Developing a Cyber Threat Intelligence sharing platform for South African Organisations

Mr Muyowa Mutemwa
Mr Njabulo Mkhonto
Dr. Jabu Mtsweni

Abstract

Cyberattacks are on the increase in severity, complexity and frequency, negatively affecting the citizens, government, and businesses. Adversely, the security and Defence role-players in developing countries, such as South Africa, are short of the required capacity and capability to adequately defend and protect the national cyberspace against these fast moving and persistent threats and attacks. Be that as it may, the South African cyberspace still requires national attention and protection by the mandated role-players, such as the Defence force and its industry partners. Thus, within the cyber domain, the various Defence force role-players can no longer rely on traditional solutions to detect, defend, and respond to the forever changing cyber threats and cyberattacks. In order to reduce cybersecurity risks and strengthen cyber resilience of the nation, strategic cybersecurity information sharing in the Defence environment is becoming a necessity. Thus, the contribution from this paper is a systematic discussion and demonstration of a conceptual cyber threat intelligence sharing model and platform that could stimulate and enable different stakeholders within the Defence environment to seamlessly and collaboratively aggregate, analyse, and timely share contextual and actionable cyber-threat intelligence that could lead to a resilient cybersecurity posture and better protection of the national cyberspace.

Keywords— Threat Intelligence, Information Sharing, Cyberattacks, Cybercrime, Cyber Threats, Cyber Intelligence, Defence Force, Defence Industry, Military.