Institution: Cardiff University		
Unit of Assessment: Computer Science and Informatics (11)		
Title of case study: Intercepting cyber-attacks using bespoke predictive AI for Airbus		
Period when the underpinning research was undertaken: 2015 – 2019		
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:**
P Burnap	Professor	01/10/2002 – present
O Rana	Professor	01/01/1997 – present
Period when the claimed impact occurred: 15/08/2015 – 15/07/2019		
Is this case study continued from a case study submitted in 2014? No		

1. Summary of the impact (indicative maximum 100 words)

Cyber-attacks are becoming more refined by masking their identifiable features, reducing the effectiveness of conventional detection methods. Cardiff's research into machine learning and network interdependencies enabled a collaboration with Airbus to create risk mitigation tools for Airbus' global digital security strategy. A Cardiff-designed unique AI-based malware prediction system is now embedded in Airbus' frontline systems, protecting the confidential data and intellectual property of 134,000 employees, and shielding key European infrastructure. This partnership facilitated the Welsh Government's commitment to cyber security within their International Strategy and spurred an £8M investment from Airbus and the Welsh Government to construct the Airbus Cyber Lab.

2. Underpinning research (indicative maximum 500 words)

As the world's largest airliner manufacturer, operating more than 180 sites worldwide, and an integral supplier of European military and transportation aircraft, Airbus is a high-profile target for cyber-attacks. Cyber-attacks can begin with undetected malware leading to unauthorised data/intellectual property access, operational technology failures, and severe safety concerns. As malware becomes more sophisticated, it is better able to mask identifiable features and become harder to detect – Google's malware repository is reported to see over one million new and unique malware variants every day – requiring novel approaches to identifying malware.

2.1 Cardiff's industrial risk assessment suite

Recognising the reach and repercussions of cyber-attacks is central to effectively combating them. Risk assessment methods, however, typically struggle to understand and measure the impacts of interdependencies between assets – how other components are affected if one part of a system fails due to cyber-attack. Between 2014-17 Airbus and the Welsh Government joint-funded a £277,000 research programme named "SCADA CSL" **[G3.1]**, which allowed Cardiff University to explore new methods to capture such interdependencies. The project produced a new goal-oriented risk assessment method and associated modelling tool uniquely able to provide a holistic overview of key processes and risks within a system.

This was achieved by substituting the prevailing failure-oriented approach with a goal-oriented one, directed to what needs to go right. Pilot tests within Airbus's complex manufacturing systems provided useful feedback. Users approved the intuitive and useful focus upon goals, which more naturally led to capturing dependencies, and therefore the cascading impact of how one goal failure easily propagates to interconnected goals **[3.1]**.

Airbus has since transitioned the research into a combined process and dependency modelling tool and risk assessment method now used to protect critical national infrastructure. The research was extended with a further ~£360,000 investment from Airbus to Cardiff University until 2020. This focused on integrating intelligence on cyber risks from the malware

detection tool, merging the two technologies to improve situational awareness performance and dynamic 'living' real-time risk assessment.

2.2 Cardiff's malware detection tool

Burnap and Rana's research on malware detection stemmed from a 2013 £1 million EPSRC grant **[G3.2]** investigating malware behaviour and technical and operational measures to create a predictive process. Early research published by Cardiff used machine learning to classify the spread of malicious URLs on Twitter in 2015 **[3.2]**. Following significant national media coverage and their existing collaboration, Airbus approached Burnap to undertake a secondment to lead research into machine learning-based cyber-attack detection across the global Airbus IT and manufacturing network.

The collaboration (between 2016-19) moved away from code signatures and other discrete activity towards observing actual trace behaviour on computer networks. This reframed how malicious behaviour is modelled to create a 'DNA profile' for cyber-attacks through fragmentary behaviour indicators rather than depending on complete profiles or easily obfuscated signatures.

The initial innovation was in distinguishing malicious from trusted behaviour on computer networks using machine learning, with features derived from the footprint left on computer systems during execution including CPU/RAM use and network traffic at a count level of bytes and packets **[3.3]**. These allow detection methods to be more flexible with samples rather than discrete features such as API calls that can be obfuscated, enabling more acute detection. The Cardiff method increased malware classification accuracy by as much as 25.7% against an unseen dataset.

Subsequent work funded by Airbus enhanced the detection methods to include a world-first in predicting attacks, both from the Web **[3.4]** and via desktop computing environments (e.g. ransomware) **[3.5]**. Prediction enables earlier responses to mitigate or entirely prevent an attack, significantly reducing damage and the cost of repair; in **[3.5]** the Cardiff team were able to detect malicious activity in ransomware with 98% accuracy after just four seconds of execution, and reduce unwanted file encryption by 83%.

2.3 Centre of Excellence in Cyber Security Analytics

Airbus and Cardiff signed a Memorandum of Understanding in April 2017 to further collaborate on teaching, research, and impact within AI for cybersecurity. The Airbus Centre of Excellence in Cyber Security Analytics was launched in October 2017 following a £1.12 million investment from Airbus. Burnap was appointed Director of the Centre of Excellence, and Airbus funded a multi-year secondment for Burnap and two PhD studentships. In 2018, the Cardiff Centre for Cybersecurity Research, within which the Airbus Centre is a core pillar of activity, was recognised by EPSRC and the National Cybersecurity Centre as a UK Academic Centre of Excellence in Cyber Security Research (ACE-CSR).

In summary, Cardiff research:

- developed and translated a goal-oriented approach to overviewing of how malware affects key processes **[3.1]**;
- produced novel real-time classification of malware, supporting a new malware detection tool **[3.2]**;
- improved the state of the art in machine learning for distinguishing between malicious and trusted behaviours on networks, enabling greater discovery of new/unseen samples **[3.3]**;
- developed a world-first malware prediction model applicable to Web **[3.4]** and desktop computers **[3.5]**.

3. References to the research (indicative maximum of six references)

[3.1] Burnap, P.et al. 2017. Determining and sharing risk data in distributed interdependent systems. IEEE Computer 50(4), pp. 72-79. DOI:10.1109/MC.2017.108

[3.2] Burnap, P., Javed, A., **Rana, O** and Awan, M.S (2015). Real-time classification of malicious URLs on Twitter using Machine Activity Data. Presented at: *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, Paris, France, 25-27 August 2015. ACM DOI:10.1145/2808797.2809281

[3.3] Burnap, P., French, R., Turner, F and Jones, K (2017). Malware classification using self-organising feature maps and machine activity data. *Computers and Security* 73, pp. 399-410. DOI:10.1016/j.cose.2017.11.016

[3.4] Javed, A., **Burnap, P**. and **Rana, O**. (2018). Prediction of drive-by download attacks on Twitter. *Information Processing and Management* 56(3), pp.1133-1145. DOI:10.1016/j.ipm.2018.02.003

[3.5] Rhode, M., **Burnap, P**. and Jones, K. 2018. Early-Stage malware prediction using recurrent neural networks. *Computers and Security* 77, pp.578-594. DOI:10.1016/j.cose.2018.05.010

Selected grants:

[G3.1] 'SCADA CSL: SCADA Cyber Security Lifecycle'. Funder: Airbus Operations Ltd (01/03/2014 - 30/06/2017). Cardiff award value: £277,665

[G3.2] 'Identifying and Modelling Victim, Business, Regulatory and Malware Behaviours in a Changing Cyberthreat Landscape'. Funder: Engineering and Physical Science Research Council - EP/K03345X/1 (23/09/2013 – 22/032017). Cardiff award value: £1,016,595

4. Details of the impact (indicative maximum 750 words)

Cardiff University's research, as outlined in Section 2, enhanced Airbus' ability to identify surreptitious malware that might have previously gone undetected, developing a suite of tools for internal and commercial defence. These prevent attacks that would cost millions of pounds in recovery for Airbus and its global clients. To date, Cardiff's research partnership with Airbus has delivered the following impacts:

- assessment of the cascading impact of risks to defend critical global infrastructure via creation of a bespoke industrial risk assessment suite;
- the world's first predictive malware detection system, which has been integrated into Airbus processes protecting Airbus' European workforce of 134,000;
- the Welsh Government's £8 million investment to create the Airbus Cyber Lab, bolstering the country's commitment to cyber security in its 2020 International Strategy.

4.1 Mitigating risks to defend critical global infrastructure

Airbus' partnership with Cardiff University began in 2014 with the quantification of risk in industrial manufacturing systems, exploring interdependencies within systems and how malicious activity can exploit vulnerabilities. Airbus and Cardiff then jointly developed this research into a risk assessment tool that combined assessment, dependency modelling, and risk method for manufacturing and industrial application.

Dr Kevin Jones, Chief Information Security Officer at Airbus, commented **[5.1]**: "*The tool is uniquely able to provide a holistic overview of key processes and risks within a system and can model the cascading effect of single points of failure*." The risk assessment tool has widespread application, and Jones noted that it is "*now used internally by Airbus' own security teams to identify and prepare to high-risk failure scenarios"* **[5.1]**.

The risk assessment package was further developed as an international commercial offering as part of the Airbus Security division within the defence business line. Jones identified Burnap's research as vital to the company's digital security culture, which was "*transformed and industrialised to form a key part of Airbus' industrial manufacturing security programme*" **[5.1]**.

The package has been successfully applied to essential systems across the world, although due to the high-value and high-risk nature of these applications, Jones was unable to provide

identifying details: "*Although we cannot name our customers for confidentiality and national security reasons, we can confirm the tool is being actively used in the defence of critical national infrastructure by operators in the UK and globally*" **[5.1]**.

4.2 Implementing the first predictive malware detection system

Jones highlighted how 'Advanced Persistent Threats' (large scale cyber-attacks by state-sponsored or criminal groups) and other malevolent behaviours are "*a constant threat to Airbus' intellectual property and manufacturing facilities – loss of which would be economically and reputational [sic] damaging*" **[5.1]**.

Unlike existing malware detection methods that check against a pre-built library of known threats, Cardiff's machine learning techniques created a system that examines the 'DNA profile' of known malicious activity using partial behaviour. Airbus praised the new software as "*the world's first predictive approach to determining the malicious state of a suspect software*" **[5.1]**.

This key advantage enables future protection and a preventative approach, as current market solutions may only detect attacks after they have occurred, and "*market technologies using machine learning are not yet able to predict and block attacks*" **[5.1]**, whereas the new software actively blocks attacks. Airbus testing found that "*Burnap and the team have demonstrated the ability to detect such malicious activity in ransomware with 98% accuracy after just four seconds*" **[5.1]**. This allows Airbus to bypass current market-leading solutions "*for which licences can run into millions of pounds annually*" **[5.1]**, delivering significant financial savings to the company.

The integration of AI into a malware detection system embedded Cardiff research at the centre of Airbus' cyber security strategy, with Jones confirming that "*these world-first predictive algorithms are now in production and integrated within the 'signal suspicious' feature of Airbus' front-line Security Operations Centres*" **[5.1]**. The cyber security package developed at Cardiff University is now *"used to protect Airbus' 134,000 employees, confidential data, and key infrastructure across Europe (France, Spain, Germany, and the UK)*" **[5.1]**.

4.3 World-first cyber security labs and defining Welsh Government international strategy

The Airbus-Cardiff collaboration was described by Jones as an example of successful academic-industrial integration, noting: "*The UK National Cyber Security Centre has cited this partnership as a 'blueprint' for university and industry collaboration – something we are very proud of as a company driven by innovation and secure operations*" **[5.1]**.

Building on the solutions developed through the Cardiff-Airbus collaboration, in 2019 the Welsh Government and Airbus co-invested £8 million to establish the new Airbus Cyber Lab within the Airbus Cyber Innovation Hub in Newport, South Wales **[5.1, 5.2]**. Jones stated that a "*key pillar*" of the Cyber Lab "*is to continue to deliver global cutting-edge Artificial Intelligence for cyber security research*" **[5.1]**. . Announcing the launch of the Cyber Lab, Airbus highlighted how the Cardiff-Airbus partnership "*has been a great asset in driving innovation and skills development forward for Wales and the wider world*" **[5.3]**.

Ken Skates, the Welsh Minister for Economy, Transport and North Wales, wrote how the Cardiff-Airbus partnership "*helped Wales to stand out as a leader in academia-industry collaboration*", and the launch of Cyber Lab further demonstrates "*leadership in cybersecurity to companies and enterprises across Wales, UK and internationally*" **[5.2]**. Together, the Welsh Government's investment in Cyber Lab and Cardiff's research formed "*a core part of the evidence required to put cybersecurity as one of the three pillars of excellence in our International Strategy*": a five-year Welsh Government plan to attract industrial investment across three areas of industry strengths within Wales **[5.2]**.

Cardiff's research and expertise was further recognised in the wider UK Industrial Strategy AI and Data Grand Challenge. In May 2019, Burnap joined the AI Council, an independent expert committee developing the UK's AI industrial strategy within the UK Government Department

for Culture, Media and Sport (DCMS) and which aims to promote its use in business and organisations **[5.4]**.

5. Sources to corroborate the impact (indicative maximum of 10 references)

[5.1] Testimonial by Dr Kevin Jones, Airbus' Global Chief Security Information Officer

[5.2] Testimonial by Ken Skates MS, Minister for Economy, Transport and North Wales, Welsh Government

[5.3] '*Airbus Cyber Innovation opens its Cyber Innovation Hub in Newport, Wales'*. Airbus Press Release, 24 June 2019

[5.4] "Leading Experts Appointed to AI Council to supercharge the UK's artificial intelligence sector", UK Government press release, 16 May 2019