Implementation Strategy for Cybersecurity

Workshop ITU 2016

Council for Scientific and Industrial Research

Joey Jansen van Vuuren

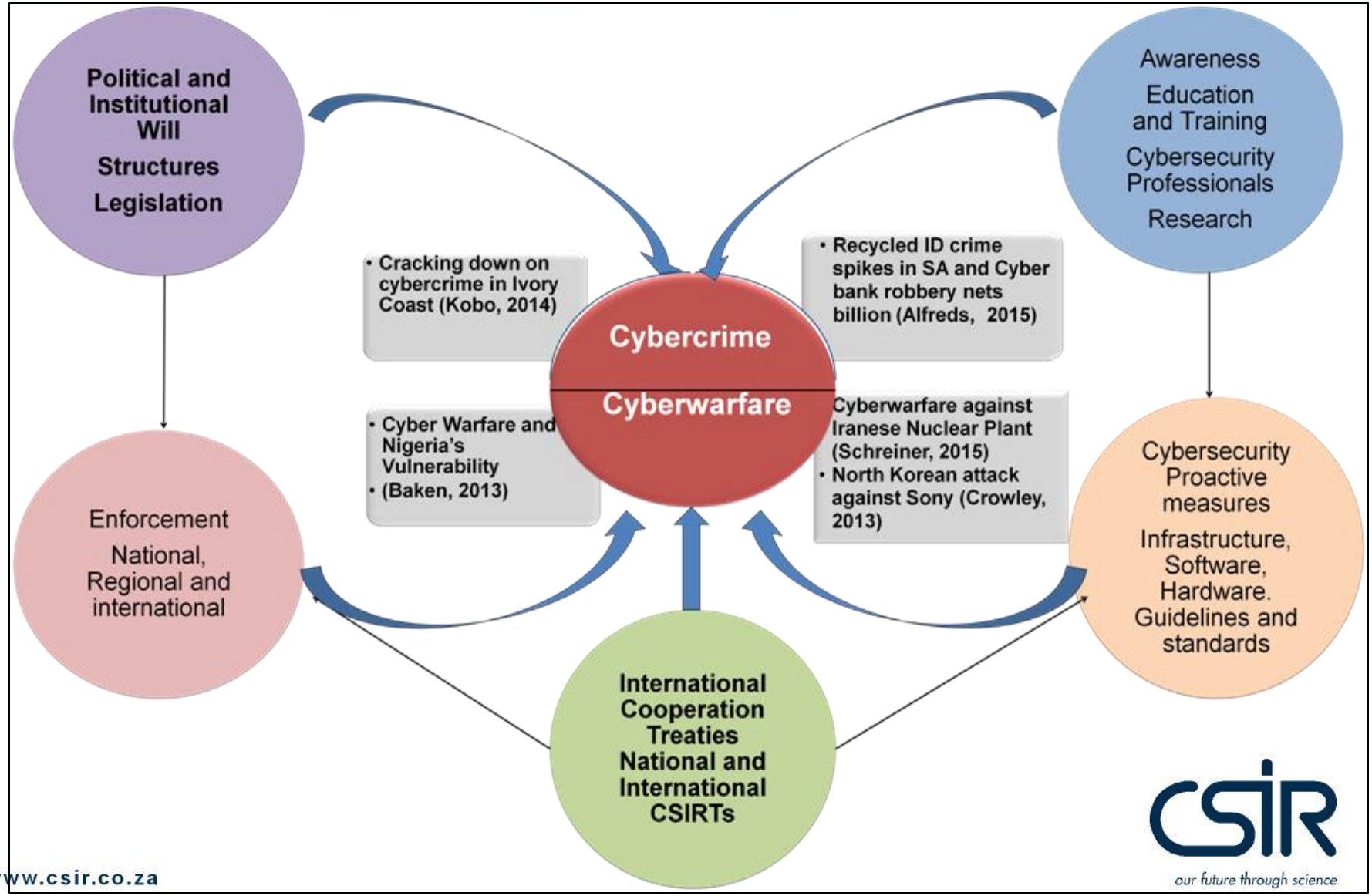
CSIR

our future through science

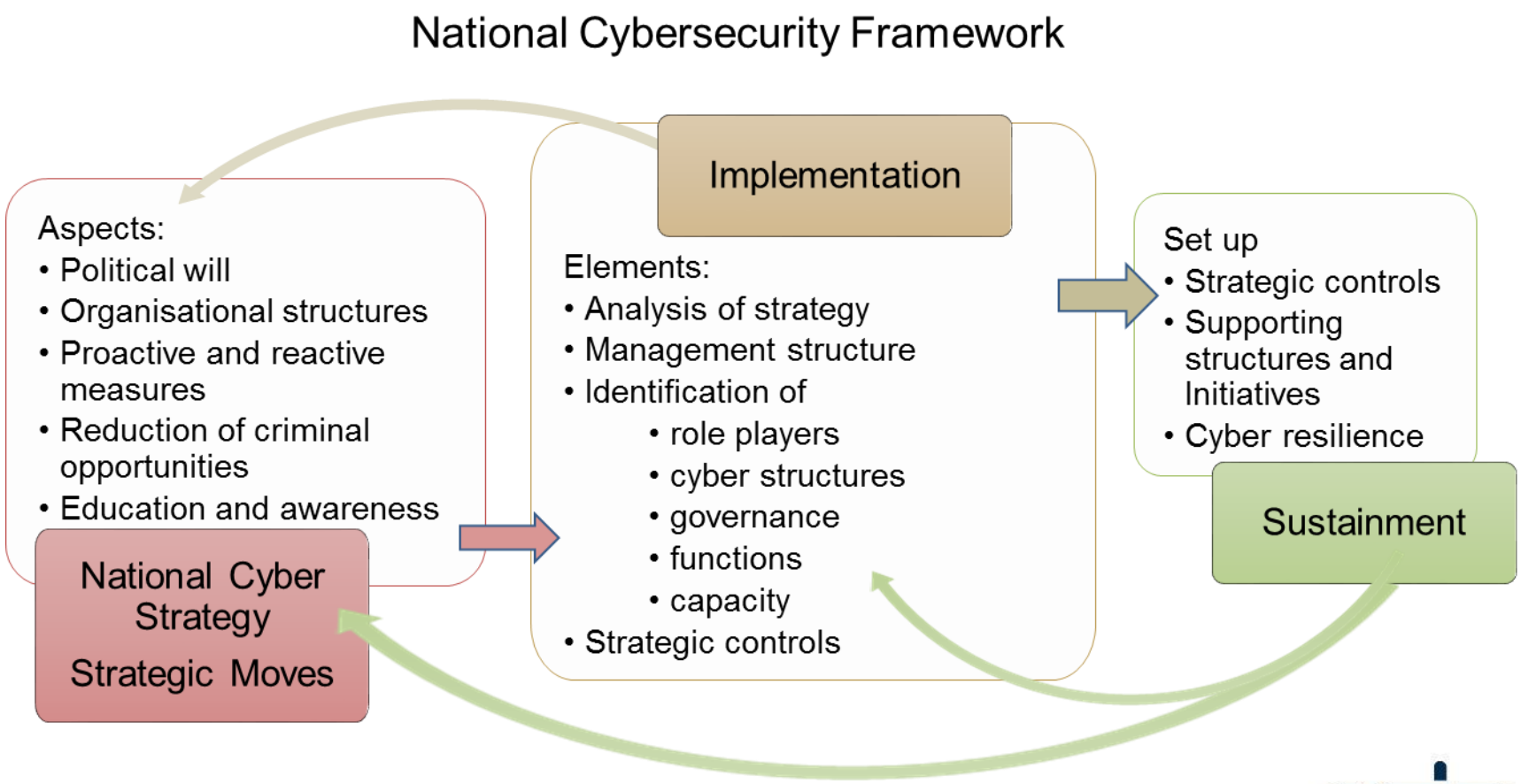
Intricacies and interdependencies cyber policies must address

- *potential attacks by individuals*
- *organised crime*
- *terrorism*
- *aggressive nations seeking to involve themselves in the internal affairs of another country with the aim of cause irreparable harm to its economy or political structures*

Elements



National Cybersecurity Implementation Framework



Cybersecurity Approach and Culture

- *Political will*
- *Adapted organisational structures*
- *Identification of accurate proactive and reactive measures*
- *Reducing criminal opportunities*
- *Education and awareness*

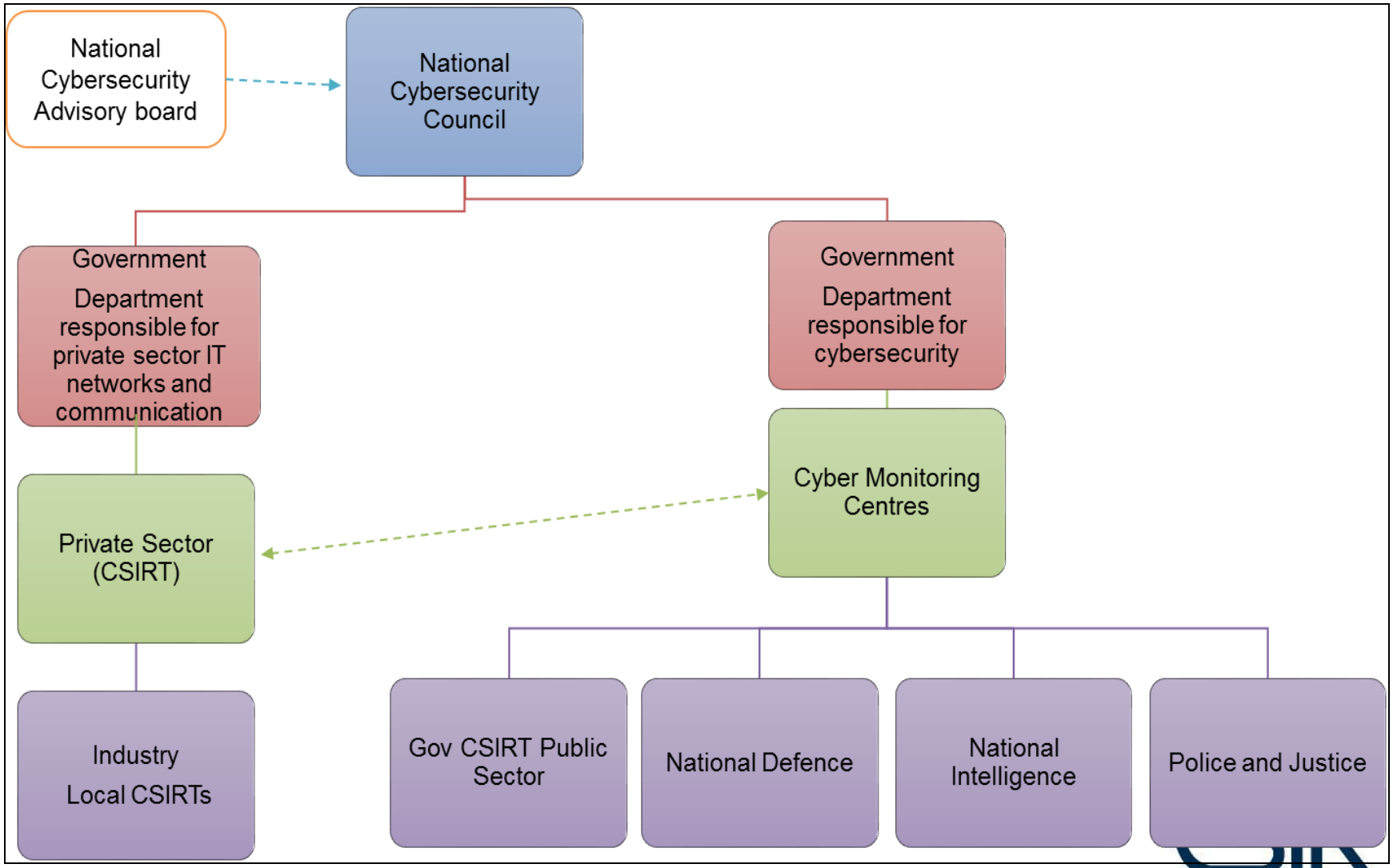
(Ghernouti-Hélie)

Implementation process

- *Do a detailed analysis of the policy strategy in manageable, comprehensible parts.*
- *Develop the governance structures responsible for the implementation of the strategy.*
- *Design strategic moves to achieve the identified strategic goals.*

(Otoom)

Proposed African Structure



Strategic Moves and Controls (1)

- ***Cybersecurity contingency plans*** that will include the national response capability and contingency plans.
- ***Cybersecurity exercises*** are used to assess the preparedness of a community for technology failures and emergencies.
- ***Baseline security requirements*** are developed in consultation with security partners.
- ***Vision, scope, objectives and priorities established using the assessment of objectives of the strategy*** that is used to evaluate and update the action plan due to operational environment changes.
- *A* ***national risk assessment approach*** ensure that all government bodies identify and monitor most significant emergencies regarding cybersecurity that citizens could face**.**

Strategic Moves and Controls (2)

- ***Evaluation of existing laws and policies*** to determine gaps in the governance models of cybersecurity.
- ***Development of governance structures*** including command, control and communication
- ***Engagement of stakeholders*** includes the identification and involvement of these stakeholders.
- *E****stablishment of information sharing platforms and mechanisms*** include the level of utilisation, actions taken based on analysis of data collected, parties involved and incidents, threats and vulnerabilities identified.

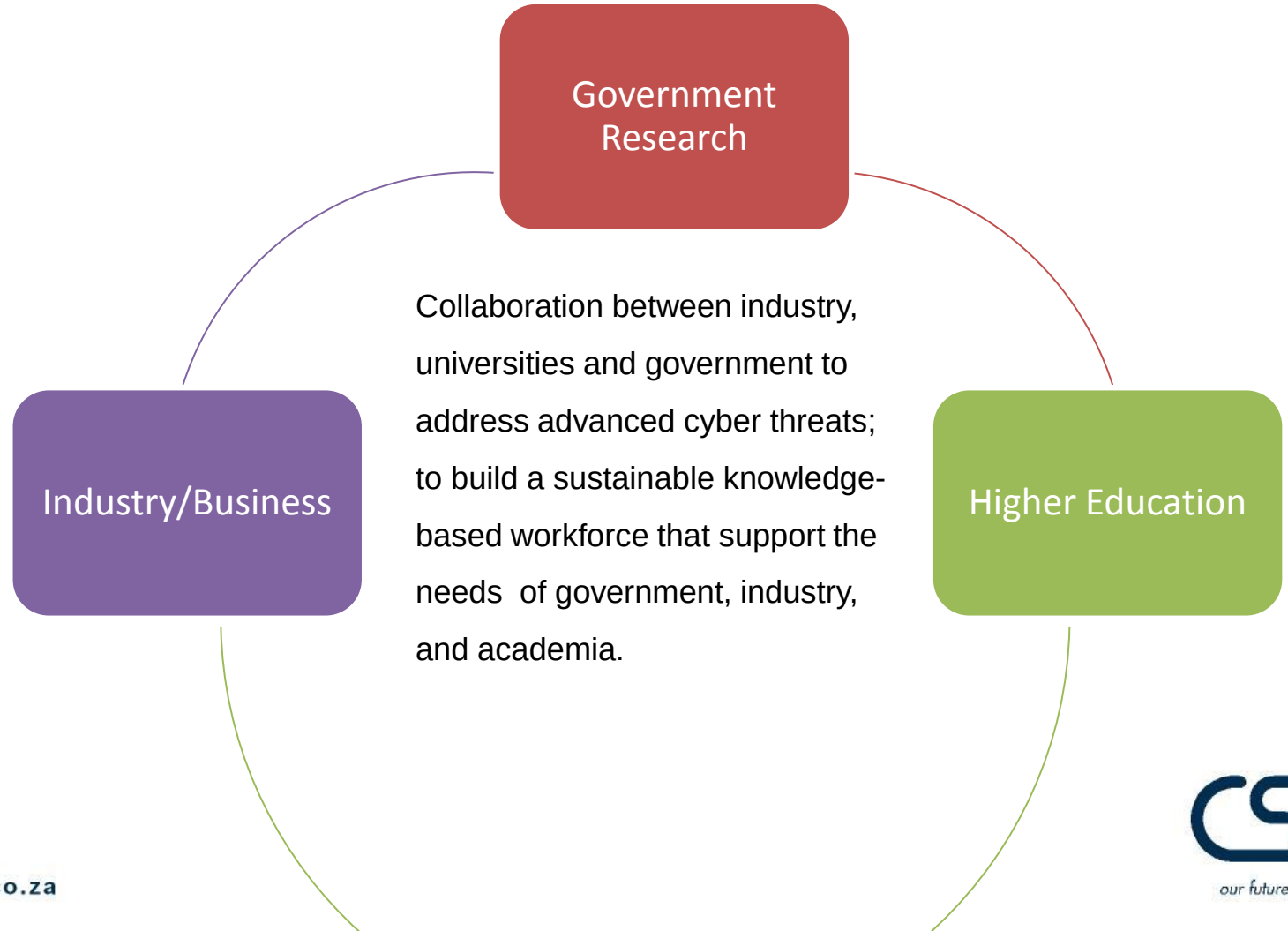
Goche and Gouveia

Resilience program

- Definition of risks that goes beyond compliance and identifies the measures that should to be in place if a cyberattack is made.
- Development of a security policy that focuses on the threats to secure assets. This includes people, processes, and technology that are connected to, or have access to those assets.
- Compilation of a cyber-recovery plan in the case of a cyberattack.
- Emergency exercises on a regular basis and testing of recovery plans to ensure that cyber resilience is in place in case the environment changes.

ENISA

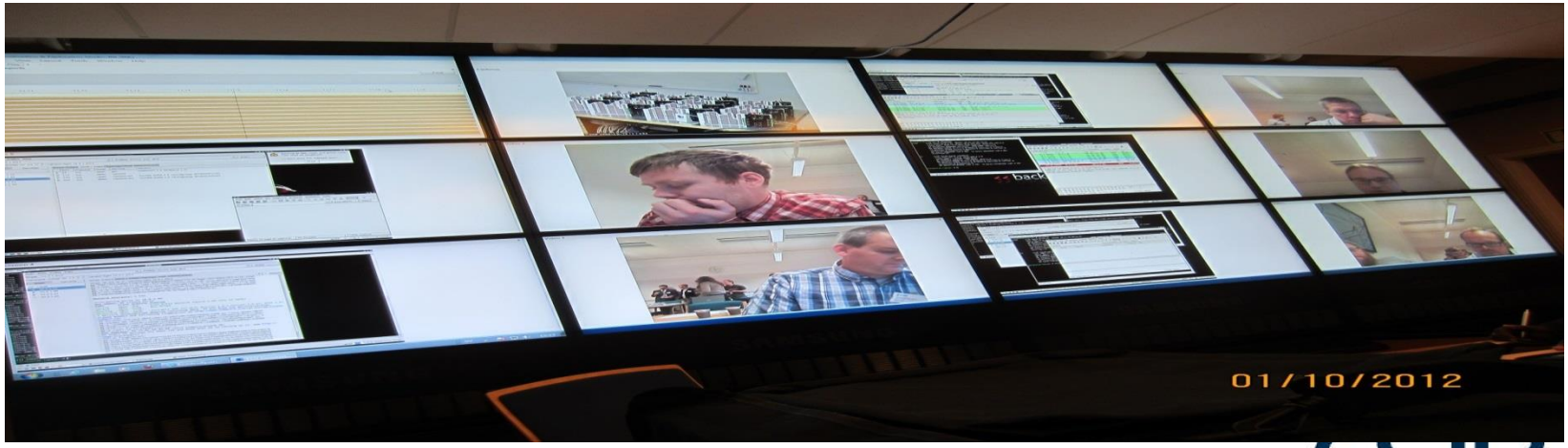
Cybersecurity Centre for Innovation



Collaboration between industry, universities and government to address advanced cyber threats; to build a sustainable knowledge-based workforce that support the needs of government, industry, and academia.

Cybersecurity Centre of Innovation

- Centre must be a world-class centre designed for cyber research and development, customer and partner collaboration and innovation.
- Centre must be fully equipped for live cyber technology exercises and demonstrations required by industry;
- Centre must be the able to do safe testing in both simulated & real world environment for development of integrated cyber solutions.



Cybersecurity Centre of Innovation

Functions:

- Coordination of collaboration to bring together expert practitioners and researchers to conduct threat analysis and share best practices under a Non-Disclosure Agreement including technical exchange meetings that can build personal relationships among front-line cyber operations staff.
- Launch of a secure Cybersecurity Web Portal to enhance information-sharing and access to key data.
- Develop R&D solutions to improve cyber defences and address cyber security gaps.
- Expand education opportunities for pipeline in the cyber security field.
- Develop new Qualifications and Certifications

Key Activities

Information Sharing

- Identify new threat indicators
- Share best practices
- Build cross sector networks and personal relations
- Technical exchange meetings
- Web portal
- (Non disclosure Agreement)

Education

- Development of a knowledgeable cyber workforce
- Availability of bursaries, internships and studentships
- Formal qualifications
- Awareness
- Cyber exercises

Research & Development

- Innovative cyber solutions
- Research chairs
- Support for policy development and legislation
- Save testing in real and simulated environments for integrated cyber solutions
- Funded by Government, Industry and NRF

Exchange Platform

- Provides a single cyber threat intelligence repository
- Leverage collective intelligence of the security community
- Turn volumes of raw data into actionable intelligence

The Platform

- Data visualisation & analysis tools

Education

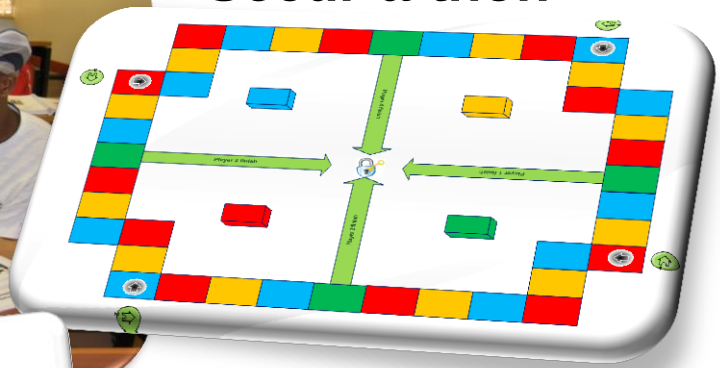
- Build a Cybersecurity pipeline and cultivate a knowledge-based workforce in the Cyber domain.
- Availability of bursaries, internships and studentships sponsored by industry and government.
- Use new educational approaches e.g. online training and collaborative environments into cyber security education.
- Create a standardised and comprehensive training and development program to grow and retain existing Cybersecurity workforce.
- Create and implement standards of performance through a professional certification system
- Courses to citizens on Cybersecurity Awareness
- Subject e.g. Cyber Science in Schools
- Curriculate new university courses pre and post graduate.

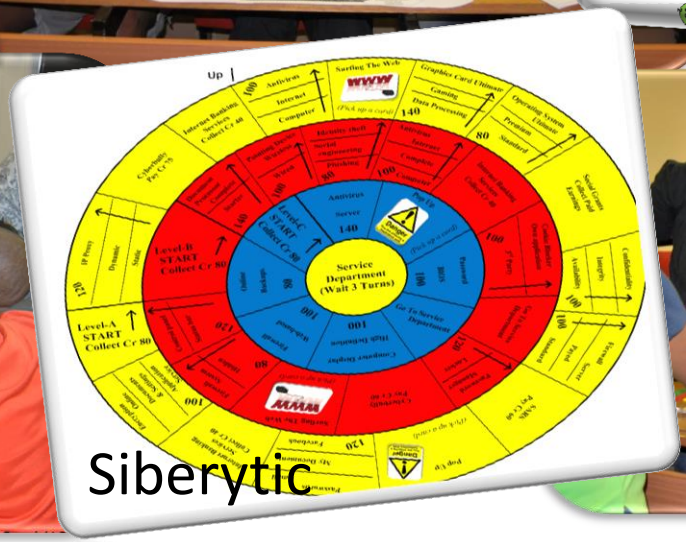
Education Qualifications

- Currently Information Security done mostly by short courses, or specialisation in Masters Degrees
- Build a Cybersecurity pipeline through academic institutions nationwide and with other key partners.
- Launch new technology degrees geared toward cultivating a knowledge-based workforce in the Cyber domain.
  - Certificate in Cybersecurity Awareness at Colleges (For workforce and citizens)
  - Diploma in Cybersecurity catering for Operators of Security Operation Centres and Network Operation Centresh
  - Cybersecurity degrees (3 years)
  - Cyber Engineering a four-year undergraduate degree that is best described as the marriage of Computer Science (CS) and Electrical Engineering (EE) applied to the cyberspace domain.
  - Post graduate Diploma in Cybersecurity (workforce)
  - Masters Degree in Cybersecurity

Games

Secur-a-thon



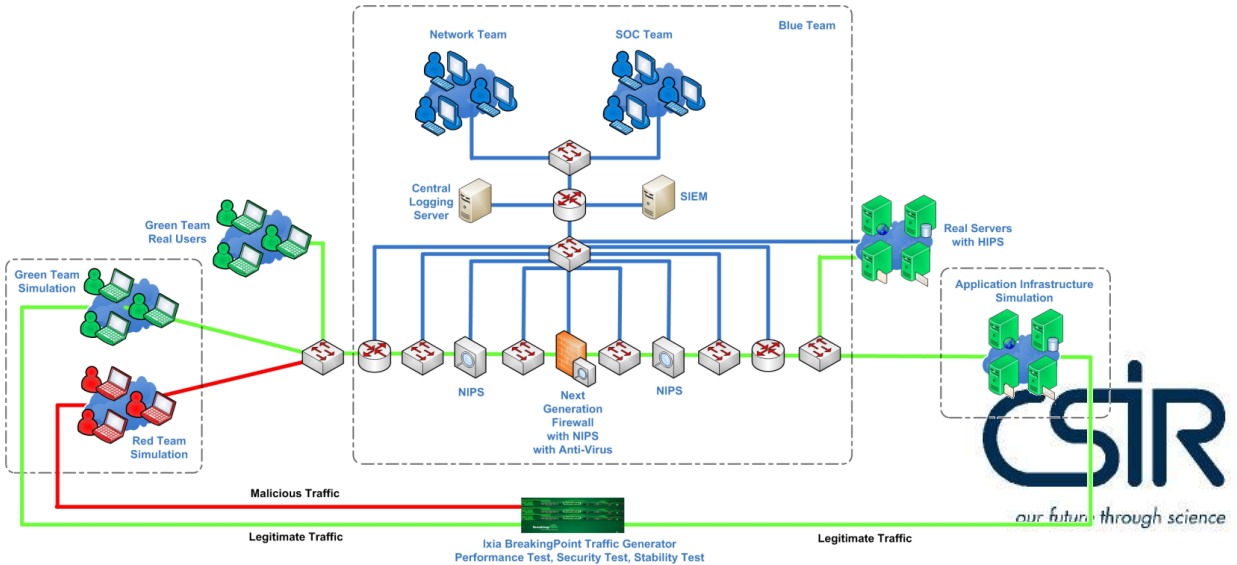


Siberytic

Training the Cybersecurity Workforce

Internet simulation platform to do

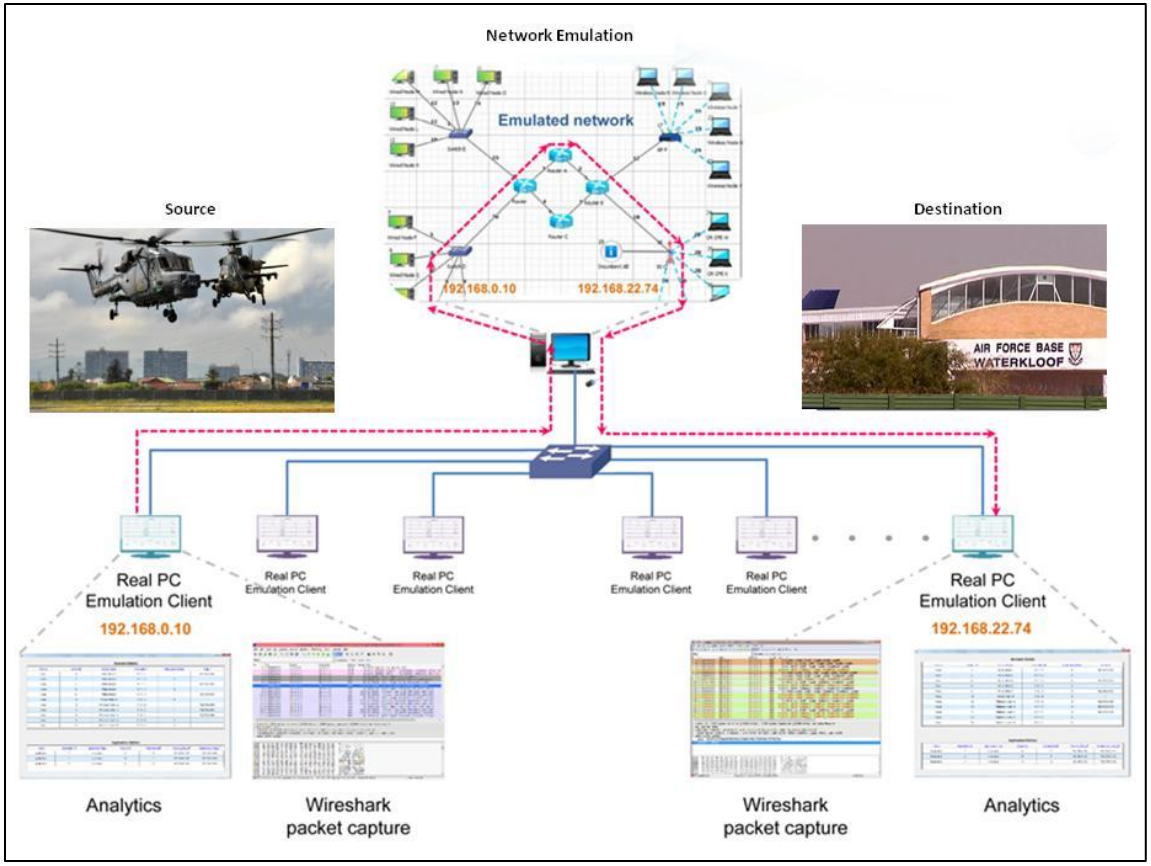
- Custom training scenario construction
- Real-time integration of users in network
- Rehearse and improve cybersecurity skills
- Real-time visualisation, management & control over training scenario



Cybersecurity Research in CCOI

- Create cybersecurity research groups
  - Identification of research staff and study leaders.
  - Identification of students.
  - Seed funding.
  - Workshops for technical training of new research groups.
  - Collaboration between institutions in geographical area.
  - Collaboration with industry.
- Scholarship and bursaries must be available to students.

Testing Facilities for Cybersecurity devices



Internet Simulator is a test range:

- Emulates realistic networking environments
- Networking technologies are tested and analysed
- Hardware is performance tested and analysed (DMZ Project)
- Before it is used in an organisation's networking infrastructure

It is also used to train the cyber-warriors and develop cyber tools to keep networks secure.

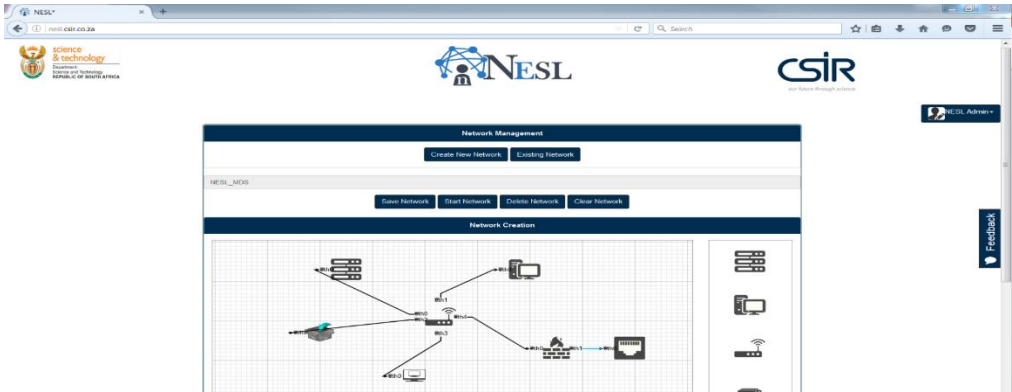
Network Emulation and Simulation laboratory (NESL)

- Security & networks research platform with high throughput rates and malware.
- (Web Based Internet Simulator) for Collaborative R D & I
- Supports:
  - Device verification and product testing.
  - Network evaluation
    - Hardware
    - Software
    - Runtime behaviour
  - Network security training and cyber exercises.
  - Industry collaborative research and product testing.

CSIR
our future through science

Capabilities

- Aims to assist researchers by providing a platform to conduct security research.
- Can emulate network nodes and simulate network traffic.
- Can provide the following capabilities:
  - Validation of a network and device configuration (hardware in the loop).
  - Conducting network performance testing.
  - Perform penetration testing and other security tests without exposing real network.
  - Testing of custom built security applications.
  - Provide a platform to conduct user training on networking and security fundamentals.
- Accessible through a web browser



Industry Collaboration

- Contacts to be made with Industry partners
- First negotiations for cybersecurity patent.

Thank You

jjvvuuren@csir.co.za

CSIR

our future through science