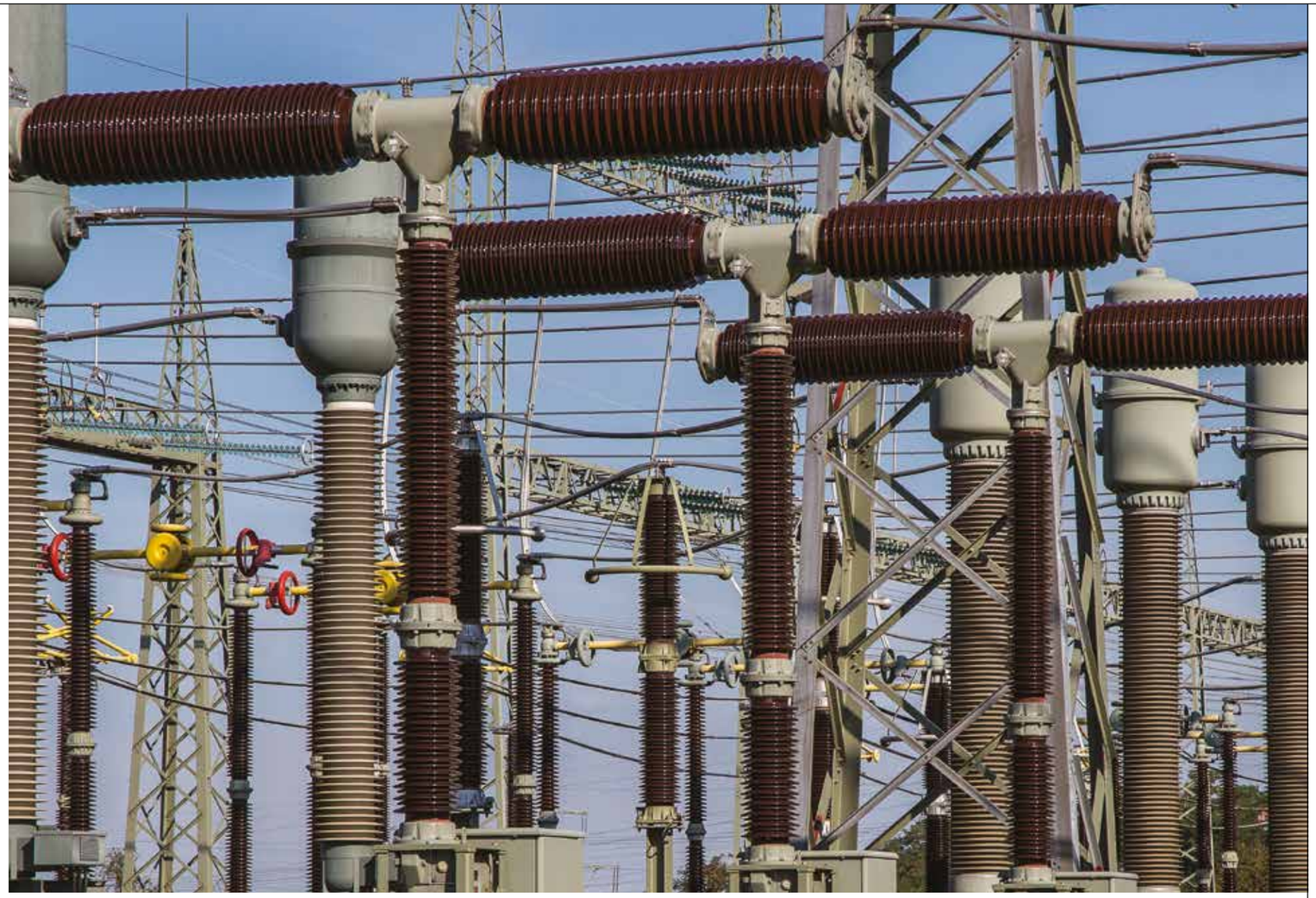
DETERRING THE THREAT

Patrick Kennedy *wonders how do we go about securing critical infrastructure as it embraces the digital age?*



The threat of an attack to power stations looms large for both the energy industry and governments

Until very recently, protecting critical national infrastructure was an entirely physical affair. Thick walls, sturdy fences and in some cases armed personnel were the key to protecting energy, transportation and water infrastructure from potential threats.

This status quo persisted for a surprisingly long time, even as almost every other aspect of our lives has become increasingly digitised. Most industries have fully embraced digital transformation in recent years, and the business world has become dependent on a highly complex web of interconnected technology. Our personal lives too are dominated by digital technology, which has become the de facto approach for everything from paying bills to tracking health.

DIGITAL TRANSFORMATION

Yet as the digital age has advanced, the industrial control systems that underlie our critical national infrastructure have remained largely isolated from the internet, while the security perimeter has been almost entirely physical. Finally though, the unstoppable impetus of digital transformation and its promise of efficiency and flexibility have overtaken the industrial world. Interconnected information and communication technologies that power the realms of business and commerce are rapidly converging with the operational technologies that control our critical infrastructure.

On balance, an interconnected infrastructure is a good thing on both a national and global scale. The combination of advanced computing and industrial automation will help to increase productivity and output. This approach also unlocks new possibilities around predictive and remote maintenance, helping to address issues before they can escalate into more costly problems that can lead to serious outages.

But as with all advances, the digital era brings a multitude of risks along with the benefits. Our infrastructure must now increasingly prepare for potentially dire threats that are far beyond the scope of security fences and armed guards to defend against.

Dealing with cyber attacks has become part of doing business in the digital age. It's rare for more than a couple of weeks to go by without reports of at least one serious security incident being suffered by a large organisation. In late July, a number of large blue-chip corporations in fields including manufacturing, pharmaceuticals, chemicals and air travel were hit by attacks from a state-backed Chinese group.

As companies have become more reliant on today's interlinked digital web, most have exposed themselves to an ever-increasing level of risk. Organisations managing critical national infrastructure are no exception, and the newly connected terrain can be used by threat actors to conduct reconnaissance, gain remote access and even mount serious attacks.

Fortunately, these incidents have so far been an order of magnitude rarer than the constant stream of attack reports we see from sectors such as finance and retail. There have only been a small number of cases around the world in the last few years. However, the repercussions of an attack on infrastructure are far greater than almost any other sector.

Whereas a breach suffered by a retail organisation will hit its bottom line and expose its customers to increase risk of fraud, a successful attack on critical infrastructure can have a much more tangible impact on a national scale – even potentially putting a number of lives at risk.

The watershed moment for cyber security in critical infrastructure came in 2015 with the first known successful attack to knock out a power grid. In December 2015, the information systems governing three energy distribution companies in Ukraine were hit with an attack that took down the grid.

> **74 PERCENT OF CITIZENS BELIEVE AN ATTACK ON UK INFRASTRUCTURE IS LIKELY IN THE FUTURE**

The attack was highly organised and complex, involving a multi-pronged approach that combined several different techniques. The opening move saw corporate networks being compromised with a powerful malware known as BlackEnergy, which was delivered via a spear-phishing email.

Once this had been established, the attackers seized control of the SCADA (Supervisory Control And Data Acquisition) systems to remotely turn off substations, as well as disabling IT infrastructure assets. Alongside this, another malware called KillDisk was used to destroy large amounts of files stored on workstations and servers, and finally a DDoS (Distributed Denial of Service) attack was used to disable a call centre and prevent consumers from receiving information about the blackout.

The attack left 225,000 citizens without access to power, with outages lasting between one and six hours depending on the area. Due to the on-going conflict between Ukraine and Russia at the time, the attack has been widely attributed to the Russian advanced persistent threat (APT) group dubbed Sandworm.

Ukraine was the victim of another serious attack on its power grid almost exactly a year later in December 2016. This second attack took out the power for more than a fifth of Kiev for close to an hour, but is believed to have been merely a test exercise from the perpetrators.

The attack used a different approach to the 2015 incident, this time revolving around a powerful malware called Industroyer, also known as Crashoverride. The malware was designed specifically to disrupt industrial control systems and contained a number of components that carry out different actions. A backdoor element was used to establish a remote connection, enabling attackers to deliver commands and execute attacks, with a secondary backdoor in place if the first is discovered. Four separate payload components then targeted particular industrial protocols, while a data wiper erased crucial registry keys and overwrote files, making it much harder to recover in the aftermath.

GROWING THREAT

While the Ukraine attacks are fortunately rather exceptional for now, the threat of a new incident looms large for both the energy industry and governments around the world.

Recent research, carried out jointly by the UK Infrastructure Transitions Research Consortium at the University of Oxford and the Centre for Risk Studies at Cambridge Judge Business School, looked to quantify the potential risk to the UK if a cyber attack was launched. Using the Ukrainian incidents as a base, researchers estimated that similar attacks on the UK could cost in excess of £111-million a day. It was concluded that even a limited incident could hit the power supplies of more than 1.5-million citizens.

A study by the Pew Research Center into public awareness and attitudes around cyber risks found that

in most cases citizens around the world believed an attack on their infrastructure was likely. US citizens were particularly pessimistic, with 83 percent saying that they thought it was likely public infrastructure would be damaged by a cyber attack in the future. The UK was only slightly more optimistic, with 74 percent believing an attack was likely.

One of the biggest challenges in cyber security is accounting for the unknown. While security personnel and detection tools can quickly adapt to account for newly discovered vulnerabilities,

INFRASTRUCTURE MUST PREPARE FOR THREATS THAT ARE FAR BEYOND FENCES AND GUARDS

malware and techniques, little can be done to prepare for previously unknown threats.

It is highly likely that many industrial systems have already been compromised by unknown malware, which is now lying in wait for instructions when the time is right. Earlier this year, Dan Coats, the US Director of National Intelligence, told Congress it was believed Moscow was staging cyber attack activity to disrupt civilian and military infrastructure in the event of a crisis.

Much as we have seen in the past with traditional weaponry, when cyber capabilities are monopolised by a small number of powerful nation states, it is possible to achieve a state of global deterrence. Overt hostility would result in counter attacks, so the states restrict their activity to small-scale incidents with a high degree of deniability.

However, unlike conventional warfare, serious cyber attacks can be orchestrated by non-state actors with comparatively few resources. Critical infrastructure presents an unappealing target for the average criminal motivated by financial gain, with many other industries offering greater rewards for less effort and risk. However, infrastructure is still potentially at risk from non-state actors such as terrorists, activists or those simply acting out of malice.

Perhaps the most significant challenge in securing the world's infrastructure is that it was never designed to be secured against these kinds of threats. Most systems were intended to be operated in highly secured environments, protected from interference by physical barriers like walls, gates and guards. This means devices often lack basic features such as authentication and encryption.

The challenge is exacerbated by the fragmented and opaque nature of the attack surface. Most of the world's critical infrastructure runs on a variety of old and obscure protocols, many of which are proprietary, making it much more difficult to gain a unified view of systems as a whole.

One of the most prominent solutions to this problem is the decision to back away from digitalisation. In July 2019 the US Government announced plans to revert critical systems to analogue and manual technology in order to isolate the grid's essential control systems. A press release on the passing of the Securing Energy Infrastructure Act (SEIA) stated that the intent was to ensure that aggressors would once again have to physically touch the equipment to disrupt or damage it.

UNDERSTANDING THE PROBLEM

However, I believe this approach of "going retro" is counterproductive and could harm innovation. The critical national infrastructure of America and other nations around the world is not vulnerable because it's digital, but because the threat actors understand the landscape better than those tasked with defending it.

We are now faced with the unusual situation of industry, rather than government, being on the front lines of potential conflict. With a large amount of critical national infrastructure bring governed by the private sector, it is largely up to individual organisations to equip themselves with the visibility into their own networks and the ability to identify and defend against threats. The industry's focus has suddenly shifted from reliability to reliance – the ability to continue running in the face of attack.

The priority should instead be to close the visibility gap that currently allows aggressors to implement elaborate attack plans without being detected. The industry must work with the government to transform today's disjointed and opaque attack surface into a transparent defence architecture that enables defenders to reliably identify threats ●

Patrick Kennedy, is a Global Security Evangelist with Claroty. With over 20 years of security industry experience at market leaders such as Symantec and Webroot, he is a frequent speaker and author on the topics of operational technology, threat intelligence and advanced anti-malware protection at several industry events.

In December 2016 an attack in Ukraine left 225,000 citizens without power

Picture credit: Getty