Cyber Operations as a Counter Insurgency (COIN) Operation

Bob Ringdahl

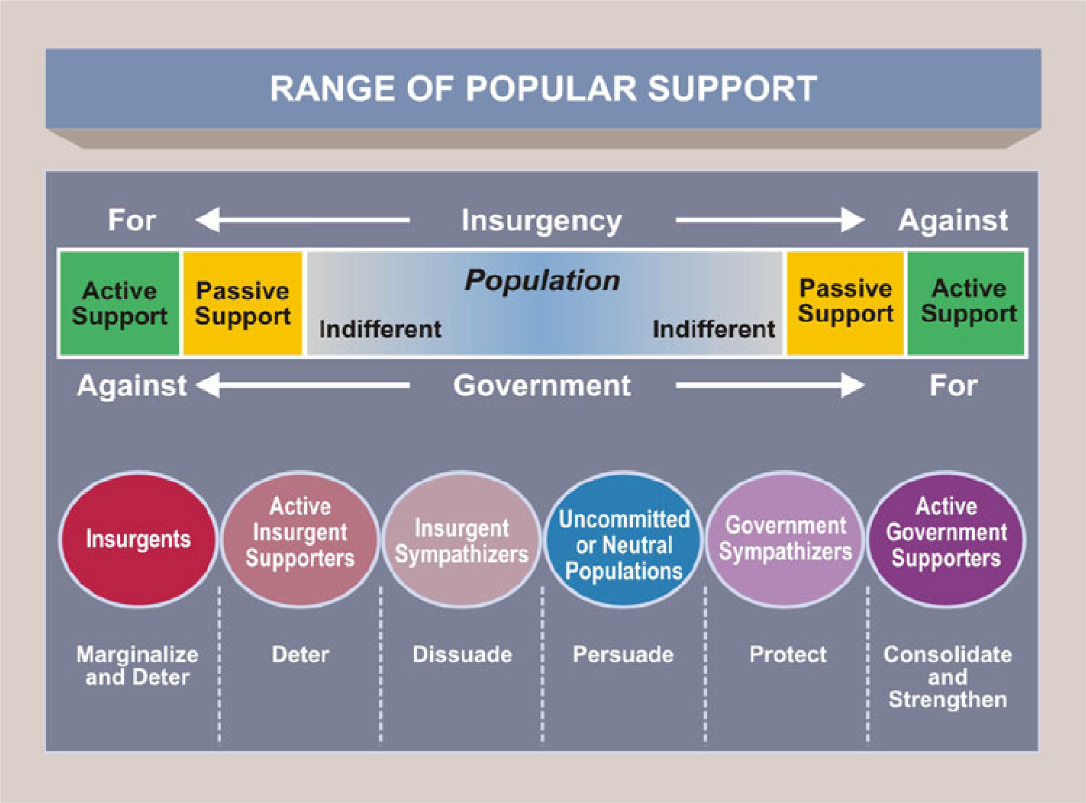
Robert.Ringdahl@gartner.com

(m) +1 571-379-6239

Gartner®

Premise

- Geography-based insurgency efforts share many characteristics with activities within the Cyber domain. Therefore, Counter-Insurgency (COIN) doctrine, tactics and processes can be applied as well to the Cyber domain, particularly in the area of Computer Network Defense (CND).



Goals

- Land Domain*: Insurgents seek to subvert or displace the government and completely or partially control the resources and population of a given territory.

- Cyber Domain corollary: Adversaries seek to subvert or displace IT organizations and completely or partially control the IT resources and user identities of a given IT environment.

*US Government CounterInsurgency Guide – Jan 09

The Adversaries

Land Domain*

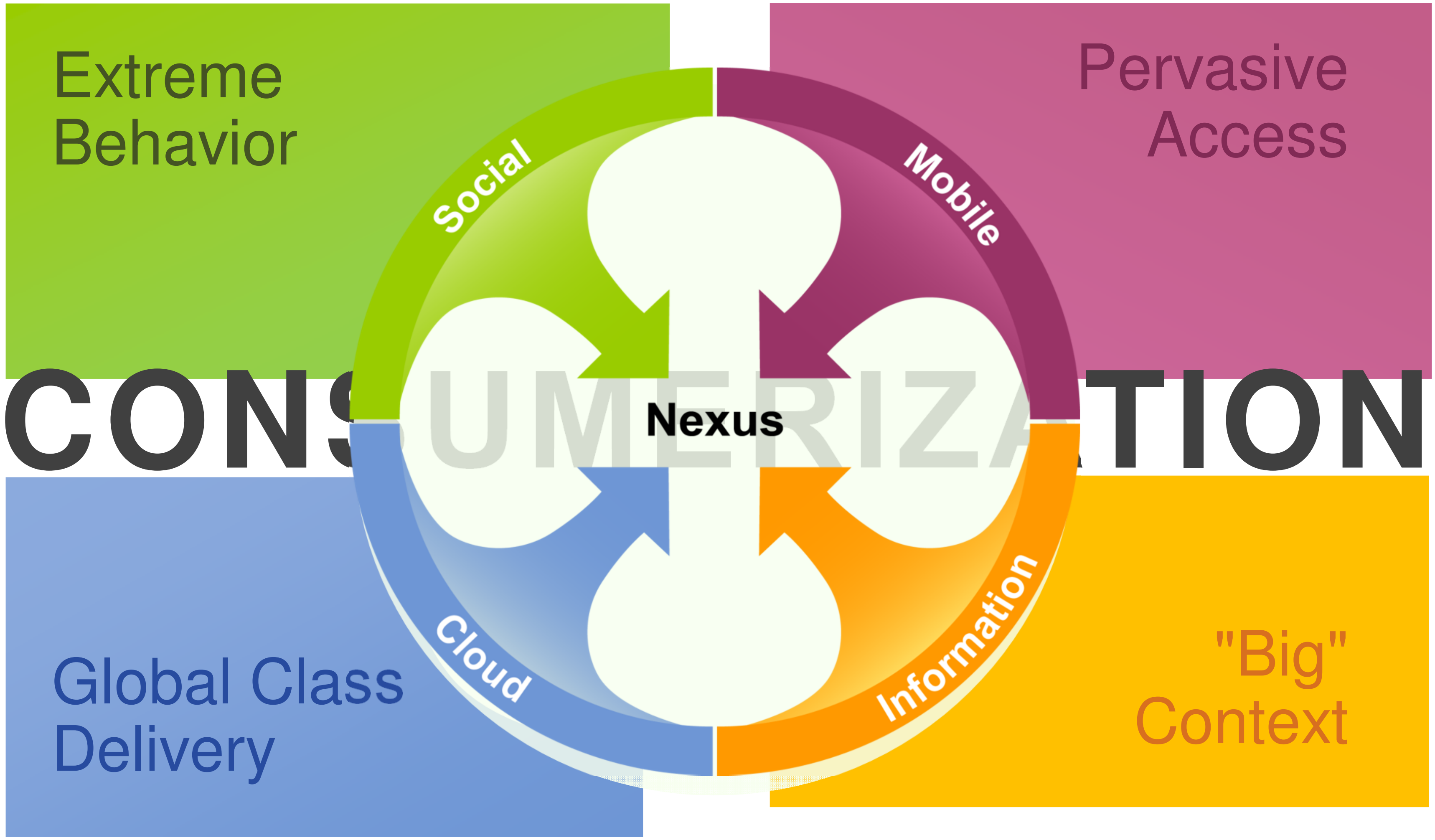
- **Some adversaries in a COIN environment directly challenge** the Host Nation, while others merely cause instability.
- **Insurgencies.**
  - **The most advanced** has an associated political party, an underground organization, and a military wing.
  - **The second** has both an underground and military component.
  - **The third** is military-focused
- **Other Major Adversaries –** drug traffickers & international terrorists.

Cyber Domain

- **Some adversaries in the Cyber domain directly challenge** the ability of the IT organization to function while others cause fear, uncertainty, and doubt (FUD)
- **Adversary Types:**
  - **The most advanced** are state (or semi-state) sponsored groups
  - **A second** is an ideologically driven organization or group of attackers.
  - **A third** is the lone or small group hacker.
- **Other major adversaries** are cyber criminals.

*US Joint Pub 3-24, Counter Insurgency Operations, 5 October 2009

The Battlespace



Extreme Behavior

Pervasive Access

CONSUMERIZATION

Nexus

Social

Mobile

Cloud

Information

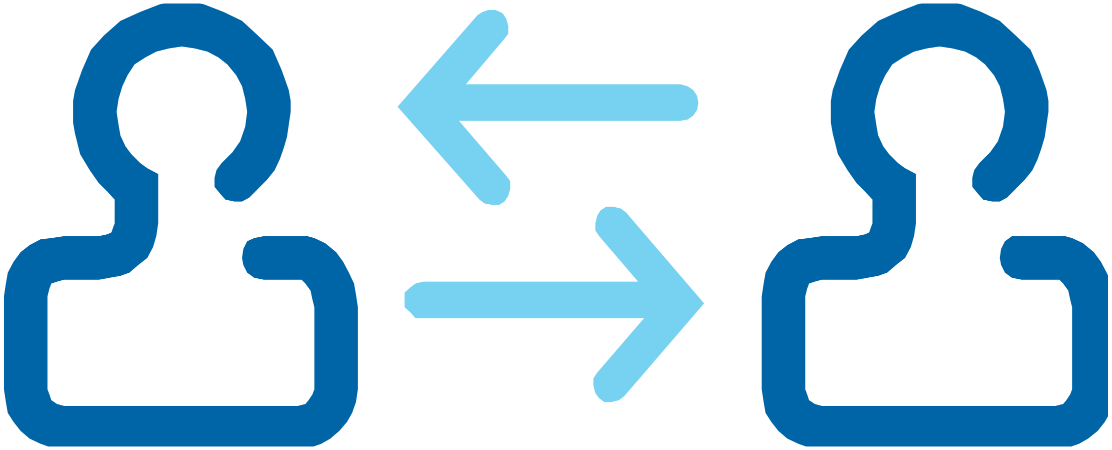
Global Class Delivery

"Big" Context

Gartner®

Selected Shared Characteristics

- Uncertainty who the enemy is
- Shared use of key infrastrucuture
- Dependency on, at least passive support of some of the population (voluntary or coerced)
- Lack of defined “battle” and “rear” area



Principles of Counterinsurgency*

- Counterinsurgents Must Understand the Operational Environment.
- Legitimacy Is The Main Objective. The primary objective of any COIN operation is to foster development of effective governance by a legitimate government.
- Unity of Effort is Essential.
- Political Factors are Primary.
- Intelligence Drives Operations.
- Insurgents Must be Isolated from Their Cause and Support.
- Security Under the Rule of Law is Essential.
- Counterinsurgents Should Prepare for a Long-Term Commitment.
- Manage Information and Expectations.
- Use the Appropriate Level of Force.
- Learn and Adapt.
- Empower the Lowest Levels.
- Support the Host Nation.

*US Joint Pub 3-24, Counter Insurgency Operations, 5 October 2009

Select COIN Principles Applied to Cyber

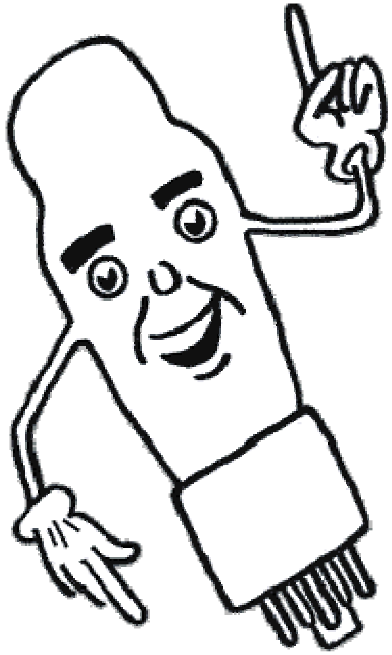
- **Understand the Operational Environment** – understand the end-user mission environment and how they use IT resources on a daily basis
- **Political Factors are Primary** – end-user acceptance and active support is critical. End-users have to feel they have a stake in the fight – peer pressure is the most effective form of self-governance.
- **Intelligence Drives Operations** – know the enemy and friendly situation on a minute-by-minute/hour-by-hour basis. Know the trends as well as the active threats. Employ “every soldier a sensor” concept to update both enemy and friendly situation.
- **Learn and Adapt** – yesterday’s solution will not prevent tomorrow’s problem. Measure performance of counter-measures and understand what works and what doesn’t. Focus on agility, virtualization, segmentation.
- **Empower the Lowest Levels** – commanders, leaders, managers at all levels of the organization need to have some decision authority over the risk acceptance and operational processes associated with their mission
  - Access to enemy and friendly intel
  - Have a personal stake in the outcome
  - Be held accountable for their decisions

Tactical Approaches Used in COIN Fight

- **Indentify and Authenticate everyone everywhere** – require overt identity verification upon access to each major capability
- **Up-Armor convoys** – encrypt all data as it traverses the network – at a minimum the WAN, but possibly the CAN as well
- **Checkpoints away from critical facilities** – perform initial packet analysis outside the DMZ
- **Have established procedures for quick response to incidents** – develop, implement, and frequently exercise incident response procedures
- **Identify and authenticate users at random checkpoints** – implement random re-authentication in mid-session
- **Multiple sensors viewing the same real estate** – use multiple sensors to monitor different aspects of a critical capability with correlation of resulting data to develop a comprehensive picture of anomalous behavior

Closing Thoughts

- Land Domain and Cyber Domain are not the same
- Challenge within the Cyber Domain is to successfully apply the lessons learned from operations in other domains in an appropriate cyber context
- Believing the Cyber approaches of the 90’s will be adequate in the “Nexus of Forces” environment is equivalent to believing the WWII approach to Land combat would work in Iraq



Suggested Reading

- US Joint Pub 3-24, Counter Insurgency Operations, 5 October 2009
- Related Gartner Research
  - Application Security Technologies Enable Enterprise Security Intelligence, ID:G00207063
  - Effective Security Monitoring Requires Context, ID:G00201284
  - SIEM Enables Enterprise Security Intelligence, ID:G00209082
  - Best Practices in User ID Formation, 2012 Update, ID:G00238344
  - Defining Authentication Strength Is Not as Easy as 1, 2, 3; Update, ID:G00219391
  - Best Practices for Managing Identity Data and Log Models to Optimize Identity Data Quality, ID:G00230033
  - Identity and Access Intelligence: Making IAM Relevant to the Business, ID:G00210038

Gartner delivers the technology-related insight necessary for our clients to make the right decisions, every day.

Acronyms

- CAN – Campus Area Network
- CND – Computer Network Defense
- COIN – Counter Insurgency
- DMZ – Demilitarized Zone
- IAM – Identity and Access Management
- IT – Information Technology
- SEIM – Security Event and Information Management
- WAN – Wide Area Network
- WWII – World War 2