KEEPING THE LIGHTS ON

Ilan Barda *reveals the cyber threat being posed to critical national infrastructure across the globe*

Last year, Ciaran Martin, the head of the UK's National Cyber Security Centre, said the country had been fortunate to avoid a category one attack, broadly defined as one that might cripple infrastructure such as energy supplies and the financial services sector. The UK's critical national infrastructure (CNI) is a natural target for such an attack because of its importance to daily life and the economy.

However, securing CNI is made more complex due to the highly proprietary Supervisory Control and Data Acquisition (SCADA) systems used in CNI applications such as energy and water generation and distribution. Many of these systems were designed with closed networks in mind and paid more consideration to physical protection than cyber security. On the other side, the cyber security systems designed for general purpose enterprise use are often ill equipped to deal with targeted attacks against the specialised protocols and non-standard interfaces used by the dozen or so vendors of SCADA and related systems commonly used within CNI.

> FINDING CYBER EXPERTS WITH KNOWLEDGE OF SCADA AND CNI HAS BEEN A MAJOR DIFFICULTY

SCADA networks are built up of multiple discreet elements. The 'brains' of the system are supervisory computers that gather data on processes and send control commands to field-connected devices such as Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs). RTUs are akin to fingers and hands, offering sensors to carry out remote functions such as reporting on temperature, current or flow with the ability to open and shut circuits and valves as needed. In some instances, PLCs with their embedded software can act as a combination of all three functions; offering a more economical and autonomous option.

Underpinning all three is the infrastructure connecting the supervisory computer to the RTUs and PLCs, which normally has a high degree of resiliency to allow multiple pathways between critical systems. Every SCADA system also has a human to machine interface for operators to issue commands, examine alerts and generate reports.

Unlike information technology systems used in corporate environments, most SCADA networks communicate using real-time operating systems that are designed for reliability and to provide more consistent performance metrics. The networks also rely on highly specialist and often vendor-specific propriety protocols for flows of data and commands.

From the sixties to the nineties, the use of SCADA has grown as either a refit to existing technologies or as a prerequisite for new build projects. The technology alone is worth around $18 billion a year, but the infrastructure it is used to control has an economic value measured in trillions of dollars. Today, the technology vendors active in the space have coalesced into around a dozen global players. Many of these have invested heavily in advancing the technology with new features such as information modelling to allow data from both traditional sources (PLCs, RTUs) and non-traditional sources (sensors, databases, networked devices) to be consolidated for visualisation, analysis, and archiving.

PHYSICAL THREATS

On the security side, CNI and the inherent SCADA systems at their heart had traditionally protected against physical threats. High fences, alarms, guards and cameras were often 95 percent of the typical security budget. As closed networks with limited accessibility to only a few highly skilled technical staff, the physical threat was deemed as the most likely attack method.

However, the turn of the millennium offered a wake-up call when a cyber attack against Iran's nuclear facilities in 2010 used Stuxnet, a custom created computer worm, to infiltrate SCADA-based computer systems controlling centrifuges used in the enrichment of uranium. The Iranians had effectively sealed off the facility from the wider area network, so the attackers instead targeted the USB sticks of contractors working in the plant to get past the firewall.

In 2012, Telvent, an information technology and industrial automation company specialising in SCADA, GIS and related IT systems for the energy sector, was attacked by hackers looking for sensitive information on its OASyS SCADA, a software application used by global energy companies for creating smart grids.

In 2015, the Ukraine power grid was the victim of a cyber attack that compromised information systems of three energy distribution companies shutting down 30 substations and temporarily disrupting the electricity supply to millions of homes.

In between these incidents that garnered widespread reporting, many experts estimate there were hundreds of smaller scale attacks that weren't reported as regulators often do not require full disclosure unless there is an external impact; and in some cases, CNI operators keep issues quiet for fear of sanction or damage to reputation.

The biggest issue that CNI faces is that far too much security reliance is based on architectural design of facilities to shield systems away from cyber security risks. These closed and uni-directional systems do not offer a comprehensive strategy from a cyber security standpoint and fail to consider that SCADA networks are increasingly connected to other operational systems.

WORKING CULTURE

Another issue is the working culture within many CNI organisations that separates operational, technology, and executive teams, which makes it much harder to develop and enact comprehensive cyber security programmes. Finding, training and retaining cyber security experts with knowledge of SCADA and CNI environments has also proven a major issue.

The last issue is the lack of security technologies designed specifically for CNI environments. Unlike a normal IT infrastructure, SCADA uses specialist hardware and software from a small set of vendors. This makes conventional security systems much less effective. An example of this issue is the 2018 attack on Saudi Armaco, the world's largest oil producer, where a specially crafted malware called Triton was used to attack a safety system known as Triconex, manufactured by the German firm Schneider Electric, to control emergency shutdown functions. Triton disrupted an unspecified industrial process, which prompted Aramco to investigate and discover the malware before it could do more harm.

It is believed that the Triton hackers, possibly state sponsored, had built the malware with a specific goal based on deep knowledge of Triconex. The attack ultimately failed, but the malware still managed to reach its target – avoiding layers of security controls including anti-malware software that would have been unable to detect its signature as the software was uniquely created for a specific target.

Regulators of CNI along with the industry at large are reacting to these threats in a concerted effort. In North America and across several nations where US energy and utility companies have joint ventures with local operators, organisations have been tasked with meeting standards from the North American Electric Reliability Corp. (NERC) and mandated by the Federal Energy Regulation Commission (FERC).

The NERC Critical Infrastructure Protection (CIP) standards set around 40 rules and almost 100 sub-requirements that mandate provisions to protect CNI from cyber threats. Within the EU, the directive on security of network and information systems (NIS Directive) focuses on the availability of crucial network and information systems in order to protect the union's

It's the unseen cyber challenge that holds the biggest threat to nuclear power stations

Picture credit: Getty

critical infrastructure and thereby ensure service continuity. NIS has 14 core elements and mandates that compliance with the NIS Regulations will be monitored through audits conducted by designated competent authorities within each nation with fines for non-compliance.

In terms of staffing and training, many CNIs are increasing investment in courses; an area that is mandated by both NERC and NIS directive, with more staff attending industry recognised courses from the SANS Institute and BSI.

On the technology front, many within CNI are deploying new cyber security tools designed specifically for SCADA environments. Unlike generic InfoSec platforms, these systems use dedicated passive probes that sit on the communication infrastructure within each facility to analyse the proprietary data flows generated by supervisory computers, RTUs and PLCs.

TOO MUCH RELIANCE IS PUT ON ARCHITECTURAL DESIGN TO SHIELD FROM CYBER RISKS

Alongside a signature database of specific vulnerabilities and threats relevant to a SCADA environment, these systems use optimised anomaly detection and measurement of operational behaviour to detect attacks. This is based on a specific understanding of the operating environment and the different proprietary data flow and control mechanisms employed by the main SCADA technology suppliers.

Another change is the use of managed security services designed specifically for SCADA environments. Although still a relatively new concept, the approach allows specialist Managed Security Service Providers (MSSP) to run specialist tools with a shared Security Operation Centre (SOC) that can monitor multiple end-customers. This approach reduces the cost and complexity of internal staffing and provides an expert team on hand for incident response.

Some early adopters of this approach are municipal water utilities in Europe with remotely operated facilities that are required by a national regulator to deploy cyber security tools to monitor their SCADA network. These municipal facilities lack the resources to employ teams of trained Infosec staff and so instead subscribe to a specialist CNI MSSP. In early 2018, one of these water utilities was infected by a crypto mining malware and the breach was detected by the MSSP SOC, which then alerted the customer. The analysis of the case showed that an IT firewall was not properly configured so the service was extended to also control the IT firewall in order to update the rules as needed.

According to the UK Government's *Cyber Security of the UK's Critical National Infrastructure* report prepared by the Joint Committee on the National Security Strategy: "The cyber threat to the UK's CNI is growing. It is also evolving: hostile states are becoming more aggressive in their behaviour, with some states – especially Russia – starting to explore ways of disrupting CNI, in addition to conducting espionage and theft of intellectual property… While states still represent the most acute and direct cyber threat, non-state actors, such as organised crime groups, are developing increasingly sophisticated capabilities."

The remedy must include a combination of education, regulatory oversight and willingness on the part of private operators to adopt new processes and technologies designed to meet the real-world challenges posed by cyber attackers. Looking to the future, the next decade will undoubtedly witness a cyber attack against CNI that inflicts a significant level of damage to a nation state that will force more draconian response from governments. For the CNI industry, prevention is the key and that starts with recognising the problem and examining every option to find a solution ●

Ilan Barda, founder of Radiflow is a Security and Telecom executive with 20 years of experience in the industry. He has deep experience in developing secure communication equipment from his service in the Information Security division of the IDF.

Much of the UK's CNI was built with physical rather than cyber security in mind

Hinkley Point B power station
You are entering a nuclear licensed site
Nuclear Installations Act 1965 (as amended)

Picture credit: Getty