

Building an Integrated Cyber Defence Capability for African Missions

Mtsweni, Jabu S; Thaba, James M

Abstract

Cyberspace has been designated by organizations such as NATO as the fifth domain for battlespace, and many nations are already having and/or building their capabilities in the cyber defence environment in order to protect and defend their assets against any onslaught by their adversaries. It is a common belief that many African countries are not well positioned or prepared to respond effectively to cyberattacks against their citizens, critical infrastructure, and government. In many instances, the gap can be traced to the shortage of skills, lack of cybersecurity readiness and preparedness, and lack of investment in cybersecurity programmes, including policies within the military's strategic, tactical, and operational environments. This paper seeks to present a conceptual approach into how African countries could develop a resilient cyber defence capability in order to effectively respond to constant cyberattacks. The approach is underpinned by an integrated capability management philosophy using case studies in large and complex environments, including strategic and capability development learnings from other military domains outside the African continent. It is envisaged that the output of this paper may influence and support African states in building their cyber defence capabilities in a coordinated and integrated manner.