School of Computing, Engineering, and the Built Environment
Edinburgh Napier University MRes

Application instructions:
Detailed instructions are available at :
https://www.napier.ac.uk/research-and-innovation/doctoral-college/how-to-apply

Project details

Supervisory Team: tbc

Subject Group: Cyber Security & Systems Engineering (CSSE)

Funding status: Self-funded

Project Title: MRes research degrees in Cyber Security & Systems Engineering

Cyber Security & Systems Engineering Research Opportunities:

The Cyber Security & Systems Engineering subject group at Edinburgh Napier University is at the forefront of research in protecting digital systems, securing critical infrastructure, and enhancing cyber resilience. Our research addresses global challenges in cybersecurity, systems engineering, and network security, ensuring that digital transformation is built on a foundation of safety, privacy, and reliability. We collaborate with industry, government, and academia to develop innovative security solutions that protect individuals, businesses, and nations from emerging cyber threats.

Research Areas in Cyber Security & Systems Engineering:

Cyber Threat Intelligence and Incident Response: We develop advanced threat detection and response strategies to identify, mitigate, and prevent cyberattacks in real time. Our work enhances digital forensics, intrusion detection, and automated response mechanisms.

Network and Cloud Security: Our research investigates secure architectures for cloud computing, edge computing, and Internet of Things (IoT) systems. We develop resilient security frameworks to protect data and applications across distributed networks.

Cryptography and Secure Communications: We explore encryption techniques, blockchain security, and cryptographic protocols to enhance secure communication, authentication, and data protection in modern digital infrastructures.

Industrial Control Systems (ICS) and Critical Infrastructure Security: Our research addresses vulnerabilities in energy grids, transportation systems, and smart cities, ensuring robust cybersecurity solutions for essential services.

Ethical Hacking and Penetration Testing: We study offensive security techniques to identify weaknesses in software, networks, and hardware, helping organisations build stronger defences against cyber threats.

Artificial Intelligence for Cybersecurity: We integrate machine learning and AI-driven security analytics to develop automated threat detection systems, predictive risk assessment models, and anomaly detection solutions.

Human-Centric Cybersecurity: We examine user behaviour, security awareness, and privacy concerns to design more effective security policies, education programs, and user-friendly authentication methods.

Systems Engineering and Embedded Security: Our research focuses on designing secure, resilient, and high-performance computing systems, with an emphasis on secure software development, embedded system security, and real-time system protection.

Our Commitment to Research Excellence

Our research in Cyber Security & Systems Engineering aligns with global security challenges, industry demands, and government initiatives, ensuring that our work contributes to a safer digital future. We actively engage with industry partners, law enforcement agencies, and academic institutions to translate cutting-edge research into real-world cybersecurity solutions.

We welcome prospective students and researchers eager to contribute to this vital field. Whether your interest lies in network security, cryptography, AI-driven cybersecurity, or critical infrastructure protection, our research community offers a dynamic and supportive environment for innovation.

For further information or to explore research opportunities, please visit our **Cyber Security & Systems Engineering** research page at Edinburgh Napier University.

Candidate characteristics

Education:
A first degree (at least a 2.2) ideally in the Cyber Security & Systems Engineering subject areas

English language requirement
IELTS score must be at least 6.5 (with not less than 6.0 in each of the four components). Other, equivalent qualifications will be accepted. Full details of the University's policy are available online.

Essential attributes:

- Experience of fundamental Cyber Security & Systems Engineering subject related knowledge
- Competent in literature review, report writing and statistical and/or qualitative analysis
- Knowledge of research topic proposed
- Strong motivation, with evidence of independent research skills relevant to the project
- Good written and oral communication skills
- Good time management