CASUGOL

Nights Out

Cyber Security, AI and Digital Futures

Presentation by

Dr. Phil Legg

Associate Professor in Cyber Security

MSc Cyber Security Programme Leader

September 2020

About Me

- Programme Leader for NCSC-certified MSc Cyber Security
- Director of UWEcyber

- Research interests:
    - Cyber security, Machine Learning, Data Visualisation

- Research domains:
    - Insider threat detection, cyber situational awareness, adversarial AI, privacy-preserving AI, visualisation for explainable AI, cyber resilience

Glasgow
United Kingdom
Isle of Man
Leeds
Dublin
Liverpool
Sheffield
Ireland
Birmingham
Bristol
London

UWE cyber

UWE Bristol University of the West of England

Cyber security for connected vehicle and highway system
Dr Neil Hoose
Visiting Professor, Centre for Transport Studies
Director, Bittern Consulting Ltd

Teaching

MSc Cyber Security (NCSC Full Certification)

BSc Cyber Security and Digital Forensics

Outreach

Unlock Cyber

NCSC CyberFirst

NCSC Cyber Schools Hub

NCSC EmPowerCyber

External Engagement

Foundry

CISSE UK

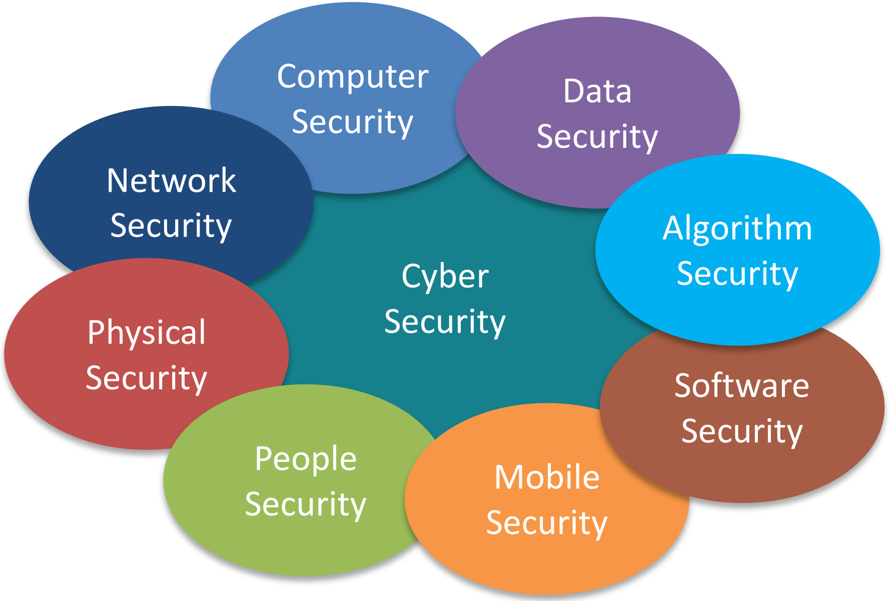
Research

- AI for Security and Security of AI
- Security Data Analytics and Visualisation
- Cryptography and Post-Quantum Security
- Malware Analysis
- Human Factors
- Industrial IoT and CAVs
- Insider Threat and Behavioral Analysis
- Systems Verification and Validation
- Network Security

Cyber Security, AI and Digital Futures

What do we mean by Cyber Security?

CYBER SECURITY
010110
0100
Application
Information
Network
Operational
Encryption
Access control
End-user education
Disaster recovery



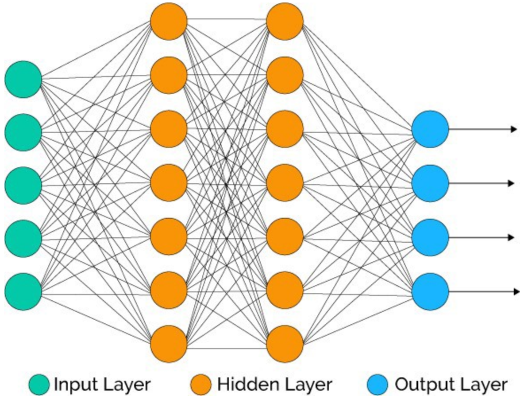
Cyber Security is the protection of ***Confidential****,* ***Integrity****,* ***Availability****, on any digital assets – including data, systems, and processes*

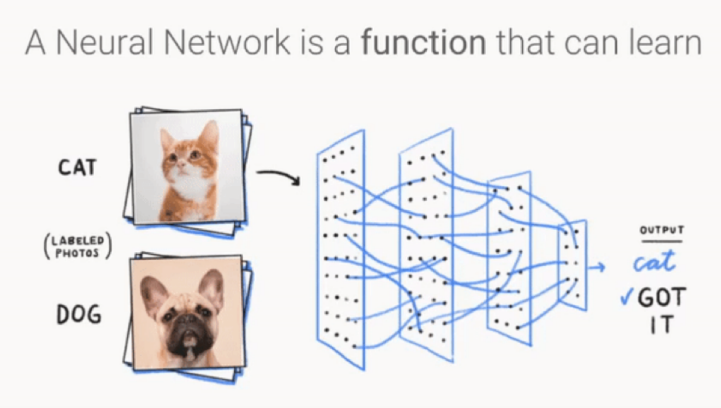
What do we mean by AI?

- A system that can learn?
- Not explicitly programmed by the developer?
- Learning from example data?

Two common tasks:

- Classification – given an input, can a function be learnt to **distinguish between discrete classes** (e.g., animals).
- Regression – given an input, can a function be learnt to **predict a continuous value** (e.g., stock market).




A Neural Network is a **function** that can learn

AI for Cyber Security

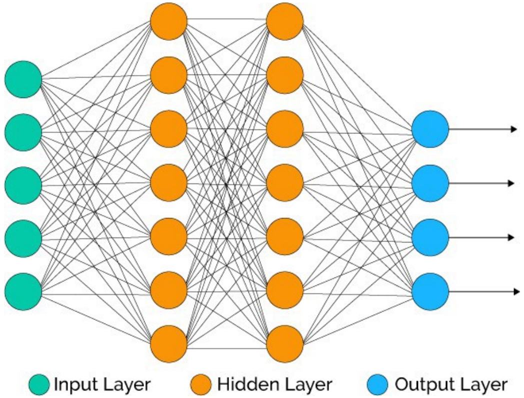
Classification

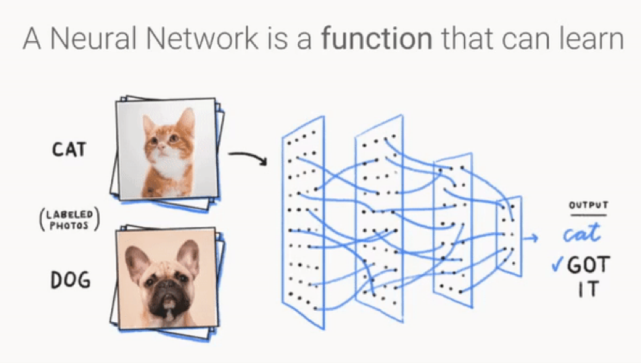
- Malware analysis – software – **malicious or benign**
- Intrusion detection systems – network traffic - **malicious or benign**

Regression

- Threat scoring – behavioural analysis – 0 to 1?
  - Use of language, Use of resources, etc.

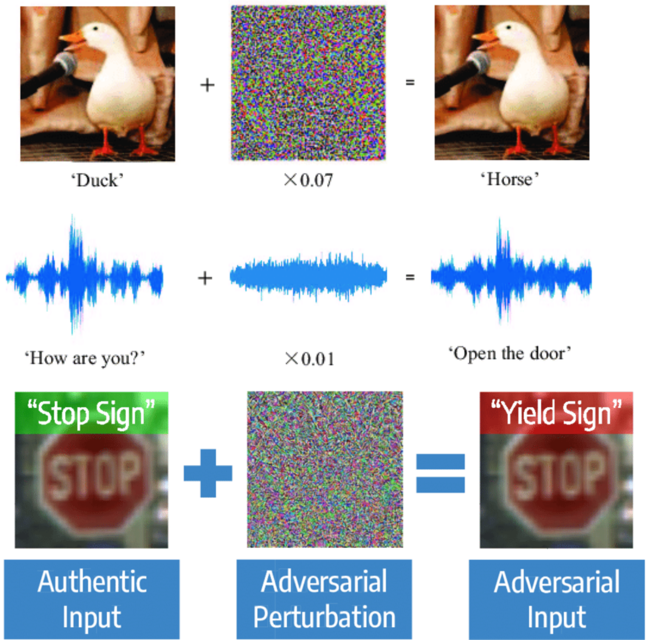
- Offers scalability for big data analysis
- Can help security analyst identify attributes that may be missed / overlooked
- Rapid decision-making to respond to threats





AI for Cyber Security

Traditional AI systems do not assume for an adversary that wants to ruin our day!



Adversarial Learning

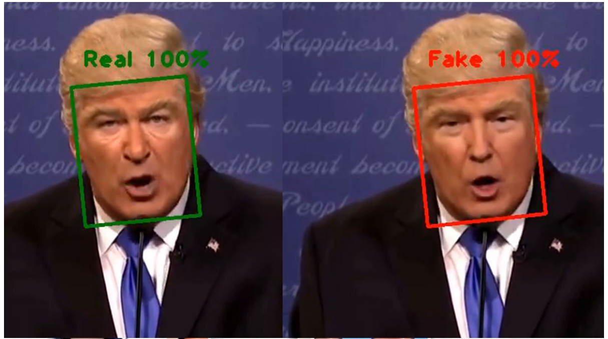
- Given a classifier, can we compromise the input or compromise the learnt model weights, to trigger an unintended output?
- Images: Panda / Gibbon, Duck / Horse examples
- Audio: Speech recognition

Shouting through letterboxes: A study on attack susceptibility of voice assistants

- Impact: Can we therefore attack voice assistants, or can we impact how CAVs identify road objects?
  - Is this a 'cyber attack'?

AI for Cyber Security

Traditional AI systems do not assume for an adversary that wants to ruin our day!



Deep Fakes

- Transfer learning – given a model, can we compromise this so that a different input will yield the same output (or a very similar output)?
- Mis-information – sophisticated social engineering
  - Is this a 'cyber attack'?

https://www.biometricupdate.com/202008/deepfakes-declared-top-ai-threat-biometrics-and-content-attribution-scheme-proposed-to-detect-them

AI for Security - Security of AI

- AI can be an effective tool for modern cyber security analysis
  - Network traffic, software, behaviour analysis, threat detection
  - Scalable, consistent big data analysis – better than human?

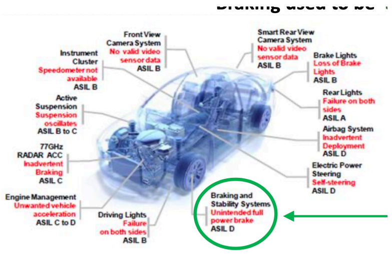
- AI is also vulnerable to attacks, so how do we have security of AI?
  - E.g., Adversarial learning, Deep Fakes
  - Requires better forms of explainable AI for assessing security properties / model edge cases / decision boundaries and better forms of human-machine collaboration
  - How to validate this for models that continually learn?

- ***CAVs, IIoT, Cyber Crime prevention, HealthTech*** – AI is being used for all of these – if the AI is insecure then they could have serious societal consequences
  – are these new ‘cyber attack’ vectors?

UWEcyber
Research Stories

UWE Bristol University of the West of England

1 Cyber Security in Connected Autonomous Vehicles



To what extent do CAVs introduce additional risk compared to traditional road vehicles?

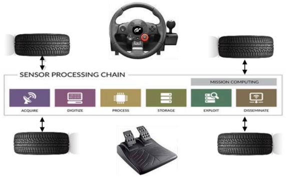
Can the perceived cyber risks in CAVs be mitigated against?

Project CAVForth "Cyber Security Assessment"

Penetration Testing on a CAV Stagecoach Bus Service across Edinburgh Forth Road Bridge

An Example Problem: Breaking the Brakes …

Braking has become Digital and 'Complicated'



Successful Cyber Attacks Against Braking Systems :

- Contradictions that may arise in the data stream
- Denial of Service – Cycles, processing out of bounds, timing
- Non Determinism – Arbitration between Complex Algorithms with no ground truth
- Transition Analog / Digital
- Interaction between technologies e.g. error correction as input to ML
- Attack Detection & Attack Management (Function and Control)

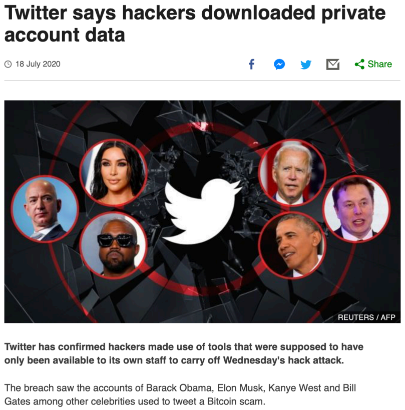
Method: Attack under controlled conditions

Without direct connection between controls and function, our assumption of ASIL-D becomes questionable – even before malevolent attacks are considered

Centre for Connected and Autonomous Vehicles

Fusion Processing

2 Protection from Cyber-enabled and Cyber-dependent Crime



Twitter says hackers downloaded private account data

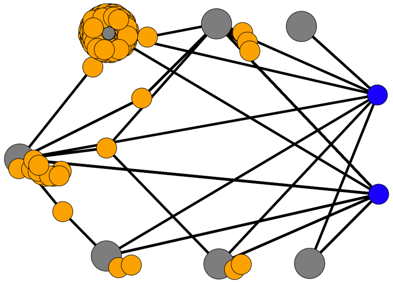
18 July 2020

Share

REUTERS / AFP

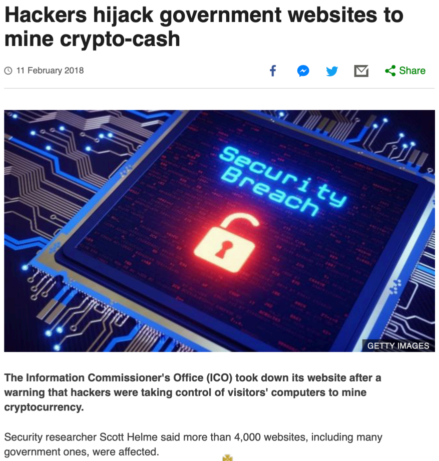
Twitter has confirmed hackers made use of tools that were supposed to have only been available to its own staff to carry off Wednesday's hack attack.

The breach saw the accounts of Barack Obama, Elon Musk, Kanye West and Bill Gates among other celebrities used to tweet a Bitcoin scam.



Bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

£100k in approx. 2 hours



Hackers hijack government websites to mine crypto-cash

11 February 2018

Share

GETTY IMAGES

The Information Commissioner's Office (ICO) took down its website after a warning that hackers were taking control of visitors' computers to mine cryptocurrency.

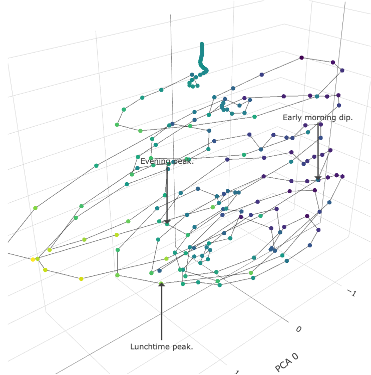
Security researcher Scott Helme said more than 4,000 websites, including many government ones, were affected.

How do we better detect, analyse, and respond, to cyber-enabled and cyber-dependent crimes?

Anti-money Laundering
Counter-Terrorism Financing
Dark Web

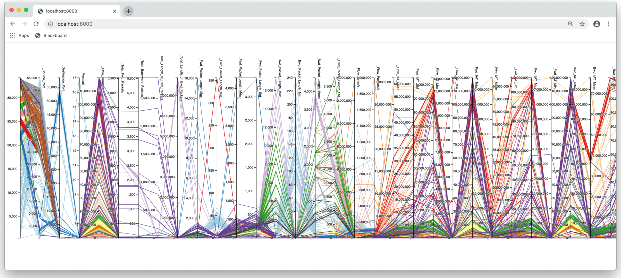
3 AI Security

- Explainable AI, Adversarial ML, and Privacy-Preservation in ML
- 3 current PhD candidates addressing these themes related to AI and Security
  - 1. How can we interrogate AI to ensure it performs as intended?
  - 2. What about when an adversary or unexpected input occurs?
  - 3. How do we achieve this whilst protecting privacy of individuals, without compromising accuracy?



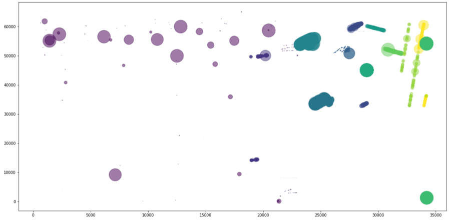
Montvieux

Simplicity from Complexity



TECHMODAL

Opportunities. Found.

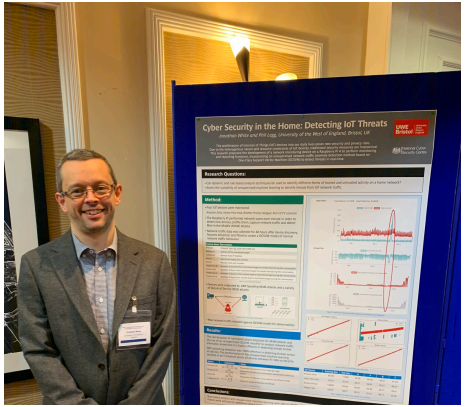


UWE Bristol University of the West of England

4 Malware, IoT, 5G

National Cyber Security Centre
a part of GCHQ

- Can we detect and dynamically defend against active malware? (NODENS)
- Can context-aware malware characteristics be interrogated using sandbox environments? (MORRIGU)
- Can we safely examine malware propagation to deploy dynamic deception networks to inform analysis? (NCSC)
- How do we examine and protect IoT devices? How do we convey IoT device activity for non-expert users to help them defend themselves? (NCSC)
- What are the security implications of 5G network slicing? (MaaStran)



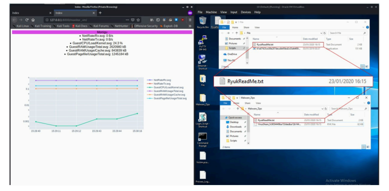


Figure 3 Screenshot to show an example of live monitoring in the MORRIGU GUI (left) when the Ryuk Ransomware has been deployed using MORRIGU within the Windows 10 testing environment (right).

Cyber First
This is a CyberFirst world. Train for it.
National Cyber Security Centre
Welcome to the NCSC Conference
"Inspiring and Educating Future Generations in Cyber Security"

5 Cyber Foundry

- Practical Hands-On Experience for Student-Industry Engagement
- **Industrial Penetration Testing** Project with VQ Communications (3rd yr Student)
- Research facility suitable for 50:50 studentship model
- Training facility for running “capture the flag” exercises with industry and outreach partners

paloalto NETWORKS

VQ COMMUNICATIONS

MONTVIEUX Simplicity from Complexity

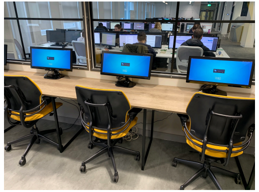
TECHMODAL Opportunities. Found.

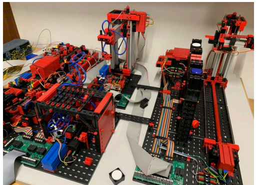
HACKTHEBOX

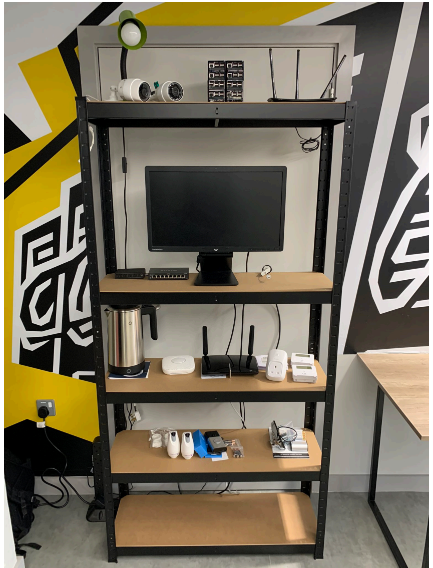
CISSE UK

unlock cyber OPENING FUTURES IN CYBER SECURITY

Cyber First







UWE cyber

UWE Bristol University of the West of England

Cyber security for connected vehicle and highway systems

Dr Neil Hoose

Visiting Professor, Centre for Transport Studies

Director, Bittern Consulting Ltd

Developing Cheltenham's future cyber generation

National Cyber Security Centre
a part of GCHQ

Innovate UK

[dstl]

Centre for Connected and Autonomous Vehicles

THE ROYAL SOCIETY

AVON & SOMERSET CONSTABULARY

CYBER CRIME CSCV
Cyber Specials Cyber Volunteers

paloalto NETWORKS

Cyber First

ROYAL AIR FORCE

MONTVIEUX
Simplicity from Complexity

unlock cyber
OPENING FUTURES IN CYBER SECURITY

JSPS

SYNALOGiK

CISSE UK

NII
国立情報学研究所
National Institute of Informatics

TECHMODAL
Opportunities. Found.

LEONARDO

BRISTOL BSIDES

Fusion Processing

VQ COMMUNICATIONS

institute of CODING

Thank you for listening

Dr Phil Legg
Associate Professor in Cyber Security

Phil.Legg@uwe.ac.uk
http://www.plegg.me.uk
http://go.uwe.ac.uk/phil

AI for Cybersecurity

Further reading on AI for Cybersecurity

- https://www.ibm.com/uk-en/security/artificial-intelligence
- https://www.computing.co.uk/sponsored/3063441/ai-is-changing-cybersecurity-but-its-not-a-catch-all-solution
- https://blog.eccouncil.org/the-role-of-ai-in-cybersecurity/
- https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/
- https://www.brookings.edu/research/how-to-improve-cybersecurity-for-artificial-intelligence/