HOW TO OPERATIONALISE AND MAINTAIN CYBER NETWORK SITUATIONAL AWARENESS?

Problem

In cyber network operations such as monitoring, triaging and penetration testing, decision-making is complex. Sensing and understanding the structure and behaviour of the network demands expertise across a diverse stack of applications, services and low-level communication network protocols. It is impractical to sense and generate telemetry at all points in the network, and detection avoidance and AAA services constrain information access and actions, leading to incomplete situational awareness. Scale and complexity make networks difficult for the human operator to interpret, so network knowledge must be presented at different, context-sensitive levels of abstraction. Network state is dynamic, demanding reactive sensing and response. Operations must continuously adapt based on intentions and a current state of knowledge.

Need and relevance to Defence

Providing network operators with tools to develop and maintain network situational awareness is essential for administering and securing defence's networks. In particular, network situational awareness facilitates preventative identification of potential vulnerabilities, deeper understanding of the consequences of network changes and faster response times in the event of network incidents.

Research questions

In a network management or operations task, how can network situational awareness (derived from a snapshot of network state) be maintained, enhanced, and leveraged to provide rapid decision support toward the operator's intent?

With an emphasis on network situational awareness with *missing or uncertain information*, work is solicited in one or more of the following themes:

- Modelling, analysis, and verification of network information and operations.
- Context-sensitive information acquisition, from network measurement or network device and traffic characterisation.
- Entity resolution and fusion.
- Context-sensitive presentation at multiple layers of abstraction.
- Robustness of the above to rapidly evolving configurations and technologies.

Expected outcomes

- Machine-readable, exchangeable and operable representations of network knowledge, operational concepts, plans and state, and uncertainty management.

- Software tooling that acts to maintain the best available network knowledge and recommend or (semi-) automate actions to sense and affect the network for operational objectives.