Leading and Developing the Cyber Workforce

Agenda

Disclaimer

Communication Challenges

Learning From the Military

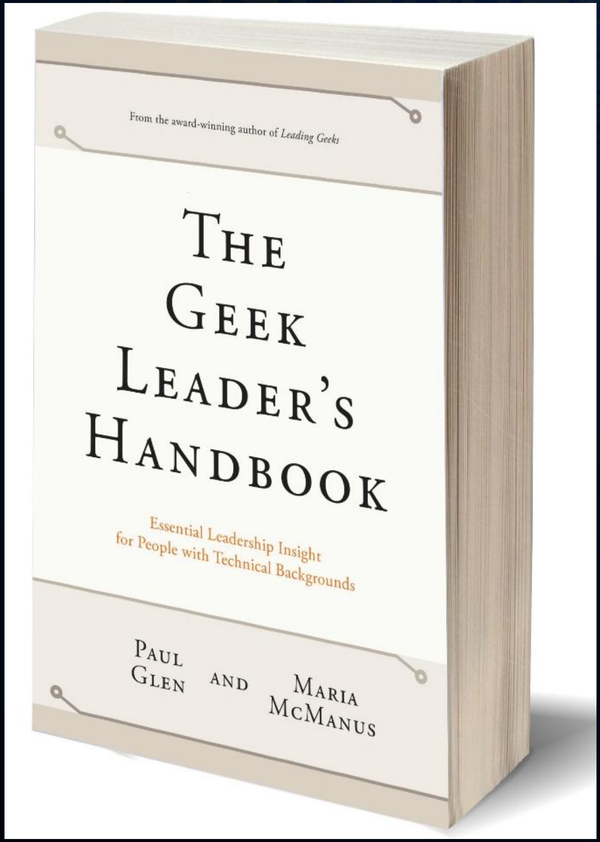
Planning

Leadership Communication and Personnel Development

Disclaimer

The following information is presented from the private perspective of the Cyber Security Forum Initiative (CSFI) and its analysis of the named subject. The presentation does not represent any official endorsement of, nor does it speak for any official US governmental agency

Challenges with Communication in Context


From the award-winning author of Leading Geeks
The Geek Leader's Handbook
Essential Leadership Insight for People with Technical Backgrounds
Paul Glen and Maria McManus

- Geeks are different.
- Geeks would rather lead technology than people, but only people can be led.
- Geeks have a hard time working with non-geeks, but those who learn to do it well become great geek leaders.

- Management and technical personnel often experience communication difficulties
- Each group has different paradigms and different views of the same problem
- Each group leaves a meeting saying the same thing "they don't get it"

Learning from the Military

Military forces learned throughout centuries of conflict that during warfare:

I. A binding force is needed to guide forces actions through uncertainty within conflict

II. Aggregated actions need to mutually reinforce each other into a teamwork approach

Case studies exist where no binding force for uncertainty existed and results were controversial and/or casualties high

Gallipoli
Battle of Jutland
Gaugamela
Cannae

- The Commander’s Intent concept evolved to the binding force

- The Unity of Effort concept ensures teamwork

Importance of the Commanders Intent

➢ No matter how much a plan changes, the Commanders Intent still guides the staff and the mission

➢ The Commanders Intent may be:

- A formal statement for a tactical mission
- Implied in staff discussions
- A broad statement or desire
- Combination of multiple communicative means (staff meetings, one on one conversation, product feed back, e-mails etc)

➢ Commanders Intent allows for decentralized execution and is omnipotent throughout the planning process and mission execution

Non-Military Use of the Commander's Intent

- Top tier organizational leaders can communicate their vision through direct and indirect means

- Organizational leaders within all tiers can use the top vision as a guiding light to influence their decision making

- Personal within all tiers can relate their actions to the organization's vision

Implied v Detailed Communication

<u>Detailed Communication</u>: Communication which desired actions are specifically stipulated and limited in scope by provided details

<u>Implied Communication</u>: Communication which desired actions and outcomes are understood and not overly detailed in transmission

<u>Implied Communications examples</u>

- E-mail Comment
- Joke made during a meeting
- A stern look of disagreement
- A smile/friendly look of agreement

Limit detailed communication to degree necessary to accomplish an effort

Understanding Paradigms

Paradigm: A theory or a group of ideas about how something should be done, made, or thought about

Source: Miriam-Webster , www.Miriam-Webster.com

http://www.stratospherenetworks.com/nocc-intro.html

http://www.celdi.ineg.uark.edu/stories.asp

http://www.hagenbusiness.com/accounting.htm

Understanding/Actioning on Intent

- Implied communication is essential
- Leaders often lack time, patience, skill, (or all of the above) to intricately detail instructions
- Understand the paradigm of the leader in order to take actions similar to what the leader would do
- Detailed communication will be common for personnel involved in technical execution details
- When in doubt, ask yourself "what would the boss do if he/she were here?"

Working as an Organism

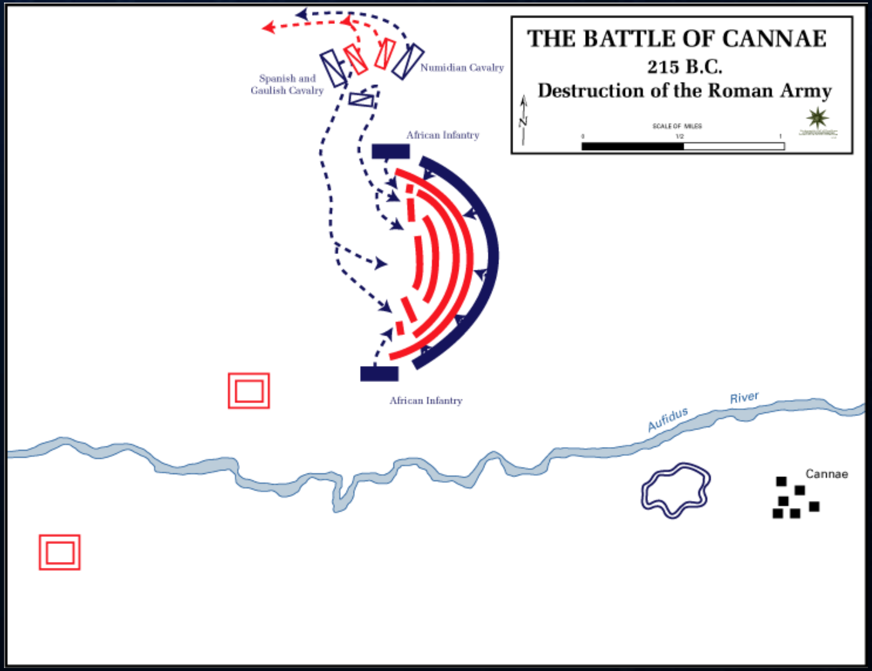
Organism: A complex structure of interdependent and subordinate elements whose relations and properties are largely determined by their function in the whole

Source: Miriam-Webster

Spartan: Total Warrior © 2005 SEGA Europe Limited. Developed by The Creative Assembly Limited. SEGA, the SEGA logo, Spartan Total Warrior are eithe

Importance of Unity of Effort

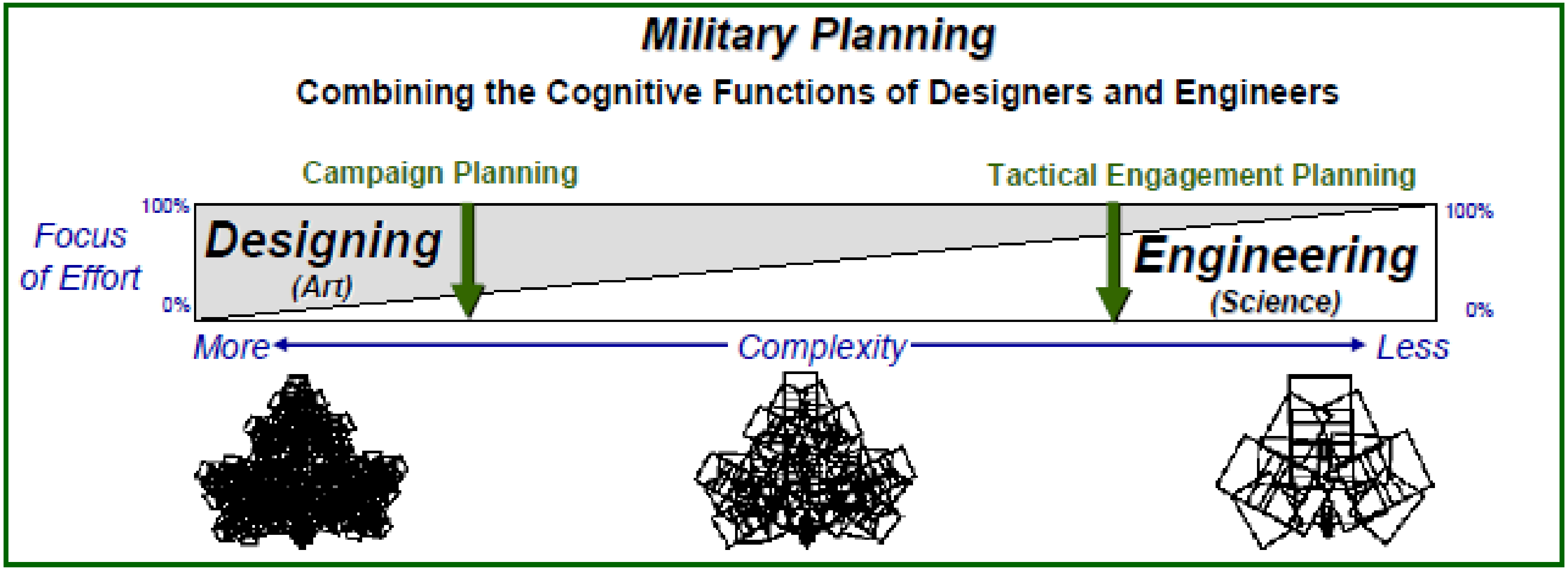
Unity of Effort: Coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization, which is the product of successful unified action.



Unity of Effort ensures:

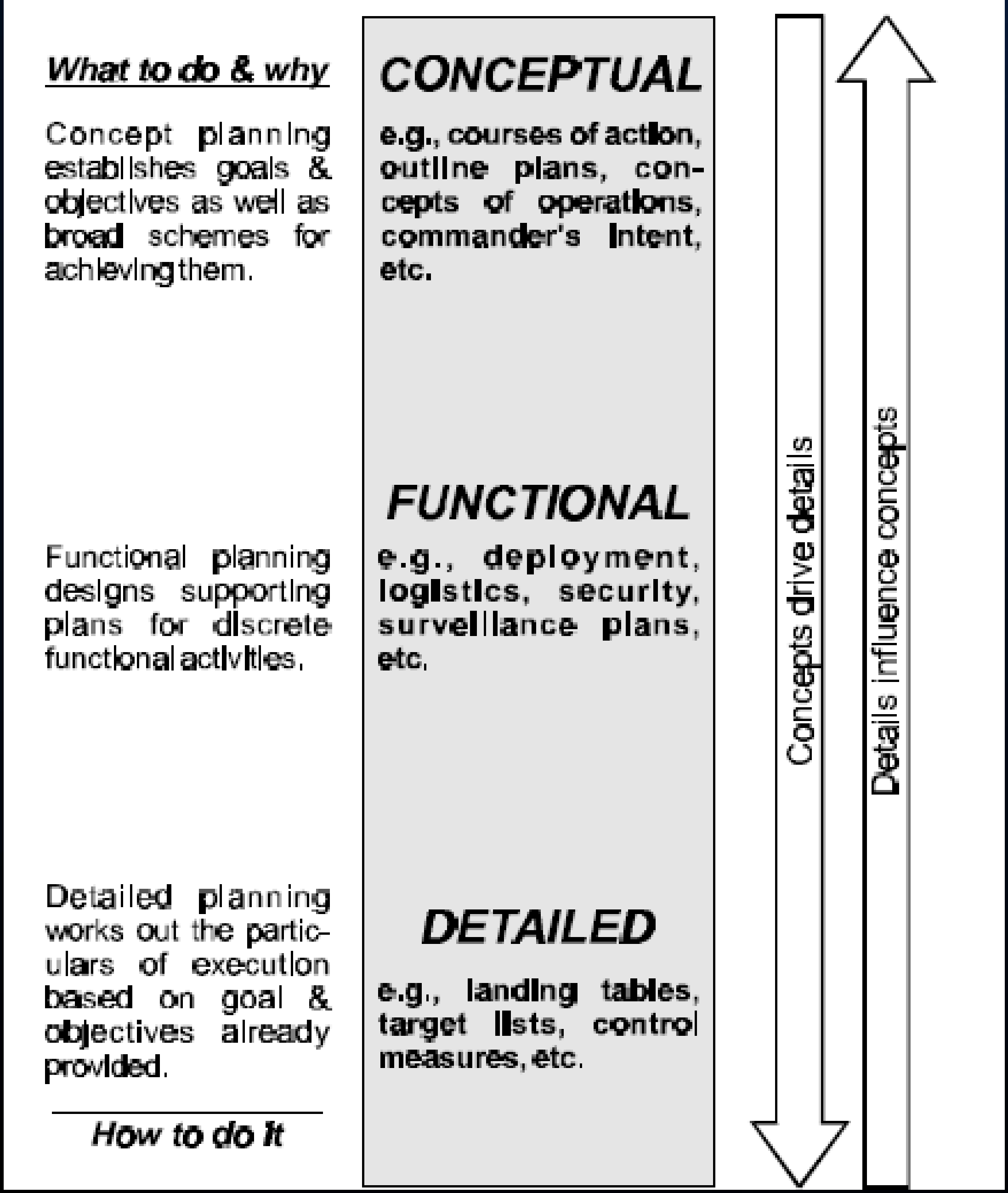
- That an individual effort mutually reinforces other efforts
- The totality of all efforts contribute to achieving the desired goal
- One Team, One Fight, One Mission

Spectrum of Planning



Source: TRADOC Pamphlet 525-5-500, Commander's Appreciation of Design , fig 1-3, pp 14

Conceptual, Functional, and Detailed Planning



What to do & why

Concept planning establishes goals & objectives as well as broad schemes for achieving them.

CONCEPTUAL

e.g., courses of action, outline plans, concepts of operations, commander's intent, etc.

Functional planning designs supporting plans for discrete functional activities.

FUNCTIONAL

e.g., deployment, logistics, security, surveillance plans, etc.

Detailed planning works out the particulars of execution based on goal & objectives already provided.

DETAILED

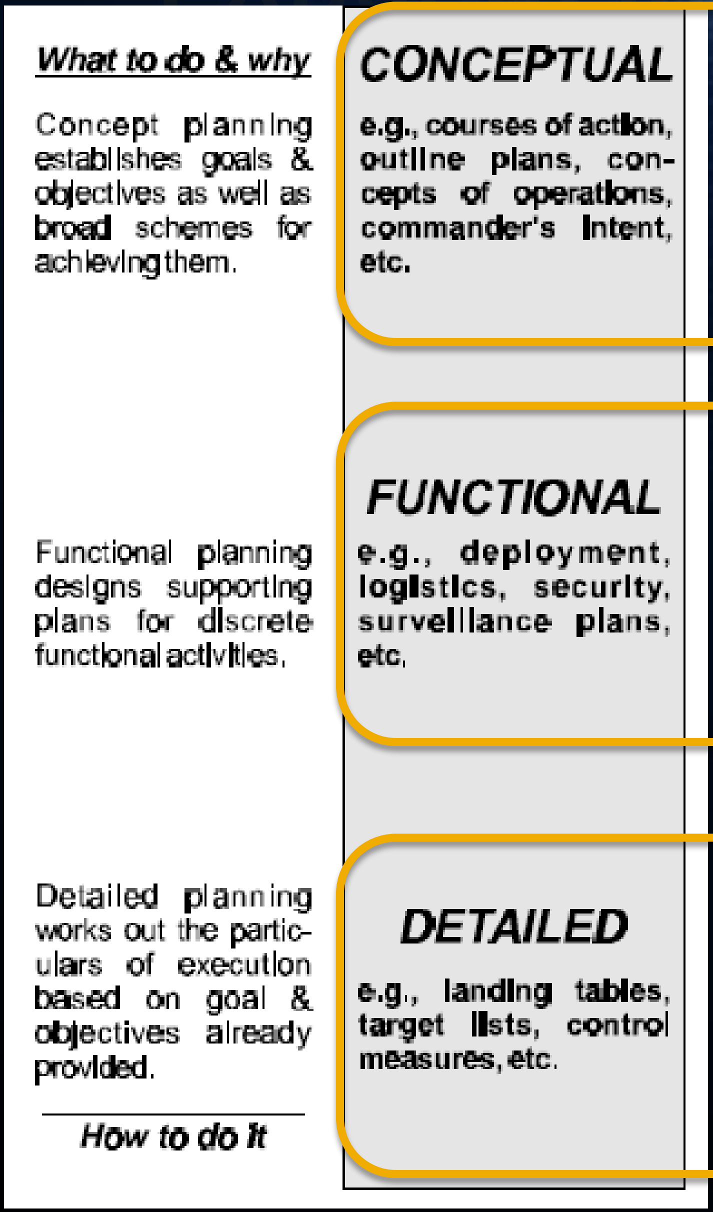
e.g., landing tables, target lists, control measures, etc.

How to do it

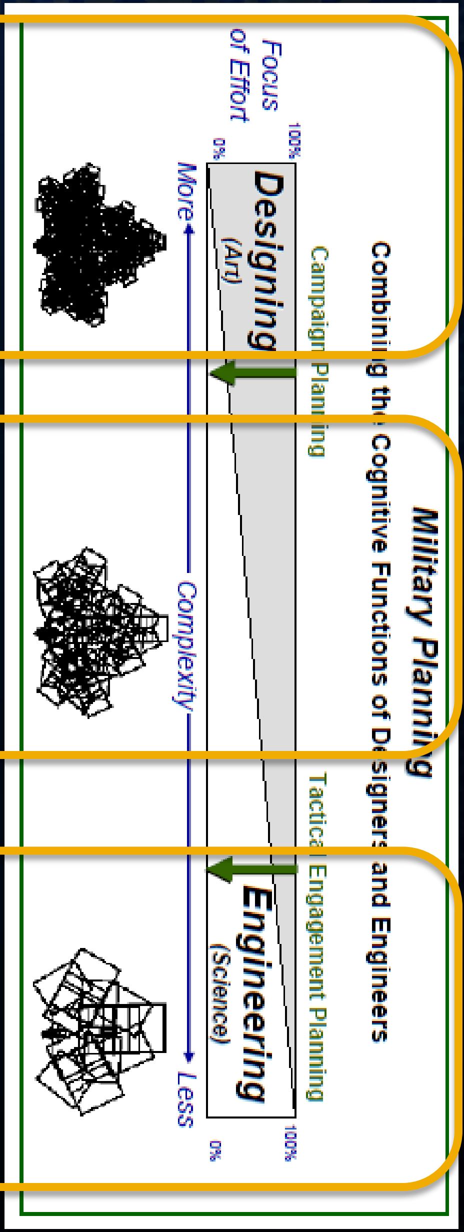
Source: MCDP 5, Planning pp 36

CSFI all rights reserved

Cyber Planning Linkages



What to do & why	
Concept planning establishes goals & objectives as well as broad schemes for achieving them.	**CONCEPTUAL** e.g., courses of action, outline plans, concepts of operations, commander's intent, etc.
Functional planning designs supporting plans for discrete functional activities.	**FUNCTIONAL** e.g., deployment, logistics, security, surveillance plans, etc.
Detailed planning works out the particulars of execution based on goal & objectives already provided.	**DETAILED** e.g., landing tables, target lists, control measures, etc.
How to do it	



Conceptual to Detailed Planning (example)

Detailed Planning	Functional Planning		Conceptual Planning	
Organizational networks comply with all applicable policies and standards	Organizational networks adhere to all legal operational requirements	Implement all necessary legal protocols for installed programs	Install and operate all network programs to support information and decision superiority	Remove all malicious activity from organizational networks and posture the organization to counter malicious threats and support information dominance
Network infrastructure is available 98% of the time	Network Services are delivered to the end user (Enterprise Management)	Operate the network: Enterprise Management, Network Management, Content Management		
Prioritize Defended Asset List (PDAL)is available 100% during specified window				
Enterprise Services are available 98% of the time				
Know Information Assurance threats are mitigated within 2 hours	Information is assured and protected, at rest, in transit and during processing (Network Assurance)			
Known Information Assurance updated are disseminated within 2 hours				
End User can access required information 98% of the time	Information is available for use when required by the end used (Content Management)			
100% of detected adversary activity is remediated within 2 hours	Locate and quarantine malicious codes within mission timelines	Mitigate malicious activity	Detect, remove, and adjust organizational networks as needed to mitigate and counter malicious activity	
Cyber Defense personnel implement preventative measures in response to successful attack/exploit				
Cyber Defense personnel provide signature details and malicious code characteristics within 2 hours	Cyber Defense personnel provides details of malicious tactics	Adjust and reorient organizational networks to evolving malicious tactics		

Science

Art

Engineering

Designing

Techie

Decision Maker

Leadership Communication

- Promulgate a vision (commanders intent)

- Develop and promote implied communication

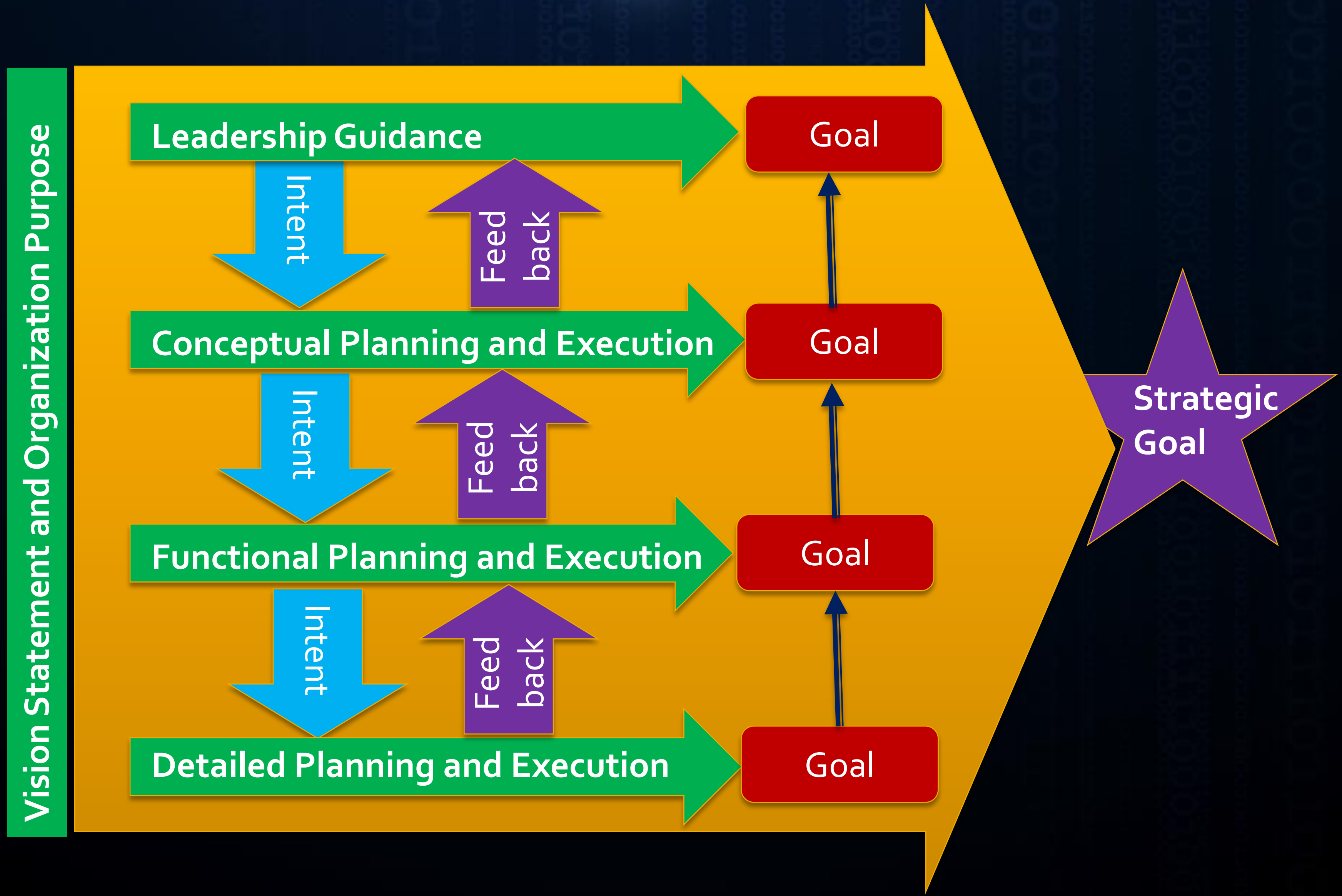
- Use key "power" words than individually convey ideas and concepts

Ex: posture, redundancy, resiliency, efficiency, harden, neutralize, restore, assess, maintain etc.

- Say as much as possible in a little as possible……convey intent

Example: Harden networks against current threats, posture against emerging threats, and build network redundancy and resiliency in order to enable continued services in a contested cyberspace environment

Feedback Loop


Vision Statement and Organization Purpose
Leadership Guidance
Goal
Intent
Feed back
Conceptual Planning and Execution
Goal
Intent
Feed back
Functional Planning and Execution
Goal
Intent
Feed back
Detailed Planning and Execution
Goal
Strategic Goal

Total Workforce Development

- Train to acquire the needed skill sets across all levels of organizational responsibility
- Training needs to include integrating all leadership tier skill sets into a cohesive mutually reinforcing effort
- Training venues and agendas need to reflect actual mission demands and expectations
- Leadership is the glue that holds the organization together and drives it to reach the desired strategic goal

Leading and Developing

Vision Statement: To provide users with consistent reliability, content integrity, and information security to support end user needs

Intent: Posture networks against current and emerging threats while maintaining the ability to provide essential functions in a degraded cyberspace environment

Leading

Conceptual	Functional	Detailed
Establish a continual network adaptation and posture program	• Update IDS with current signatures • Est heuristic analysis for emerging threats • Est emergency restoration program	➢ Source latest signatures ➢ Analyze and categorize emerging threat characteristics ➢ Develop emergency response procedures ➢ For: Operating systems, Server Farms ➢ Routers etc.
End State: Services continuously maintained concurrent with networks postured for continued threat adaptation		

Developing

Conceptual	Functional	Detailed
Train in a dynamic VM environment to test and evaluate work force environmental adaptation and readiness	• Use Red Teams to emulate current and emerging threat • Create network degradations to develop and test adaptation procedures • Create difficult operating environments to assess readiness	➢ Emulate current threats ➢ Expose sensors to known signatures ➢ Emulate emerging tactics ➢ Array emulation via hardware ➢ Array emulation via software ➢ Disable vital functions for assessment ➢ Recon for 0 day vulnerabilities
Training End State: Personnel trained against environment threats and networks postured for continued service		

Conclusion

- Promulgate a vision to generate an omnipotent intent
- Use detailed communication when necessary
- Promote and foster implied communication
- Use power words in communication means to say as much as possible in as little as possible
- Convey intent within conceptual, functional, and detailed planning in order to generate and promote a Unity of Effort
- Training and developing the cyber workforce reflects actual mission demands across the spectrum of the workforce and all leadership tiers