

## **Annex**

### **Factsheet on the CSA Cyber Forensics Laboratory**

The CSA Cyber Forensics Laboratory is set up to support CSA's operational role in investigating and responding to cyber incidents that affect Critical Information Infrastructure (CII) sectors and cyber incidents of national significance.

Occupying a total floor space of 370 square metres, the Cyber Forensics Laboratory comprises multiple specialised areas and supports concurrent investigations for multiple cyber incidents during emergencies. Capabilities within the Laboratory fall into a few categories:

#### Evidence Collection and Preservation

- Forensic acquisition tools and case exhibit inventory system
- Onsite triage kits to perform rapid on-site response to cyber incidents
- Room with enhanced security for storing case exhibits

#### Digital Forensics

- Software applications that aid forensic analysts in performing in-depth analysis of system artefacts

#### Log Analysis

- Infrastructure to support analysis of network and system logs which could hold information regarding cyber incidents under investigation

#### Mobile Forensics

- Tools to perform forensic acquisition and analysis of mobile devices

#### Malware Analysis

- Tools that help malware analysts carry out in-depth analysis of malicious files so as to determine mitigation measures.

The Cyber Forensics Laboratory can accommodate up to 80 analysts working concurrently on multiple cyber incidents.