**PhD Project Proposal**

School of Electronics, Electrical Engineering and Computer Science

|  |
| --- |
| **Proposed Project Title:** Defending ML-based Network Security Systems from adversarial attacks |
| **Principal Supervisor:** Dr. Sandra Scott-Hayward **Second Supervisor:** |
| **Project Description:**  With the increasing deployment of Machine Learning (ML) models, ML classifiers are threatened by adversarial attacks. In an adversarial attack, an attacker can poison or evade the decision generated by the ML algorithm by manipulating inputs. A body of research exists focussed on the impact of adversarial attacks on image classification. However, machine learning is gaining traction in the implementation of network security systems such as intrusion detection systems. Will network security systems be the next target of poisoning and evasion attacks?  The main goal of this PhD thesis is to investigate the vulnerability of network security machine learning algorithms to attack. Novel solutions will be proposed for the design of algorithms and systems that are resistant to adversarial attacks.  *The student will have access to a state-of-the-art network testbed in the Centre for Secure Information Technologies (CSIT), Belfast.* |
| **Contact details**  Supervisor Name: Dr. Sandra Scott-Hayward Tel: +44 (0)28 9097 1898  QUB Address: Email: [s.scott-hayward@qub.ac.uk](mailto:s.scott-hayward@qub.ac.uk) |