices on which our infrastructure is based. Within that infrastructure a significant percentage of the industrial, building and city control systems that are widely used directly or indirectly in critical infrastructure such as power generation and transmission are utilising internet connectivity (usually wireless) to improve efficiency. Enabling control systems to talk to a range of devices and each other, offers the potential for a 'fourth industrial revolution', and experts predict more than half of new businesses will utilise IoT by 2020.

The technology

The term IoT encompasses physical devices connected to the internet, but it is increasingly being used to define objects that talk to each other. The Internet of Things is made up of devices – from simple sensors to smartphones and wearables – that are connected together. By combining these connected devices with automated systems, it is possible to gather information, analyse it, and create an action to help someone with a particular task, or learn from a specific process. It is also possible to control these devices remotely, from a phone or a computer.

IoT offers opportunities to be more efficient, saving time and money in the process. It allows companies, governments and public authorities to re-think how they deliver services and produce goods. And it enables a greater understanding of how assets and systems are performing. This helps avoid errors and identify potential issues before they can have a material impact.

The technology itself is not often complex. It usually involves the integration of a simple chipset designed to enable network connectivity, either wired or wireless (or both), and the update of firmware to enable the device in question to access and use that functionality. That simplicity makes it cost-effective and therefore attractive to manufacturers and operators. But it can also increase the risk to the systems that rely on IoT-enabled devices.

Threats

Simplicity

The relative ease and low cost of connecting previously dumb devices makes it simple for non-specialists to connect a range of them to corporate networks as part of modernising industrial control systems. If they have not checked the security of those networks and undertaken a thorough risk assessment these devices could be accessed by a far wider range of people within the organisation than is desirable, and potentially by anyone outside the organisation too. The simplicity of integration drives a focus on functionality without similar attention to the risks involved.

Component security

The risk above is exacerbated if the components to enable network connectivity are themselves insecure. The cost of these chipsets has dropped dramatically. Many can now be purchased for little more than a pound. At this price they rarely have adequate security for use in critical systems. To achieve that level of security the spend typically needs to increase tenfold. Many manufacturers are working on slim profit margins so they opt for the cheapest part. As a result, many IoT-enabled devices end up in critical services without a sufficient level of security for their environment, increasing their chances of being compromised by malicious attacks.

Software maintenance

Many IoT devices are everyday pieces of equipment that contain mini computing systems. They all run on software so updating and patching that software and firmware is a critical part of maintaining their security. But with so many devices becoming connected, software companies cannot always keep pace. They will usually provide software updates for three to five years but beyond that operators can be faced with stark choices – to rip out the infrastructure and replace it with a new version, or to leave it where it is, albeit with reduced security. The former is expensive, requires a disposal strategy, and lots of manpower. The latter requires nothing.

Data quantity

IoT demands a rich stream of data flowing between devices. This abundance of data attracts cyber criminals and hackers intent on either stealing that data or disrupting its flow, preventing the effective operation of critical services.

Data integrity

While most of the public discussion regarding cyber threats is focused on the confidentiality and availability of information, by far the most serious cyberattacks are those that change or manipulate electronic information in order to compromise its integrity. Data used in critical infrastructure can be an easy target for manipulation by external attackers or insiders. Because the IoT increases the volume of data on which critical services rely, this is a growing threat with significant consequences.

Established infrastructure

Our infrastructure utilises a wealth of modern technology but its foundations often remain dated, as do the Supervisory Control And Data Acquisition (SCADA) systems that allow them to function correctly. Simply connecting these to a network may seem like a quick fix but it ignores the fact that the established protocols on which they operate have not been designed with IoT or networked security in mind. When combined with a potentially insecure network and a lack of professional risk assessment, disrupting their operation becomes trivial.

Examples of ubiquitous electronics threats in action

In October 2016, the largest ever DDoS attack was launched using an IoT botnet. This lead to huge portions of the internet going down, including Twitter, the Guardian, Netflix, Reddit, and CNN. This IoT botnet was made possible by malware called Mirai. Once infected with Mirai, computers would continually search the internet for vulnerable IoT devices and then use known default usernames and passwords to log in, infecting them with malware as well. These devices were simple consumer items including digital cameras and DVR players.

In 2016 St. Jude Medical's implantable cardiac devices were found to have vulnerabilities that could allow a hacker to access a device. Once in, they could deplete the battery or administer incorrect pacing or shocks. The devices, like pacemakers and defibrillators, are used to monitor and control patients' heart functions and prevent heart attacks.

Recommendations for risk mitigation

Training and education

The majority of individuals and teams adding IoT functionality are experts in the systems being enhanced, not the connectivity technology itself or the security threats involved. They may not have had sufficient training in how to improve cyber security or conduct suitable risk assessments. A training strategy that integrates cyber security and digital risk management into the skillsets of critical infrastructure technical and facilities managers would help close this gap.

Isolation and segmentation

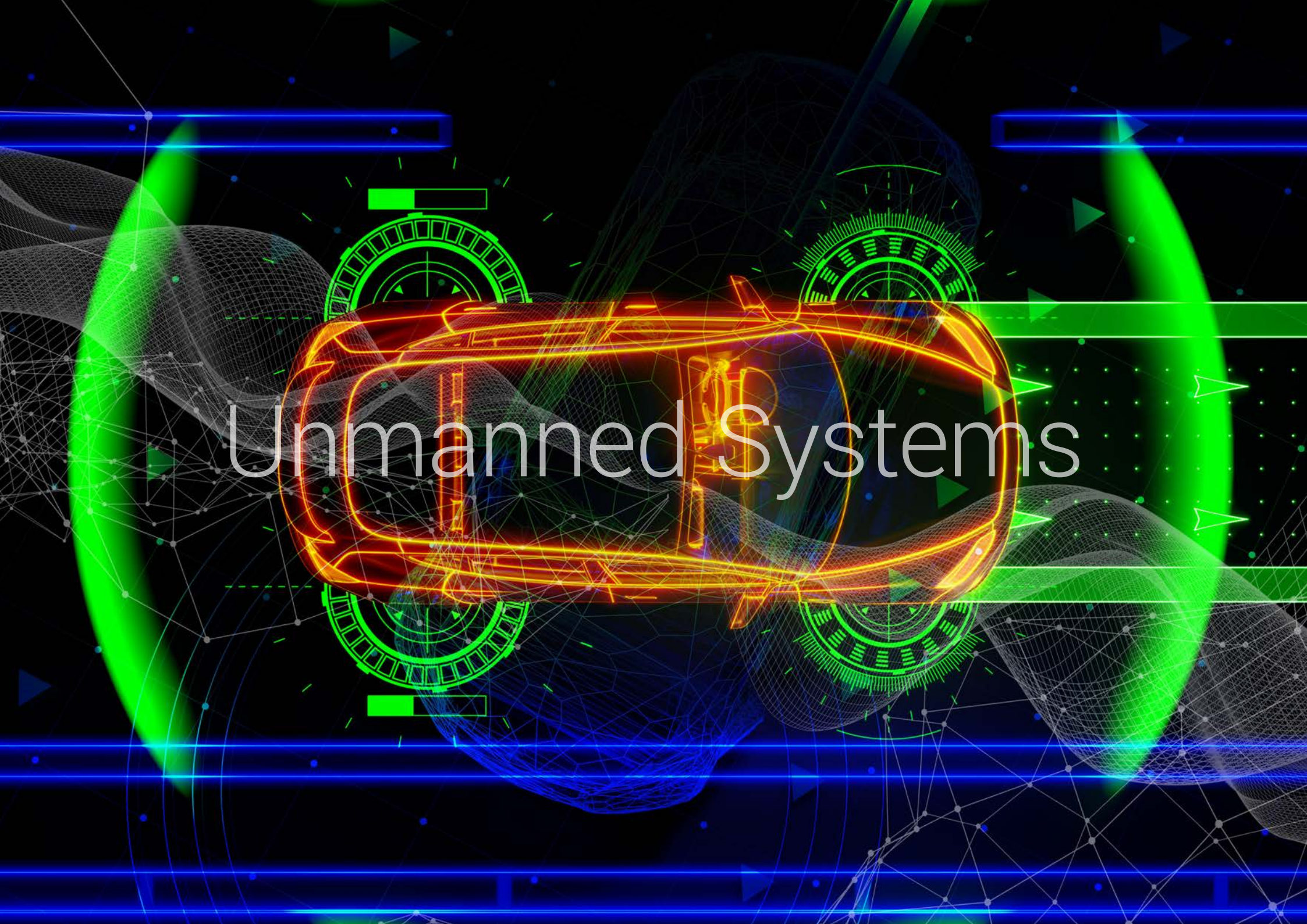
Just because a device can be connected to the Internet doesn't mean it should be. By understanding data paths through the network, engineers can be more selective about where IoT has a role to play and where it doesn't. Isolating components in an existing system reduces the number of potential vulnerabilities and should be encouraged. The most effective path is to design a secure architecture that accommodates the exploitation of IoT only where it is needed and isolates connected devices from other systems prior to procurement.

Audit logging

One of the best ways to reduce the risk of IoT implementations is to maintain an accurate understanding of what is happening on the network. Organisations should use audit logging to identify what has happened and build it into their planning for how to prevent and recover from future outages and attacks.

Governance

More rigorous policies and the introduction of well-developed codes of practice can stimulate significant behavioural change. Systems should be regularly penetration tested by certified professionals; passwords should be changed from default to secure as a matter of course; those with full control over IoT-enabled technology should be limited to a small trusted pool of users; and installation and maintenance contractors should be certified to ISO 270001 or equivalent.


Unmanned Systems

Unmanned Systems. The rapid development of artificial intelligence and automated systems is increasing the number of unmanned systems in use today. Vehicles and devices that require only partial human input, or that can operate as a fully autonomous system, have become widely available to both corporate and individual users. Like all emerging technologies the potential benefits are substantial; if the accompanying potential risks can be overcome.

The technology

'Unmanned systems' encompasses a variety of systems, vehicles and devices with varying levels of autonomy from remote piloting of drones to fully autonomous systems capable of understanding and responding to changes in its surroundings. Across this scale they can broadly be split into four categories:

Remote piloting/control

At this level the full control of the system sits with a human operator who does not need to be physically present at the same location. Remote-controlled mining machines are an example much like CAT's Command system for autonomous hauling, dozing and drilling.

Decision support

At this level operators control the system but the system also prompts them for decisions. The choices made sit entirely with the operator but the feedback and data from the system stimulates a response.

Operator in the loop

At this level systems become more capable of reacting and responding to their surroundings. However, they are cannot make complex decisions without the involvement of a human being. The operator in this case has much less of the cognitive burden because basic decisions still reside with the system.

A good example is the automated factories being developed and deployed by advanced manufacturing companies. These undertake the majority of production line tasks but require a human to oversee the totality of the production line to monitor for safety, security, quality, and efficiency.

Full autonomy

Full autonomy is rare. It is characterised by systems that require no human intervention. They can begin, end and choose to continue their functions when they deem the circumstances require it. They can monitor their own surroundings and make independent decisions about how to respond to change. They can also seamlessly interact with other systems and devices as required.

Threats

Unmanned systems offer the opportunity to streamline processes and reduce the cognitive burden on users. But as they move further up the levels of autonomy the risks start to increase for critical infrastructure organisations, both as users, and as potential targets for disruption and attack.

How quickly they can find ways to identify and mitigate those risks dictates how rapidly the benefits can take effect.

New ground for safety

Unmanned systems represent unknown territory when it comes to safety.

Whilst we have centuries of experience training people to be safe, we have precious little when it comes to training advanced technology systems to do the same. As humans we know how bad weather affects us, we know how we will react when new challenges come our way. We know our limits. With unmanned systems we have to make a lot of assumptions, creating uncertainty and risk.

More channels for communication

In unmanned systems the role of people is scaled down but the role of communications is scaled up. Human interaction is replaced with communication channels. This increases the number of technologies that could be compromised either by failure or malicious attack.

Widely available, easily adapted

Over the past five years the availability of unmanned systems has increased dramatically. What was once prohibited by cost and complexity is now widely available as consumer gadgetry.

The most advanced devices remain out of reach to most individuals but the majority of the technology is now inexpensive. This makes it simpler to disrupt our critical infrastructure. You only need to look at the trouble caused at UK airports in 2018 by off-the-shelf drones to understand the scale of the issue. What makes this more acute is how easy it has become to modify many of these systems and adapt them for a variety of uses.

With such wide-ranging opportunities for innovation, the chances of critical infrastructure operators being out-innovated by malicious actors is high. It has become very difficult to predict what unmanned systems may be used for next.

Lack of regulation

Beneath all the risks from unmanned systems is the challenge that comes from a lack of clear regulation. As a relatively new area of technology the landscape is complex, and in a constant state of flux. The lack of defined regulation means loopholes and gaps can be exploited without clear consequences.

Examples of Unmanned threats in action

There has been a dramatic increase in the number of safety reports involving drones and aircraft in the US over the last few years according to the US Federal Aviation Administration. In December 2018 a drone collided with a Boeing 737 commercial aircraft as it approached its destination in Mexico from the USA. The nosecone of the aircraft was severely damaged but the aircraft landed normally and no one was injured. Whilst most nations prohibit drones from flying in areas reserved for airliners, the millions of small consumer devices purchased around the world cannot be tracked on radar, making it difficult for authorities to enforce that rule. In addition many users don't know the rules and therefore don't follow them.

Recommendations for risk mitigation

Deep analysis

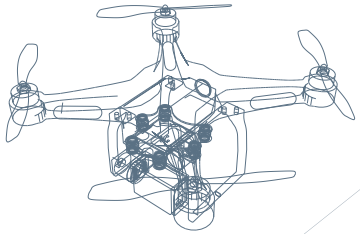
Because there is so much we don't yet know about these systems it is important not to make too many assumptions in the absence of sufficient data. A deep structured analysis of potential risks needs to be undertaken in each market. This means looking beyond the technology itself and into the second and third order issues that come from understanding how the technology impacts a wide variety of stakeholders and variables including users, businesses, supply chain, and other technologies.

Continuous modelling and live testing

As part of that structured analysis organisations seeking to either deploy unmanned systems, or reduce their risk to operational safety and security from them, need to model scenarios and test technologies. This will boost their understanding of how potential threats could develop and therefore be addressed. The speed of development in unmanned systems means this process needs to be continuous if organisations are to keep up with the pace of change and have any chance of being able to effectively mitigate those threats ongoing.

A layered approach to regulation

It goes without saying that organisations affected by unmanned systems should work closely with regulators to support the development of the rules that protect their environment. But due to the way in which these threats can penetrate deep into different stakeholder groups, they need to do more. They should consider a layered approach that involves working with these various communities to create a framework of regulation that takes into account the challenges across the whole of the ecosystem. This means understanding the concerns of the supply chain, industry bodies, employees, and local communities. Only by looking more broadly, and understanding the second and third order threats can critical infrastructure organisations ensure that the frameworks emerging from regulatory bodies can reduce real risks.




Ubiquitous Electronics

Ubiquitous Electronics. The amount of electronics in our world has been growing at an astounding rate for the last 20 years. Electronics underpins the Fourth Industrial Revolution; it enables our homes and workplaces to function efficiently and safely; and it has become the bedrock for many of our critical infrastructure services. While the importance of electronics as an enabling technology cannot be denied, it also represents one of the most obvious yet underestimated sources of vulnerabilities to those services. Building awareness of the risks and the mitigation strategies is essential for increasing their resilience.

The technology

Electronics, and in particular the semiconductor sector, has become the foundation technology of modern society. In everything from the modern office environment and children's toys to transport and power stations, electronics are fundamental to the way we live and work.

The growth of electronics has been remarkable. But what has been more astonishing is how the pace of that growth has accelerated as a result of greater consumer and corporate technology demand in recent years. That trajectory is expected to continue unabated, especially as the emergence of the Fourth Industrial Revolution drives the rapid development of new intelligent, adaptive, connected systems that rely on electronics to function.

Threats

Although electronics become more complex year on year, the vulnerabilities they present remain worryingly simple to exploit. At the same time, the threats themselves are difficult to identify, increasingly powerful, and much more accessible. Organisations continue to invest heavily in technology and systems that protect them from sophisticated cyberattacks and physical security incidents. Very few are placing the same emphasis on electromagnetic interference.

This is defined as the intentional malicious generation of electromagnetic energy to introduce noise or signals into electric and electronic systems, thus disrupting, confusing or damaging these systems for terrorist or criminal purposes. Such electromagnetic attacks can shut down any electronics component in seconds and cause serious disruption to the equipment or services where those components reside. They can also deny access to the radio spectrum on which many electronic devices rely for communication with other technologies. In environments where uptime is critical this has significant impact including economic loss, reputational damage, and personal safety.

It is essential that critical infrastructure organisations understand the relevance of this type of attack to the following systems so they can work out how to mitigate their impact, and plan appropriate recovery measures:

Internet of Things

The world is becoming ever more connected. As the price of wireless electronic components drops, and the cost of hard wired cabling (and associated installation) rises, wireless connectivity has become economically seductive in the cost-sensitive environments where critical infrastructure sits. But wireless-enablement adds additional electronic components that can be exploited by electromagnetic interference attacks.

IoT relies on the ability to transmit data from one device to others using the radio spectrum. When the components that enable this function are compromised, the data cannot be transmitted because the spectrum cannot be accessed. This is often referred to as spectrum denial. When critical systems are denied spectrum access, the ensuing disruption can have severe consequences.

Autonomous systems

Unmanned systems such as UAVs or autonomous cars are highly sophisticated connected computer systems augmented with a vast array of sensors to enable them to achieve a level of situational awareness. Using electromagnetic interference to disable, disrupt, or spoof any of their electronic components could render them useless or dangerous.

Peripheral systems

If disrupting wireless components represents the front door for electromagnetic threats then the peripheral systems that support our infrastructure could be considered the back door. Data centres are a good example. As infrastructure organisations have increased the use of connected electronics in their operations, their reliance on data centres to host, manage and secure their data has also grown. Those data centres see security as a priority and invest heavily in cyber security systems to prevent attacks. But they also use electronic systems to keep the data centres secure and running including sophisticated electronic physical access systems, cooling systems and generators for power.

These systems usually sit on the outside of a data centre's buildings, making them exposed to electromagnetic interference that could disrupt their ability to function.

Cyber security breaches can have a considerable impact on data security. Raising the temperature of the data centre by five degrees or cutting its power can shut down several critical organisations in minutes.

Power and accessibility

The technology required to create electromagnetic interference has been widely available for many years to anyone with the means and motive to acquire. Readily available online, radio frequency jammers are particularly prevalent. The power of these devices is increasing, giving them the potential to deliver an effect from greater distances. The rules and regulations around the purchase, ownership and usage of these devices lacks clarity and bite. This needs to be addressed before the threat of electromagnetic interference can decrease.

No evidence

What makes these attacks such a challenging threat is that they leave no physical trace. Unlike cyber or physical attacks there is no footprint and no indication that anything out of the ordinary has taken place other than the wreckage of the disruption or damage. It is likely that many more electromagnetic interference attacks have taken place than we realise but that most have been dismissed as a technical fault. Finding a way to quickly identify that such an attack is underway is a major but vital challenge critical infrastructure organisations need to address.

Examples of ubiquitous electronics threats in action

- Netherlands: an individual disrupted a local banks computer network because he was refused a loan
- Japan: two Yakuza criminals were caught using an electromagnetic interference generator on a gaming machine to trigger a false win
- St. Petersburg, Russia: a criminal used electromagnetic interference to disable a security system on a jewellery store, so that he could commit a robbery
- London: a city bank was the target of blackmail attempt whereby the use of electromagnetic interference was threatened against the bank's systems
- Moscow, Russia: a telecommunications centre was targeted by electromagnetic interference and was put out of commission for 24 hours denying service to 200,000 subscribers

Recommendations for risk mitigation

The most important change any critical infrastructure organisation can make to reduce their exposure to electromagnetic interference in a ubiquitous electronic environment is to shift their stance from security to resilience. Security is about building bigger walls and fences – both physical and digital to prevent an attack. It is expensive and does not always work as a long term solution because the speed of technology development means that security measures can quickly become outdated. Resilience is about acknowledging that an attack is inevitable but that it is the speed of effective recovery that matters most.

Resilience to electromagnetic interference is about ensuring that those services, which are critical to modern society, can get back up and running to an acceptable percentage of full capability, in the shortest time possible. Becoming resilient to this threat requires three things:

Becoming resilient to this threat requires three things:

Robust evidence

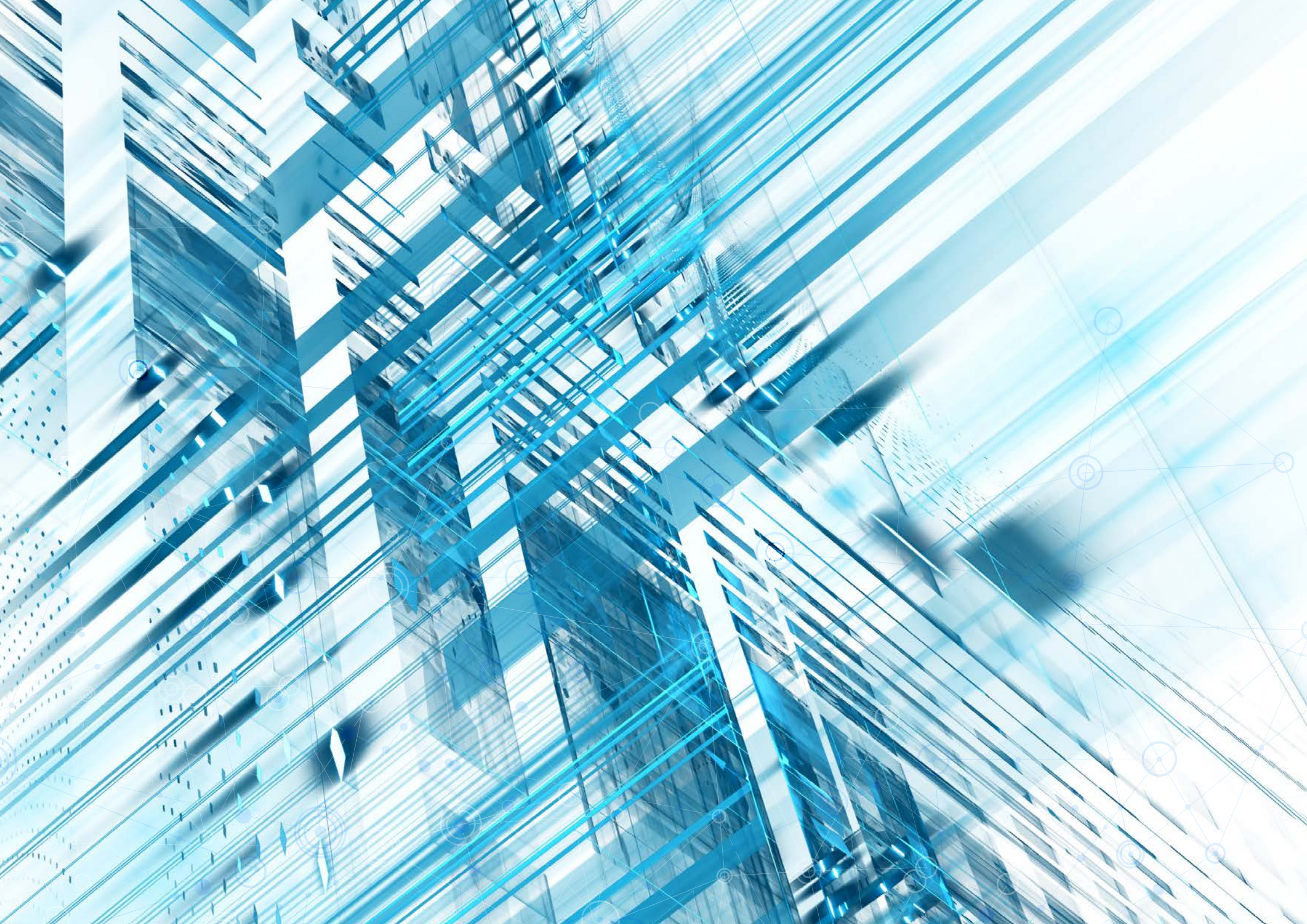
Emerging technology is presenting critical infrastructure with new opportunities to prove that electromagnetic disturbances have taken place. Understanding what has happened and what technologies have been affected enables organisations to quickly and accurately gather the evidence they need.

Horizon scanning

The ability to maintain constant awareness of the technology developments that have the potential to disrupt critical services. Knowing what is coming reduces the challenge of responding quickly to the unexpected.

Training and rehearsal

Ongoing and highly realistic training and rehearsal exercises around recovery scenarios are vital to achieving resilience. They ensure that organisations are well drilled on the steps to take when an electromagnetic interference attack takes place and reduce the chances of panic, confusion, or mistakes.



Recommendations

The recommendations for dealing with emerging threats from Fourth Industrial Revolution technologies can be distilled into four main categories: human-machine teaming; continuous monitoring and testing; training and education; and horizon scanning.

In closing, we summarise the actions we believe organisations operating within our critical infrastructure should take to bring them to life.

Human-machine Interaction?

Throughout history, new technology has been a driver of industrial adaptation and advantage. Whether moving from sail to steam, or the introduction of new manufacturing processes, the results have often been transformative. However, machines do not yet perform as well as a human brain. So realising the potential from emerging technologies within critical industries will depend on understanding the relative strengths of humans and machines, and how they best function in combination.

Developing the right blend of humans and machines to deploy inside our infrastructure is vital. Critical industries must determine how much they trust machines. As part of this, they need to better define the split of roles and responsibilities to achieve the fine balance of practical advantage and reduced risk.

This can only happen collaboratively and so the creation of an independent central forum for the establishment of how humans and machines work together would be a positive proactive step. Furthermore, the level of trust in machines will not remain static. It will flex as technology develops, confidence improves, and evidence builds. A central forum would therefore have an ongoing role to play to ensure that the balance of trust is adjusted according to current technologies, experiences, and applications in critical industries.

Continuous monitoring and testing

In many instances the Fourth Industrial Revolution takes us into uncharted territory. As we delve into unfamiliar experiences the most effective way to mitigate the risks outlined in this report is to continuously monitor new systems and new processes, and to rigorously test both their security and performance. This requires experience and independence. It will be important for organisations delivering our critical infrastructure to work with external specialists that are detached from their operation to ensure accurate and impartial findings.

The speed of technological development dictates that this process needs to be continuous if organisations are to keep up with the pace of change.

Training and education

Any change in technologies, processes, systems, or support represents a risk and a potential new threat if the people involved are not trained to deploy and use them safely and effectively. In highly critical industries, that training must be realistic to properly prepare appropriate mitigating strategies. Moving beyond traditional training exercises and into more advanced rehearsal techniques that blend live and simulated approaches is therefore recommended. Only by integrating these methods can organisations operating in critical environments offer truly accurate representations of the threats their people may have to address, and encourage the levels of resilience required.

Horizon scanning

The amount of technology change in the past five years has been unprecedented. What is truly astonishing is how the pace of that change has accelerated over the same period. The timeframe for technical development exponentially increases the risks involved while at the same time the amount of time organisations have to prepare for any new threats decreases. It is therefore essential that critical infrastructure organisations put in place a formal process for horizon scanning to maintain constant awareness of the technology developments that could impact their operations. Knowing what is coming makes it far easier to either move quickly to adopt and take advantage, or build resilience against potential consequences.

Conclusion

This report has highlighted the fantastic opportunities presented by the adoption of Forth Industrial Revolution related technologies and their very real threats to business resilience if appropriate design considerations are not incorporated. When you consider these opportunities collectively, the need for going beyond individual tactics, and instead implementing a holistic and more fundamental change in approach becomes apparent – one that delivers true resilience and is much more than tactical security solutions.

To deliver infrastructure resilience this demands proactive and holistic design, rather than purely reactive defensive measures. The complexity of these technologies and their inter-dependencies demands building infrastructure resilience into critical organisations through a clearer understanding of at the design stage of vulnerabilities and as they evolve during infrastructure operation. Using expertise that is able to span these different complex areas and independently assesses vulnerabilities it is possible to proactively reduce the impact of continually evolving threats and to reduce reactive crisis management.

Cody Technology Park
Ively Road, Farnborough
Hampshire, GU14 0LX
United Kingdom

+44 (0)1252 392000
prototypewarfare@QinetiQ.com
www.QinetiQ.com

QINETIQ