**Institution: University of Wolverhampton**

**Unit of Assessment: 11 Computer Science and Informatics**

**Title of case study: Protecting critical national infrastructure through innovations in cybersecurity**

**Period when the underpinning research was undertaken: 2016 – 2020**

**Details of staff conducting the underpinning research from the submitting unit:**

| **Name(s):** | **Role(s) (e.g. job title):** | **Period(s) employed by submitting HEI:** |
|---|---|---|
| Professor Amar Aggoun | Professor of Visual Computing | 2016 - Present |
| Professor Keith Burnham | Professor of Industrial Control Systems | 2016 - Present |
| Professor Prashant Pillai | Professor of Cybersecurity | 2018 - Present |
| Dr Haider Al-Khateeb | Reader in Cybersecurity | 2018 - Present |
| Dr Gregory Epiphaniou | Reader in Cybersecurity | 2018 - 2020 |
| Mirko Bottarelli | Lecturer in Cybersecurity | 2019 - Present |
| Dr Herbert Daly | Senior Lecturer in Computer Science | 2018 - Present |

**Period when the claimed impact occurred: 2018 - 2020**

**Is this case study continued from a case study submitted in 2014? N**

## 1. Summary of the impact

The cyber research team at the University of Wolverhampton worked on underpinning technologies to support cyber resilience for complex systems in Critical National Infrastructure (CNI). This has laid the foundation for the business case to establish a new GBP9,000,000 centre; the Midlands Centre for Cybersecurity in Hereford. The centre stimulated a base of Small & Medium-Sized Enterprises (SMEs) engaged in cybersecurity solutions. Underpinning research has also been utilised to train practitioners from 25 local SMEs through a unique Business Assistance Programme in the UK. Cydon Ltd, a new viable university spin-off company, was created from the research IP and the company fills a need for effective and secure data sharing across business units. Additionally, the research findings have been utilised in outreach activities to engage over 2,000 professionals through a series of over 30 specialist workshops.

## 2. Underpinning research

Critical National Infrastructure (CNI) such as power networks, transport systems and NHS are central to the ability of our modern society to function. A major attack on any of these would have an enormous societal and business impact. The Wolverhampton Cyber Research Institute (WCRI), established in 2017, brings together academics from the School of Mathematics and Computer Science and builds on the established strength of its members in the areas of network and communication security, artificial intelligence, big data, and cyber-physical systems. Based on the experience and expertise within the group, the overarching focus for the cybersecurity research pillar has been set as: “Security for Critical National Infrastructure”. Within this remit, our research produced the following findings [F], which underpin complex systems for CNI.

F1. Improved security for M2M wireless communications

Part of our current research activities is formalised around securing Vehicle Ad-hoc Network (VANET) communications for connected cars with a focus on crypto-key generation. Aimed at producing highly random and symmetric cryptographic keys, results indicate a significant improvement in bit mismatch rate and key generation rate in comparison to sample indexing techniques. Secure and more efficient key generation is inherently important for CC and Social Internet of Things networks, including in adversarial settings (e.g., battlefields) [R1]. The unification of the shared secret key must also adhere to error correction principles and valid processes around privacy enhancement techniques. Therefore, a novel non-interactive zero-knowledge (NIZKP) authentication protocol was proposed [R2]. It enables symmetric operation between peers with confidentiality assurance by minimising information exchange for the method of correcting bit mismatch between transceivers. Laboratory simulation indicates empirical evidence for the suitability of our method for authentication purposes in resource-constrained IoT environments.

F2. Cyber resilience through proactive cyber threat detection

With an emphasis on automation and proactive measures to mitigate cyber threats, we introduced proactive anomaly detection to a use-case of physical and cyber hijacking affecting connected cars (CC) to improve cyber-resilience [R3]. We deploy a Bayesian estimation technique to predict future states and cyber-threats and minimise the reaction time window when encountering anomalies using real-time GPS data in CC. A quantitative data research methodology was selected underpinned by location data to facilitate experiments on mathematical modelling to correlate routes.

F3. Intelligent decentralised data management platform for supply-chain security

The benefits of collaboration across the supply chain (SC) are well-recognised, but the effective management of such collaboration remains a challenge. Effective use of data can create £66 billion of new business and innovation opportunities in the UK, yet most companies surveyed estimating that they are analysing just 12% of their data (https://www.rand.org/pubs/research_reports/RR1284.html). Additionally, 75% of companies are concerned about security across the supply chain. The inability to adequately control data flows within the SC can impose significant security risks that can manifest an adverse impact on data restoration processes and critical business operations. This research [R6] addressed the problem with a patented [R5] dedicated data management platform based on a patented algorithm that utilises smart ledgers for electronically regulating data sharing within a supply-chain. The technology enables quick and immutable search, regulates the creation and processing of data across different organisational units, and provides authorised and faster access to secure distributed data.

F4. Orthogonal Defence-in-depth framework for Industrial Control Systems

Industrial Control Systems are responsible for the automation of different processes and the overall control of systems that include highly sensitive potential targets such as nuclear facilities, energy-distribution, water-supply, and mass-transit systems. Given the increased complexity and rapid evolvement of their threat landscape, and the fact that these systems form part of the Critical National Infrastructure (CNI), makes them an emerging domain of conflict, terrorist attacks, and a playground for cyber exploitation. Our work seeks to articulate a framework where multiple functional and assurance controls are introduced at each layer of Industrial Control System architectural designs to further enhance security while maintaining critical real-time transfer of command and control traffic [R4].

## 3. References to the research

All the research papers have been published following a rigorous peer-reviewed process. Research questions were investigated empirically and contributed to the knowledge base. Content from each of the 6 papers has been utilised to generate funding and deliver impact on commerce, practitioners, delivery of professional services, and public awareness. R5 and R6 have been underpinned by Innovate UK grants (see below).

R1. Epiphaniou, G., Karadimas. P., Ismail, D.K.B., Al-Khateeb, H.M., Dehghantanha, A. & Choo, K.K.R. (2018). Non-reciprocity compensation combined with turbo codes for secret key generation in vehicular ad hoc social IoT networks, *IEEE Internet of Things Journal*, 5(4), 2496 – 2505. https://www.doi.org/10.1109/JIOT.2017.2764384.

R2. Walshe, M., Epiphaniou, G., Al-Khateeb, H.M., Hammoudeh, M., Katos, V. & Dehghantanha, A. (2019). Non-interactive zero knowledge proofs for the authentication of IoT

devices in reduced connectivity environments. *Ad Hoc Networks*, 95, 101988. https://www.doi.org/10.1016/j.adhoc.2019.101988. (REF 2 Output).

R3. Al-Khateeb, H.M., Epiphaniou, G., Reviczky, A., Karadimas, P. & Heidari, H. (2018). Proactive threat detection for connected cars using recursive Bayesian estimation. *IEEE Sensors Journal*, 18(12), 4822 - 4831. https://www.doi.org/10.1109/JSEN.2017.2782751. (REF 2 Output).

R4. Mackintosh, M., Epiphaniou, G., Al-Khateeb, H.M., Burnham, K., Pillai, P. & Hammoudeh, M. (2019). Preliminaries of Orthogonal Layered Defence using Functional and Assurance Controls in Industrial Control Systems. *Journal of Sensor and Actuator Networks*, 8(1), 2224-2708. https://www.doi.org/10.3390/jsan8010014.

R5. Epiphaniou, G., Pillai, P., & Aggoun, A. (2020). Distributed ledger system. GB. Patent GB2576160A. Available: https://www.ipo.gov.uk/p-ipsum/Case/PublicationNumber/GB2576160.

R6. Epiphaniou, G., Pillai, P., Bottarelli, M., Al-Khateeb, H.M., Hammoudeh, M. & Maple, C. (2020). Electronic Regulation of Data Sharing and Processing Using Smart Ledger Technologies for Supply-Chain Security. *IEEE Transactions on Engineering Management*, 67(4), 1059-1073. https://www.doi.org/10.1109/TEM.2020.2965991. (REF 2 Output).

Underpinning Grants
Epiphaniou, G. & Pillai, P. Cydon: An intelligent decentralised data management platform. Innovate UK. GBP95,551. 2018 – 2019. Underpins R5 & R6

Epiphaniou, G. & Pillai, P. Violent and Sexual Offenders Online Monitoring System(s) Using GDPR Compliant Private Blockchain. Innovate UK. GBP15,889. 2018. Underpins R5 & R6

Epiphaniou, G. & Pillai, P. A GDPR compliant Private Permissioned Blockchain for Secure Distributed Data Storage and Processing. Innovate UK. GBP15,970. 2018. Underpins R5 & R6

## 4. Details of the impact

Our research impacted on commerce and the economy including research-informed training to enhanced practitioner's performance and the delivery of professional services.

I1. Impacts on commerce and the economy
Research on innovative cyber solutions [F1-4] has laid the foundation for the business case of a new Midlands Centre for Cybersecurity in Hereford, created a new university spin-off company and established the viability of a new product for supply-chain security.

The team's research on innovative cyber solutions and services such as secure communications [F1] and cyber resilience [F2] informed further studies improving the overall supply-chain security [F3, F4]. This has laid the foundation for the business case to establish a new GBP9,000,000 centre; the Midlands Centre for Cybersecurity in Hereford, also known as Cyber Quarter [C1]. The need for the centre is in alignment with the DEFEND elements of the UK's national cybersecurity strategy. It tackles the growing threat of cyber-attacks which could significantly impact local, regional and national businesses. It was completed on the 9th December 2020 and has already stimulated a significant base of SMEs engaged in cyber-security solutions. Earlier to that, the SMEs engaged directly with experts in cybersecurity at the university to benefit from consultancy and training.

The multi-million pound spend on the centre has injected substantial money into the local economy over the 2 years build time. Furthermore, there are 4 FTE jobs already and supported a further 6 jobs through the partner SMEs [C2]. Up until 31st December 2020, the number of companies registered was 29, they have accessed resources at the Centre and the University of Wolverhampton, to drive up levels of innovation activity in the local economy. There have been 2 new cyber-related products/services in development with the formation of 2 start-up companies and 2 University spin-offs (from the R&D carried by the team) [C2]. Councillor David Hitchiner, leader of Herefordshire Council, described the Centre as "a key investment to support the creation of high-income, knowledge-based jobs in the county" and enthusiastically proclaimed "we are already home to a highly regarded cyber economy, and the knowledge, expertise and opportunities that the centre brings will help to establish Herefordshire as one of the capitals of the cybersecurity sector" [C3]. Additionally, Hereford's Enterprise Zone Chairman and LEP Board Member, Andrew Manning Cox, stated "This is a trail-blazing project which will boost investment on Skylon Park while supporting businesses to protect themselves from hacking and data disruption" [C3]. Funding for the Centre included contributions from the Marches LEP and ERDF [C4]. Overall, the Midlands Centre for Cybersecurity represents a state-of-the-art and much-needed resource which will provide benefits to the cybersecurity of businesses in the Midlands region for many years to come.

A new university spin-off, namely Cydon Ltd (company number: 11773171), was incorporated on 17th January 2019. The value proposition of a new product was developed based on the team's research findings at the University [F3]. The product is an intelligent and secure decentralised data management platform to help organisations share data across their boundaries and supply chains. It was selected by the Innovate UK academic start-up programme (CyberASAP, Year 2) [C5], which helped to develop a comprehensive market validation activity [C6], assessed by an independent industrial panel and a Minimal Viable Product (MVP). Furthermore, Cydon has been selected to be part of BetaDen Business Accelerator and the Cyber Den Innovation Competition, held as part of CyberUK 2019 and to showcase at the DCMS Innovation. Cydon was also one of the 20 new businesses named the Brightest Stars of UK Cyber Innovation that competed for the title of the UK's Most Innovative Small Cybersecurity Company. The main algorithm utilised in Cydon has been patented [R5] to help the company grow, attract overseas investment and develop the product for export [C6]. Collecting and sharing data between different departments, offices and across the supply chain is a growing global problem addressed by the Cydon platform.

I2. Impacts on practitioners and delivery of professional services, including enhanced performance
Our research [F1-F4] led to training businesses and the creation of a unique Business Assistance Programme for SMEs in the Marches area, contributing to continuing personal and professional development of practitioners in this specialised area.

The team's research findings [F1-F4] have been used to develop a research-informed Cyber Industrial Curriculum (CIC). This in turn formed the business case to secure HEFCE Catalyst funding  aimed at closing the skills gap and supporting the Industrial Strategy through curriculum development with a total project cost of approximately GBP941,000. CIC was used to develop a new Level 7 course (MSc Cyber Security) at the University, and a series of Continuing Professional Development (CPD) courses. The course amalgamates Governance, Risk and Compliance (GRC) with the technical skills required by Cyber Security Professionals to secure jobs in areas such as Penetration Testers, Information Security Analysts, and Security Auditors. The MSc Cyber Security was successful started with 19 enrolled students in 2018/2019, then 26 students in 2019/2020, and expanding to 48 students in 2020/2021.

During the lifetime of the project (2018-2019), 4 main training events for businesses and educators took place in venues such as the Science Park at the University and the National Exhibition Centre in Birmingham. As part of their final report in October 2019, the Catalyst Fund Officer from OfS acknowledged the impact on practitioners: "It was good to see how much work has been achieved over the lifetime of the project and what impact it has had" [C7]. Thereafter, CIC was utilised to train practitioners from 25 local SMEs to improve insight on cyber-security challenges and opportunities across the Marches. The CEO of a participating SME which specialise in cyber resilience found the programme to be:

> "well balanced with added-value to keep the SMEs safer or to understand the state-of-the-art to improve the business strategy and internal policies, the programme is highly recommended to all businesses no matter your sector!" [C8].

Additionally, the team utilised its research [F1-4] to engage over 2,000 professionals through a series of over 30 specialist workshops and high-profile conferences on cyber resilience and digital transformation in cybersecurity as demonstrated in [C9]. Selected examples of events and number of attendees include “Forensics Europe Expo” at London Olympia (invited presentation, 50 attendees), “West Midlands Growth Company - Commercial Partner Event” (100 attendees), “Cyber Security Summit Brazil 2018” (200 attendees), “West Midlands Forum for Growth” event (150 attendees), “VSAT Global & Next General Satellite Applications” Conference (300 attendees), “UK Construction Week” (30 attendees), “5th Annual Industrial Control Cyber Security Europe Summit” (200 attendees), “CBI Cyber Security: Business Insight Conference” (200 attendees), “Cyber UK” conference and exhibition (100 attendees), House of Lords Showcase event (150 attendees) [C9]. These research-informed workshops and training events promote scholarship and collaboration, knowledge sharing, and strengthening professional ties between academia and the industry.

Overall, the cyber-threat landscape in the Midlands has been altered with new proactive defence capabilities based on the research and innovation of the cyber research team at the University of Wolverhampton. More precisely, this impact case study demonstrates commitment and significant contribution to tackling the growing threat of cyber-attacks against complex systems for CNI.

## 5. Sources to corroborate the impact

C1. Press Release, “Funding awarded for new Herefordshire cyber security centre.” Skylon Park.

C2. ERDF Outputs Tracker file.

C3. News Article, “Inside Hereford's new 'trail-blazing' cyber security centre.” Hereford Times.

C4. Grant Agreement, The Marches Local Enterprise Partnership (LEP).

C5. Spend profile (Cydon), Q1 Progress Review Meeting.

C6. Document, Investment Event & Final Demo, presented at Level 39, Canary Wharf, 17th January 2019. Event by CyberASAP.

C7. Project Sign-off Letter (HEFCE for Cybersecurity Industrial Curriculum).

C8. Contact details of CEO, Cyclopz Group Ltd.

C9. Events tracker document.