Australian Government
Department of Defence
Science and Technology

POSITION DESCRIPTION

Position Title:	**Automated Cyber Vulnerability Analysis Researcher**
Position Reference Number:	ECRCEWD003
Division	Cyber and Electronic Warfare Division
Position Classification:	S&T 3-4
Position Location:	Edinburgh (SA)
Security Level:	NV2
Minimum Academic Qualification:	Masters
Enquiries:	Chris North, chris.north@dst.defence.gov.au , 08 7389 6717

Academic Disciplines

□	Aerospace/ Aeronautical Engineering, Naval Architecture	□	Chemical, Radiological, Biological, Food sciences	□	Materials Science
■	Computer Sciences, IT, Software Engineering, Telecommunications	□	Mathematics and physics	□	Psychology and Social Sciences
□	Mechanical and Mechatronic Engineering (including robotics)	□	Electronic/ Electrical Engineering	□	Other

Position Overview

The Automated Cyber Vulnerability Analysis Researcher will undertake research into developing tools and techniques to automate the vulnerability analysis of military systems and analyse cyber vulnerabilities.

Through the application of machine learning and data mining, and in conjunction with mission and system modelling, Military Systems Automated Vulnerability Analysis aims to manage the scale and complexity of modern military platforms when undertaking cyber assessments. In addition to scalability and managing complexity, Military Systems Automated Vulnerability Analysis needs to develop tools and approaches that provide repeatability, timeliness, accuracy and coverage in any cyber vulnerability analysis.

The position will collaborate on aligned research areas focusing on cyber terrain characterisation, cyber dependency mapping, and autonomous cyber red teaming.

Position Duties

- Undertake applied research in automating Cyber Vulnerability Analysis that may incorporate AI, Machine Learning and data science approaches.
- Conduct software development to prototype tools and techniques.
- Work closely with the Australian Defence Force to understand the requirements and opportunities for automating vulnerability analysis of cyber military systems and shape and conceive a work program supporting these requirements.
- Build constructive relationships with team members and stakeholders.
- Represent and communicate research to clients, visitors and other stakeholders.
- Build collaborations and relationships with Australian academia in the area of automated vulnerability analysis.

Other Requirements

A strong applied research track record in cyber security research and development.