ANALYSIS

# Responding to Cyber Security Threats in Critical Infrastructures — Challenges for Australia and Europe

**Prof Helge Janicke, Director of Research Cyber Security Cooperative Research Centre and Edith Cowan University**

November 2019

## About the Author

Prof. Helge Janicke is the Research Director of the Cyber Security Cooperative Research Centre, Australia. He is affiliated with Edith Cowan University and holds a visiting Professorship in Cyber Security at De Montfort University. Prof. Janicke's research interests are in the area of cyber security, in particular with applications in critical infrastructures using cyber-physical systems, SCADA and Industrial Control Systems. Prof. Janicke's current research investigates the application of Agile Techniques to Cyber Incident Response in Critical Infrastructure, Managing Human Errors that lead to Cyber Incidents, and research on Cyberwarfare & Cyberpeacekeeping. Prof. Janicke established DMU's Cyber Technology Institute and its Airbus Centre of Excellence in SCADA Cyber Security and Forensics Research. He has been the Head of School of Computer Science at De Montfort University, before taking up his current position as Research Director for the Cyber Security CRC. Prof. Janicke founded the International Symposium on Industrial Control System Cyber Security Research (ICS-CSR) and contributed over 100 peer reviewed articles and conference papers to the field that resulted from his collaborative research with industry partners such as Airbus, BT, Deloitte, Rolls-Royce, QinetiQ, and General-Dynamics.

**Critical infrastructures are organisational and physical infrastructures essential to our nations' economy and the well-being of its citizens. A disruption or degradation of these infrastructures directly impacts on key responsibilities of the state to provide essential services to its citizens.**

Whilst definitions as to what constitutes essential services vary across nations, they all share a common understanding as to the importance of a mature approach to their cyber security.

The European Union (EU) identifies Energy, Transport, Banking, Financial Market Infrastructures, Health, Water, and Digital Infrastructures as critical in its Network and Information Systems (NIS) directive [1]. This directive came into force in May 2018, but leaves the concrete implementation and identification of Operators of Essential Services (OES) to its member states, whilst providing guidance and advice on the assessment methodologies to create consistency in approach across the EU. The NIS thus balances the need for a consistent and coordinated approach across its member states with the individual member states operational realities and their local governance structures with the overarching aim to establish a coordinated approach to the response to major cyber security incidents. Similarly, the Australian Government recognises 8 critical infrastructures: banking & finance, government, communications, energy, food & grocery, health, transport, and water in its Critical Infrastructure Resilience Strategy[2]. It specifically identifies operators of critical infrastructure assets in its Cyber Security of Critical Infrastructure Act 2018[3], in particular regulating reporting requirements and powers with respect to critical electricity, gas, ports, water assets. In its draft Cyber Security Strategy 2020[4] Australia is consulting on the adoption of additional measures similar to the European NIS directive.

The impacts of a degradation or disruption of essential services on a nation's economy can be significant, and are difficult to quantify. Work by Schmidthaler and Reichl [5] provides computer based models to estimate the economic impact of power outages across the EU using a power outage across Italy as an example. They estimate the economic impact of this 3-16h (depending on region) outage on Sunday the 28th February 2003 across Agriculture, Manufacturing, Services and Households to have been €1182 million. Given the significant losses, understanding the impact and the potential for cascade failures due to long term disruptions is important to prepare for cyber incidents[6].

Whilst disruptions of essential services due to cyber attacks remain comparatively rare in comparison to functional failures or natural disasters, they are a real and significant risk. Recent examples of sophisticated cyber incidents are the 2015 BlackEnergy attack[7,8] on the Ukrainian energy sector, disrupting power supply to over 200,000 households. Whilst the earlier 2010 Stuxnet attack[9] on an Iranian nuclear enrichment plant already alerted to the potential of cyber warfare[10] and the vulnerabilities of Industrial Control System components to cyber attacks. The BlackEnergy incident highlighted the increasing connectivity between corporate Information Technology (IT) systems and frequently vulnerable Operational Technology (OT) that controls the physical infrastructure. It also demonstrated the increasing sophistication and coordination of cyberattacks to impact on critical infrastructures.

Not all attacks are specifically targeting OT used to deliver essential services. In 2017 the WannaCry ransomware[11] impacted significantly the operations of the UK's National Health Service, until systems could be restored. WannaCry clearly demonstrated the vulnerabilities and direct impact on public services, especially if these are already operating under stress. Whilst the response and the recovery from backups was swift, it exposed significant risks associated with the maintenance and secure use of large corporate IT networks. This incident also affected thinking in the OT space - where a recovery from a large scale ransomware infection would in many infrastructures be harder, and more time-consuming. That this is a persistent threat to many organisations is clear: the global shipping company Maersk[12] suffered significantly from the NotPetya[13] ransomware in 2017, and is still in legal proceedings with its insurers over the incident.

These examples illustrate some of the cyber security risks that industries face today. Over the last decades many industries benefited from increased IT/OT integration and automation, without sufficiently addressing the increasing cyber security risks, to the extent that for many of these industries a fall-back to more manual processes is either incurring large losses or is simply infeasible. These risks are balanced with the cost of implementing better security, and investment in upgrading the OT infrastructure to offer better security. For industries that operate critical infrastructures the situation is more complex, as regulators and national interests are exerting influence on the management of cyber security risks.

A complicating issue when protecting essential services are the intertwined responsibilities for the protection of critical infrastructures. At a macro level these typically involve a variety of stakeholders that influence the development and operation of these services. Whilst the state has regulatory oversight of critical infrastructures, the delivery of the service is typically the responsibility of a private corporation. To increase competition and disrupt monopolies, governments frequently favour a separation of the provision of a service from the underpinning distribution networks with complex interplays between these systems. An example of this is Network Rail, which owns the majority of the UKs rail infrastructure through its "devolved routes" business model but works with a variety of train operators to deliver a transport service to the UK's population and businesses. Similar examples exist in other essential services. Combatting any disruption due to a cyber attack hence requires significant coordination between a number of (potentially competing) organisations that together make up the service.

At a micro-level, there is often a disconnect between the IT focused Cyber Security expertise and the coordination with other stakeholders in the business and the engineers on the shop-floor, making a coordinated and effective response to attacks on OT difficult to achieve. Whilst most nation's security strategies for critical infrastructures emphasise the need for Operators of Essential Services to coordinate and

> This pace of technology adoption makes protecting large scale infrastructures a herculean task. Many installations have been operational for 20 years or more, and evolved over time as they needed to integrate with newer technologies in an increasingly digital world.

collectively prepare for cyber attacks, the adoption of cyber security controls in critical infrastructures is clearly outpaced by the development of IT/OT connectivity and integration of new technologies such as 5G and modern Industrial Internet of Things (IIoT) infrastructures.

This pace of technology adoption makes protecting large scale infrastructures a herculean task. Many installations have been operational for 20 years or more, and evolved over time as they needed to integrate with newer technologies in an increasingly digital world. These legacy installations make it difficult to overcome security vulnerabilities that are often inherent in their architecture and the details of their implementation. Overhauling this infrastructure en-mass can be very costly. It is also typically is not planned in the original business case and thus negatively affects the return on investment and hence profits of the organisations providing the service. Updating infrastructure brings further risks and disruption as large scale tests are often infeasible and whole-sale technology change has a history of overrunning in time/cost and causing severe disruption to services.

Given these difficulties, it is clear that we need to better understand these complex systems[14] and equip organisations that are contributing to their operation with the capability and capacity to manage cyber attacks. It also raises the question how we quantify cyber security risks as part of business decision making in this sector – what effect has the fast-paced evolution of IT on the traditionally longer life-times of OT infrastructure. The IT world is ahead in its maturity to deal with cyber security threats, regular patching regimes, secure by default device configurations, strong authentication and encryption, firewalls, DMZ, Intrusion Detection systems and the swift recovery from backups (in the case of Ransomware) are all part and parcel of any modern IT heavy organisation.

In the OT sector the ability to deploy these mechanisms is far more limited, as legacy systems cannot be easily replaced without (expensive) re-certification of safety cases; for similar reasons patching is often not feasible. The introduction of tried and tested IT security controls bears dangers[15] as they can negatively affect the functioning of the system especially when additional network latencies are critical and can jeopardize the safe operation of the system[16], e.g. in energy distribution networks. These additional challenges for securing OT infrastructure are however not only technical in nature, there still is a lack of awareness and understanding in how to architect secure OT infrastructures with many large organisations relying on a small number of skilled individuals. The majority of reported cyber attacks on critical infrastructures reached the OT infrastructure through cyber security breaches of corporate IT networks

– whilst this should not be a reason to be complacent about OT security it shows that even the more mature IT protections were the first to fail, typically through simple human errors[17].

For future technologies, underpinning our increasingly smart infrastructures and smart cities, Artificial Intelligence (AI) techniques and scalable Big-Data analytics[18] will undoubtedly play a role in helping to overcome some of these issues. However, they are not a panacea for all our critical infrastructure cyber security ills. AI technologies can assist to manage the large amounts of sensor data and help in the identification of system anomalies[19] as well as improving the immediate response to cyber incidents through automation. However, it is important to recognise that cyber security is an arms-race and many of the tools that help us defend our systems equally can be used to subvert them. Data-Analytics in the form of open source intelligence and automation are already tools of the trade in sophisticated Advanced Persistent Threats (APTs) and aid in the targeting and execution of cyber-attacks. The idea that an AI that is deployed to protect a system can be subverted and used sparked a whole area of AI research called adversarial machine learning[20]. It is clear that technological innovation in newer, better cyber security tools is part of the solution, but it clearly alone cannot rise up to the challenge.

Securing the critical infrastructures that underpin our daily lives and well-being requires a coordinated approach and a long-term vision and strategy to provide direction and support to providers of essential services such as the National Cyber Security strategies of many nations in the industrialised world. Their implementation must challenge current organisational structures, employee behaviours, and at times business models that prioritise efficiency savings and productivity increases over the prudent management of critical cyber security risks. Many of the cyber security challenges are not rooted in technology but its effective use and the organisational structures that surround it. This means that education and awareness across all walks of life and professions that develop, operate and indeed use our critical infrastructures is an essential tool in combatting cyber attacks in our increasingly digitised world.

## Endnotes

**1** European Commission, “The Directive on security of network and information systems (NIS Directive) | Digital Single Market,” Eur. Comm., 2016.

**2** Australian-Government, “Critical Infrastructure Resilience Strategy: PLAN,” 2015.

**3** Australian-Government, “Cyber Security of Critical Infrastructure Act 2018,” 2018.

**4** Australian-Government, “Australia’s 2020 Cyber Security Strategy - A call for views,” 2019.

**5** M. Schmidthaler and J. Reichl, “Assessing the socio-economic effects of power outages ad hoc,” Comput. Sci. - Res. Dev., 2016.

**6** G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou, G. Lykou, and D. Gritzalis, “Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures,” Int. J. Crit. Infrastruct. Prot., 2016.

**7** R. Khan, P. Maynard, K. McLaughlin, D. Laverty, and S. Sezer, “Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid,” 2016.

**8** Department for Homeland Security, “Cyber-Attack Against Ukrainian Critical Infrastructure | ICS-CERT,” ICS-CERT, 2016. .

**9** R. Langner, “Stuxnet: Dissecting a cyberwarfare weapon,” IEEE Secur. Priv., 2011.

**10** M. Robinson, K. Jones, and H. Janicke, “Cyber warfare: Issues and challenges,” Comput. Secur., vol. 49, 2015.

**11** National Audit Office, “Investigation: WannaCry cyber attack and the NHS - National Audit Office (NAO),” National Audit Office, 2017. .

**12** L. Matthews, “NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million,” Forbes, 2017.

**13** S. Mansfield-Devine, “Ransomware: the most popular form of attack,” Comput. Fraud Secur., 2017.

**14** C. Islam, M. A. Babar, and S. Nepal, “A multi-vocal review of security orchestration,” ACM Computing Surveys. 2019.

**15** A. Cook, H. Janicke, L. Maglaras, and R. Smith, “An assessment of the application of IT security mechanisms to industrial control systems,” Int. J. Internet Technol. Secur. Trans., vol. 7, no. 2, 2017.

**16** D. Hunter, J. Parry, K. Radke, and C. Fidge, “Authenticated encryption for time-sensitive critical infrastructure,” in ACM International Conference Proceeding Series, 2017.

**17** M. Evans, Y. He, L. Maglaras, and H. Janicke, “HEART-IS: A novel technique for evaluating human error-related information security incidents,” Comput. Secur., vol. 80, 2019.

**18** E. Bertino, S. Nepal, and R. Ranjan, “Building Sensor-Based Big Data Cyberinfrastructures,” IEEE Cloud Comput., 2015.

**19** R. Luh, G. Schramm, M. Wagner, H. Janicke, and S. Schrittwieser, “SEQUIN: a grammar inference framework for analyzing malicious system behavior,” J. Comput. Virol. Hacking Tech., vol. 14, no. 4, 2018.

**20** D. L. Marino, C. S. Wickramasinghe, and M. Manic, “An adversarial approach for explainable AI in intrusion detection systems,” in Proceedings: IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, 2018.

### Copyright

### Editor

Katja Theodorakis

### Publisher

Konrad Adenauer Stiftung (Australia) Limited
Regional Programme Australia and the Pacific

11/3 Sydney Avenue
Barton, ACT 2600
Australia

Tel: +61 2 6154 9322

www.kas.de/australia

### Disclaimer

The opinions expressed in this publication rests exclusively with the authors and their interpretations do not necessarily reflect the views or the policy of the Konrad Adenauer Stiftung.

### Design, Layout and Typeset

Swell Design Group

### Paper

100%
FSC
www.fsc.org
RECYCLED
Paper made from
recycled material
FSC® C102086

ecoStar+ is an environmentally responsible paper. The fibre source is FSC Recycled certified. ecoStar+ is manufactured from 100% post consumer recycled paper in a process chlorine free environment under the ISO 14001 environmental management system.