British Embassy Kuwait

المركز الوطني للأمن السيبراني
National Cyber Security Center

cerc 2024

THE 6TH CYBERSECURITY EDUCATION & RESEARCH CONFERENCE

Title: Leveraging AI for Enhanced Cybersecurity Solutions

Dr. Tawfik Al-Hadhrami
Computer Science Department
School of Science and Technology
Nottingham Trent University
Nottingham, United Kingdom

KUWAIT COLLEGE OF SCIENCE & TECHNOLOGY
كلية الكويت للعلوم والتكنولوجيا

جامعة الكويت
KUWAIT UNIVERSITY

UK Science & Innovation Network

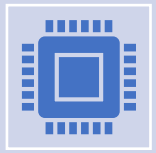
125 عاماً من الشراكة الكويتية البريطانية
125 YEARS OF KUWAITI-BRITISH PARTNERSHIP

Outlines

- AI and Cybersecurity, Roadmap, Applications, Challenges and Benefits
- Securing Critical National Infrastructure and AI (S-CNI&AI)
- CNI- Power Security
- Assistive Artificial Intelligence (AAI) Benefits and Requirements
- Sustainable Model to ICS Environment: CIM Framework 1,2 &3
- CNI - Security in Power Systems: Facts for Future
- Any Questions?

What is AI in Cybersecurity?

AI is Cybersecurity refers to the use of AI & Machine learning algorithms & techniques to enhance the security of Computer systems & networking

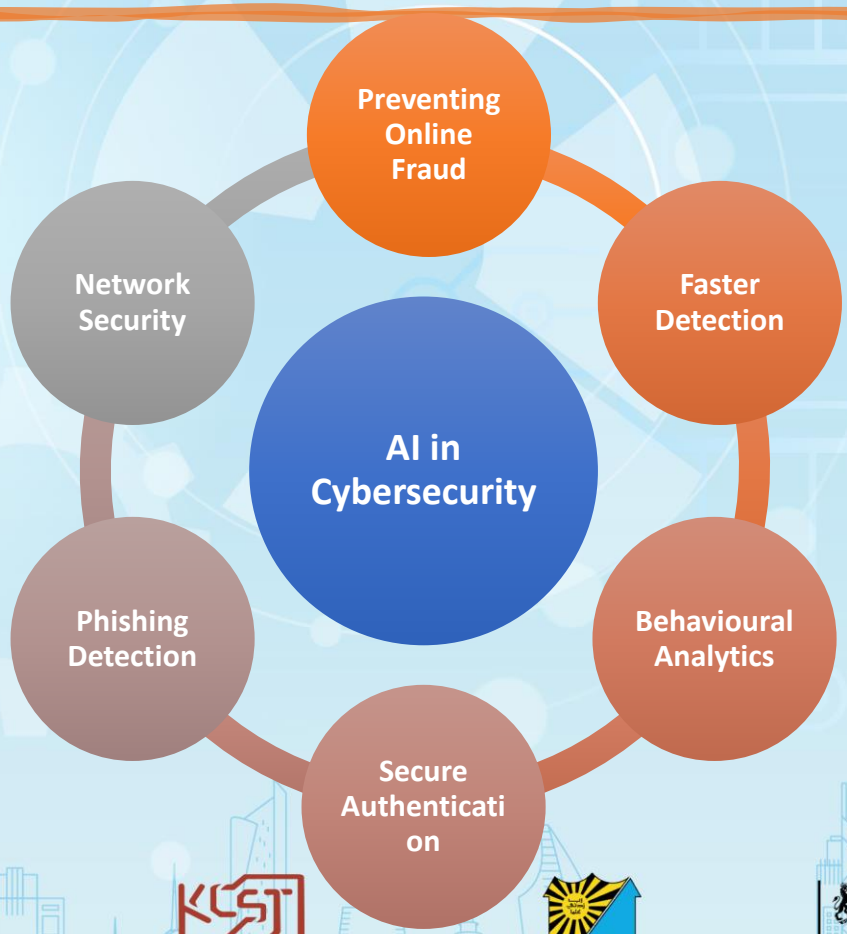


The Goal of AI in Cybersecurity is to automate the process of detecting, and preventing & mitigating security threats, thereby making Cybersecurity more efficient and effective

Some of the ways AI is being used in Cybersecurity include:

- Threat detection
- Intrusion Prevention
- Malware Detection
- Vulnerability management

AI in Cybersecurity



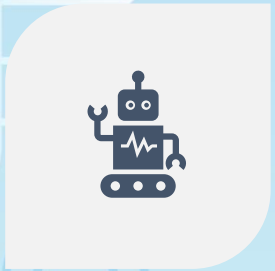
cerc 2024
THE 6TH CYBERSECURITY EDUCATION & RESEARCH CONFERENCE

AI in Cybersecurity Roadmap

IMPROVED THREAT HUNTING BY INTEGRATING BEHAVIOUR ANALYSIS

STRENGTHENING INDUSTRIAL IOT OR SMART FACTORY (INDUSTRY) 4.0

AI-POWERED MANAGE SECURITY SERVICES WITH PROFOUND BENEFITS FOR MSPS



AUTOMATION OF HUMAN ACTIONS VIA AI-DRIVEN SECURITY OPERATION CENTRES

المركز الوطني للأمن السيبراني
National Cyber Security Center

British Embassy Kuwait

KUWAIT COLLEGE OF SCIENCE & TECHNOLOGY
كلية الكويت للعلوم والتكنولوجيا

جامعة الكويت
KUWAIT UNIVERSITY
1966

UK Science & Innovation Network

125 عاماً من الشراكة الكويتية البريطانية
125 YEARS OF KUWAITI-BRITISH PARTNERSHIP

AI Applications in Cybersecurity

NETWORK SECURITY

VULNERABILITY MANAGEMENT

PASSWORD PROTECTION & AUTHENTICATION

PHISHING DETECTION & PREVENTION

AI in Cybersecurity General Challenges

- Bias in training data algorithms
- Lack of transparency in the AI decision-making process
- Integration with existing security systems and processes
- High computational requirements and technical expertise required
- Ethical considerations surrounding the use of AI in security applications
- Vulnerability to adversarial attacks
- Protentional for false positive and false negative results
- Difficulty in ensuring the reliability and security of AI systems
- Difficulty in collecting and labelling sufficient data training AI models
- Need for ongoing monitoring & maintenance to ensure the continued effectiveness of AI systems

Benefits of Using AI in Cybersecurity

cerc 2024
THE 6TH CYBERSECURITY EDUCATION & RESEARCH CONFERENCE

- Handle a lot of Data
- Learn more over time
- Better Vulnerability
- Securing Authentication
- Better Overall Security
- Duplicative Processes Reduce
- Identifies Unknown Threats
- Accelerates Detection & Response Time

المركز الوطني للأمن السيبراني
National Cyber Security Center

British Embassy Kuwait

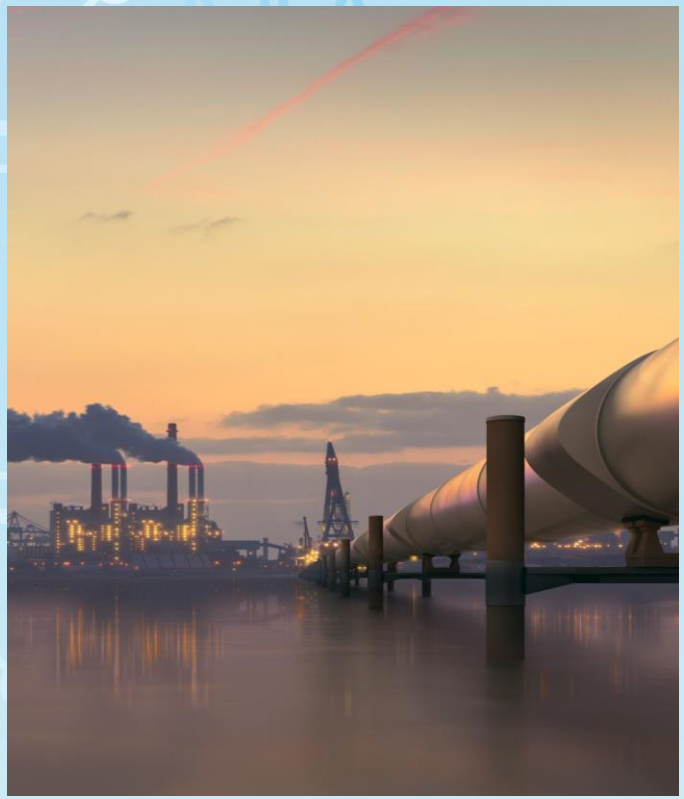
KUWAIT COLLEGE OF SCIENCE & TECHNOLOGY
كلية الكويت للعلوم والتكنولوجيا

جامعة الكويت
KUWAIT UNIVERSITY
1966

UK Science & Innovation Network

125 عاماً من الشراكة الكويتية البريطانية
125 YEARS OF KUWAITI-BRITISH PARTNERSHIP

Securing Critical National Infrastructure (CNI)



- Securing Critical National Infrastructure (CNI) is essential to ensure modern ways of living
- In the past, critical national infrastructure sites were more secure as exploiting them required gaining physical access
- Power stations, water facilities, and other sites are now connected to the communications network to be monitored and managed remotely
- While this has reduced costs and increased flexibility for operators
- **it has opened these sites to threats from cyber-attacks**

cerc 2024
THE 6TH CYBERSECURITY EDUCATION & RESEARCH CONFERENCE

Securing Critical National Infrastructure and AI (Sec-CNI&AI)

Power Infrastructure

المركز الوطني للأمن السيبراني
National Cyber Security Center

British Embassy Kuwait

KUWAIT COLLEGE OF SCIENCE & TECHNOLOGY
كلية الكويت للعلوم والتكنولوجيا

جامعة الكويت
KUWAIT UNIVERSITY

UK Science & Innovation Network

125 عاماً من الشراكة الكويتية البريطانية
125 YEARS OF KUWAITI-BRITISH PARTNERSHIP

CNI- Power Security

Staff within the organisation will be better prepared

- To deal with cyber incidents
- Reducing the potential impact on customers
- Saving money in downtime costs

Hybrid Cyber Platform Development

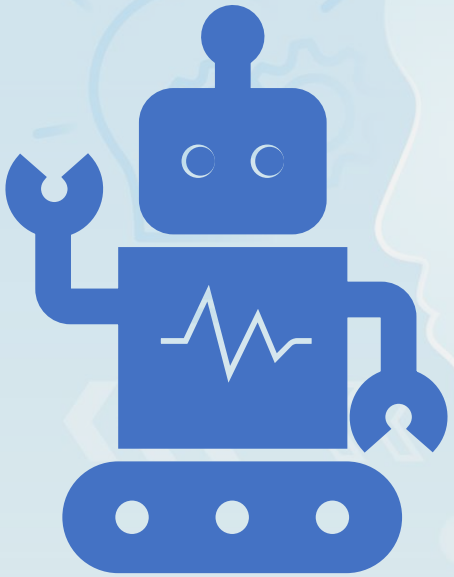
Multi-stakeholder Risk Approaches

The Industrial Control Systems (ICS) providing secure infrastructure are difficult to protect from cyber-attacks due to:

- The combination of complexity
- The age of many devices
- The prohibitive costs
- Production downtime
- The commonness of legacy systems

Improve the situational awareness of defenders

Assistive Artificial Intelligence (AAI) Benefits



- **Assistive Artificial Intelligence** solutions provide many benefits to organisations:
  - Allowing the automation of many tasks and
  - Incorporating a wide knowledge base of learned information
  - Provides a controlled environment
  - Ensure AI solutions have been trained on data
  - “human-in-the-loop” paradigm will be presented
  - Rather than those provided by vendors which will be more generalised
  - Not fully automating all tasks

Assistive Artificial Intelligence (AAI) Requirements

- Develop AI policies for Industrial control systems (ICS)
- Create an AI solution to aid logging and monitoring
- Train AI solutions on real-world data
- Develop AI policies for learning enrichment
- Develop AI policies/Solutions for automated testing

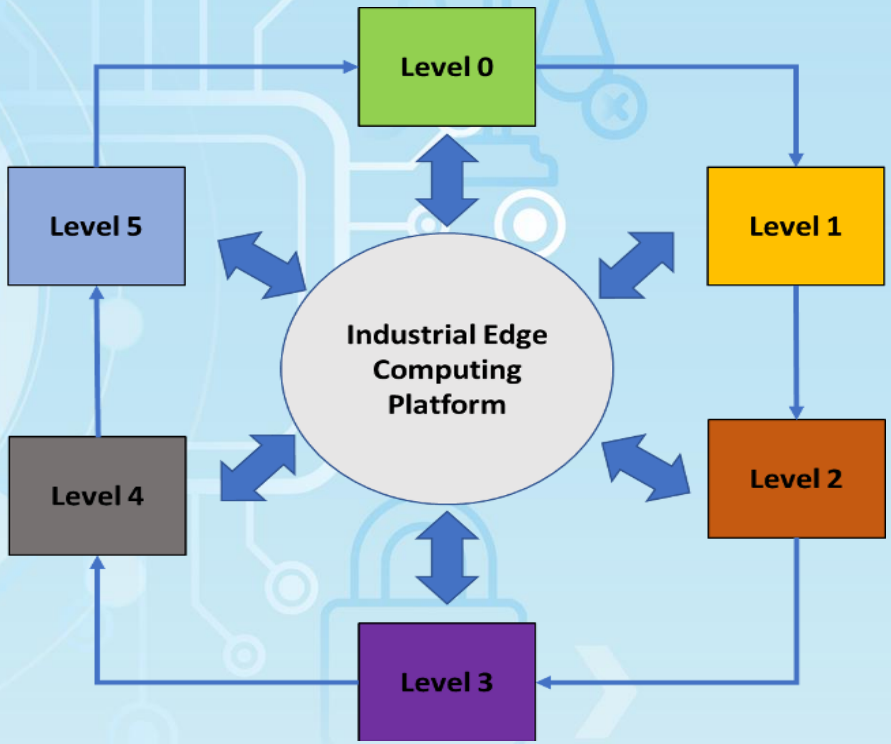
Sustainable Model to ICS Environment: CIM Framework 1

- Providing standardised data connectivity, accessibility, and interoperability across the entire energy system
- Boost the usability of information and make real-time grid morning data more accessible for improved system analysis, forecasting, optimisation, and visualisation
- Increase energy resources and the integration of low-carbon technologies with more sophisticated and rapid automation features
- Offer reliable, secure, low-latency data interchange and high-quality data and services
- Granting customers greater control over data access

Sustainable Model to ICS Environment: CIM Framework 2

- Improve digital processes
- Improve information exchange among all digitised data sources
- Improve the digital products and business applications
- To deliver transmission network applications
- To maximize renewable generation integration through a smart grid function application
- Improve the customer engagement
- To deliver real-time energy price information exchange application
- To ensure the ICS system data integrity and cyber security

Sustainable Model to ICS Environment: CIM Framework 3



The Purdue Model with an Industrial Edge Computing Platform(www.automationworld.com)

Cyber Platform Solution

- **A Cyber platform** is required
- **The proposed Hybrid Cyber Platform** is a powerful tool to replicate existing information systems, to test and develop abilities such as:
  - Pen-testing
  - Network protection
  - System hardening
  - Incident response,
  - TTPs (Tactics, Techniques & Procedures)

CNI – Security Recommendations for Power Systems

- Improved Cyber Resilience
- Digital Transformation And New Technology
- A Hybrid Virtualisation Platform
- Increases Protection Of Legacy Systems
- Dynamic Risk Assessment
- Training And Incident Response
- Multi-stakeholder Risk Approach
- Smart Monitoring And Logging Systems
- Assistive AI Tools In Power Architecture

cerc 2024
THE 6TH CYBERSECURITY EDUCATION & RESEARCH CONFERENCE

المركز الوطني للأمن السيبراني
National Cyber Security Center
British Embassy Kuwait
KUWAIT COLLEGE OF SCIENCE & TECHNOLOGY
كلية الكويت للعلوم والتكنولوجيا
جامعة الكويت
KUWAIT UNIVERSITY
UK Science & Innovation Network
125 عاماً من الشراكة الكويتية البريطانية
125 YEARS OF KUWAITI-BRITISH PARTNERSHIP

cerc 2024
THE 6TH CYBERSECURITY EDUCATION & RESEARCH CONFERENCE

The Forum for Industry, Government and University Research Knowledge Exchange (FIGURE)

FIGURE FORUM is a joint platform for academics and industrial experts in the cybersecurity field

FIGURE Co-founders: **From Academics and Industry in the UK**

FIGURE FORUM

المركز الوطني للأمن السيبراني
National Cyber Security Center

British Embassy Kuwait

KUWAIT COLLEGE OF SCIENCE & TECHNOLOGY
كلية الكويت للعلوم والتكنولوجيا

جامعة الكويت
KUWAIT UNIVERSITY

UK Science & Innovation Network

125 عاماً من الشراكة الكويتية البريطانية
125 YEARS OF KUWAITI-BRITISH PARTNERSHIP

Thanks for listing
Any Questions!