The Hague Centre for Strategic Studies
Stellenbosch University Iyunivesithi Universiteit
School for Data Science and Computational Thinking
ISikolo seNzululwazi ngeDatha neNgqiqo yokuBala
Skool vir Datawetenskap en Rekenaardenke
cair CENTRE FOR ARTIFICIAL INTELLIGENCE RESEARCH
Ministerie van Buitenlandse Zaken

Infrastructure Cyber Resilience

DataGr8® EFFICIENCY MADE VISIBLE

Introduction

African nations are increasingly reliant on digital infrastructure for economic, social, and governmental functions. This reliance makes cyber resilience – a system's ability to prepare for, respond to, and recover from cyber-attacks – a critical concern.

In this scenario assume you are advising a government agency responsible for national infrastructure. How can this agency develop and implement a strategy to protect critical infrastructure from cyber threats?

The following considerations should be brought to bear:

- Potentially unique challenges faced by African countries (for example risk concentration into of large single operator entities for NCI for e.g. national electricity companies, which create potential massive single point of failure.)
- Resource limitations to manage and mitigate cyber risk.
- Africa's rapidly evolving cyber threat landscape.
- The proliferation of threat actors in both the digital and physical spaces potentially acting in tandem.
- Is sufficient attention being paid to national crisis response architectures at state level within the region – and specifically to coordinate national responses to significant cyber events? How is this managed in other parts of the world?

Objective and key tasks

1. Examine successful models of cyber resilience from around the world, especially those implemented in environments with similar challenges.
2. Identify the key components that make these models successful and applicable to the African context.
3. Propose a detailed strategy that includes not only technological solutions but also emphasizes the importance of public-private partnerships, workforce development in cyber security, and international cooperation.
4. Your proposal should outline a multi-layered approach that addresses prevention, detection, response, and recovery from cyber incidents, with specific recommendations for each aspect.
5. **April 16th, 12:00PM SAST is the deadline for you to hand in a video of max. 3min** to cyberschool@hcss.nl, in which you explain your Challenge solution and proposal. This is the **final submission moment** and from this submission, a Challenge-winning team will be determined. More information on this will be communicated via email.

Contributor

DataGr8 is a South African-based company that provides services to customers across Africa. At DataGr8, data is in our name. We started with Email and File Data Archiving in 2009, then moved into unstructured and SAP migration. We have taken our focus on data and looked at the future of data and transformed DataGr8 into a company that provides technology and services, looking at the future but not forgetting that traditional data is still around. We believe that the future is Cloud and 4IR. Today DataGr8 offers services to store, backup, secure, migrate and orchestrate data, whether it comes from IT or IoT. At DataGr8, we offer backup and cyber security solutions through our E-commerce platform. We take pride in helping organizations of all sizes to secure and back up their valuable data, without compromising on quality or affordability.