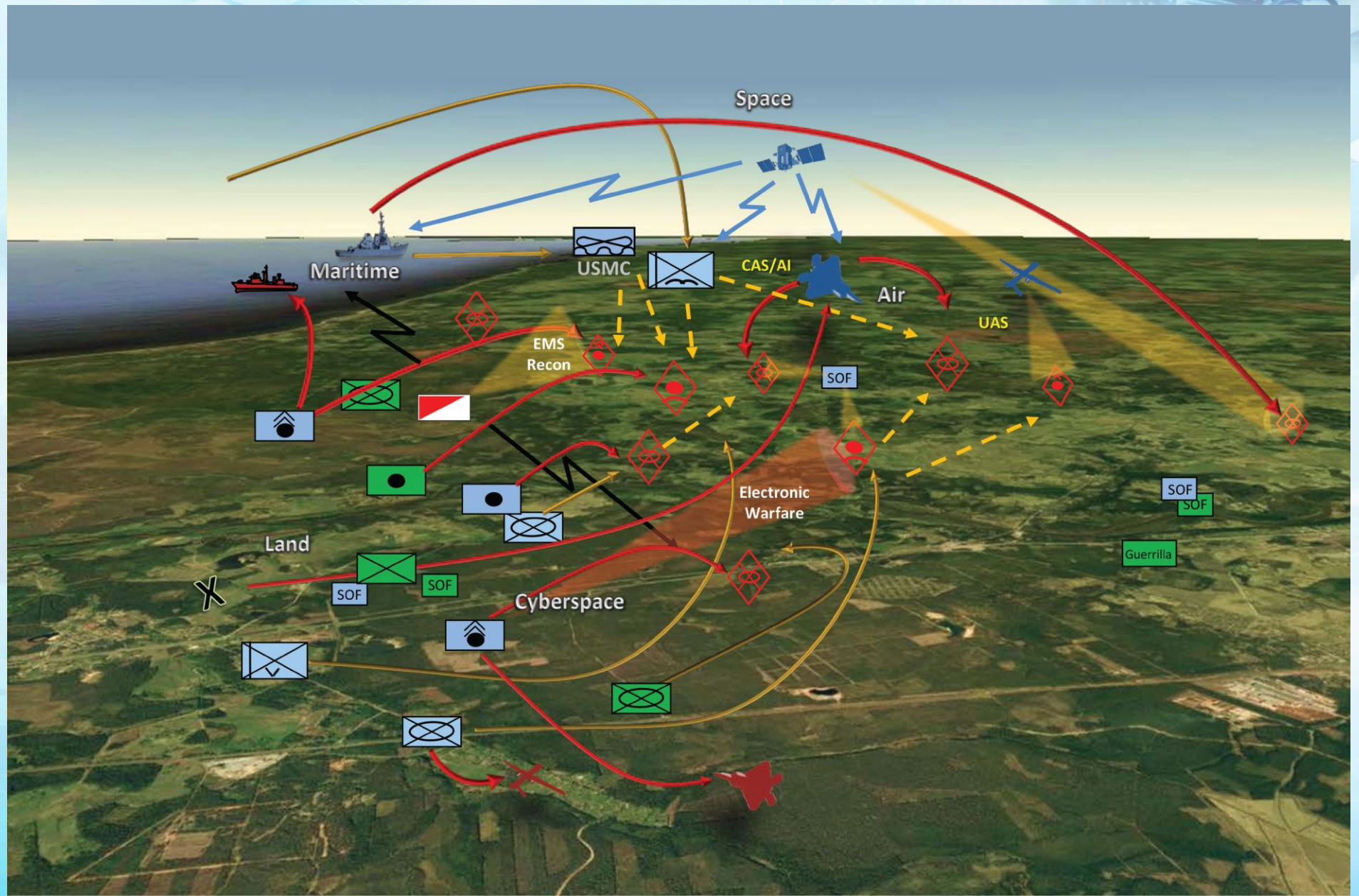
Developing Cyber Capabilities as an integral part of Command and Control

James Mphahlela Thaba
Council for Scientific and Industrial Research (CSIR)
jthaba@csir.co.za

our future through science

The Multi-Domain Battlespace



Technology Evolution

- ***Space and cyber*.** There are no lessons learned documents, no historic battles to study, no precedent for how warfare in these domains might play out .
- ***Artificial intelligence, big data, machine learning, autonomy, and robotics*.** Military operations enabled by these technologies, may unfold so quickly that effective responses require taking humans out of the decision cycle.
- ***A new generation of high tech weapons*.** These new weapons will dramatically increase the speed, range, and destructive power of conventional weapons beyond anything previously imaginable.
- ***The unknown x-factor*.** Secret technologies developed by friend and foe alike will likely appear for the first time during the next major war

Doing smart things
(Innovation)

Doing things smarter
(efficiency and agility)

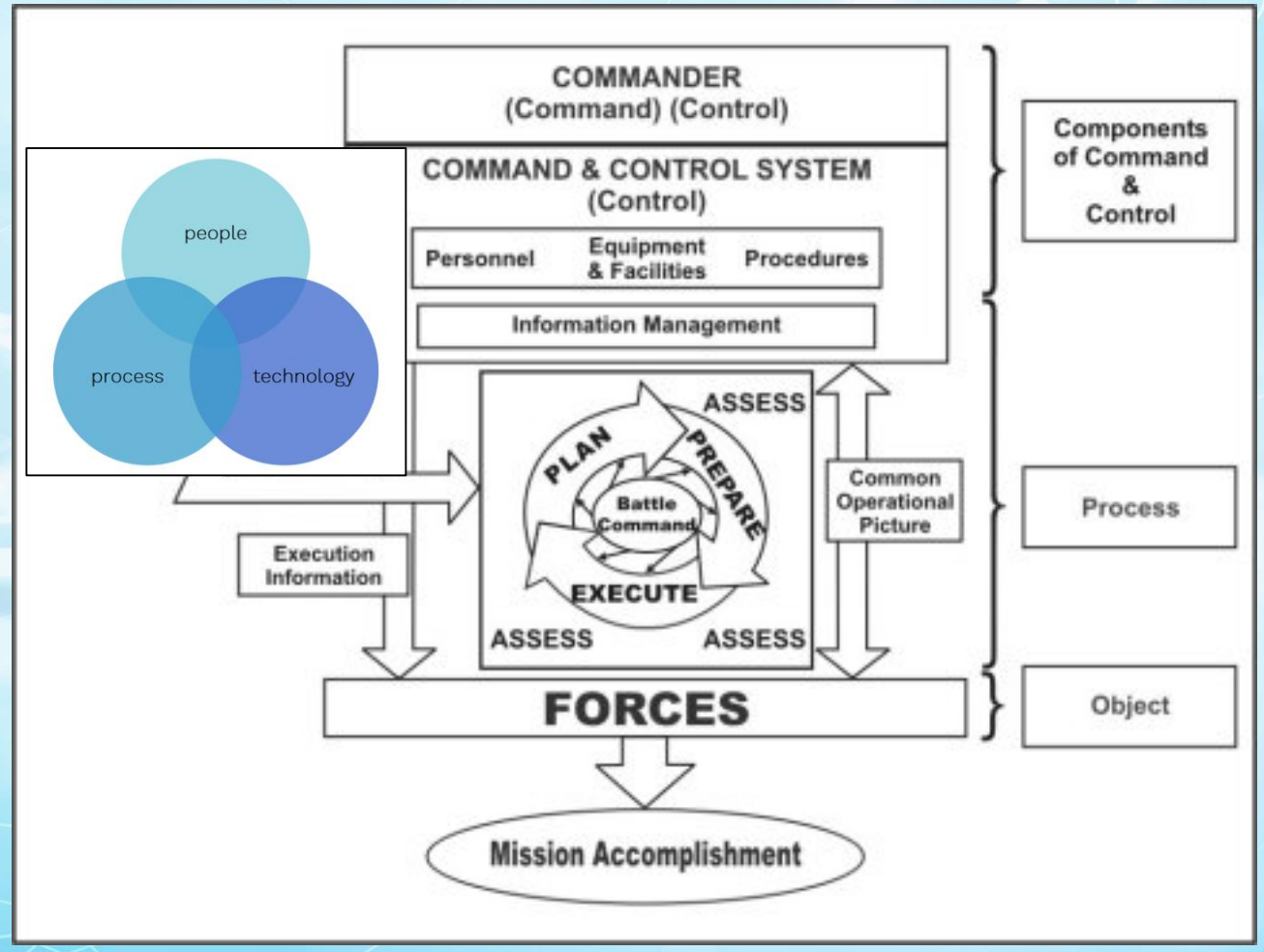
Wider risk surface
(safety and security)

"The study of warfare has always heavily relied upon scrutinizing past battles to discern the lessons of those as yet unfought."

Command and Control Capability

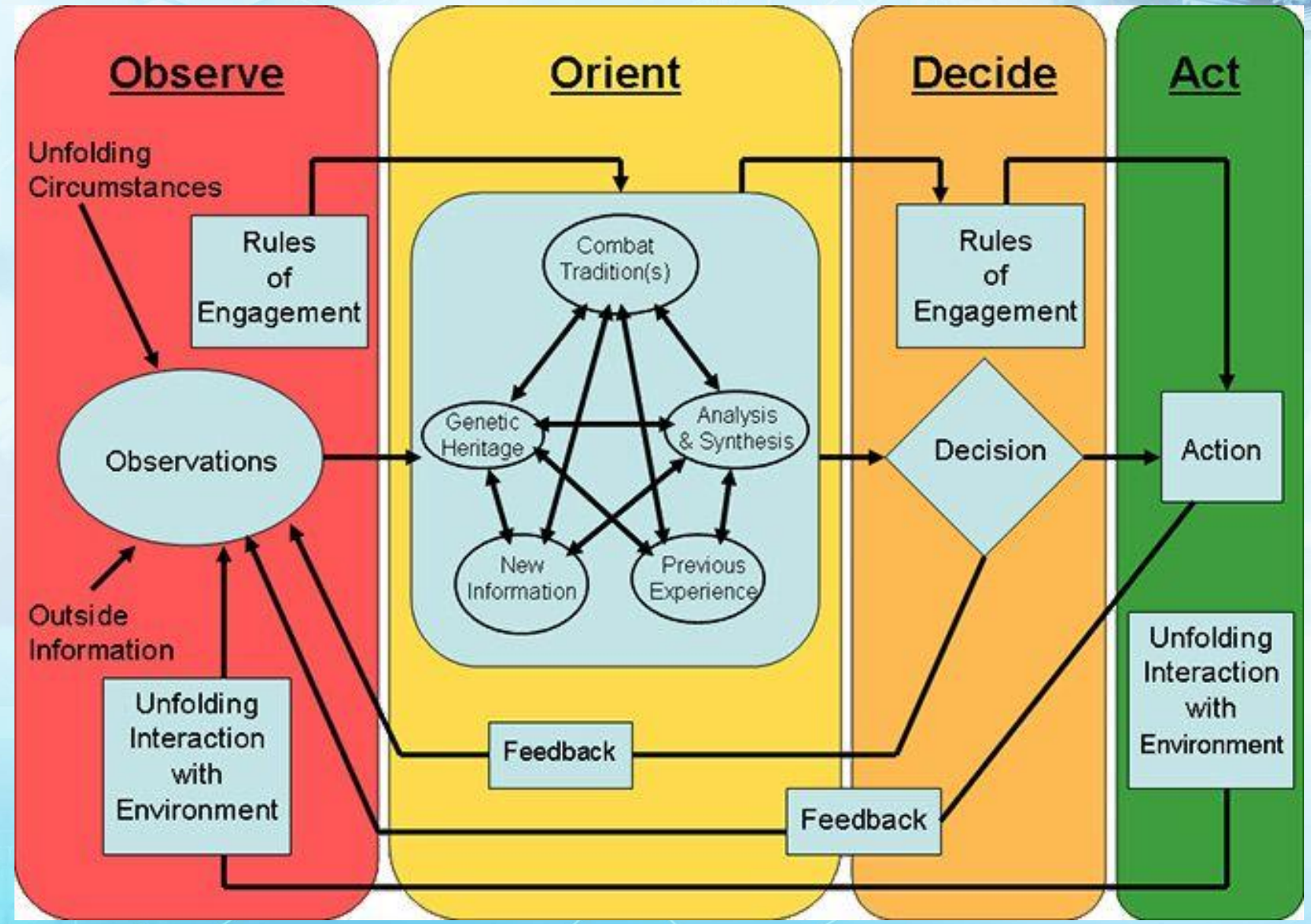
The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of a mission.

- The ability to **Plan**
- The ability to **Task**
- The ability to **Coordinate**
- The ability to **Control**



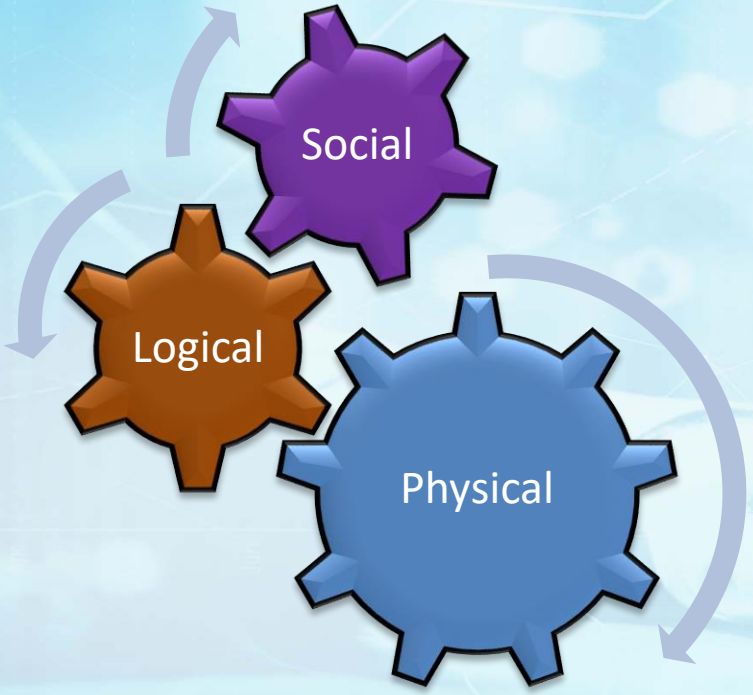
Source: https://www.globalsecurity.org/military/library/policy/army/fm/6-0/chap1.htm#fig1-1

Commander's Decision Making Loop



Boyd's OODA Loop

The Cyberspace: What are the Considerations?



Step 1: Understanding the Operating Environment

Step 2: Understanding the Problem

Step 2a
Mission Analysis
(Determine objectives and end state)

Step 2
Define Art of the Possible
(Object and Factor Analysis)

Step 2c
Commander's Confirmation
(Confirm essentials of the Mission, articulate theory of change)

Step 3: Formulate Broad Options
Sequence of the Campaign Objectives
(What to achieve)

Step 4: Develop and Validate CoA
Develop and Sequence Support Effects

Step 5: Evaluate CoA
CoA Feasibility, Comparison Data, Ops Analysis

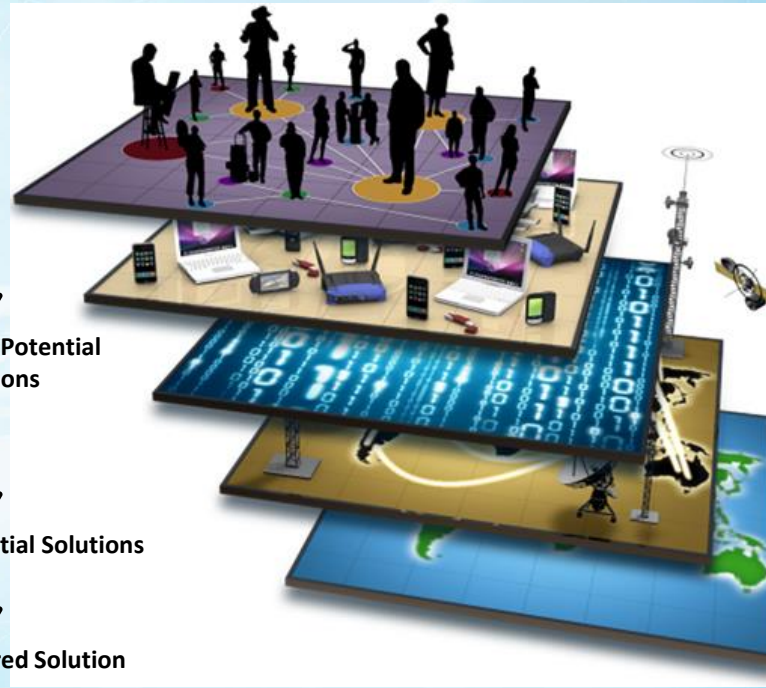
Step 6: Commander's Decision
Final approval of preferred solution

Develop Commander's Intent

Determine Potential Solutions

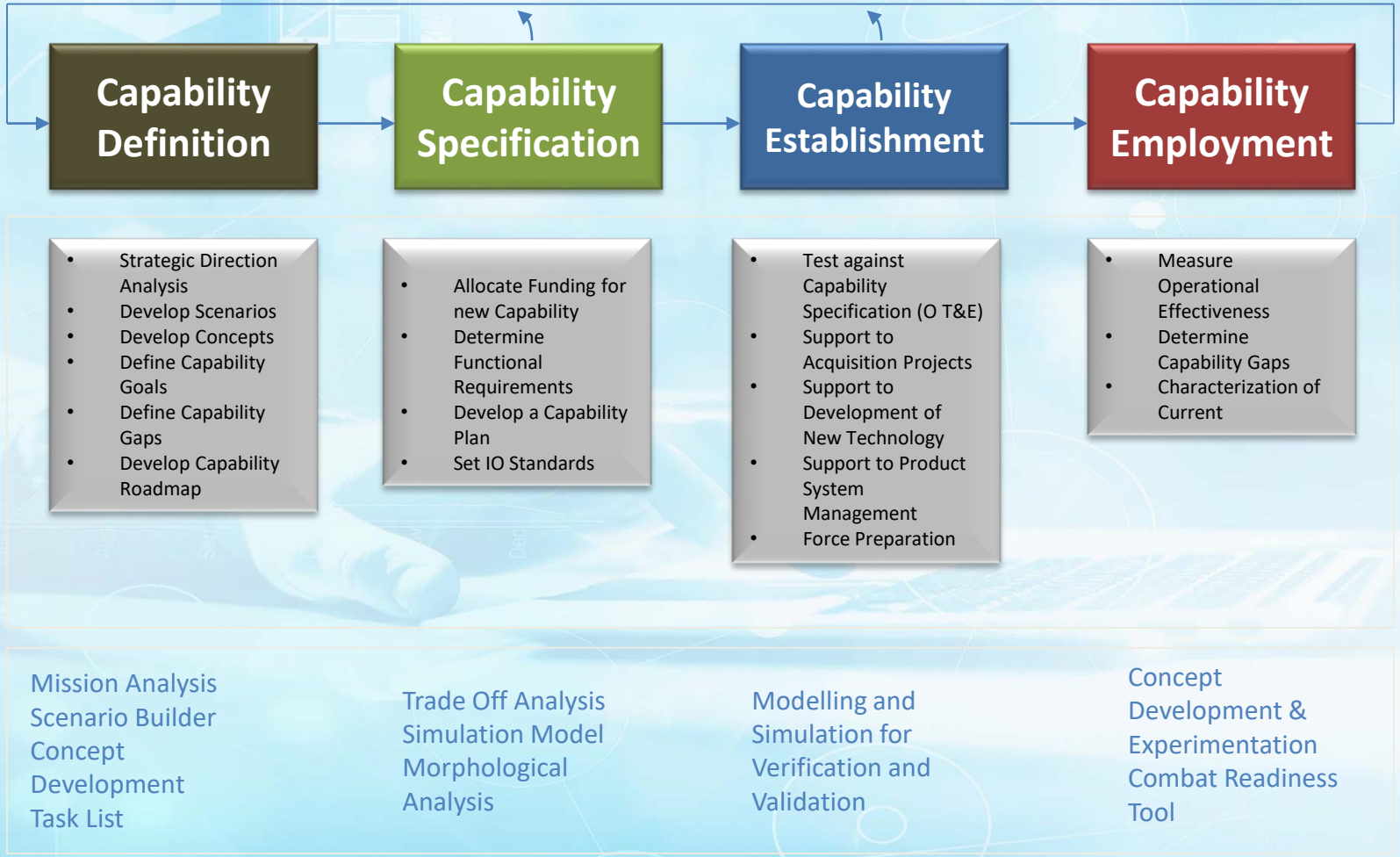
Evaluate Potential Solutions

Select Preferred Solution



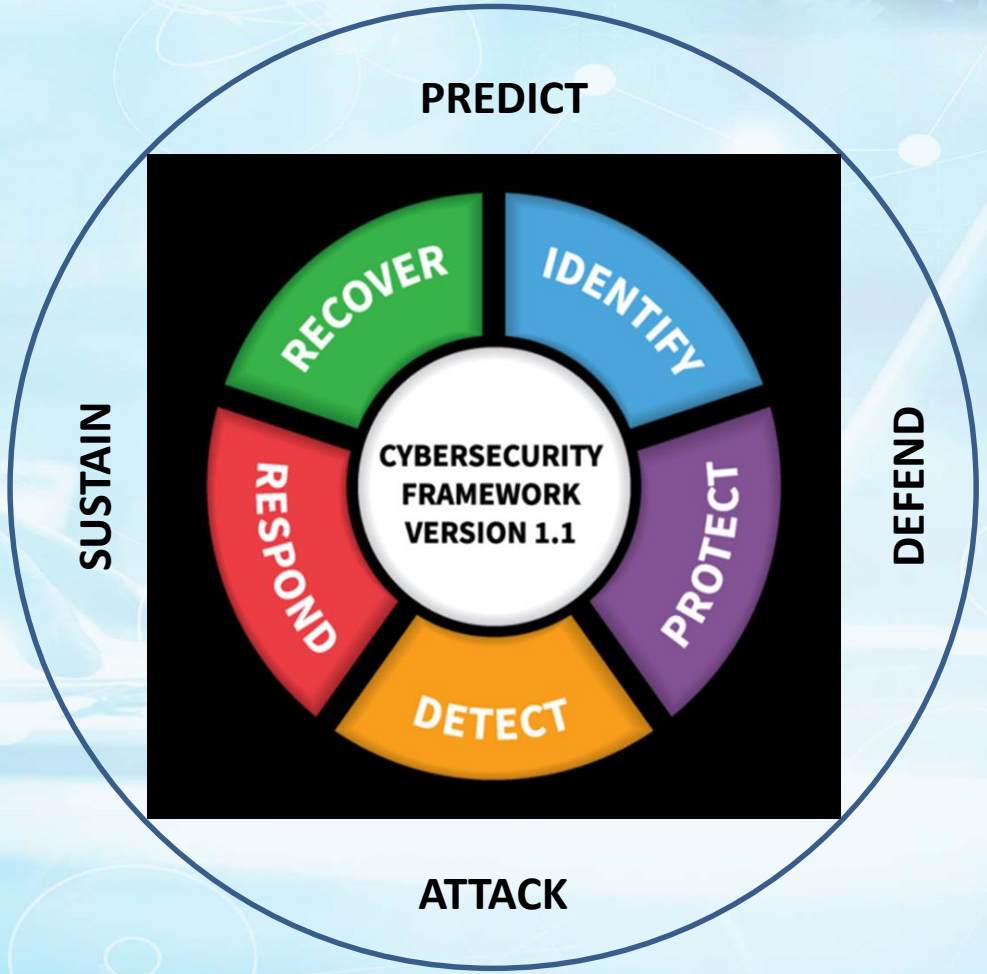
The Cyberspace Complicates the Military Planning!

Capability Development Framework



Capability Requirements: Function?

- **Predict**: What could possibly happen?
- **Attack**: Launch the Offensive
- **Defend**: Resist possible offensive against own forces:
  - Identify: Know Info Assets
  - Protect: Against any possible Attack
  - Detect: Any possible Intrusion
  - Respond: Against Intrusion
  - Recover: In the Case Intrusion occurred
- **Sustain**: Maintain superiority throughout the Mission



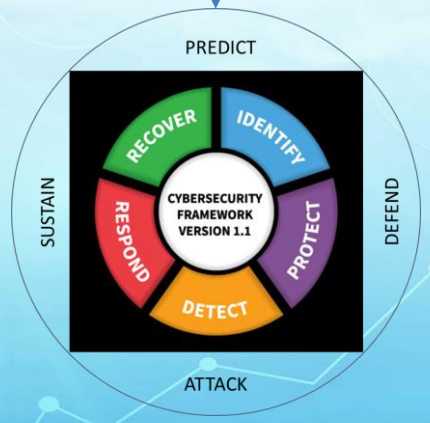
Milestones

Strategic Guidelines

Capability Definition → Capability Specification → Capability Establishment → Capability Employment

VALIDATION: CD & E

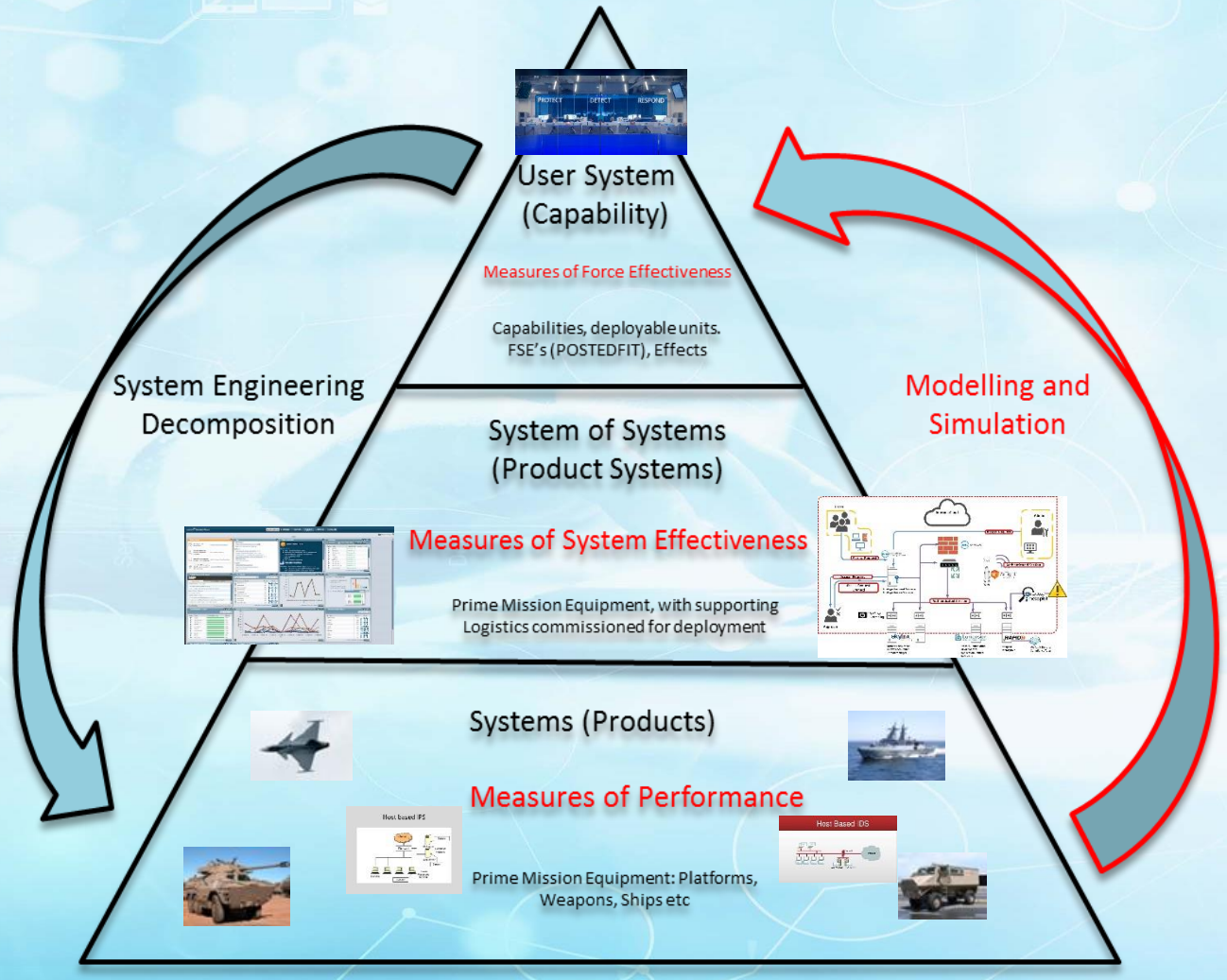
VERIFICATION: OT & E



READY CYBER CAPABILITIES

DEPLOYED CYBER CAPABILITIES

Modelling and Simulation: Validate and Verify



CD and E Results: Modern Headquarters Structure

- 1: Personnel
- 2: Intelligence
- 3: Operations and training
- 4: Logistics
- 5: Contingency Planning
- 6: Signals operations
- 7: Force Development
- 8: Chaplaincy
- 9: Cyber Operations

Conclusion

- The cyberspace forms an integral part of the commander's operating environment.
- This forces commanders to consider factors in the cyberspace for analysis as part of planning and execution of operations.
- The NIST cybersecurity framework has been demonstrated as one of the ways to guide analysis of the cyberspace,
- The ability to control the cyberspace could be advantageous to the commander's ability to successfully conduct operations.
- If not well considered, it could be exploited by the opposing force at the detriment of own forces.
- Cybersecurity specialists and the team should form an integral part of the commander's staff compliment.
- Cyberspace offensive operations, as and when required must be sanctioned by the highest command authority available, and must be carefully assessed for military benefit, before implemented. This remains a Command function.

QUESTIONS

James Mphahlela Thaba
+27 (12) 841 3446
+27 (83) 387 4545
jthaba@csir.co.za

Lines of Development (POSTEDFIT)

SYSTEM ELEMENTS	DEVELOPMENT ACTIONS
P-Personnel	Develop a creative, talent-focused strategy to recruit, assess, select, develop, manage, and retain the cyber warrior in an era of persistent competition for talent.
O-Organization	• Transform current structures to leverage/optimize/enable evolving Cyberspace Domain that is an enabler for all warfighting domains. • Establish clear C2 construct to facilitate the wise execution of full spectrum operations in, through, and from cyberspace
S- Support	Determine support required to sustain Cyber operations in theatre and over protracted periods
T-Training	• Cyberspace training must be dynamic and adaptive in support of the operational environment. • Cyberspace operations training must be integrated into all Professional Military Education Schools at all levels
E-Equipment	Facilitate the design of operational and technical architectures that enable defensive (“see ourselves”) and offensive (“see our enemy”) ops
D-Doctrine	Define Cyberspace Operations as related to EMSO, EW, IO, NETOPS, Knowledge and Information Management, among others); develop construct for cyber-related operations
F-Facilities	Build facilities that are located in locations which enable responsiveness to Geographic Combatant Command requirements while simultaneously supporting global integration of cyberspace operations
I-Intelligence	
T-Technology	Leverage technology, 24/7 cyberspace-related centers, labs, and simulation centers to create an inspiring 21st Century home station training architecture that integrates cyber into a live, virtual, and constructive environment

References

- Andrew Dakin, L. (2012). Defence Capability Development Handbook 2014. Retrieved from
- Christopher, J. D., Gonzalez, D., White, D. W., Stevens, J., Grundman, J., Mehravari, N., … Dolan, T. (2014). Cybersecurity Capability Maturity Model (C2M2). Department of Homeland Security, (February), 1–76.
- Jordan, F., & Hallingstad, G. (2013). Towards Multi-National Capability Development in Cyber Defence. Information & Security: An International Journal, 27, 81–89.
- Liang Tuang, N. (2018). the Fourth Industrial Revolution ' S Impact on Smaller Militaries : Boon or Bane ? (November).
- Mtsweni, J., Gcaza, N., & Thaba, J. (2018). A Unified Cybersecurity Framework for Complex Environments.
- NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity.
- Office of the Deputy Under Secretary of Defense for Acquisition and Technology - Systems and Software Engineering. (2008). Systems Engineering Guide for Systems of Systems. In Technology.
- Porche, I. (2016). Emerging Cyber Threats and Implications. Emerging Cyber Threats and Implications. https://doi.org/10.7249/ct453
- Stuart, W. D. (1980). Guide to the Systems Engineering Body of Knowledge (SEBoK) v1.8. American Society of Mechanical Engineers, Applied Mechanics Division, AMD, 42, 73–80.
- Thaba, J., & Benade, S. (2014). Aligning force planning and systems acquisition. INCOSE International Symposium, 24(s1), 514–527.
- U.S. HOUSE COMMITTEE ON ARMED SERVICES. (2010). CYBER OPERATIONS: IMPROVING THE MILITARY CYBER SECURITY POSTURE IN AN UNCERTAIN THREAT ENVIRONMENT. Sda.
- US Joint Chiefs of Staff. (2018). CYBERSPACE Operations. Joint Publication 3-12, (June), 104.