CYBER DEFENCE STRATEGY

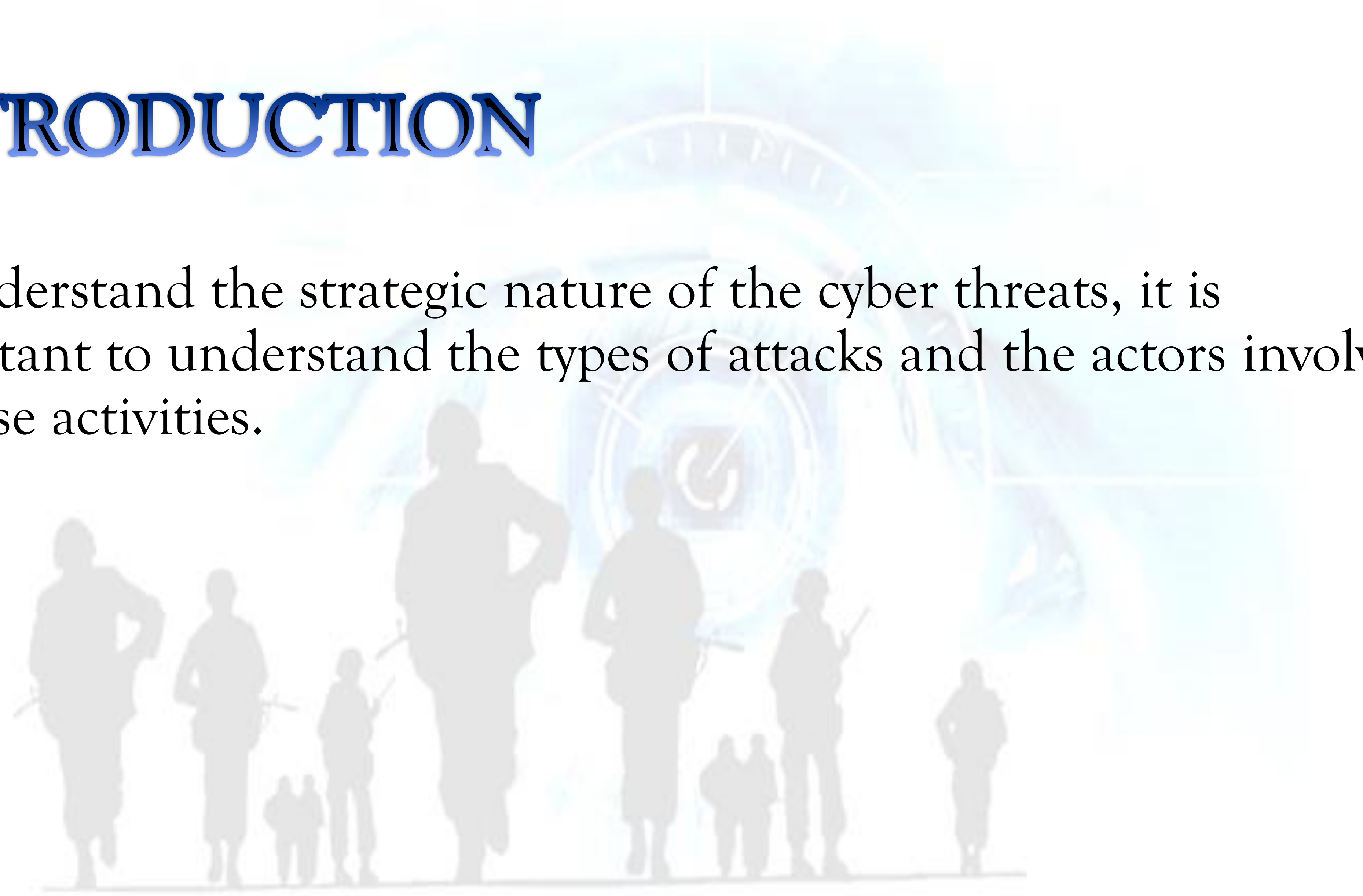
Presented by
Maj Gen B. Ngcobo

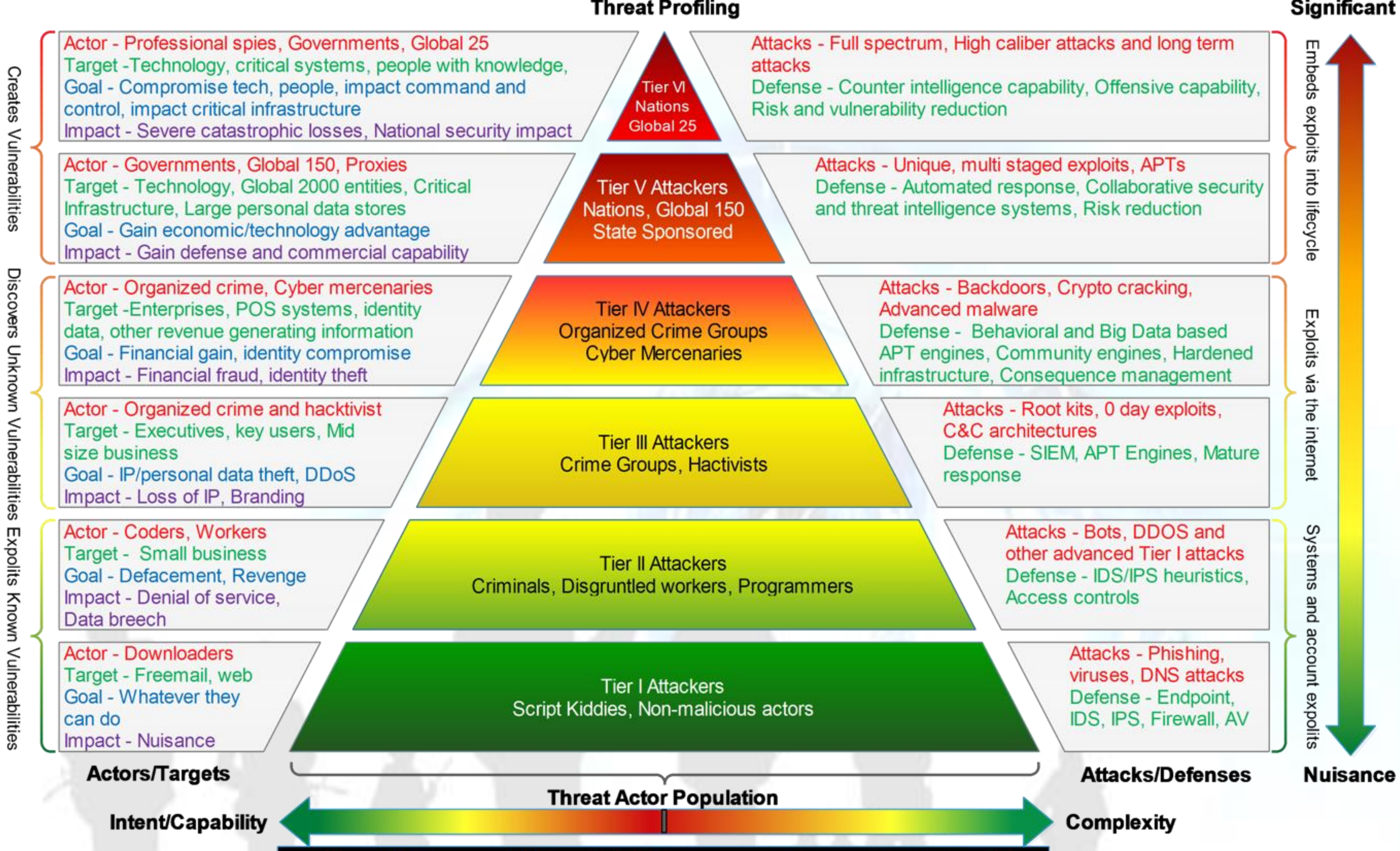
Cyber Command
SANDF Defence Intelligence

d
e Intelligence

INTRODUCTION

To understand the strategic nature of the cyber threats, it is important to understand the types of attacks and the actors involved in these activities.





Threat Profiling

Significant

Tier VI Nations Global 25

Actor - Professional spies, Governments, Global 25
Target -Technology, critical systems, people with knowledge,
Goal - Compromise tech, people, impact command and control, impact critical infrastructure
Impact - Severe catastrophic losses, National security impact

Attacks - Full spectrum, High caliber attacks and long term attacks
Defense - Counter intelligence capability, Offensive capability, Risk and vulnerability reduction

Tier V Attackers Nations, Global 150 State Sponsored

Actor - Governments, Global 150, Proxies
Target - Technology, Global 2000 entities, Critical Infrastructure, Large personal data stores
Goal - Gain economic/technology advantage
Impact - Gain defense and commercial capability

Attacks - Unique, multi staged exploits, APTs
Defense - Automated response, Collaborative security and threat intelligence systems, Risk reduction

Tier IV Attackers Organized Crime Groups Cyber Mercenaries

Actor - Organized crime, Cyber mercenaries
Target -Enterprises, POS systems, identity data, other revenue generating information
Goal - Financial gain, identity compromise
Impact - Financial fraud, identity theft

Attacks - Backdoors, Crypto cracking, Advanced malware
Defense - Behavioral and Big Data based APT engines, Community engines, Hardened infrastructure, Consequence management

Tier III Attackers Crime Groups, Hactivists

Actor - Organized crime and hacktivist
Target - Executives, key users, Mid size business
Goal - IP/personal data theft, DDoS
Impact - Loss of IP, Branding

Attacks - Root kits, 0 day exploits, C&C architectures
Defense - SIEM, APT Engines, Mature response

Tier II Attackers Criminals, Disgruntled workers, Programmers

Actor - Coders, Workers
Target - Small business
Goal - Defacement, Revenge
Impact - Denial of service, Data breech

Attacks - Bots, DDOS and other advanced Tier I attacks
Defense - IDS/IPS heuristics, Access controls

Tier I Attackers Script Kiddies, Non-malicious actors

Actor - Downloaders
Target - Freemail, web
Goal - Whatever they can do
Impact - Nuisance

Attacks - Phishing, viruses, DNS attacks
Defense - Endpoint, IDS, IPS, Firewall, AV

Creates Vulnerabilities

Discovers Unknown Vulnerabilities Exploits Known Vulnerabilities

Embeds exploits into lifecycle

Exploits via the internet

Systems and account exploits

Actors/Targets

Attacks/Defenses

Nuisance

Threat Actor Population

Intent/Capability

Complexity

Commitment	Intensity	Low	Medium	High	Fanatical	Multiple, Scopes	Multiple, Multiple Sources	Multiple, Single Source	One	Components	
	Timing Sensitivity	Days	Weeks	Months	Years						
	Stealthiness	Noisy			Undetectable						
Capability	Personnel	Ones	Tens	Tens of Tens	Hundreds	High	Medium	Low	Low	Funding (Impact)	Multipliers
	Knowledge	Limited	General	Specialized	Multi Scope	High	Medium	Low	NA	Assets	
	Access	None	Through Others	Indirect	Direct	Low	Medium	Low	NA	Technology	

Cyber Command
Defence Intelligence Division
Department of Defence

AIM

To present the Cyber Defence Strategy.

SCOPE

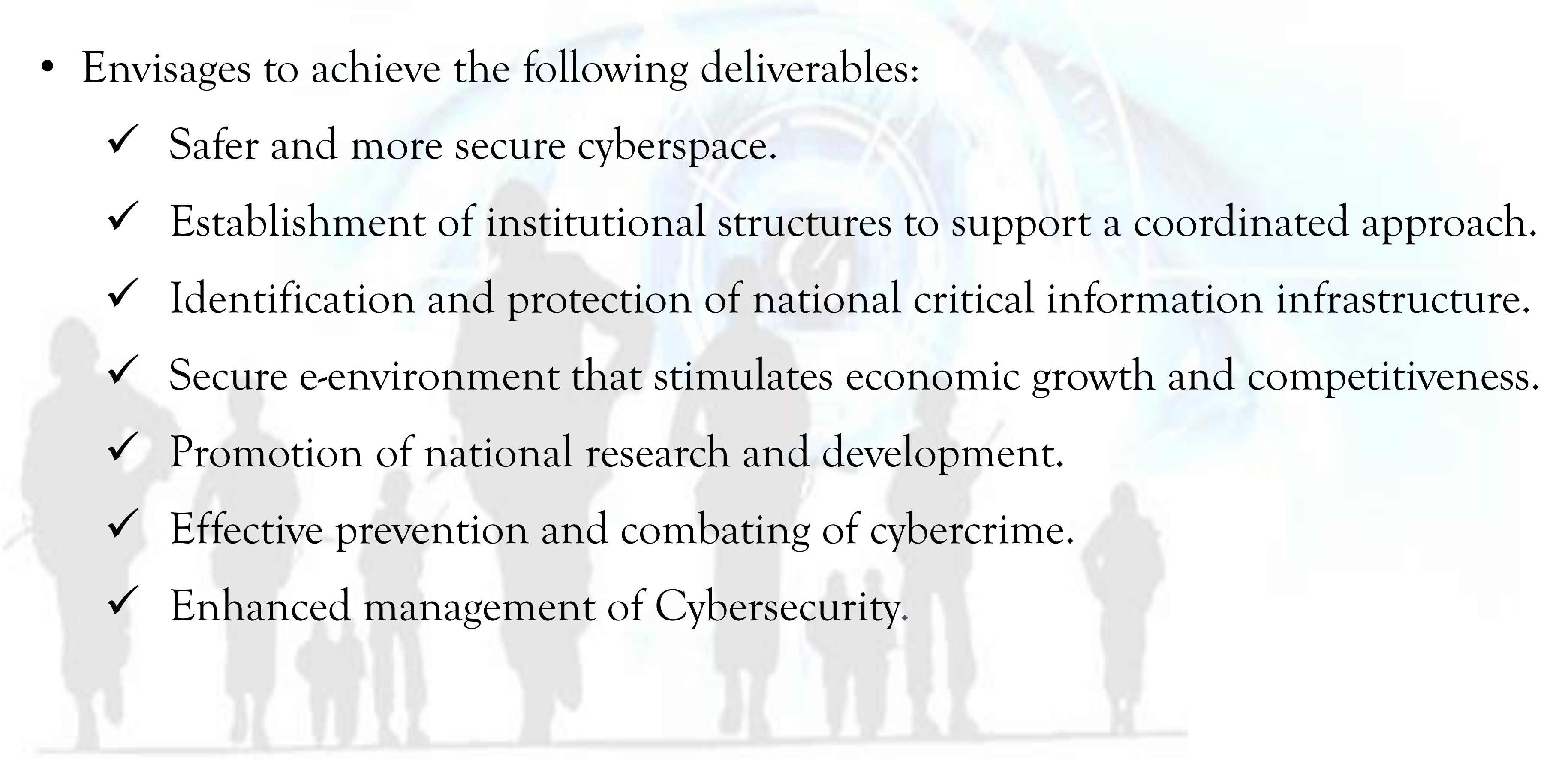
- National Cybersecurity Policy Framework
- Cybercrimes and Cybersecurity Bill
- Current Status
- Elements of Strategy
- Strategic Positioning -> Good To Great

NATIONAL CYBERSECURITY POLICY FRAMEWORK

- Cabinet approval of the NCPF – 07 March 2012
  - Cyber Warfare
    - 13.1 “In order to protect its interests in the event of a cyber-war, **a cyber defence capacity has to be built**. The NCPF thus promotes that a Cyber Defence Strategy, that is informed by the National Security Strategy of South Africa, be developed, guided by the JCPS Cybersecurity Response Committee”. (page 24)

    - 16.5 “The Department of Defence and Military Veterans (DOD&MV) **has overall responsibility** for coordination, accountability **and implementation of cyber defence measures in the Republic** as an integral part of its National defence mandate. To this end, the Department will develop policies and strategies pursuant to its core mandate.

NATIONAL CYBERSECURITY POLICY FRAMEWORK



- Envisages to achieve the following deliverables:
  - ✓ Safer and more secure cyberspace.
  - ✓ Establishment of institutional structures to support a coordinated approach.
  - ✓ Identification and protection of national critical information infrastructure.
  - ✓ Secure e-environment that stimulates economic growth and competitiveness.
  - ✓ Promotion of national research and development.
  - ✓ Effective prevention and combating of cybercrime.
  - ✓ Enhanced management of Cybersecurity.

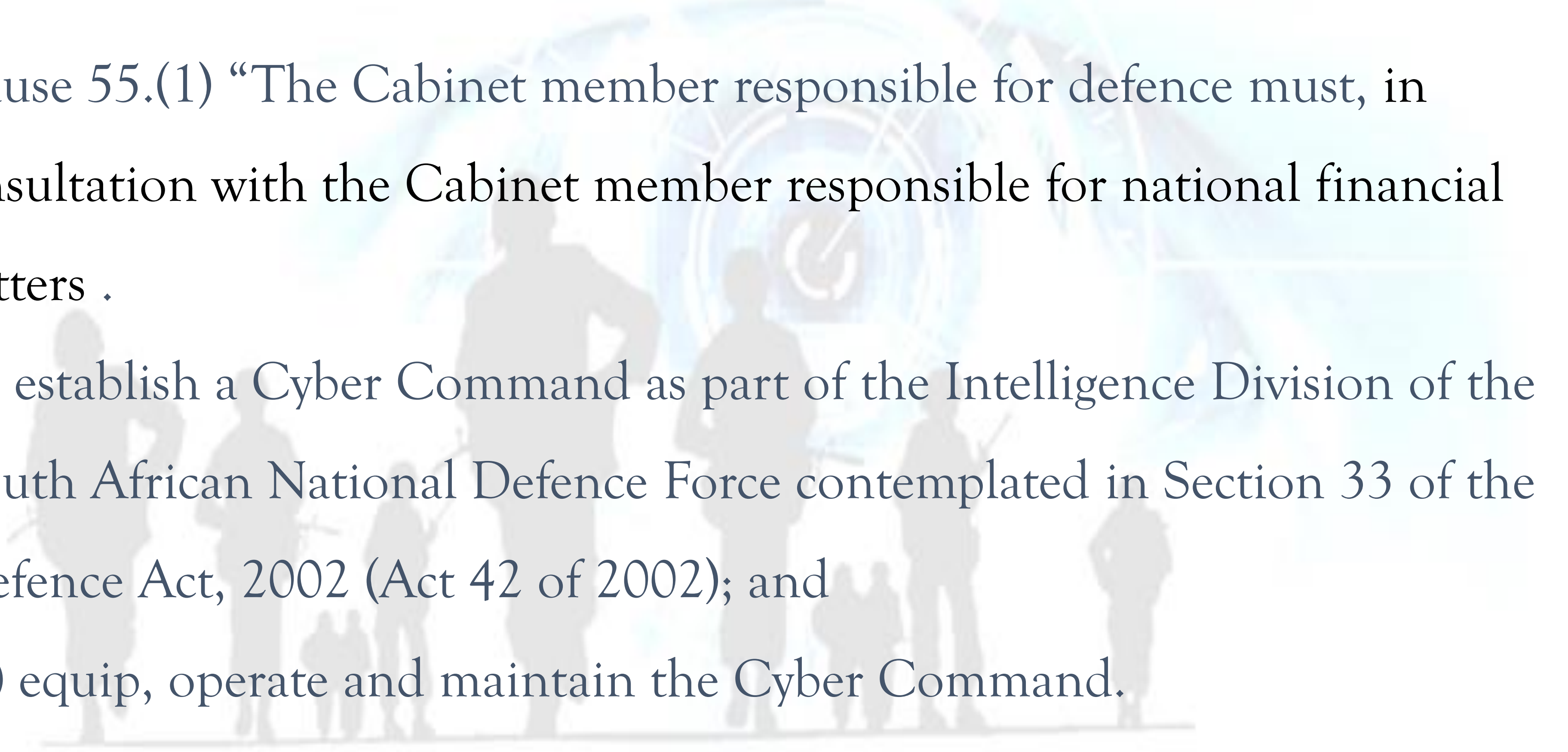
CYBERCRIMES AND CYBERSECURITY BILL (2015)

- **CHAPTER 10: STRUCTURES TO DEAL WITH CYBERSECURITY [54 (3) (a) (i-ii)]**
  - ✓ Establish and maintain a **cyber offensive** and **defensive** capacity as part of the defence mandate of the South African National Defence Force;
  - ✓ Co-operation with any **institution of higher learning**, in the Republic or elsewhere;
  - ✓ Develop and implement **accredited training programs** for members of the South African National Defence Force.

DEPARTMENT OF DEFENCE MANDATE

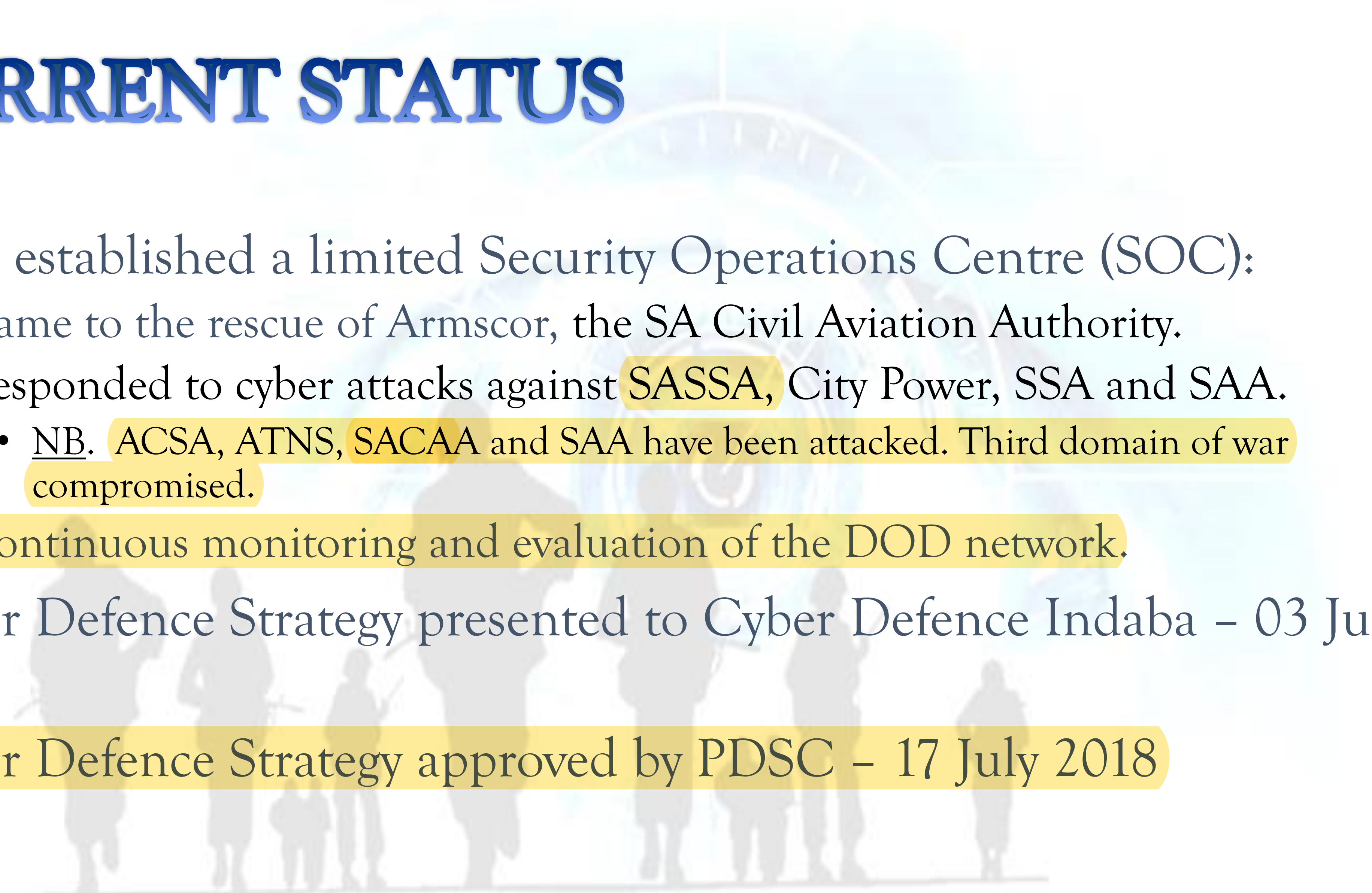
- Establish a unified Cyber Command to protect **National Critical Information Infrastructure** (**NCII**).
- Lead the effort to establish **cybersecurity capabilities** that will encounter current scourge of cyber-attacks.
- Protect South African National Defence Force (SANDF) against **malicious actors in cyberspace**.

CYBERCRIME AND CYBERSECURITY BILL (2015)



- Clause 55.(1) “The Cabinet member responsible for defence must, in consultation with the Cabinet member responsible for national financial matters .
- (a) establish a Cyber Command as part of the Intelligence Division of the South African National Defence Force contemplated in Section 33 of the Defence Act, 2002 (Act 42 of 2002); and
- (b) equip, operate and maintain the Cyber Command.
- This section has been omitted in the latest version.

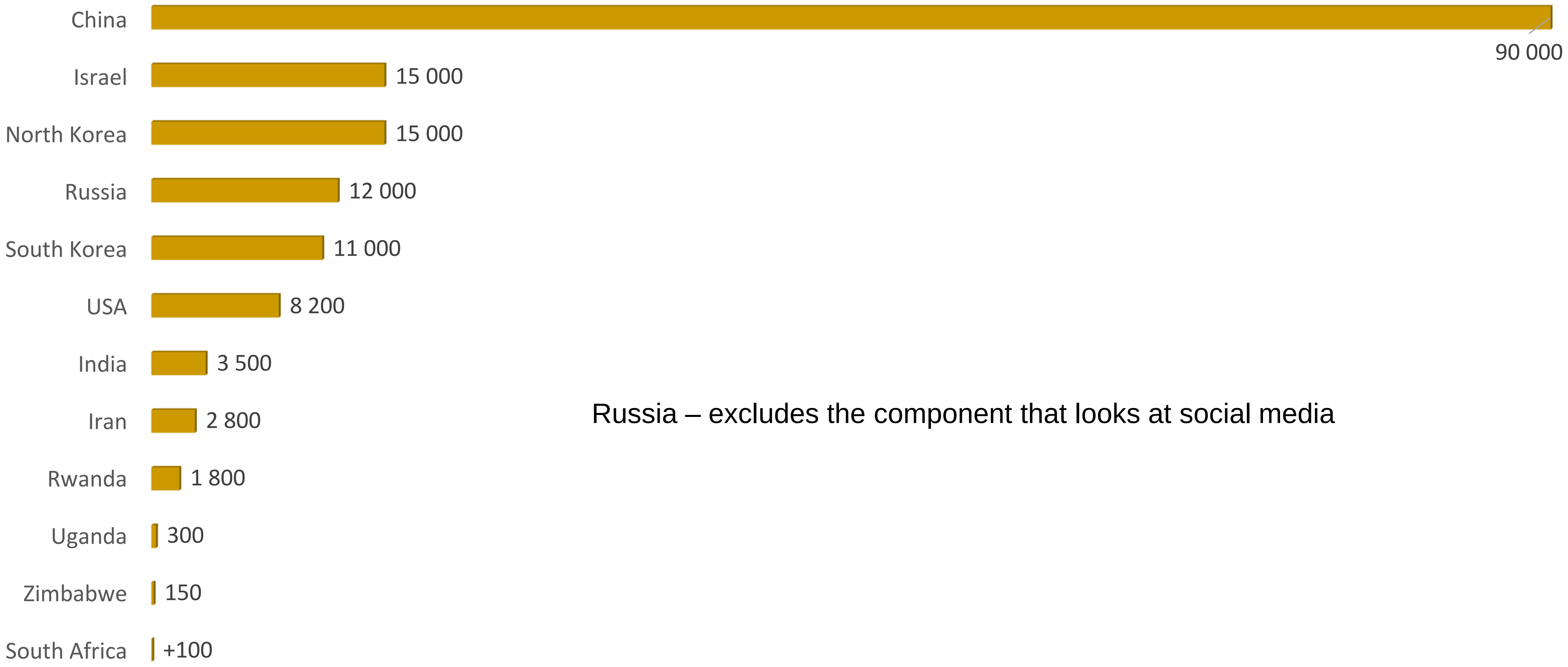
CURRENT STATUS



- Have established a limited Security Operations Centre (SOC):
  - Came to the rescue of Armscor, the SA Civil Aviation Authority.
  - Responded to cyber attacks against SASSA, City Power, SSA and SAA.
    - NB. ACSA, ATNS, SACAA and SAA have been attacked. Third domain of war compromised.
  - Continuous monitoring and evaluation of the DOD network.
- Cyber Defence Strategy presented to Cyber Defence Indaba – 03 July 2018
- Cyber Defence Strategy approved by PDSC – 17 July 2018

GLOBAL COMPARISONS (estimates)

CYBER COMMAND – SERVING WITH HONOUR



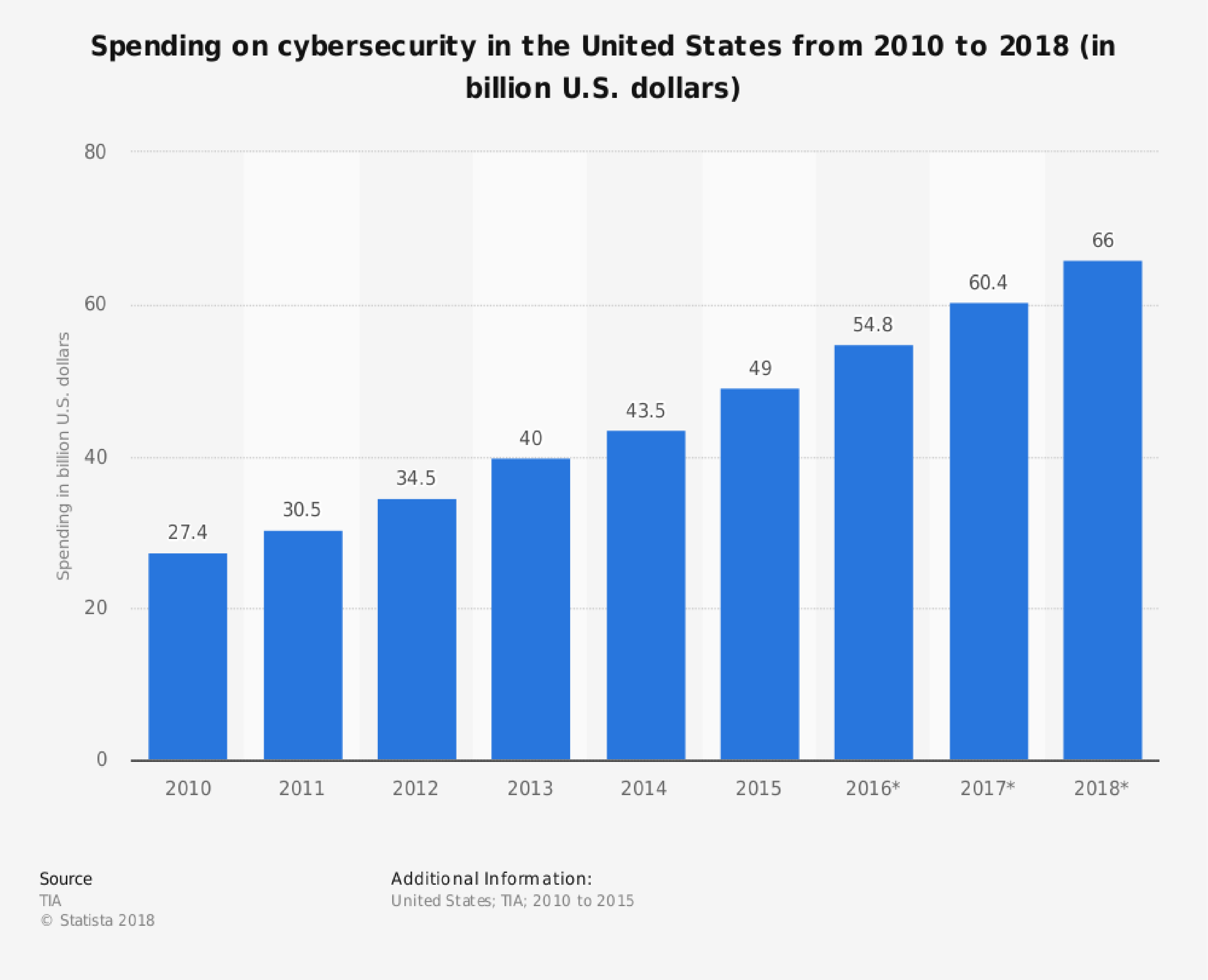
Russia – excludes the component that looks at social media

GLOBAL COMPARISONS (estimates)

CYBER COMMAND – SERVING WITH HONOUR

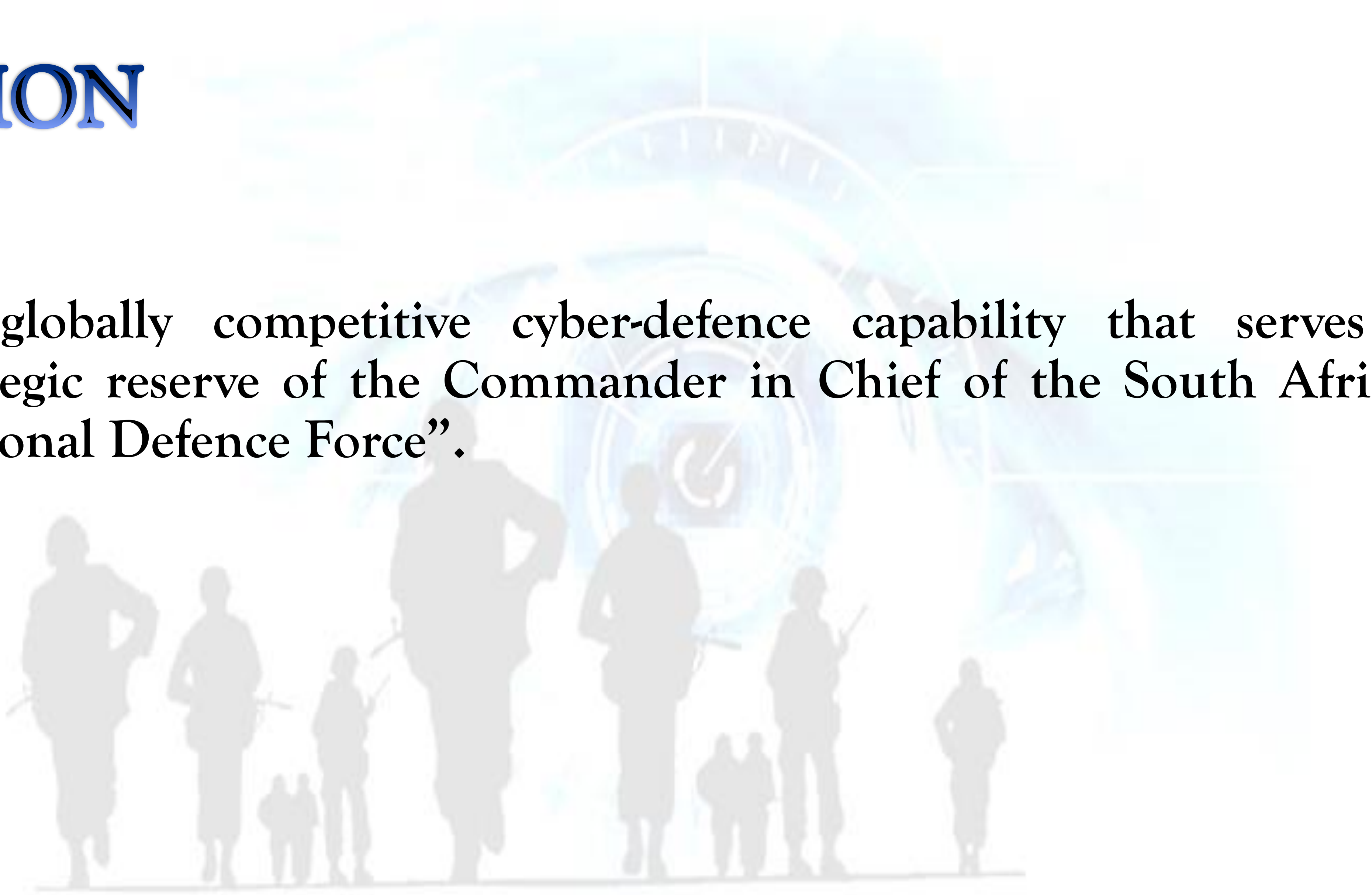
Country	Year	Cyber Spend (USD)
USA	2010	$27,400,000,000
USA	2011	$30,500,000,000
USA	2012	$35,000,000,000
USA	2013	$40,000,000,000
USA	2014	$43,050,000,000
USA	2015	$49,000,000,000
USA	2016	$55,000,000,000
USA	2017	$60,000,000,000
USA	2018	$66,000,000,000

(Source TIA Statista 2018)



VISION

“A globally competitive cyber-defence capability that serves as strategic reserve of the Commander in Chief of the South African National Defence Force”.



MISSION AND END STATE

- **Mission**

  To maintain a safe, secure and resilient NCII and DOD C^{4}I^{3}RS capability whilst pursuing a state of cyber sovereignty.

- **Desired End State**

  The RSA's NCII is insulated from cyber attacks and all major cyber threats against the DOD's C^{4}I^{3}RS have been neutralised through sovereign and indigenised technology manned by a highly skilled human resource component that is a thought leader on matters of cyber defence nationally and globally.

PHILOSOPHY

- A resilient Cyber Defence capability developed through a meticulous process of recruitment and training of highly skilled and patriotic Cyber Workforce, guided by a visionary leadership as well as high levels of innovation, research and development of cutting edge sovereign technologies.

VALUES

- Adaptability. Ability to cope with new cyber threats.
- Patriotism. The Cyber Workforce serves the country with unwavering loyalty and commitment.
- Agility. Ability to think and act timeously as the situation changes.
- Defence Digital Diplomacy. Thought leadership on policy and technology matters internationally. Development of alliances and strategic partnerships

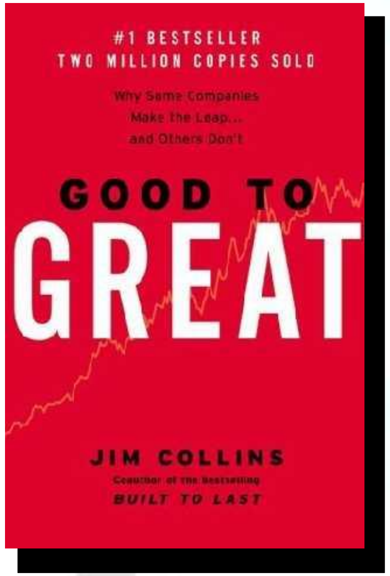
GOALS AND OBJECTIVES

- **GOAL 1: CYBER DEFENCE CAPABILITY DEVELOPMENT**
  - Objective 1: Workforce establishment and retention.
  - Objective 2: Develop operational capabilities.
  - Objective 3: Develop Cyber Command infrastructure.
- **GOAL 2: CYBERSECURITY AWARENESS, RESEARCH & TRAINING**
  - Objective 1: Securitise the DOD environment.
  - Objective 2: Digitise the Military.
  - Objective 3: Cyber-weaponise the DOD.
  - Objective 4: Develop research, development and innovation capacity

GOALS AND OBJECTIVES CONT'D

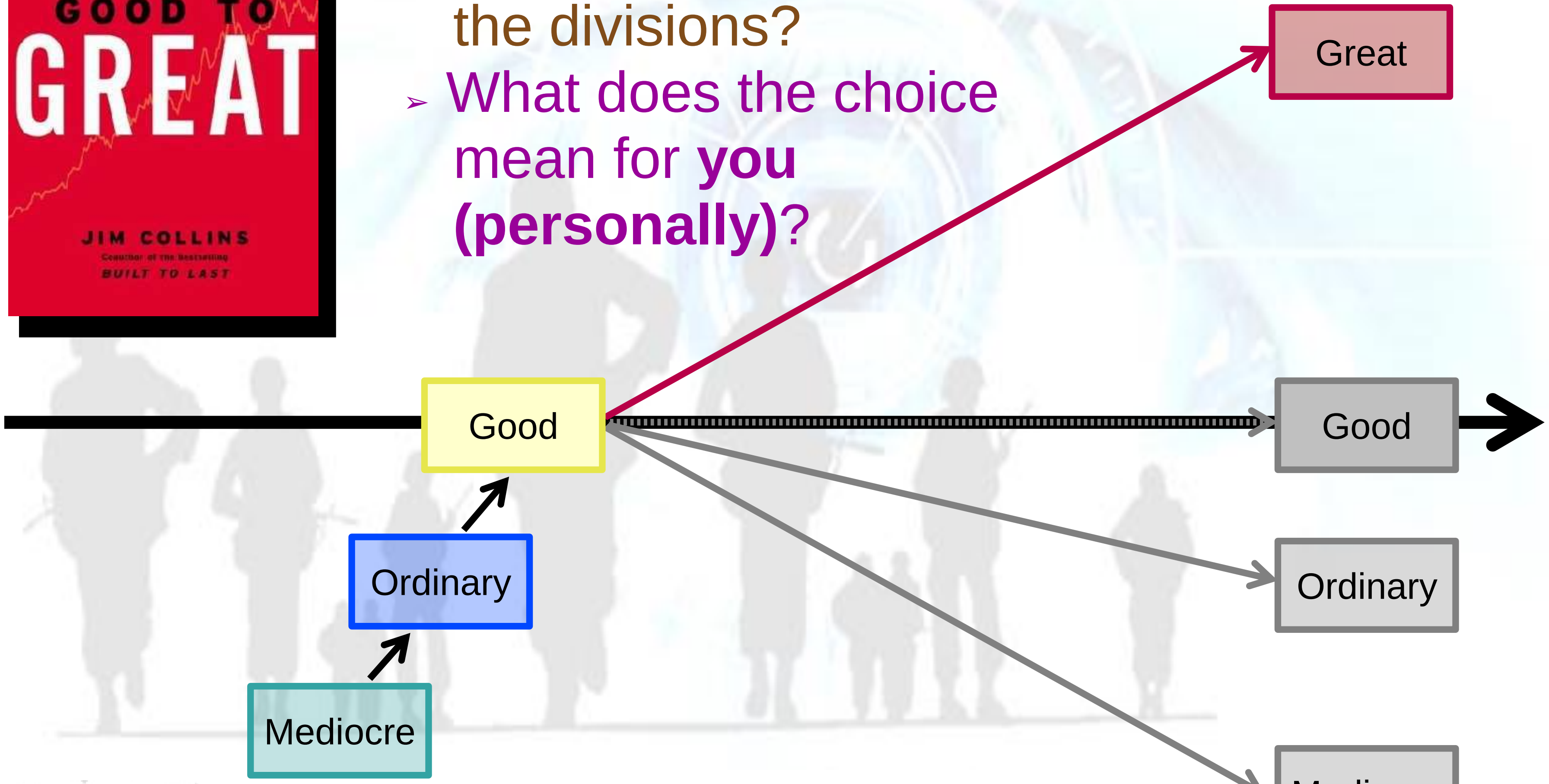
- **GOAL 3: NATIONAL AND INTERNATIONAL COORDINATION/COLLABORATION**
  - Objective 1: Monitoring, incident response and information sharing
  - Objective 2: Defence digital diplomacy
  - Objective 3: Confidence and Security Building Measures (CSBMs).

STRATEGIC POSITIONING


#1 BESTSELLER
TWO MILLION COPIES SOLD
Why Some Companies Make the Leap... and Others Don't
GOOD TO GREAT
JIM COLLINS
Coauthor of the bestselling
BUILT TO LAST

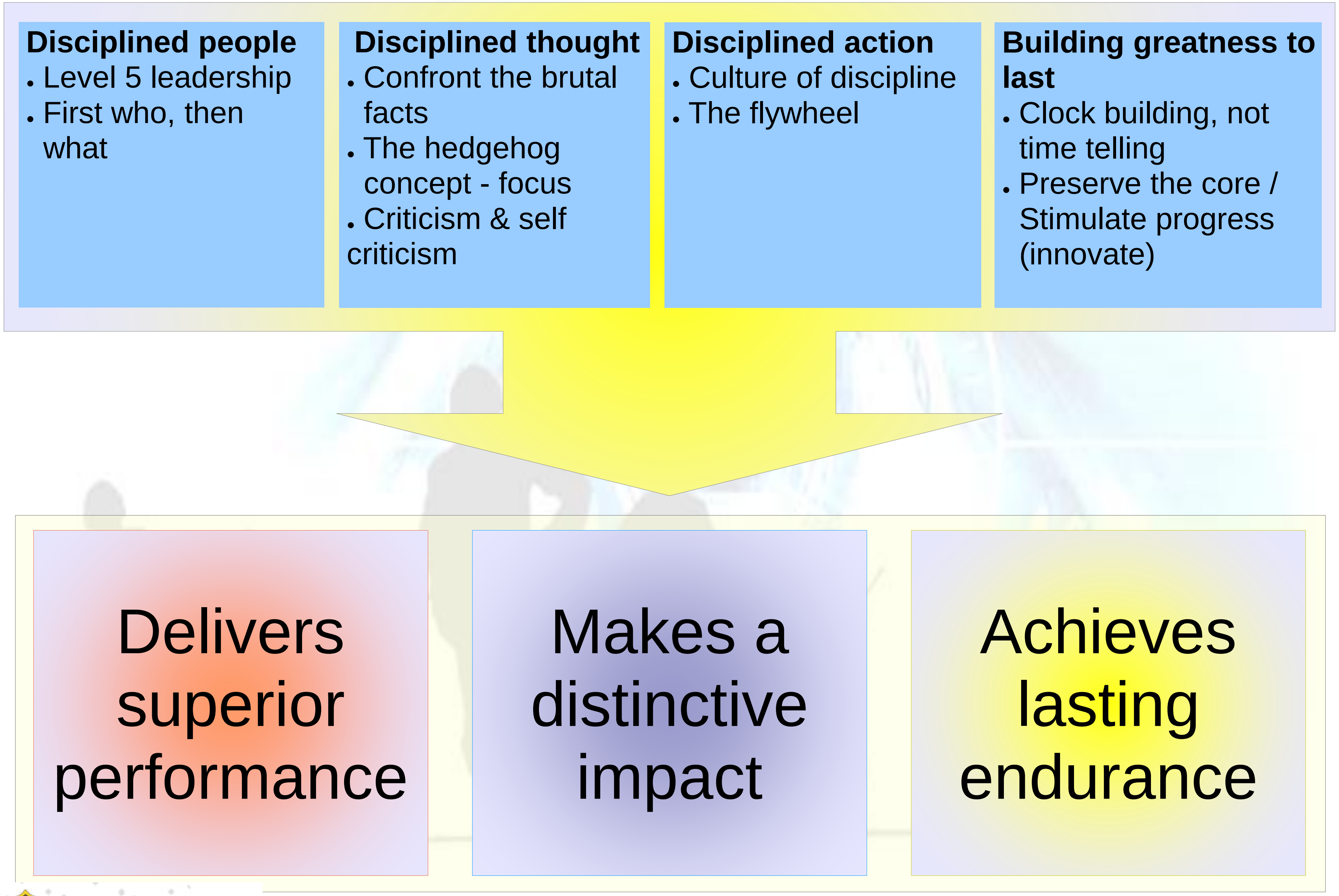
Four possible journeys

- Which journey do you want to be on? ☑
- What does the choice mean for the divisions?
- What does the choice mean for **you (personally)**?



FIVE LEVELS OF LEADERSHIP

- LEVEL 1. Position – follow because they have to
- LEVEL 2. Permission – because they want to
- LEVEL 3. Production - because of what you have done for the organisation
- LEVEL 4. People development – what you have done for them
- LEVEL 5. Pinnacle – who you are and what you represent (believe in the course)



Disciplined people

- Level 5 leadership
- First who, then what

Disciplined thought

- Confront the brutal facts
- The hedgehog concept - focus
- Criticism & self criticism

Disciplined action

- Culture of discipline
- The flywheel

Building greatness to last

- Clock building, not time telling
- Preserve the core / Stimulate progress (innovate)

Delivers superior performance

Makes a distinctive impact

Achieves lasting endurance

Delivers superior performance

Helps the DOD to achieve greatness in fulfilling its vision.

Makes a distinctive impact

Has such a positive impact on the DOD, and the communities it serves, performing with agility and excellence.

Achieves lasting endurance

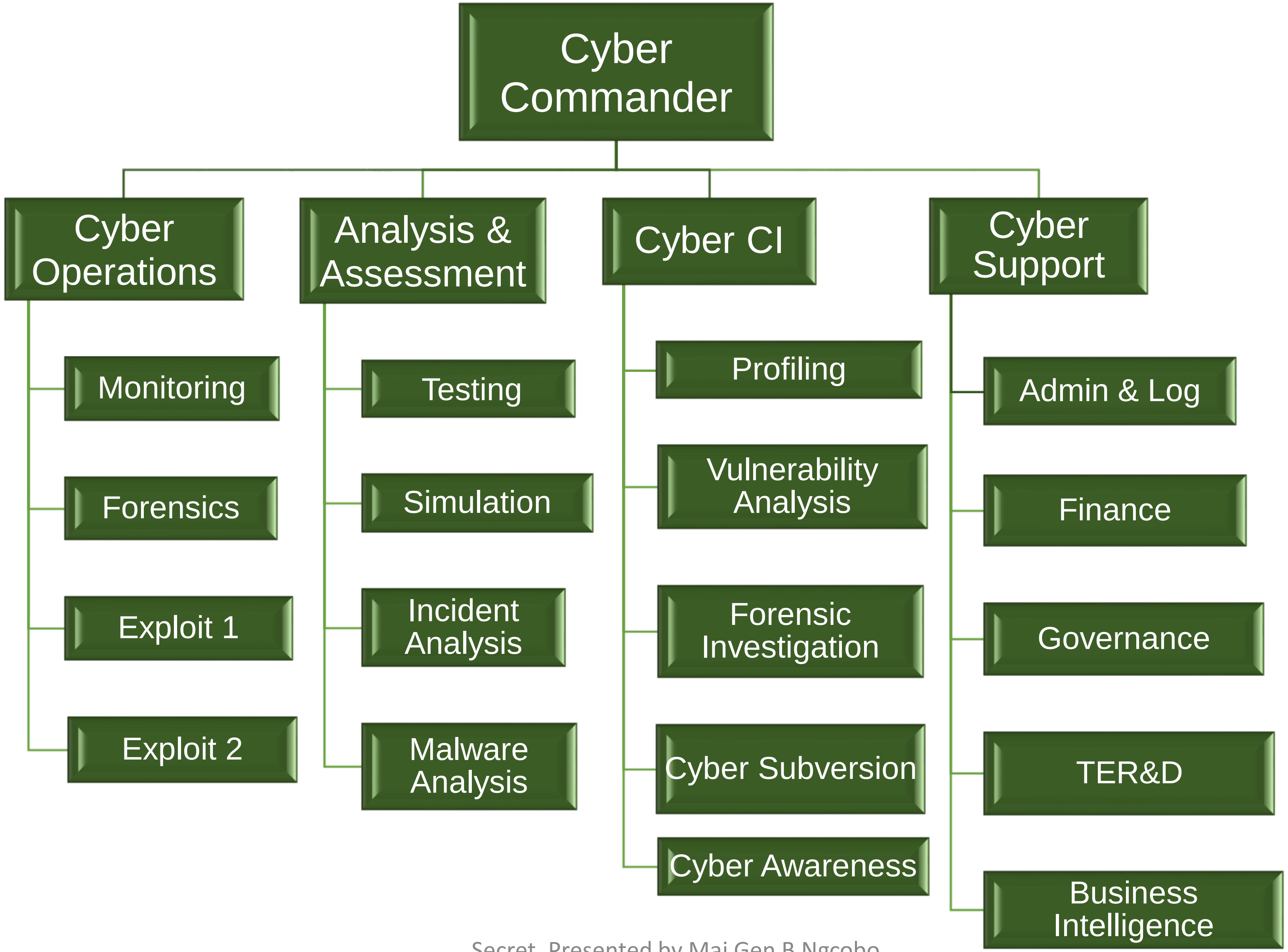
Sustained positive impact on the DOD over a long time, beyond the participation of any individual, single leader, or the implementation of any single great idea. Bounces back from setbacks.

QUALITATIVE INDICATORS FOR THE CYBER COMMAND

Ordinary	Good	Great
Others control our destiny, especially vendors	We implement other people's ideas well	Other people implement our ideas

CYBER COMMAND STRUCTURE

CYBER COMMAND – SERVING WITH HONOUR



- Cyber Commander
  - Cyber Operations
    - Monitoring
    - Forensics
    - Exploit 1
    - Exploit 2
  - Analysis & Assessment
    - Testing
    - Simulation
    - Incident Analysis
    - Malware Analysis
  - Cyber CI
    - Profiling
    - Vulnerability Analysis
    - Forensic Investigation
    - Cyber Subversion
    - Cyber Awareness
  - Cyber Support
    - Admin & Log
    - Finance
    - Governance
    - TER&D
    - Business Intelligence

CRITICAL ASSUMPTIONS/SUCCESS FACTORS

- Budget
- Approval and funding of Cyber Command Structure
- Sovereign Technology - Indigenisation
- Highly Skilled Workforce
- Solid operating processes and procedures
  - Emergency cyber response line (Armscor and DI HQ)
- Close cooperation - DOD, SADRI, local Private Sector, Institutions (research and higher learning)

CONCLUSION

Establish the Cyber Command as a force multiplier in the protection of the NCII and the DOD's C^4I^3RS and the attainment of national interest.

Q & A

Anikie

Yesterday, 19:49

Interview in an IT company

So, what makes you suitable for this job?

I hacked your computer and invited myself for this interview

Good 😂