

# The Principle of Maneuver in Cyber Operations

Scott D. Applegate

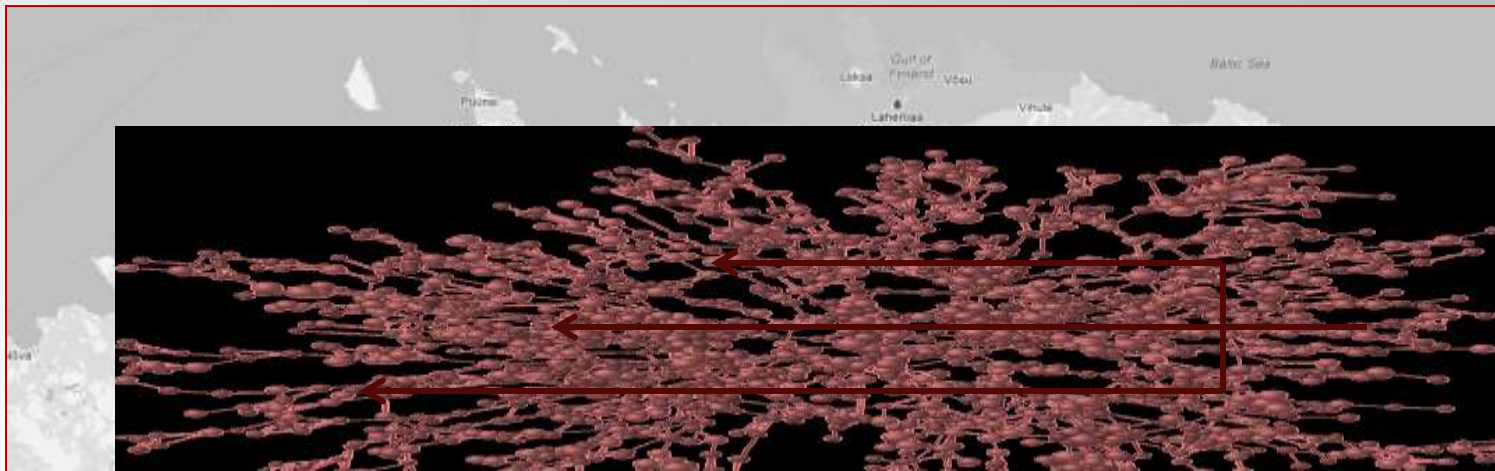
-Lieutenant Colonel, United States Army

-George Mason University

-E-mail: [scott.applegate@us.army.mil](mailto:scott.applegate@us.army.mil)

-E-mail: [scoticus.rex@gmail.com](mailto:scoticus.rex@gmail.com)

-Twitter: [@ScoticusRex](https://twitter.com/ScoticusRex)



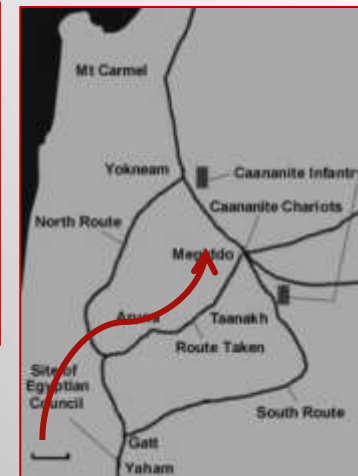
# Agenda

- Introduction
- Maneuver Defined
- Cyber Maneuver Defined
- Characteristics of Cyber Maneuver
- Offensive Cyber Maneuver
- Defensive Cyber Maneuver
- Sovereignty Issues
- Analysis & Conclusions
- Questions & Discussion



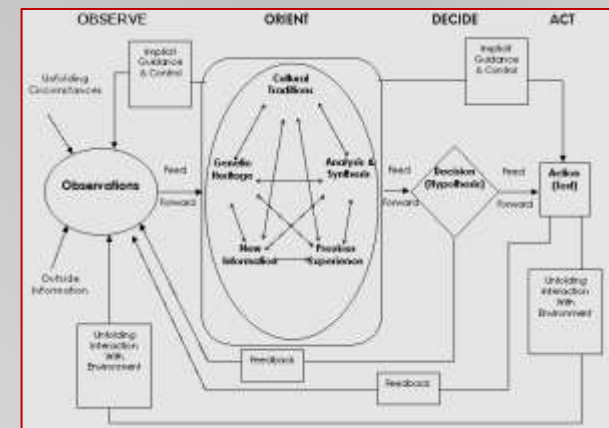
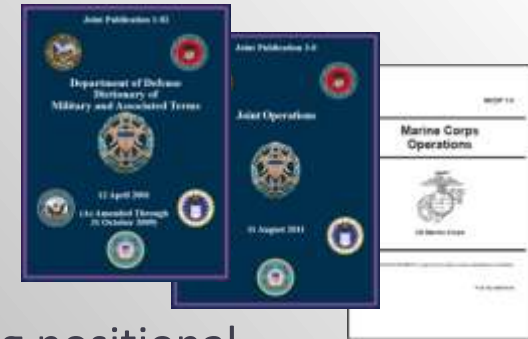
# Introduction

- Maneuver has been a central concept in warfare for thousands of years
  - A determining factor in warfare since some of the earliest recorded battles
  - A concept that has continually evolved throughout history with changes in technology and strategy
  - A concept that has been necessarily altered as new warfighting domains have been added to the spectrum of warfare
- Cyberspace is now considered a Warfighting Domain in the US military
  - It is a unique environment which can distinctly alter many of the time honored principals of war
  - There are a number similarities and differences this domain brings as a warfighting domain in comparison to land, sea, air and space as warfighting domains
  - Cyberspace has manifested itself as a domain of constant conflict involving states, non-state actors and private entities
  - As states build and develop cyber warfare programs, understanding how principles of war apply to this new warfighting domain becomes increasingly important as it is these principles that are used to develop strategy and doctrine



# Maneuver Defined

- The disposition of forces to conduct operations by securing positional advantages *before or during* combat operations and by *exploiting tactical success to achieve operational and strategic objectives* – JP 3.0
- Employment of forces in the operational area through movement in combination with fires *to achieve a position of advantage* with respect to the enemy in order to accomplish the mission – JP 1.02
- The movement of forces for the purpose of gaining an advantage over the enemy – MCDP 1.0
- To operate inside an adversary's observation-orientation-decision-action (OODA) loops or get inside his mind-time-space to penetrate an adversary's moral-mental-physical being in order to isolate him from his allies, pull him apart and destroy his will to resist – Col. John Boyd



# Cyber Maneuver Defined

- The methods and processes employed to attack and defend information resources in cyberspace constitute maneuver as they are undertaken to give one actor a competitive advantage over another
- Cyber Maneuver is the application of force to capture, disrupt, deny, degrade, destroy or manipulate computing and information resources in order to achieve a position of advantage in respect to competitors
  - Force, in cyber maneuver, is the special purpose code written to accomplish the attacker's or defender's objectives and is implemented at the time and virtual location of their choosing
- Cyber Maneuver must take into account, not just nation-state adversaries, but other entities participating in cyber conflict
  - Non-state actors, private entities, surrogates and proxies all engage in hostile operations in cyber space

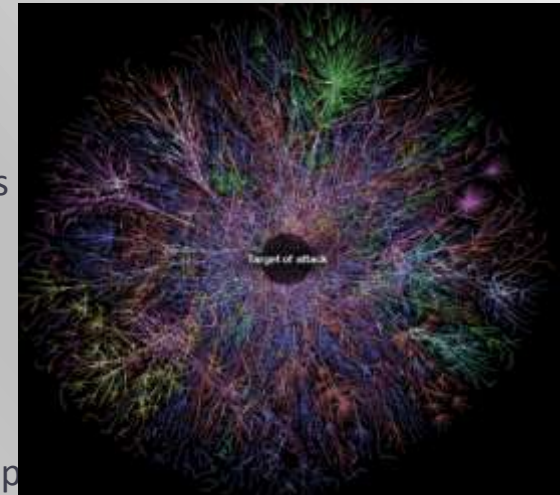


# Characteristics of Cyber Maneuver

- Speed
  - Maneuver at machine speeds, responses often at human decision speeds
  - Speed favors the side which has gained the initiative
- Operational Reach
  - Distance over which military power can be concentrated and employed is almost unlimited
- Access & Control
  - Requires access to friendly, neutral and enemy systems to be effective
  - Move the point of attack forward to systems that are not attributable to source
- Dynamic Evolution
  - Environment is evolving rapidly with new technologies, convergence, political and legal aspects

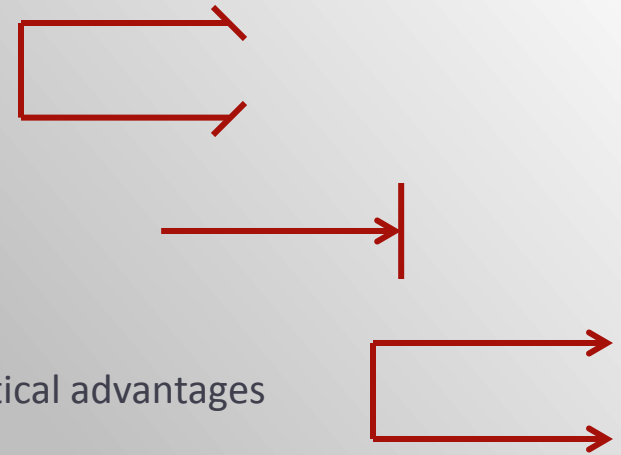
# Characteristics of Cyber Maneuver

- **Stealth & Limited Attribution**
  - Attribution difficult, especially in time sensitive situations
  - Actors make use of virtual anonymity to mask controversial actions
- **Rapid Concentration**
  - Capability for rapid escalation
  - Can rapidly generate distributed mass effects against targets
  - Non-state, informal allies may join actions and become force multipliers
- **Non-serial & Distributed**
  - Actions can be done in parallel against multiple targets creating non-linear effects
  - Non-linear effects can create dilemmas for resource constrained actors who must allocate limited resources
  - Can simultaneously create tactical, operational and strategic effects



# Offensive Cyber Maneuver

- Exploitive Maneuver
  - Capturing information to gain strategic, operational or tactical advantages
  - Information is analogous to terrain in cyber operation
  - Capture and exploitation of key information resources can have decisive results
- Positional Maneuver
  - Capture or compromising key physical or logical nodes in the information environment to be leveraged for follow-on operations
  - Impose will on enemy, increase an enemy's dilemma and gain or maintain initiative
- Influencing Maneuver
  - Use of cyber operations to get inside an adversary's decision cycle or force that decision cycle through direct or indirect means





# Defensive Cyber Maneuver

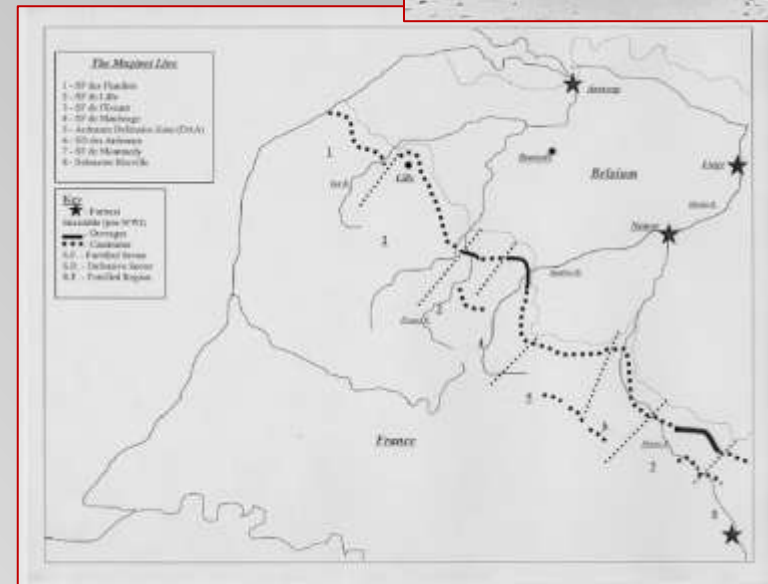
## ■ Perimeter Defense & Defense-in-Depth

- Creating a hard, fixed defensive perimeter to protect interior systems or information resources
- Often mitigated by hardening interior systems
- Highly susceptible to offensive maneuver



## ■ Moving Target Defense

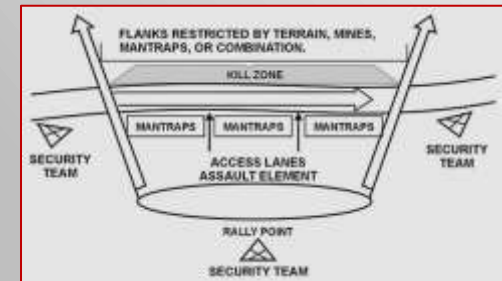
- Uses technical mechanisms to constantly shift aspects of target systems
- Makes it difficult for attacker to identify, target and successful attack targets
- Increases complexity and cost for attacker
- No real kinetic analogy



# Defensive Cyber Maneuver

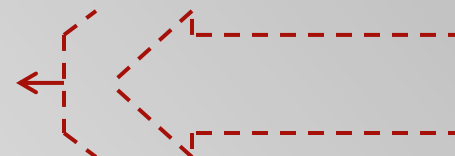
## ■ Deceptive Defense

- Uses processes to lure an attacker into committing actions which reveal methodology or assist defender in attribution
- Can assist defender in gaining initiative and waste attacker resources
- Virtual analogy to kinetic ambush



## ■ Counter-Attack

- Direct virtual analogy of kinetic counter attack
- Execution complicated by difficulty in attribution and use of third-party systems by attacker



# Sovereignty Issues

- Cyberspace often described as borderless
  - Issues of jurisdictional uncertainty and transcendence of international borders
  - Use as a global commons
  - Balkanization
- More accurate view would be of a vast virtual frontier with millions of small enclaves that are interconnected
  - States often have a vested interest in protecting these enclaves and exercising control & authority over them
  - How can states exercise sovereignty over portions of cyberspace?
    - Geographic borders
    - Logical borders

# Sovereignty Issues

- Maneuver in cyberspace and sovereignty

- What would constitute a violation of sovereignty in cyberspace?

At what point does this become a hostile act?

- Third party states and cyber maneuver

Would permission from friendly or neutral states be required before conducting digital maneuver through their systems?

Use of third-party systems to mask attribution





# Analysis & Conclusions

- Maneuver in cyberspace has unique aspects, but its basic objective remains the same – to gain a position of advantage and leverage that position for decisive success
  - Information is the terrain and currency of warfare in cyberspace
  - Initiative is vitally important in cyber maneuver since actions are far quicker than reactions in this domain
  - Actors must take into account that not just states, but non-state actors and private entities are directly involving themselves in cyber conflict
  - Unlimited operational reach combined with non-linear effects add to complexity faced by decision makers in this domain
  - Difficulty in attribution makes it possible to conduct hostile acts with little or no retribution

# Analysis & Conclusions

- Sovereignty issues will play an important role in cyber maneuver as the international community tries to come to consensus on how borders are applicable in cyberspace and how to define them





# Future Work

- Defining cyber maneuver at the strategic, operational and tactical levels of war and understanding how this concept applies to the joint force commander
- Developing an empirical framework for analyzing and contrasting maneuver in cyberspace with maneuver in the other warfighting domains
- Expanded analysis of other key principles of warfare in relation to cyber operations

