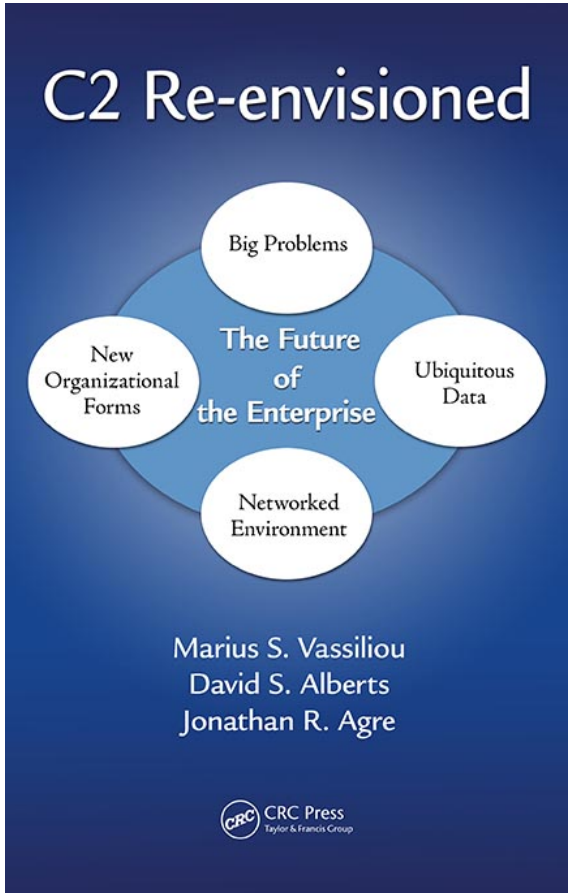
Mission Success: Agile Organizations and Assured Communications are Key

Presented at George Mason University
Fairfax, VA, 31 Oct. 2016

Marius Vassiliou, PhD
Institute for Defense Analyses,
Science & Technology Division
Alexandria, VA
mvassili@ida.org

Context

- **Big-picture conceptual study of Command, Control, Communications at Institute for Defense Analyses (IDA)**
- **For US DoD, Office of Assistant Secretary of Defense for Research & Engineering**
  - Cindy Dion-Schwarz
  - David Jakubek
  - Syed Shah
- **Part of study:**
  - Studied 20 operational cases of C2 failure since WW1
  - Military operations
  - Terrorist Attacks
  - Disaster & Emergency Response



Shameless plug?

C2/Enterprise Failures—Bottom Line

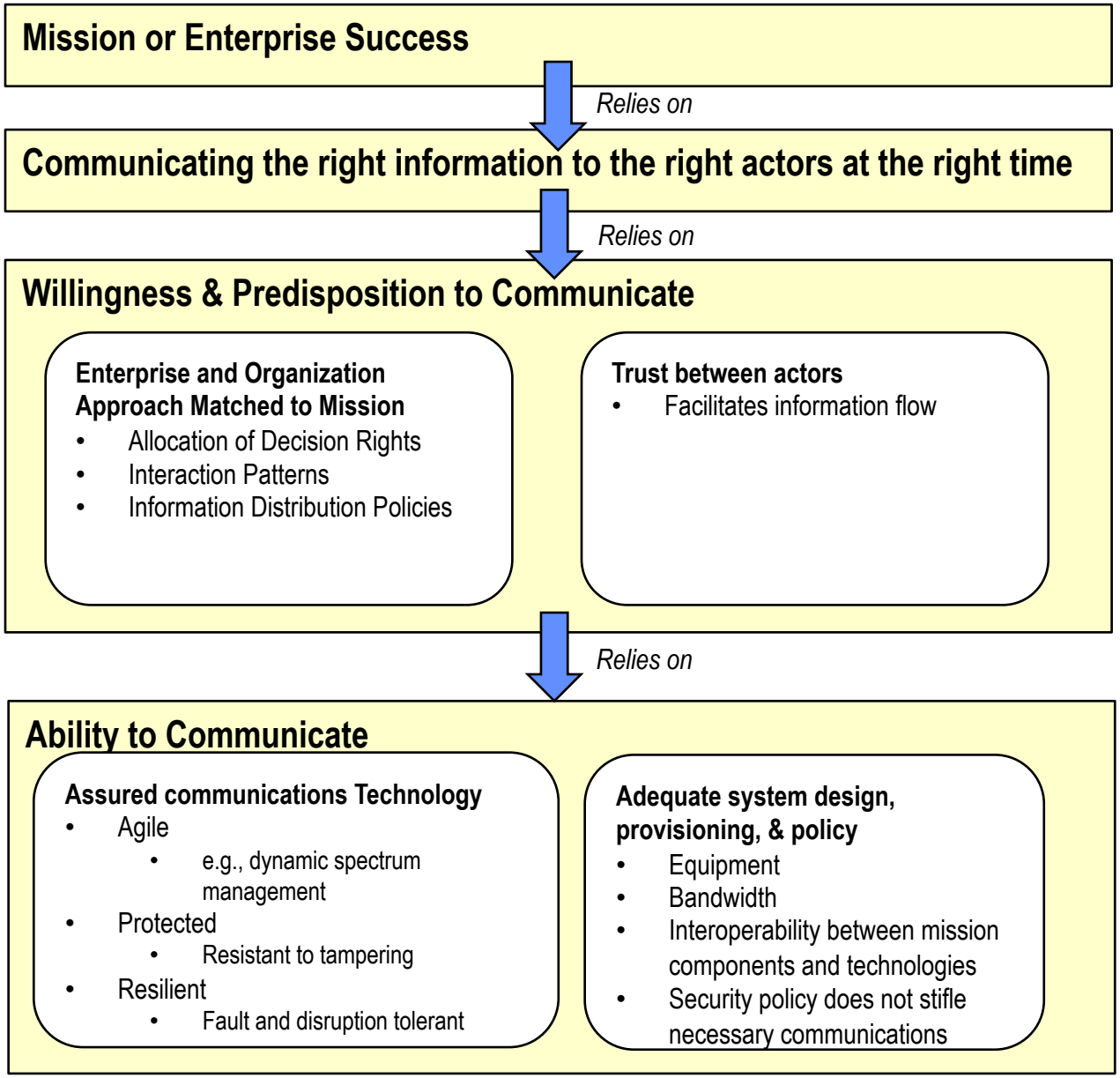
Somebody *couldn't* talk to somebody

or

Somebody *didn't* talk to somebody

"Talk" = Communicate, share, interact, speak, etc. etc.

Mission or Enterprise Success



Couldn't or Didn't

Couldn't Talk

- *Because of **circumstances***
  - Infrastructure/Equipment destruction, damage
  - Physical constraints
  - Denial by adversary
- *Because of **system design or policy shortfalls***
  - Interoperability Problems
  - Equipment or bandwidth shortage
  - Security constraints

Exacerbates ←

Inappropriate Enterprise Approach/Organization Design

Didn't Talk

- Behavioral failures
- Lack of will
- Lack of incentive
- Lack of Knowledge
- Lack of Trust (Individual)
- Lack of Trust (Institutional)
- Lack of Tools

Causes ←

Inappropriate Enterprise Approach/Organization Design

C2 Failure Characterization—Military Cases

Military Operations

Incident	Inappropriate C2 Approach/Organization Design	Behavioral Failure to Communicate	Inability to Communicate: Because of system design or policy shortfalls: Lack of Interoperability	Equipment or Bandwidth Shortage	Security Constraints	Because of circumstances: Infrastructure/Equipment Destruction or Damage	Physical constraints	Denial by Adversary
Great Retreat of 1914, First World War	■	■		■			■	
German army in runup to 1st Battle of the Marne, First World War	■	■		■	■		■	■
1st Battle of Savo Island, Guadalcanal Campaign, Second World War	■	■						
Mayaguez Incident	■	■		■		■		
US Hostage Rescue Mission	■	■	■	■	■	■	■	
US Invasion of Grenada			■	■				
First Gulf War, Operation Desert Storm, FSCL	■							
Russia-Georgia War	■		■	■				

Didn't Talk

- **Battle of Savo Island, Aug. 8, 1942 (Guadalcanal Campaign, WW2**
  - Cruiser groups of Allied screening force guarded against Japanese naval attack
  - On night of battle, commander of the screening force, Rear Adm. V.A.C. Crutchley, took his ship out of the southern cruiser group to attend conference with Admiral Richard Turner
  - Did not inform 2nd-in-command, Capt. Frederick Riefkohl, who was in the northern cruiser group
  - Riefkohl remained ignorant that he was now in command of the screening force
  - Moreover, a crucial radio message warning of an impending attack was not relayed to Riefkohl, because of human error
  - Japanese attacked, with no coordinated response

http://upload.wikimedia.org/wikipedia/en/6/69/V_A_C_Crutchley.jpg

Adm. Crutchley

http://navyphotos.togetherweserved.com/2113785.jpg

Capt. Riefkohl

http://www.ibiblio.org/hyperwar/USN/USN-CN-Savo/img/USN-CN-Savo-1.jpg

Iran Hostage Rescue (1): *Couldn't* Talk

Security

- C-130 transport airplane heading to landing site ("Desert One") encountered a large desert dust cloud (a *haboob*)
- *Haboob* not a major problem for the airplane but serious threat to 8 helicopters following far behind
- C-130 did not warn the helicopters because of strict dictate of radio silence
- Helicopters entered *haboob*
- Because of radio silence could not tell each other what they were doing or where they were going
- One helicopter had to abort because of a suspected blade failure Two others left *haboob* & landed
  - First: Group Leader
  - Second: Helicopter carrying spare parts
- Leader made secure call to U.S. command center in Egypt
  - Told to proceed to the rendezvous landing site ("Desert One")
  - But none of the other helicopters could hear the conversation
- Second made independent decision to return to aircraft carrier *Nimitz*
  - None of the helicopters could talk directly to Desert One and thereby learn that landing site was clear
  - Later he said he would have continued had he known
- Critical loss of needed helicopters and crucial spare parts at Desert One

Interoperability

- Army Rangers guarding landing site in the Iranian desert used radios that could not communicate with Delta Force or Air Force personnel
- Rangers unable to inform ground commanders in a timely fashion when a bus full of Iranian civilians appeared, complicating the operation.
- Landing site could not talk to the helicopter fleet

Example of a *haboob* (Iraq, 2005)

http://upload.wikimedia.org/wikipedia/commons/7/75/Sandstorm.jpg

http://dmn.wpengine.netdna-cdn.com/wp-content/uploads/2012/07/RH-53-Sea-Stallions-Iran-Operation.jpg

Iran Hostage Rescue (2): Enterprise Approach

Not predisposed to effective communication

- Highly complex operation
- Several organizations
  - US Army Delta Force
  - US Army Rangers
  - US Air Force Pilots
  - US Navy Helicopter Pilots
- Compartmentalization & mutual mistrust
- Lack of unified command
  - No single component commander to unify AF airplanes and Navy helicopters
  - No single ground component commander to unify Delta Force & Rangers
- Put this together with communications interoperability problems, security constraints, and bad luck, and you get disaster

The Franco-German Wars: Enterprise Approach & Communications

- **Mission Command ("auftragstaktik")**
  - Prussian/German tradition beginning 19th Century
  - Stresses individual initiative by commanders
  - Orders are general, leave details of execution open
  - Can create coordination problems

1871 → **1914** → **1940**

Franco-Prussian War 1870-1871
- Northeast France, over 10 months
- Largest battles ~100K men on each side
- No motorization, no electronic communications
- Combination of scale, speed, communications & approach meant coordination burden manageable

German Western Offensive 1914 (WW1)
- Belgium & France, over 1 month
- Culminating Battle of Marne ~1M men on each side
- Some motorization, primitive electronic communications
- Combination of scale, speed, communications & approach meant coordination burden unmanageable

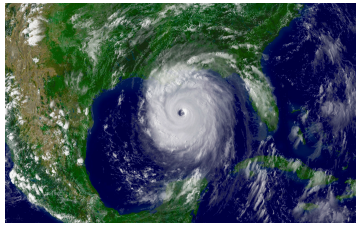
Battle of France, 1940 (WW2)
- Low countries & France, over 1.5 month
- ~3M men each side
- Considerable motorization, improved electronic communications
- Combination of scale, speed, communications, & approach meant coordination burden manageable

C2 Failure Characterization—Terrorist Cases

Terrorist Attacks

Incident	Inappropriate C2 Approach/Organization Design	Behavioral Failure to Communicate	Inability to Communicate: Because of system design: Lack of Interoperability	Because of system design: Equipment or Bandwidth Shortage	Because of system design: Security Constraints	Because of circumstances: Infrastructure/Equipment Destruction or Damage	Because of circumstances: Physical constraints	Because of circumstances: Denial by Adversary
Oklahoma City Bombing Response	■		■	■				
911 Attacks Response and Possible Prevention	■	■	■	■	■	■	■	
7/7 London Bombings Response			■	■		■		
2011 Norway Attacks Response	■	■						

C2 Failure Characterization—Disaster Response Cases



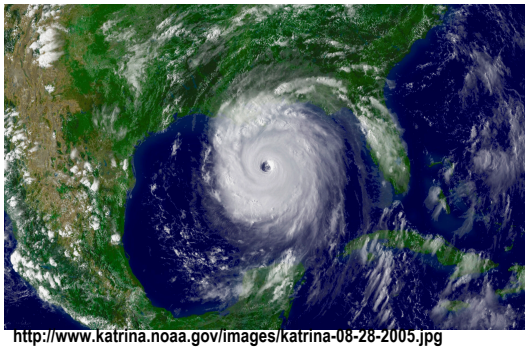
Disasters and Emergencies

			Inability to Communicate:					
			Because of system design			Because of circumstances		
Incident	**Inappropriate C2 Approach/Organization Design**	**Behavioral Failure to Communicate**	Lack of Interoperability	Equipment or Bandwidth Shortage	Security Constraints	Infrastructure/Equipment Destruction or Damage	Physical constraints	Denial by Adversary
King's Cross Underground Fires Response	■	■	■	■		■	■	
Clapham Railway Junction Accident Response	■	■		■		■		
Hillsborough Stadium Disaster Response	■	■				■		
Hurricane Andrew Response	■	■	■	■		■		
Columbine High School Shootings Response	■		■					
Indian Ocean Tsunami Response	■	■	■	■		■	■	
Hurricane Katrina Response	■	■	■	■		■	■	
Black Saturday Fires Response	■	■	■	■		■	■	

Couldn't Talk: Interoperability

Hurricane Katrina, 2005

- DoD no information sharing protocol for situational awareness between all deployed military units
- Interoperability problems between units of different federal, state, & local agencies on the ground
- Joint Task Force Katrina, National Guard, & States of Louisiana and Mississippi could not talk to each other



http://www.katrina.noaa.gov/images/katrina-08-28-2005.jpg

Australia Black Saturday fires, 2009

- Metropolitan & regional police forces--incompatible radio systems
- No interoperability between different emergency agencies

http://www.sydneycare.org.au/content/r337173_1529332.jpg

King's Cross Underground fire 1987

- No interoperability between different emergency agencies
- No interoperability and between them & London Underground
- Identified as problem in Fennell Report (1988)
- But recurred at least partially in response to the 2005 "7/7" London bombings

http://secondsfromdisaster.net/wp-content/uploads/2013/01/kings-cross-fire.jpg

Couldn't Talk: Interoperability

- **9/11 Run-up**
  - No interoperability between IT & C2 systems of FAA & NORAD
- **9/11 Aftermath**
  - Units of first responders on the ground often unable to communicate with each other
  - Port Authority Police Department radios could not talk to those of the FDNY

http://totallycoolpix.com/wp-content/uploads/2011/10092011_remembering_9_11/nyc_002.jpg

http://totallycoolpix.com/wp-content/uploads/2011/10092011_remembering_9_11/nyc_008.jpg

Couldn't Talk: Interoperability

Russia-Georgia War, 2008

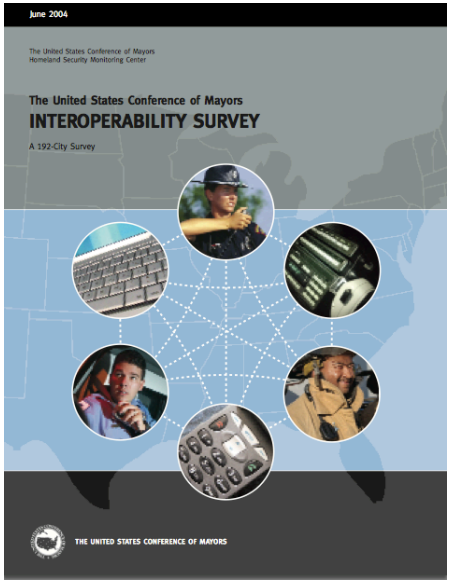
- Ground units unable to communicate with space-based &electronic intelligence assets
  - Russians could not employ electronic warfare systems to full advantage to suppress Georgian air defenses
  - Could not make full and effective use of satellite targeting support or precision guided munitions
- Interoperability problems between units of different services of Russian armed forces
- Ground commanders very little control over needed air support
  - Reportedly, Colonel General Aleksandr Zelin directed air operations personally by mobile phone from Moscow

http://www.defence.pk/forums/military-forum/170680-russian-commander-explains-air-force-acquisition-plan.html

Interoperability

Study of 192 U.S. cities published 2004 by U.S. Conference of Mayors

- 86% did not have interoperable communications with their state transportation department
- 83% not interoperable with the DoJ or DHS
- 60% not interoperable with their state emergency operation centers
- 49% not interoperable with state police.



Considerable effort and progress since then, but problem is still pervasive around the world

- e.g., in UK, interoperability problems were rife in 1987 King's Cross Underground Fire; 20 years later in the 7/7 2005 attacks, many still persisted
- In US, congress established Office of Emergency Communications under DHS, with interoperability an important goal
- Audit in 2012 still found pervasive interoperability issues; second report in 2015 found problems persisting

Promising technical approaches

- Project 25
- EU FREESIC
- But problem of huge legacy base in thousands of agencies still persists
- More an acquisition/technology/logistics problem than an R&D problem?

Enterprise Approch “No one in charge”

Incident	Quote	Reference
Black Saturday Fires Response	"...roles of the most senior personnel were not clear, […] **no single agency or individual in charge**…"	Parliament of Victoria, 2009 Victorian Bushfires Royal Commission (2010), p.8
Hurricane Andrew Response	"...**failure to have a single person in charge** with a clear chain of command."	Florida Governor’s Disaster Planning and Response Review Committee (1992), p. 60
9/11 Attacks	"...**no one was firmly in charge** of managing the case...Responsibility and accountability were diffuse." [about intelligence]	National Commission on Terrorist Attacks upon the United States (2004), p.400
King's Cross Fire Response	"...**uncertainty over which** of the London Underground **staff was in charge**…"	Fennell (1988), pp. 73-74
Iran Hostage Rescue	"…confusion about '**who was in charge**'"	Anno & Einspahr (1988), p.10
	"…**uncertainty as to who was in charge**."	Thomas(1987) p.10
	"…**no one..who was in overall charge**…"	Gass (1992), p.15
	"...**no way to** quickly **find out** or locate **who was in charge**…"	Holloway (1980), p. 51
Mayaguez Incident Response	"[planning activity] lacked coordination…**No one seemed to be in charge**."	Toal (1998), p.18
Hurricane Katrina Response	"...**no single individual who took charge**…"; "State officials and FEMA **disagreed about who was in charge**…"	Moynihan (2006), pp. 22,24
	"Too often, because everybody was in charge, **nobody was in charge**."; "…**no consensus on who was in charge**."; "... **disagreed on who was in charge**,**could not find out who was in charge**, or **did not know who was in charge**…"	U.S. House of Representatives (2006), pp. xi, 185, 186
Indian Ocean Tsunami Response	"...coordinating meetings were 'very unwieldy' and 'internal coordinating meetings were a shambles.'"	Huber et al. (2008), p.4
Columbine High School Shootings	"…**'Who's in Charge?' No one could answer the question**."	Moody (2010), p.39

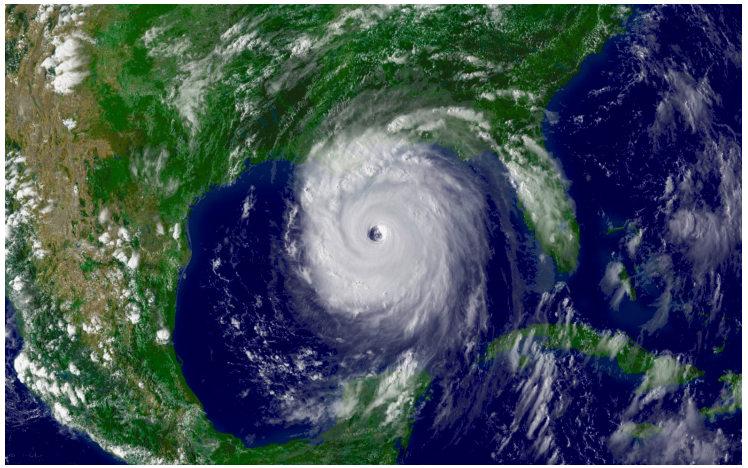
This Does Not Mean a Single Entity Always has to be “in Charge”

- Key is C2 approach matched to mission & circumstances
- Shared awareness & intent
- Roles & responsibilities understood

Inappropriate Enterprise Approach

Hurricane Katrina, 2005

- Roles of U.S. federal agencies were not properly delineated
- Neither was relationship to state & local agencies
- Major structural *a priori* coordination deficits between
  - DoD
  - FEMA
  - State of Louisiana
- E.g., Both local police & National Guard working at Louisiana Superdome
  - But each side said the other was supposed to lead
  - This led to security problems, & many responders left



http://www.katrina.noaa.gov/images/katrina-08-28-2005.jpg

Inappropriate Enterprise Approach

Similar problems in other disasters

- **Indian Ocean Tsunami, 2004**
  - Militaries from 11 countries
  - Each had different relationship with Indonesian Government
  - Lack of coordination between:
    - The various militaries
    - The militaries & NGOs
    - The International NGOs & Indonesian NGOs
    - US & UN agencies
  - Meetings “a shambles” [NATO SAS 065]
- **Australia Black Saturday Fires, 2009**
  - Roles of senior personnel unclear
  - Victoria Country Fire Authority (CFA) & Victoria Dept. of Sustainability & Environment (DSE) followed inconsistent operating procedures
- **King’s Cross Underground Fire, 1987**
  - London Underground uncoordinated, haphazard
  - Poor coordination between London Underground, Police, & Fire Agencies

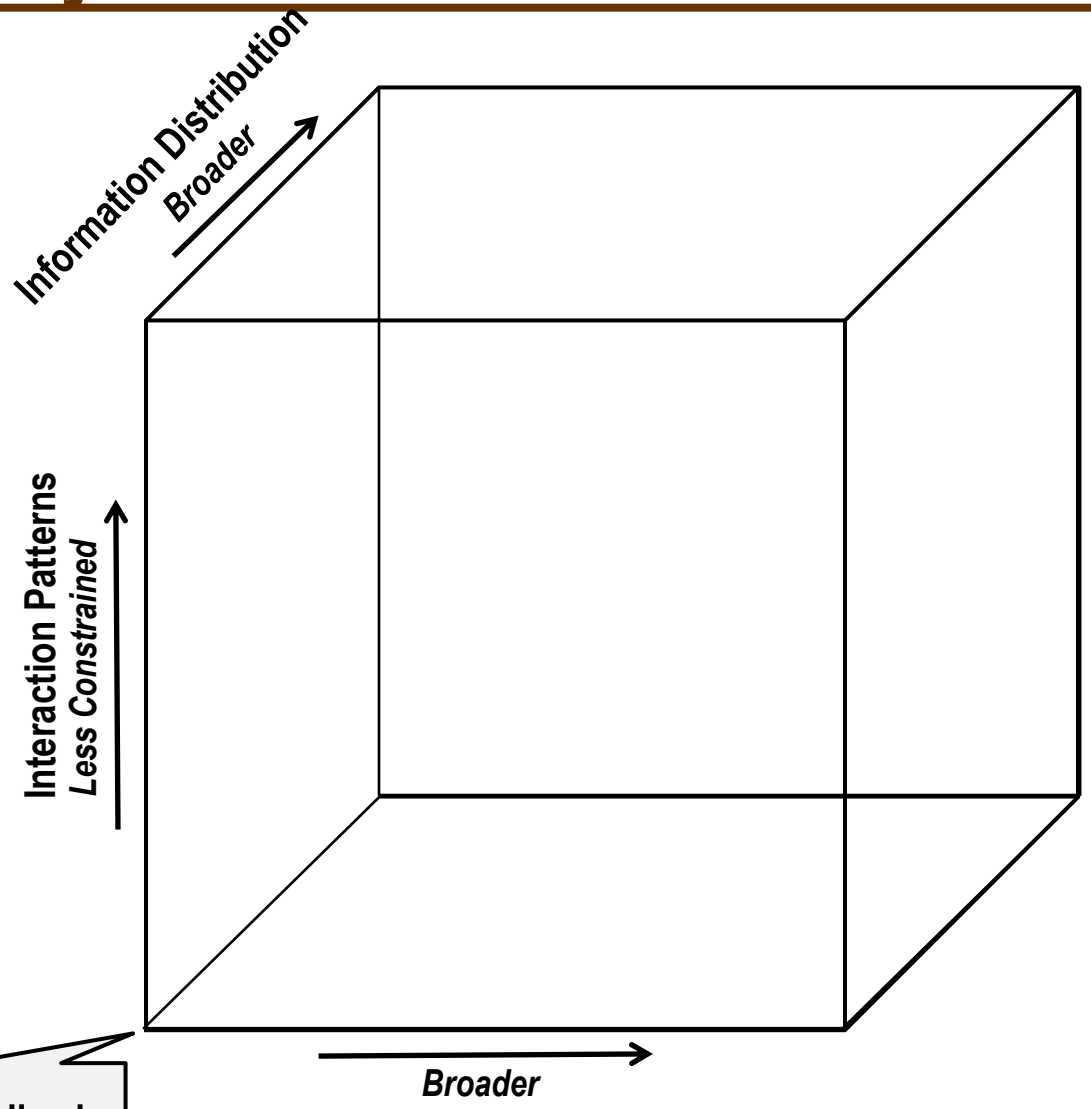
http://www.sanandreasfault.org/Sumatra1.jpg

http://www.sydneycare.org.au/content/r337173_1529332.jpg

http://secondsfromdisaster.net/wp-content/uploads/2013/01/kings-cross-fire.jpg

Enterprise Approach: Alberts-Hayes Characterization

- Less Centralized
- More Net-Enabled



- More Centralized
- Less Net-Enabled

Can apply to single organizations or to collectives of multiple organizations

Burgess & Fisher Command Level Framework (CLeF)

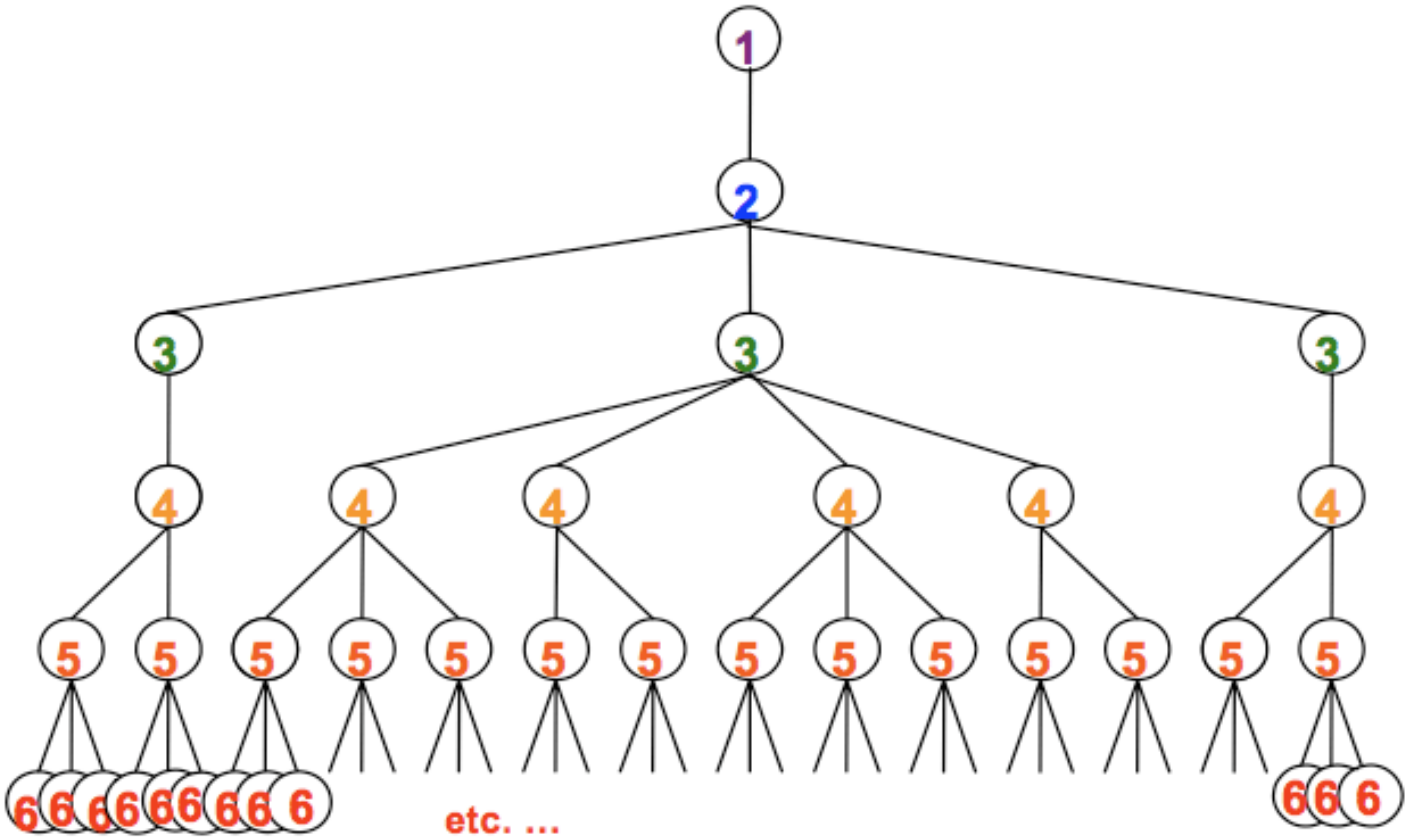
- **Cast in terms of conventional hierarchical descriptors**

CLeF No.	Key Function	Conventional descriptor	
1	What is the problem? Who is: us, the enemy, our allies and others?	National Strategic	Strategic
2	What can we do about it? Who plays and who pays?	Military Strategic	
3	How and when will we deal with it? When, where - resources to be used?	Operational	Operational
4	Who? - team formation, preparedness, orchestrate the effects.	Joint	
5	How? – Targets for effects	Tactical	Tactical
6	Actions required - individual	Individual	

Burgess & Fisher, Australia DSTO-TN-0826 (2008)

Command Level Framework (CLeF)

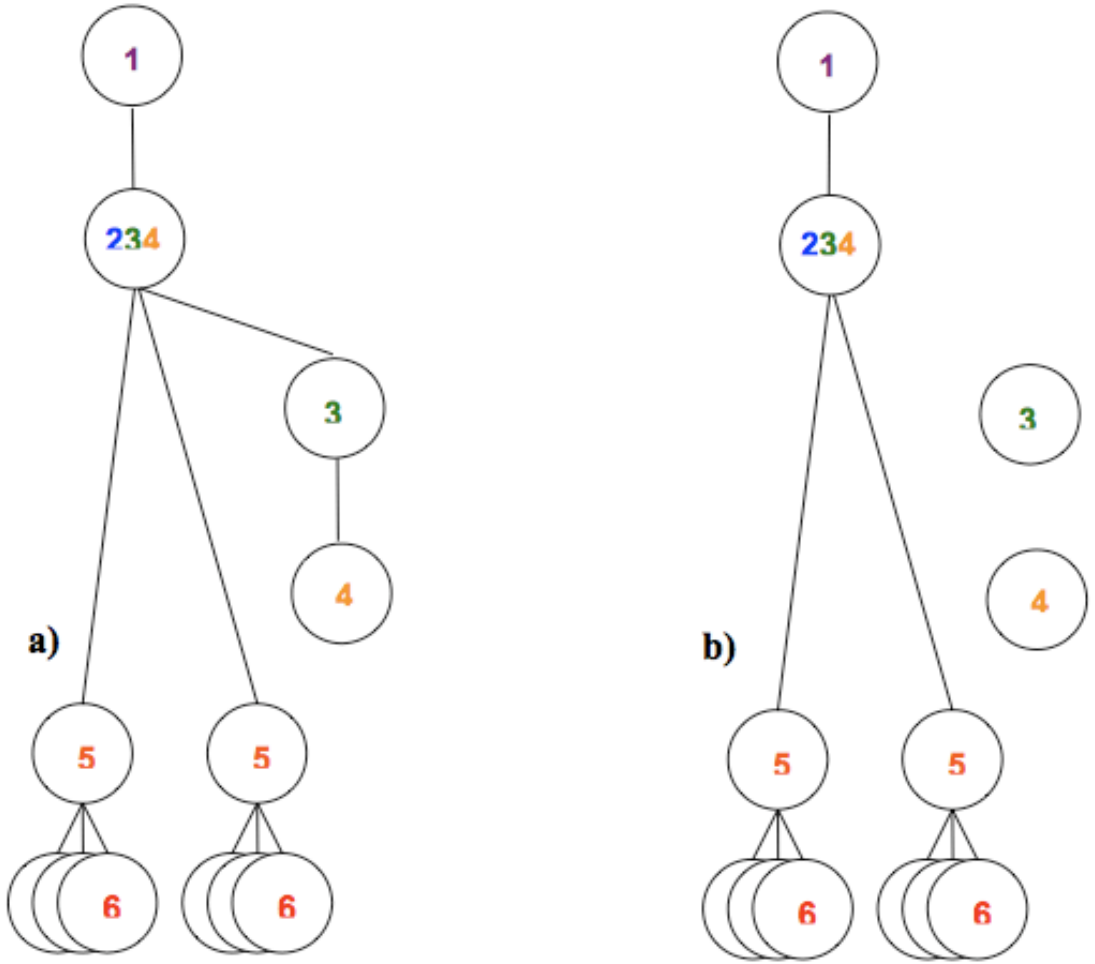
- Traditional hierarchical command structure



Burgess & Fisher (2008)

Command Level Framework (CLeF)

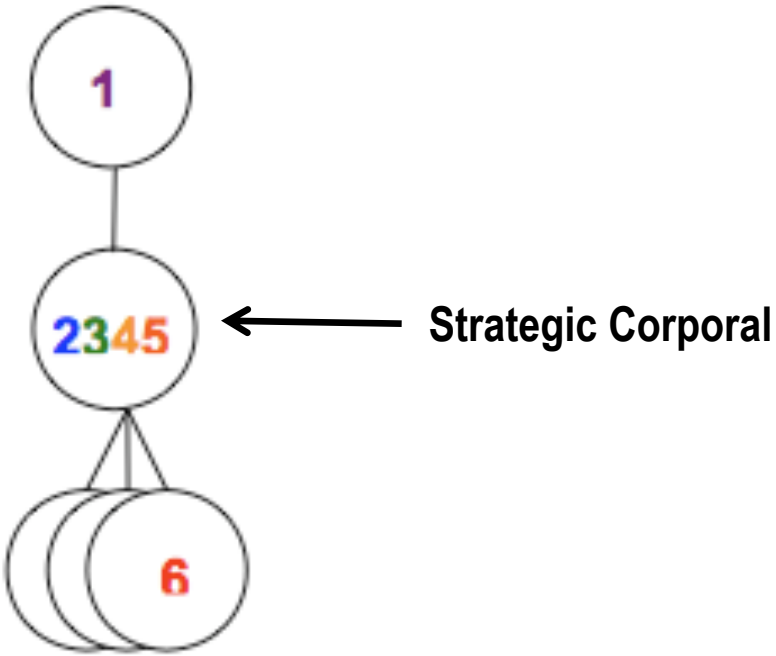
- The “6,000-mile long screwdriver”



Burgess & Fisher (2008)

Command Level Framework (CLeF)

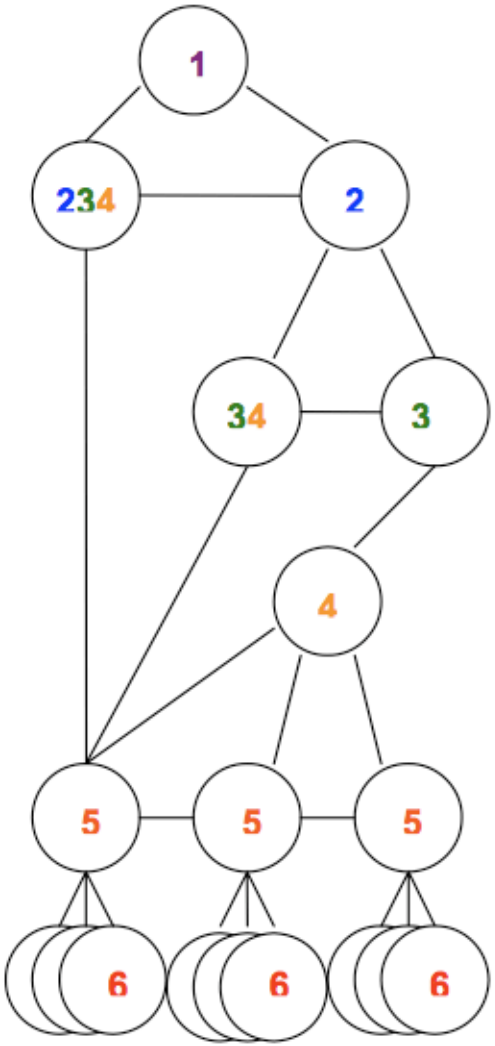
- The “Strategic Corporal” in a “3-block war”
- Consistent with Mission Command Concepts



Burgess & Fisher (2008)

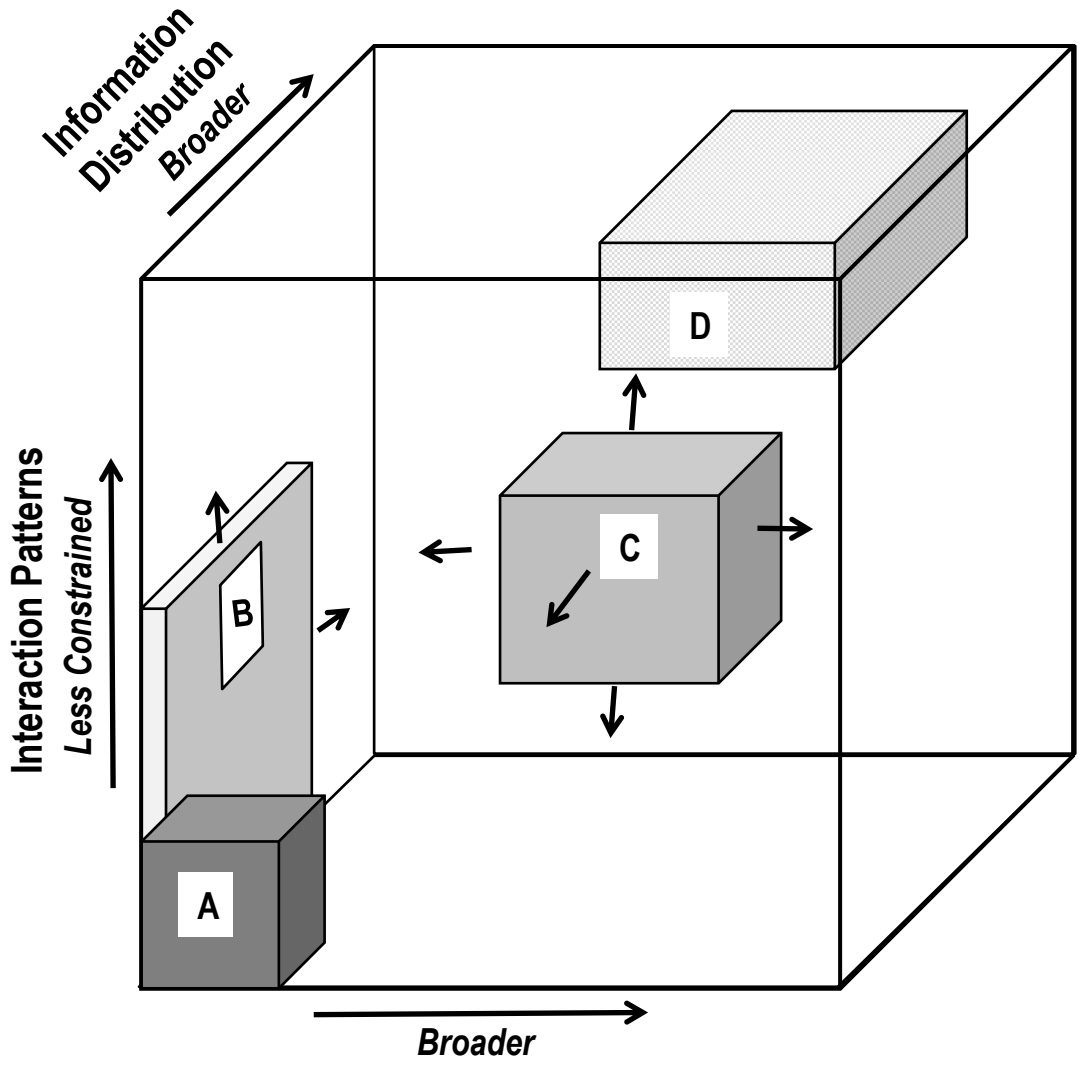
Burgess & Fisher Command Level Framework (CLeF)

- “Modern” networked force



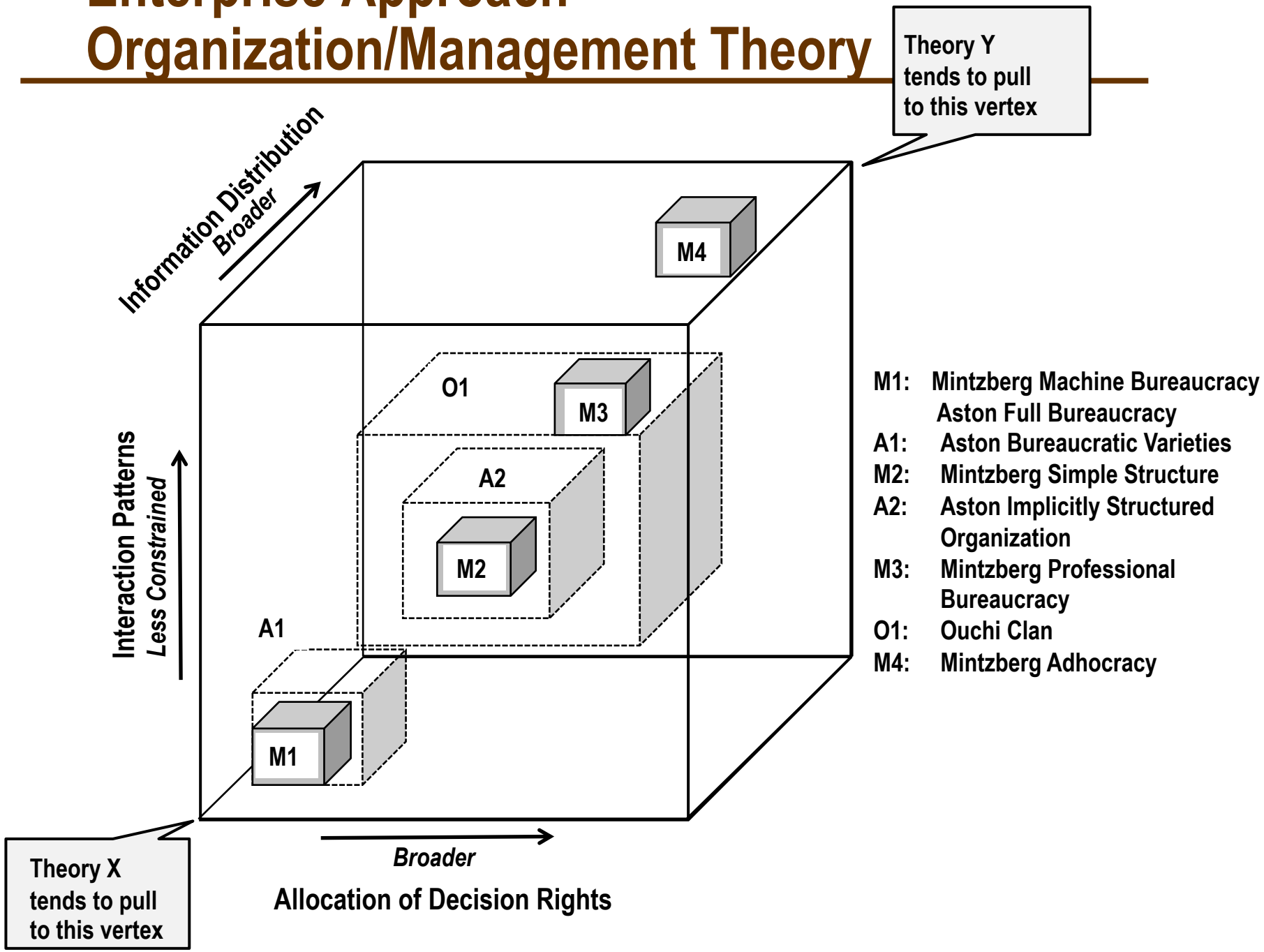
Burgess & Fisher (2008)

Enterprise Approach

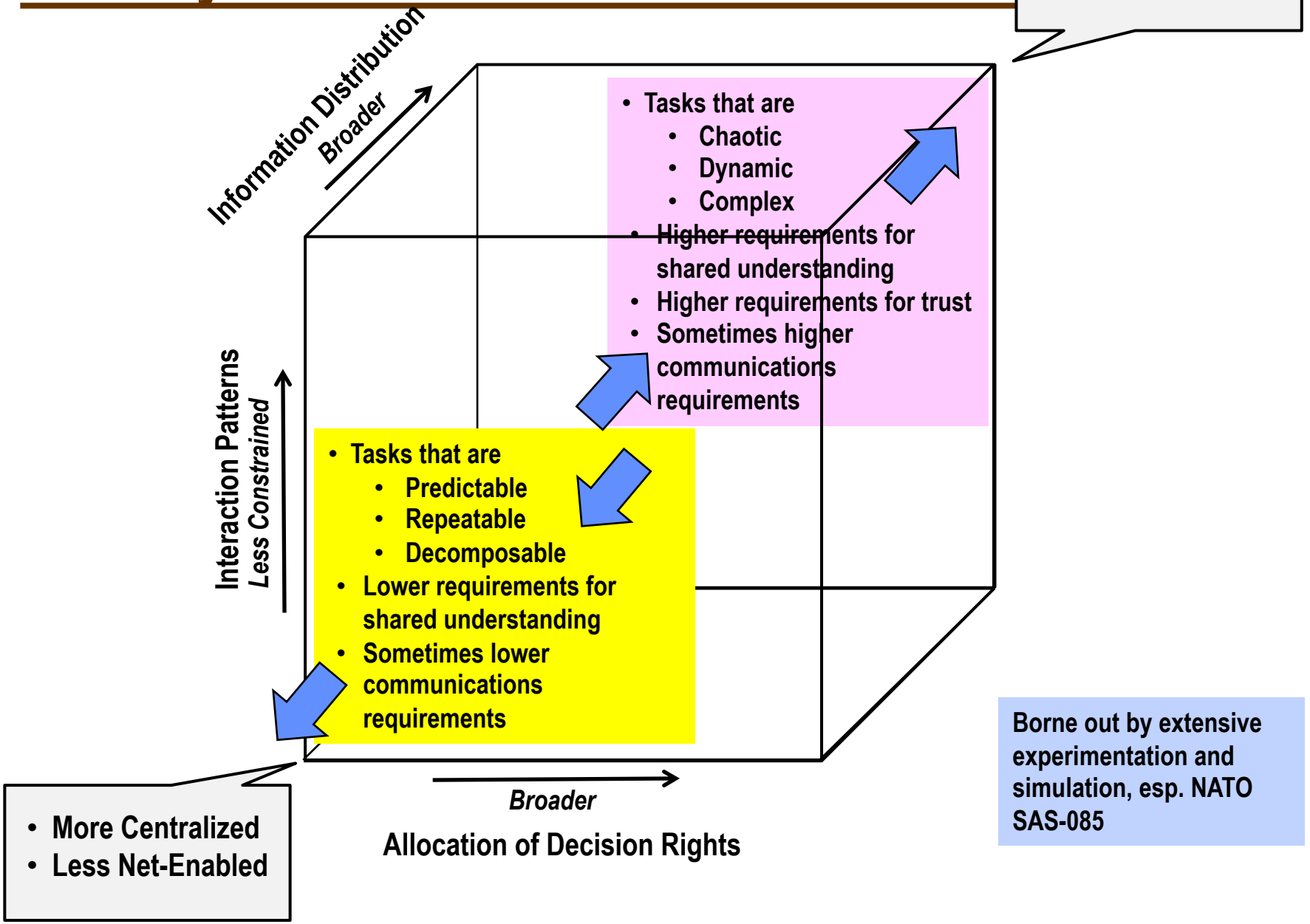


A: Hierarchical C2
B: 6,000 Mile Long Screwdriver (Micromanagement)
C: Modern Networked Force
D: Strategic Corporal/Small Autonomous Unit

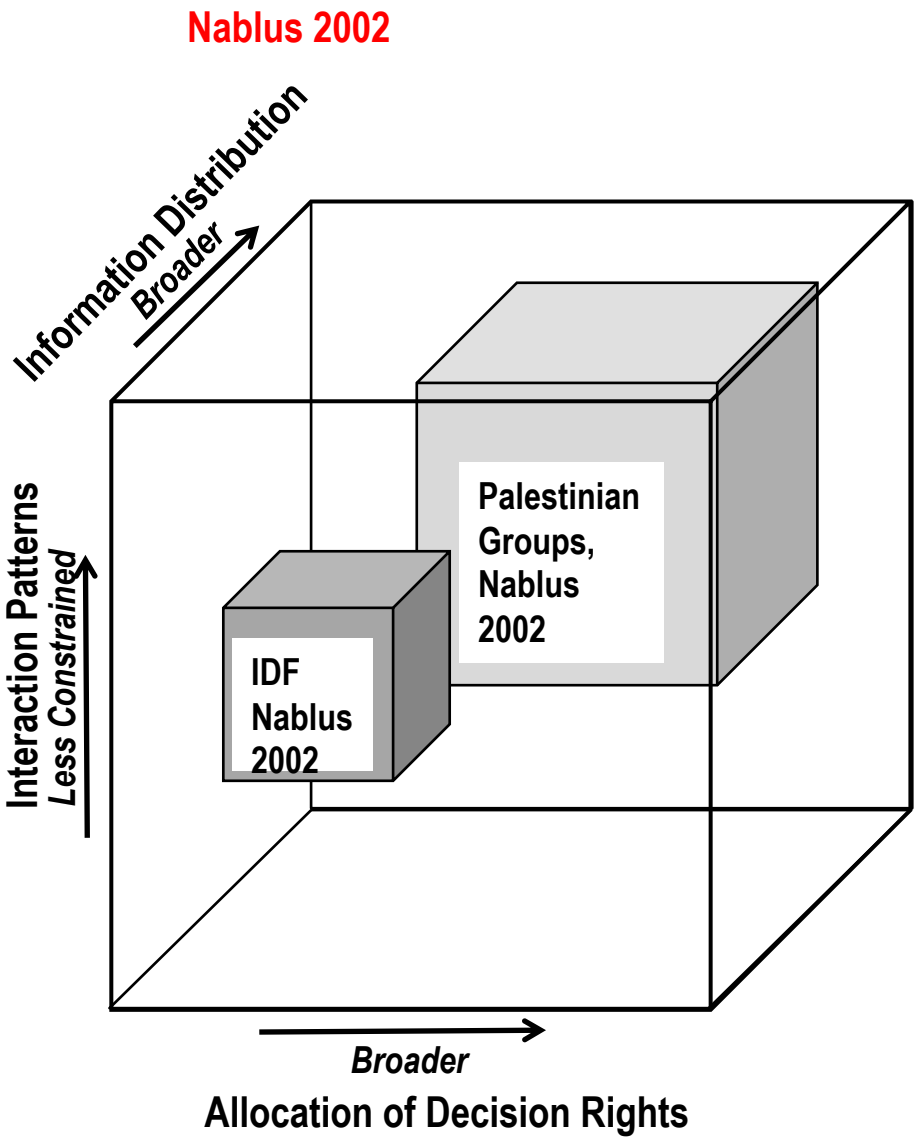
Enterprise Approach—Organization/Management Theory

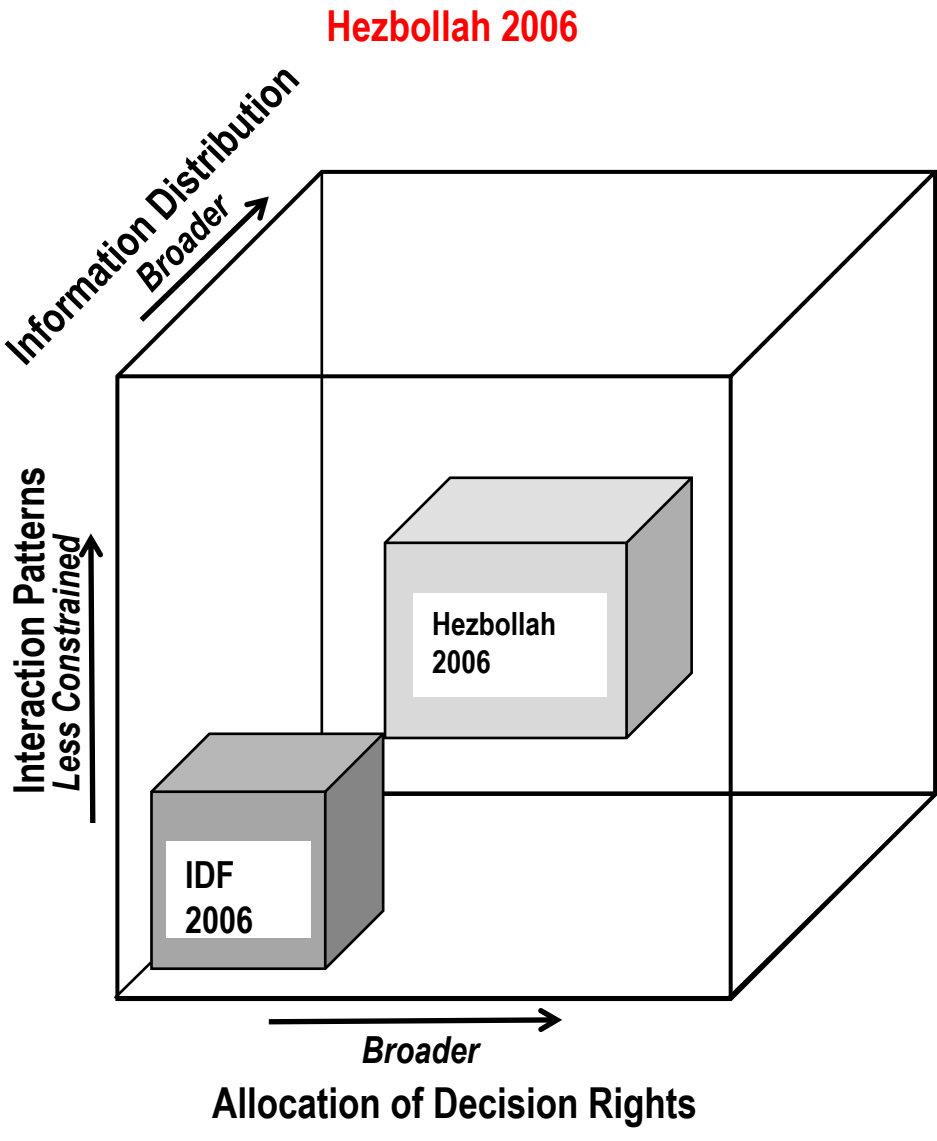


Enterprise Approach: Alberts-Hayes Characterization

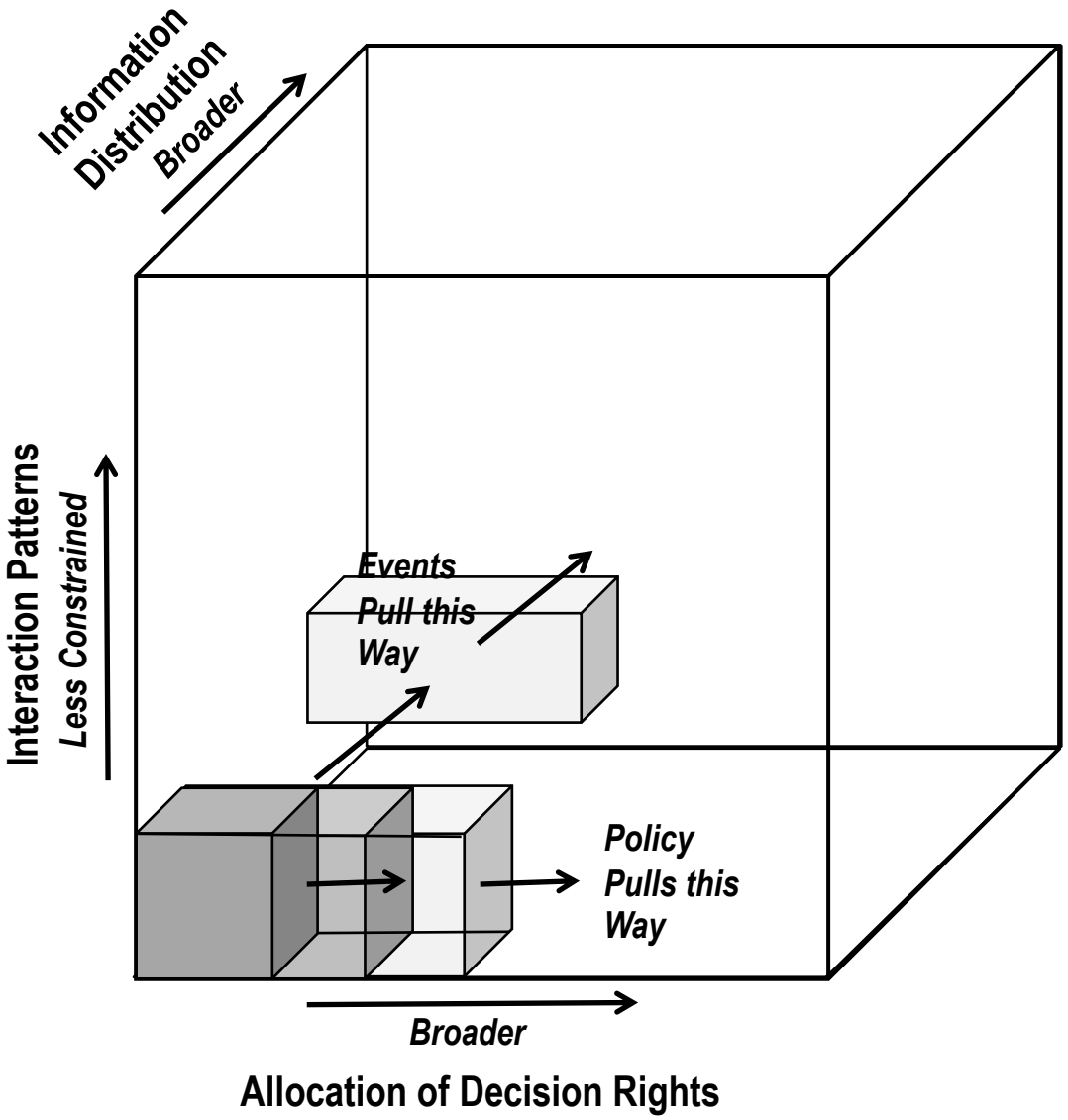


Enterprise Approach: IDF





Enterprise Approach: Mission Command

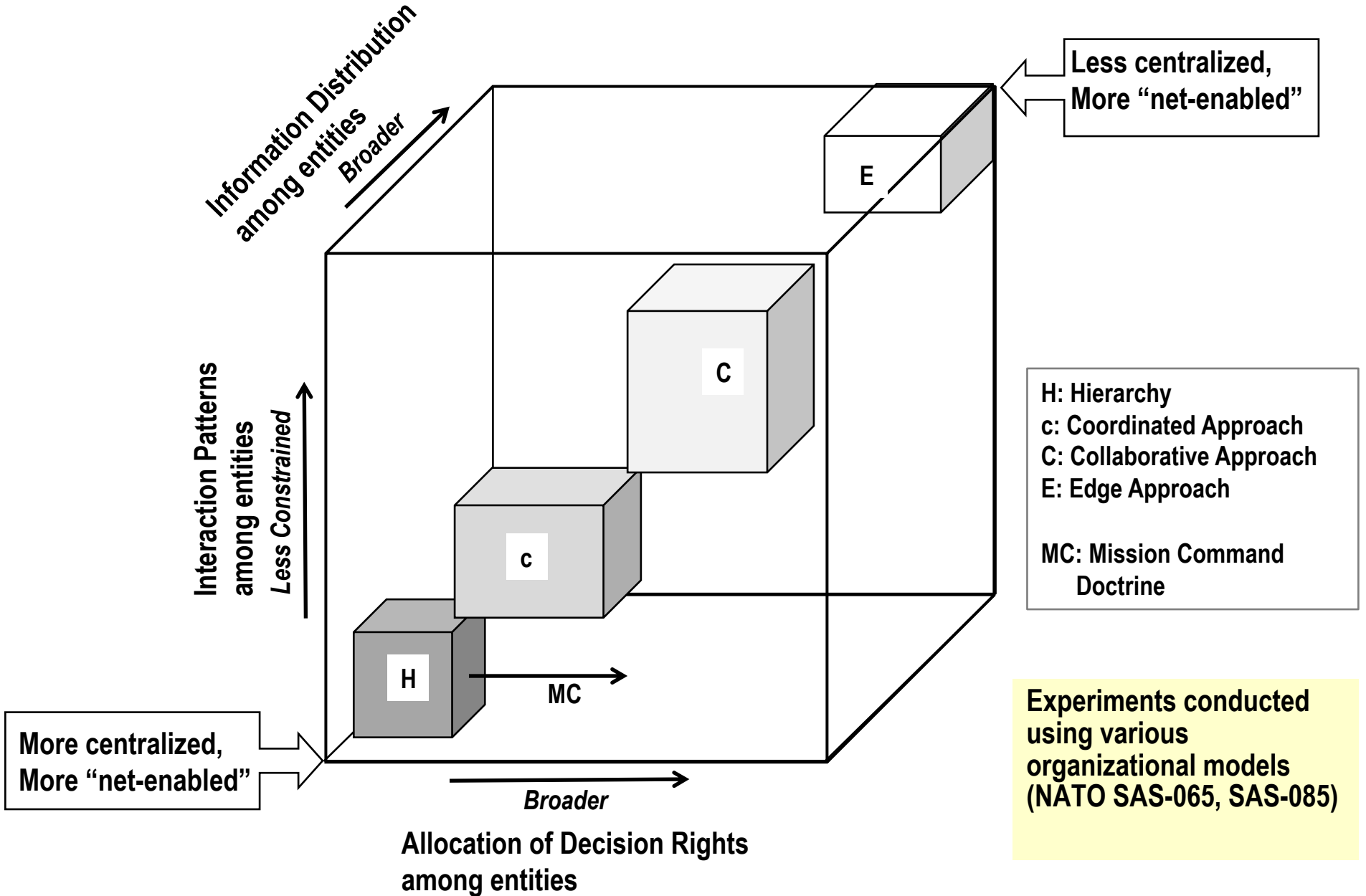


Von Moltke the Elder

- Non-detailed orders
- Shared intent
- Individual initiative
- Trust

"Auftragstaktik"

Enterprise Approach Space

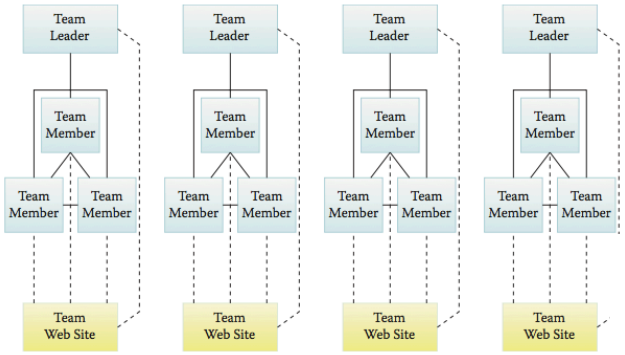


H: Hierarchy
c: Coordinated Approach
C: Collaborative Approach
E: Edge Approach

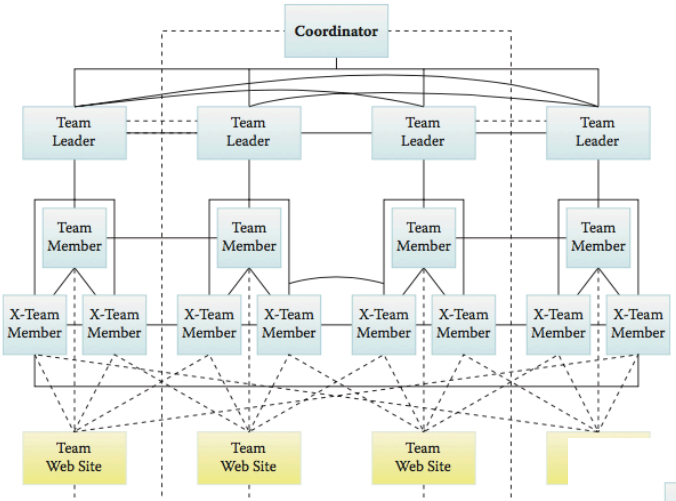
MC: Mission Command Doctrine

Experiments conducted using various organizational models (NATO SAS-065, SAS-085)

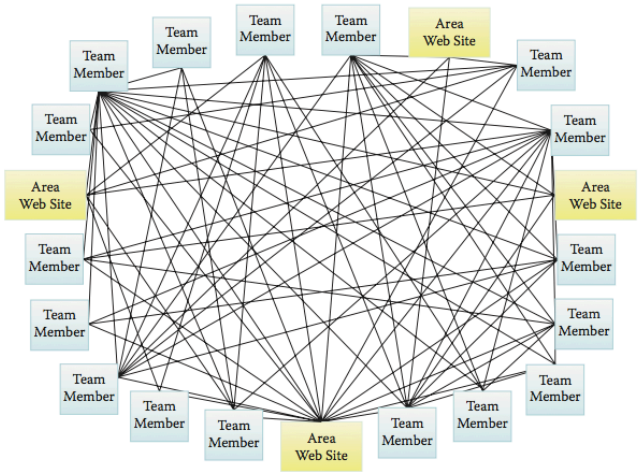
Experimental Instantiation



Strict Hierarchy

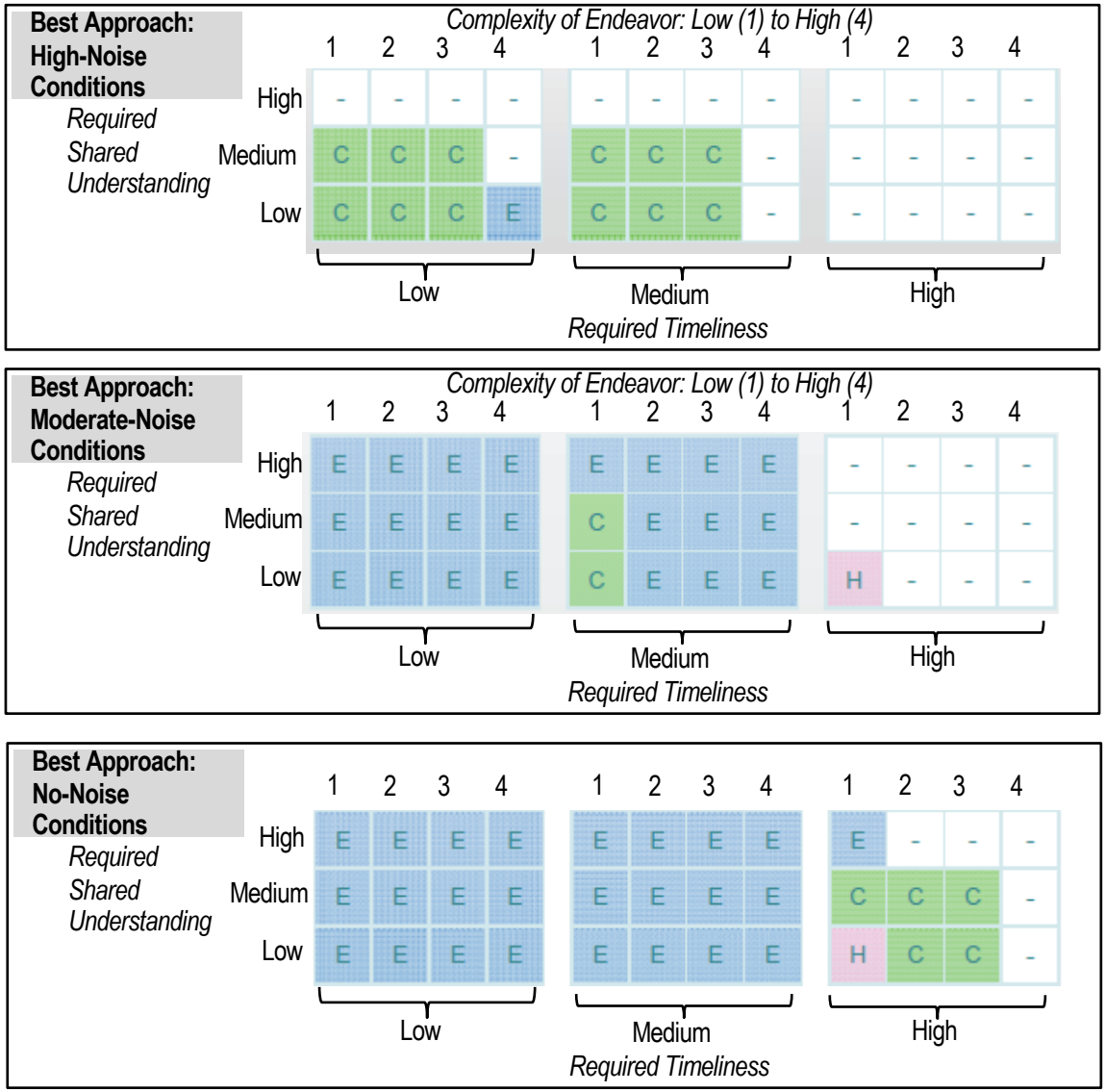


Collaborative



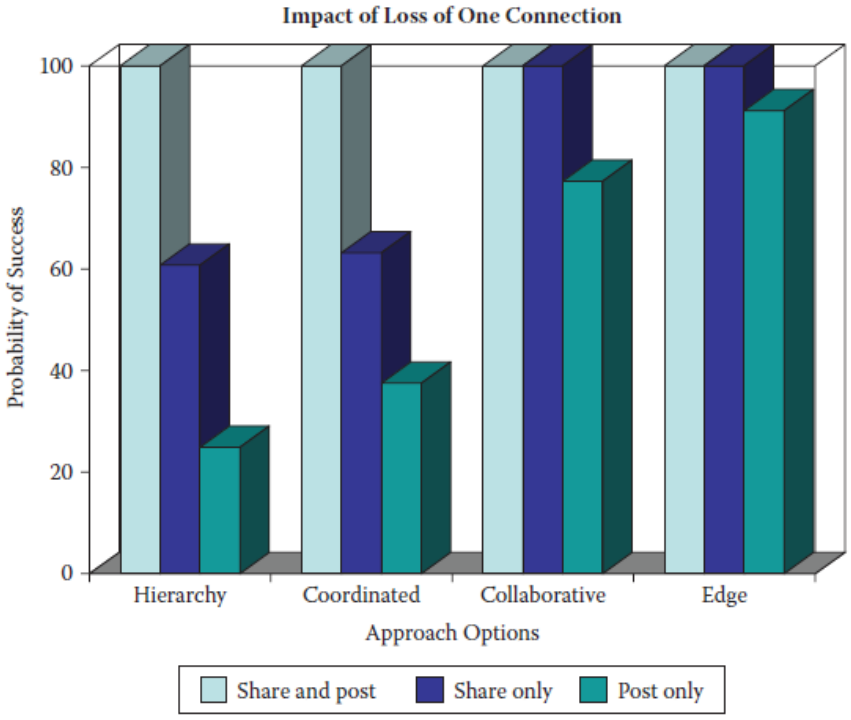
Edge

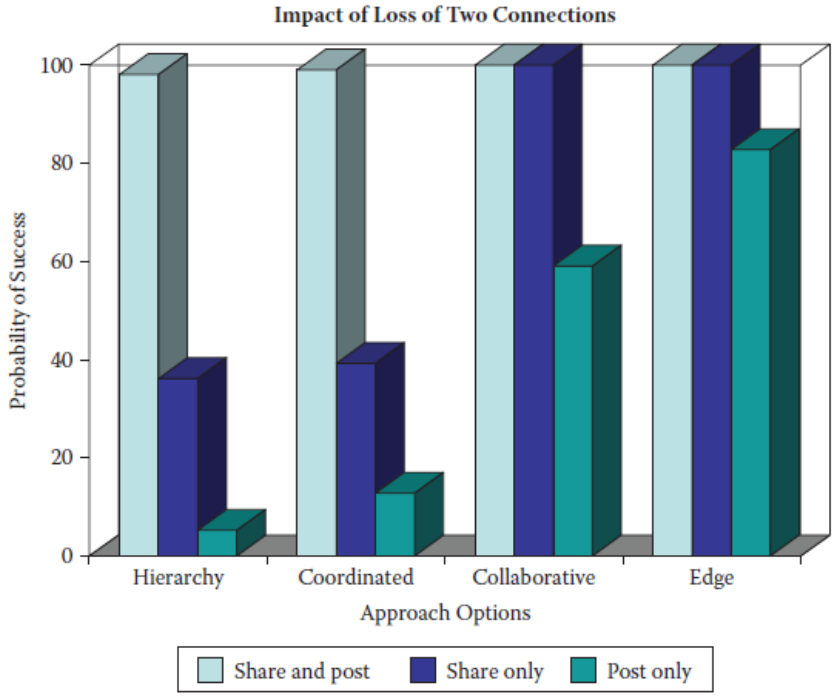
No Universal Approach



Adapted from Alberts (2011); p. 362

Experiments on Effects of Degraded Communications





Information Sharing Behaviors

- Share only: point to point information transfer
- Post only: post information to a website
- Share and post: both

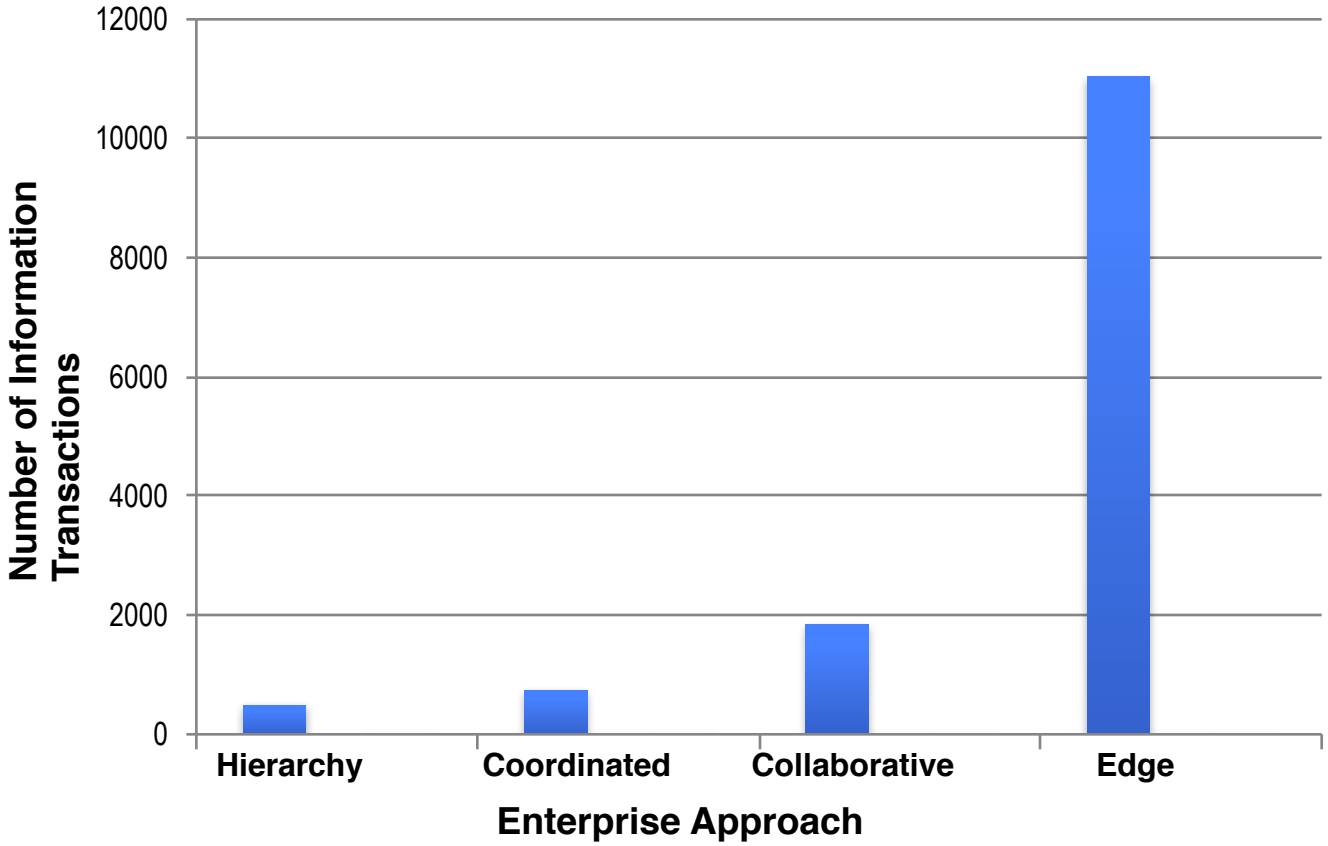
Link loss in the Experiments

- Prevents a pair of individuals from directly communicating
- Requires information to flow through other individuals or a web site

- **Broader information sharing policies make collective endeavor more resilient to communications disruption**
- **More networked C2 approaches are more resilient to information disruption**

Alberts (2011); as published in Vassiliou et al. (2015)

But there is a Price to Pay

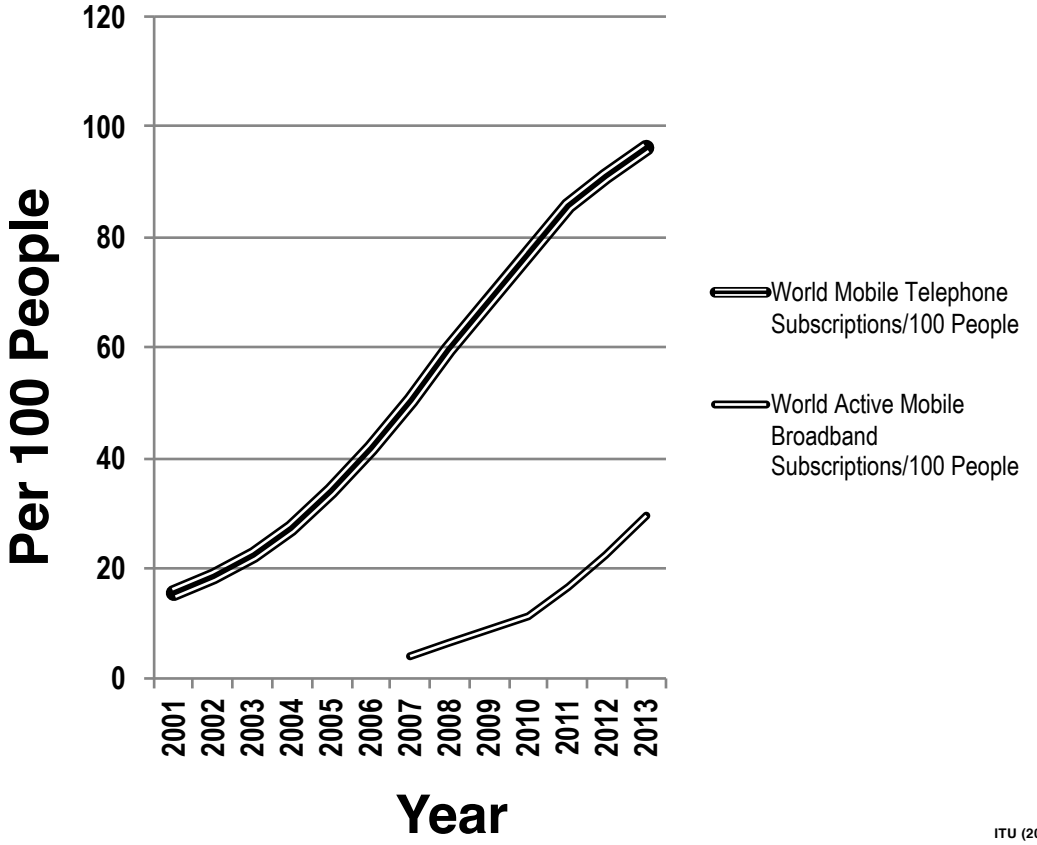


OK!

- We need the right enterprise approach
- And it has to be supported by effective communications technology
  - But that's the easy part, right?
  - JUST BUY the technology?
  - After all, the commercial world is so far ahead?
  - *…not quite*

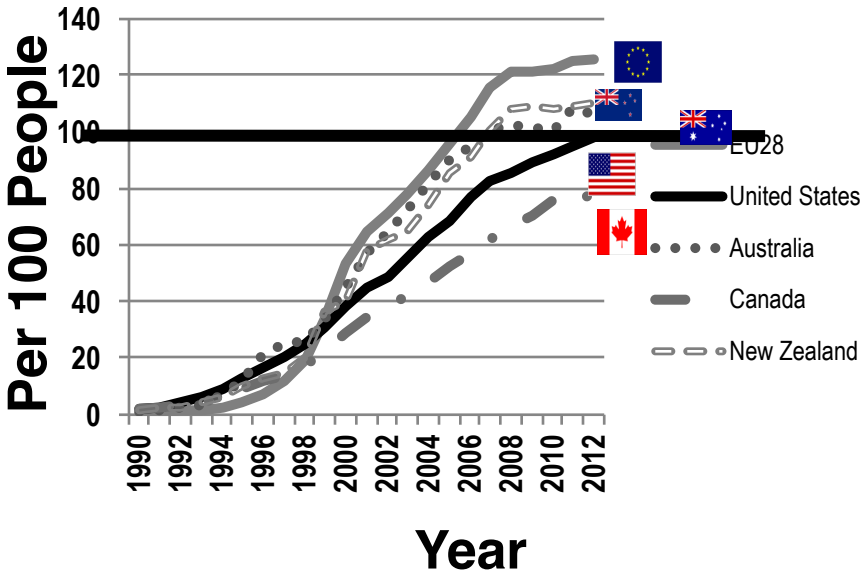
Explosion in Commercial Communications Technology

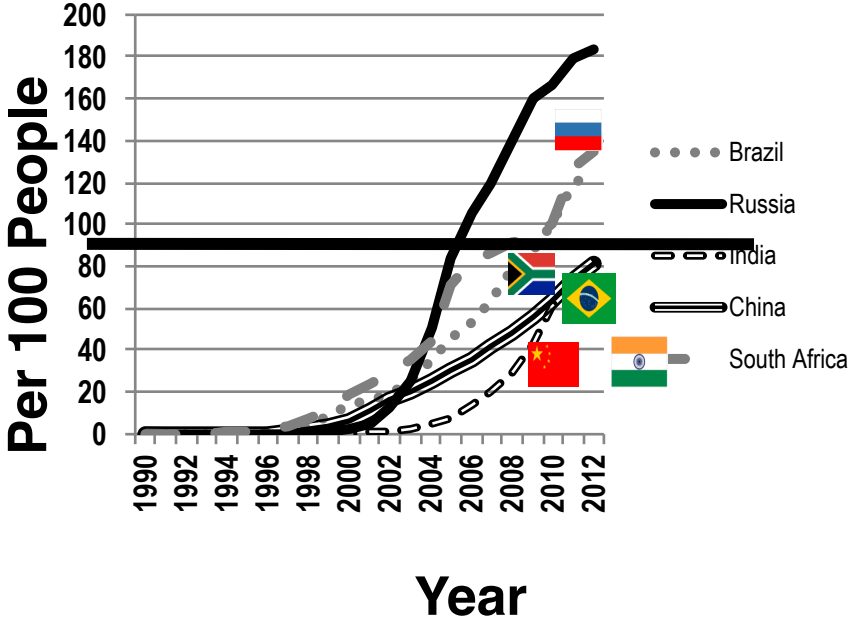
Mobile Telephone Subscriptions and Mobile Broadband Subscriptions Worldwide per 100 People



ITU (2013). *ITU Statistical Database.* Geneva, Switzerland: International Telecommunications Union.

Explosion in Commercial Communications Technology

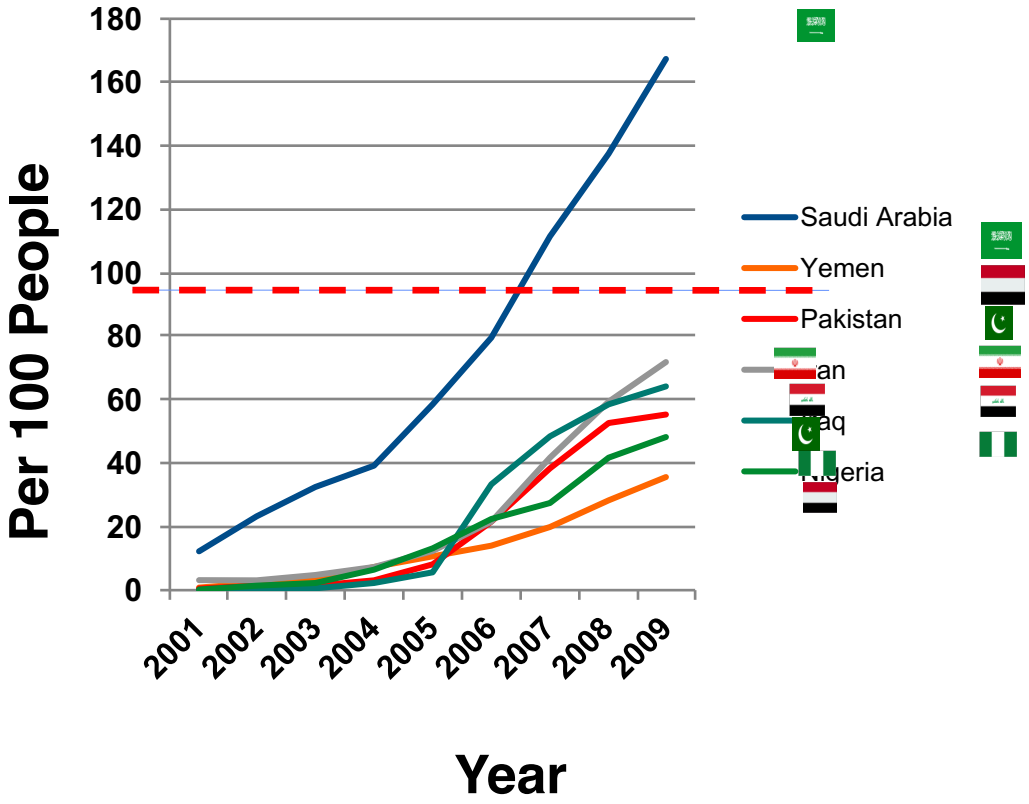




ITU (2013). *ITU Statistical Database.* Geneva, Switzerland: International Telecommunications Union.

Explosion in Commercial Communications Technology

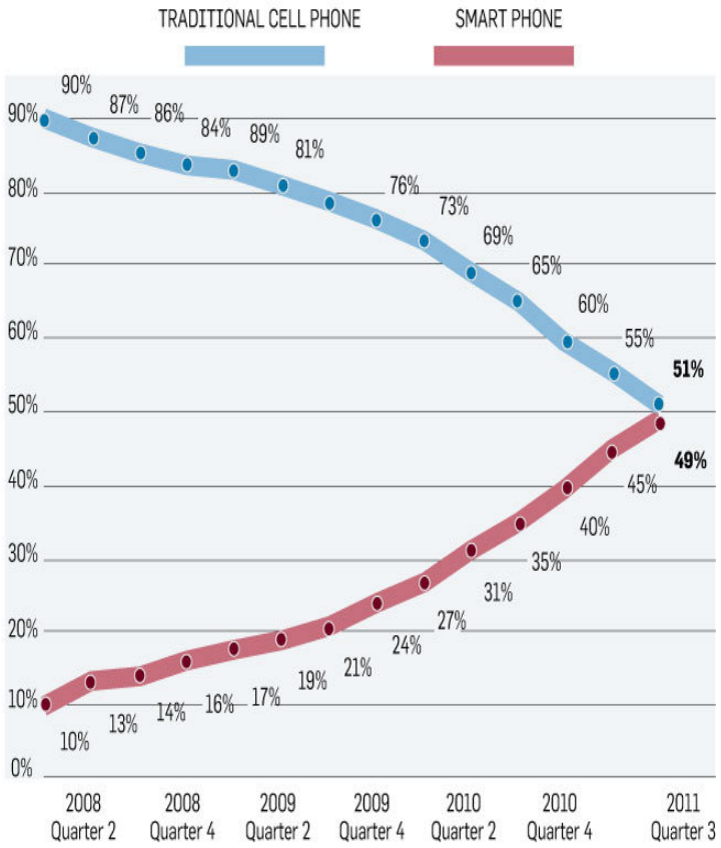
Other Countries of Interest



ITU (2013). *ITU Statistical Database*. Geneva, Switzerland: International Telecommunications Union.

Phones also Increasingly Powerful

- **Smartphones less than 10% of US market at start of 2008; nearly 50% by end 2011**
- **For new shipments, end 2011: Smartphones 65% in US, about 30% global**



http://media.nj.com/business_impact/photo/iphonesjpg-01a3c51253810e8e.jpg

Phones also Increasingly Powerful

3.4
MFlops

http://www.cisl.ucar.edu/computers/gallery/cray/images/cray1.jpg

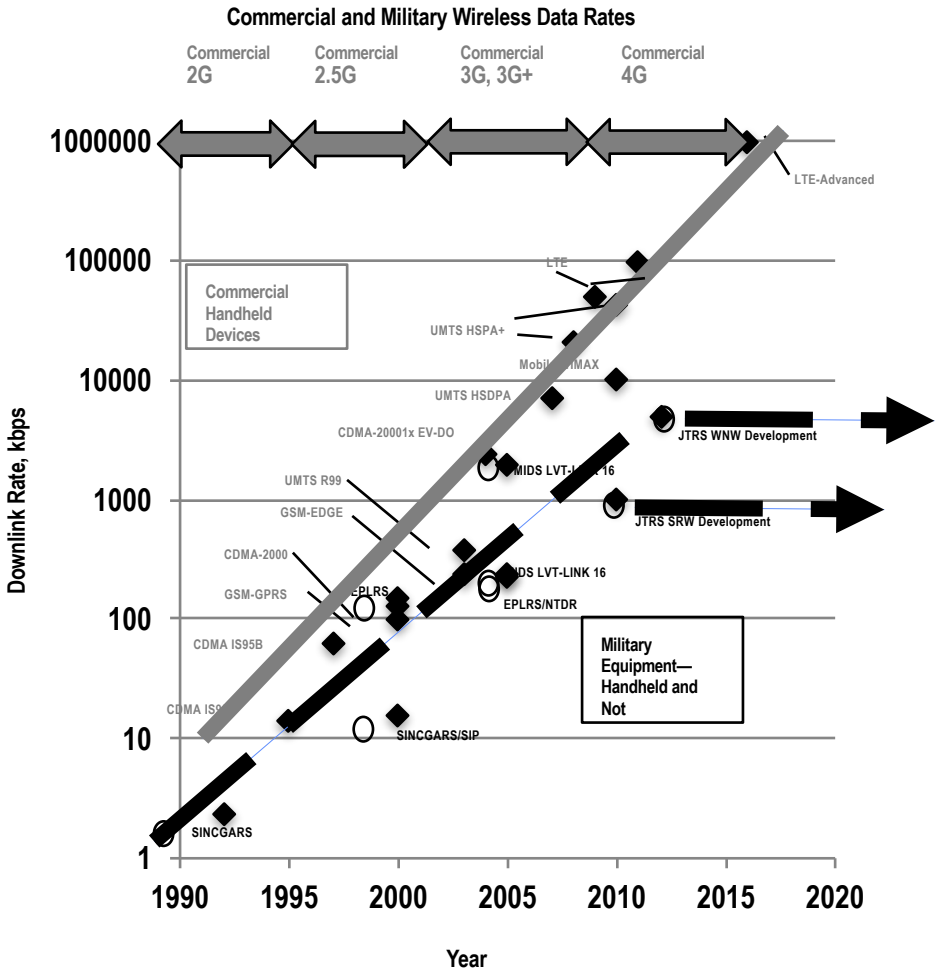
- CRAY-1 Supercomputer, fastest in the world in 1979

258.7
MFlops

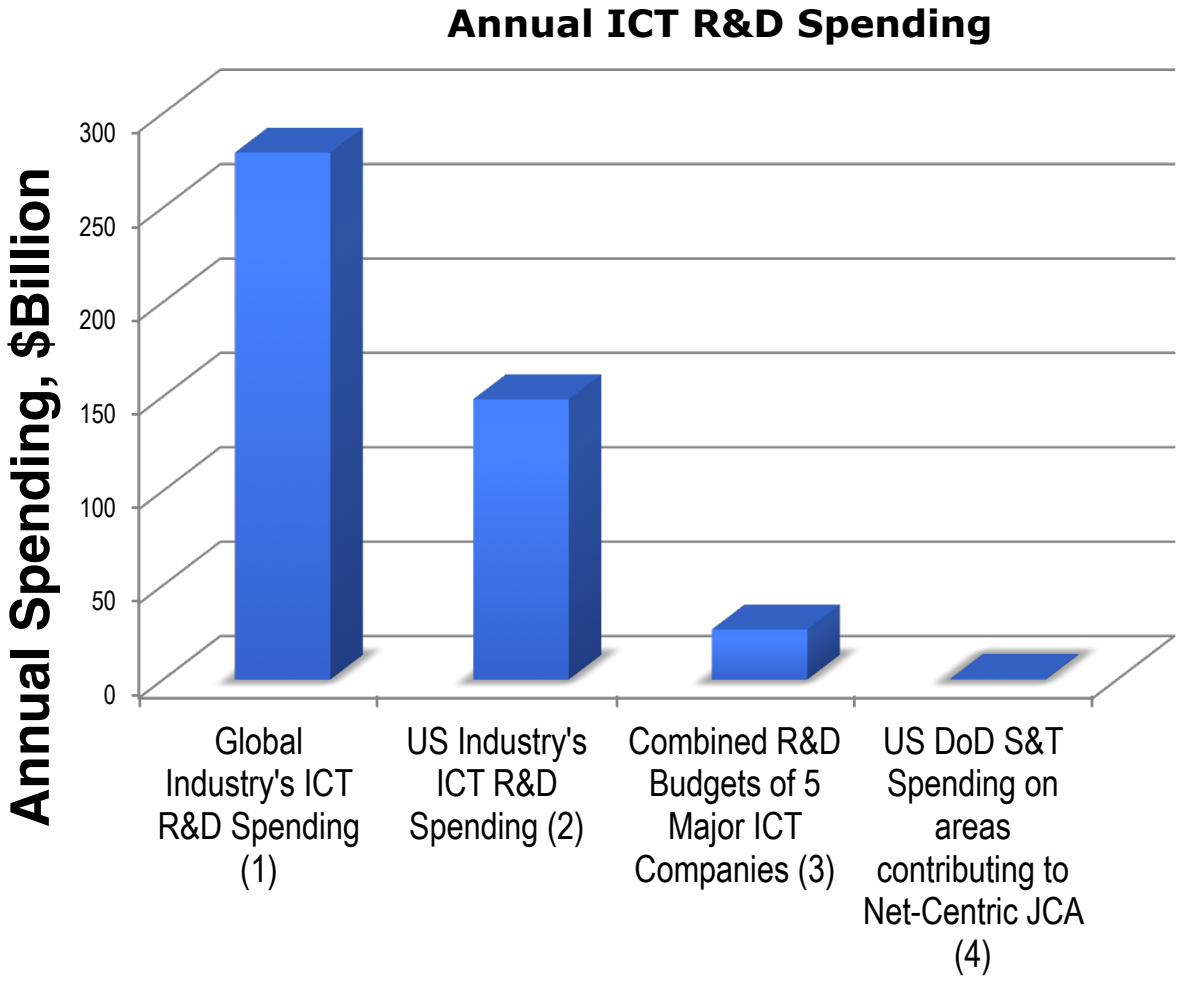
http://i52.tinypic.com/dy55ao.jpg

- LG P999 Smartphone, 2012

Commercial vs. Military Wireless Data Rates



DoD Not the Main Driver



Notes:
(1): 2009
(2): 2009
(3): Apple, Microsoft, Cisco, Google, Qualcomm
(4): Estimate for 2012

DoD Not the Main Driver

- **DoD and other military establishments are doing their best to make use of commercial end-user device technology,**
  - With which young soldiers are already very familiar
- **In some cases, commercial smart phones are being used as is.**
- **In others, vendors are adapting their devices (*e.g.*, by increasing ruggedness) to the special needs of the tactical environment.**
- **DoD and the Intelligence Community are also pursuing their own adaptations**
  - In these cases, essential properties of the devices are being preserved;
  - E.g., the ability to run third-party "apps" is retained by employment of the Android operating system.
  - Commercial chipsets, such as cellular Long-Term Evolution (LTE) chipsets, are also being used in purpose-built devices
- ***Despite all this, there remain critical differences between the tactical communications and networking environment and the commercial one that cannot be easily bridged. There are a number of long-term research and technology needs that military establishments cannot wait for the commercial sector to fill.***

Crucial Difference 1: Lack of Infrastructure

- **Commercial cellular systems & enterprise wireless networks heavily based on well-considered deployment & maintenance of a supporting infrastructure.**
- **Not as practical or robust for tactical edge network domain that are**
  - Highly mobile
  - May not provide time or ability to install infrastructure
  - Undergo continuous disruption and dynamics
- **Infrastructure-centric networking has also influenced technology development in certain ways**
  - E.g. frequent dominance of client-server paradigm
    - » Centralized management, where military often needs the opposite
  - More centralized points of failure
  - Infrastructure networks typically have high capacity provisioning
    - » Allowed many modern information services to be developed at a rapid pace *without* a lot of scientific understanding of the tradeoffs that must occur for these to operate effectively and with high assurance in more dynamic or limited communication environments
- **Robust, effective tactical edge information services will need more distributed models of network communication**
- **Dynamic distributed systems are complex and difficult to analyze.**

Crucial Difference 2: Multihop Networks

- ***Ad hoc* civilian wireless networks typically "one-hop" wireless networks**
  - One wireless link from a user device to a hub connected to a wired infrastructure
- **In military operations where there is little infrastructure, there may be multiple wireless links concatenated together before reaching a wired or fiber infrastructure**
  - For extended range and increased robustness (through diversity of paths)

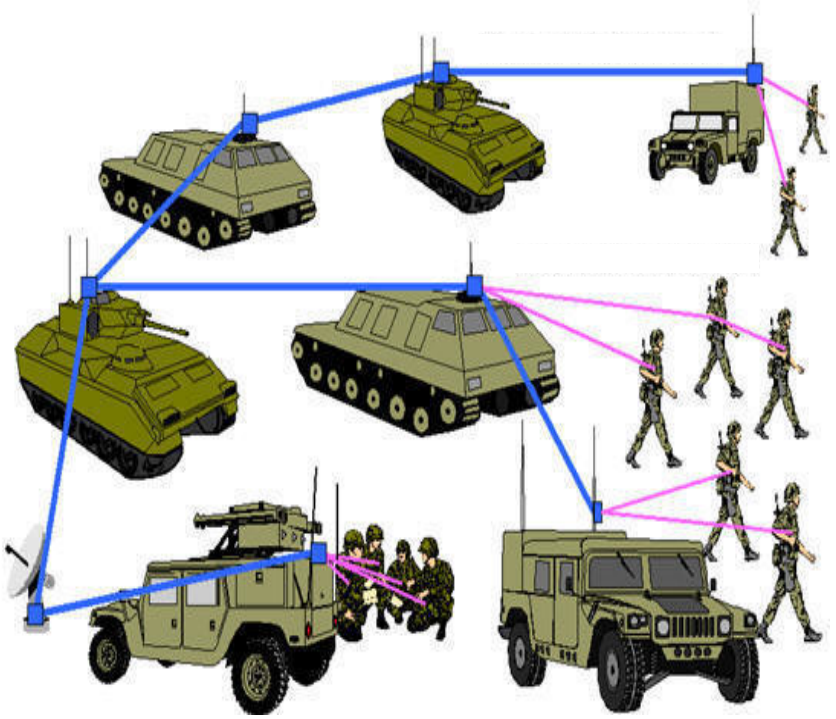
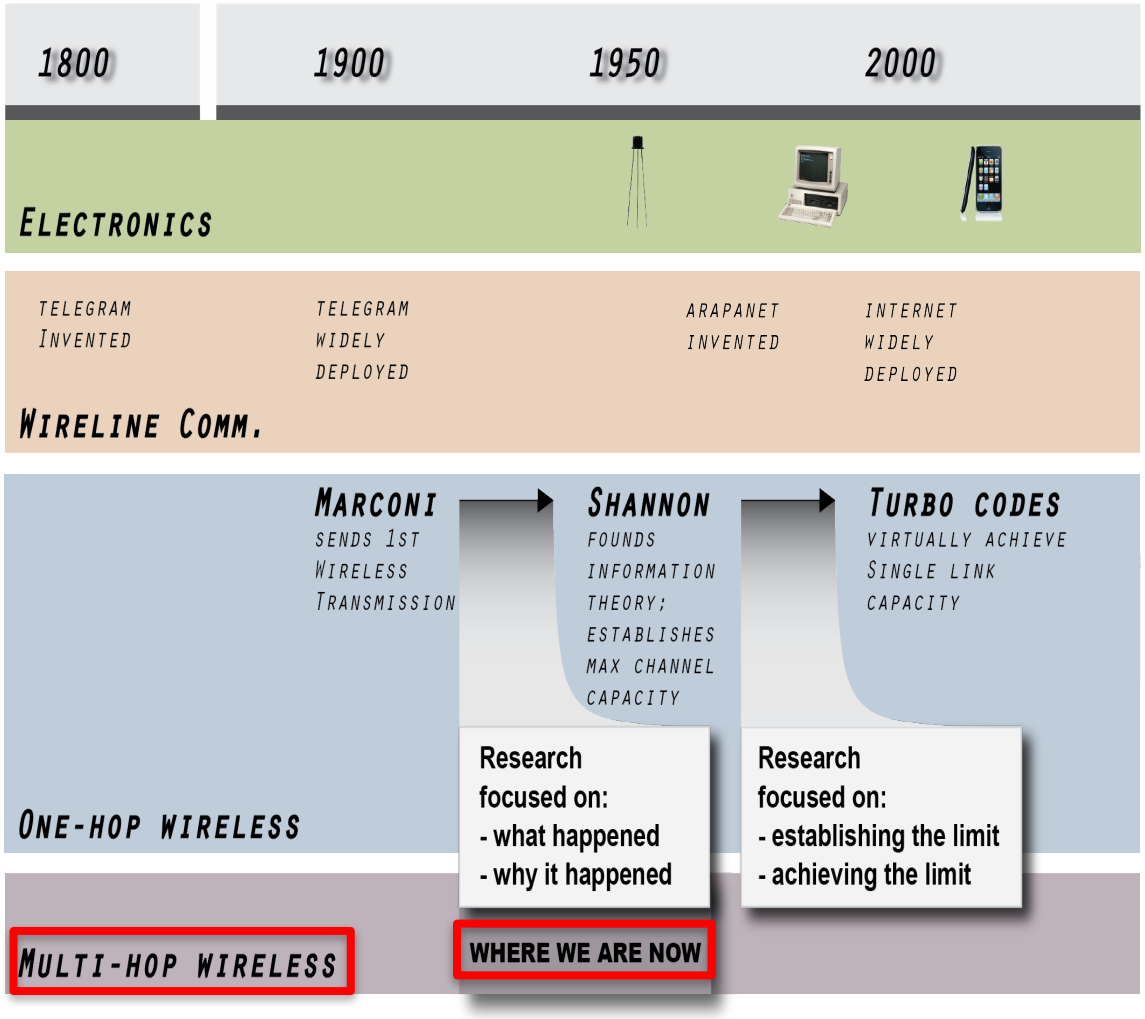


Image: http://www.atacwireless.com/adhoc.html

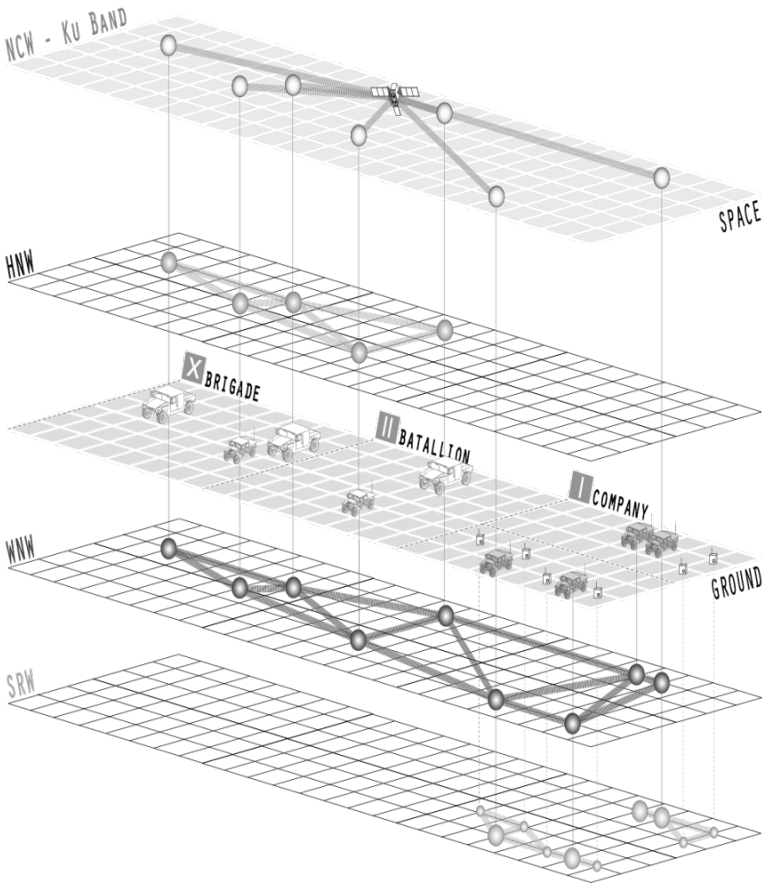
Crucial Difference 2: Multihop Networks

- **Theoretical foundation for multihop networks not as well developed as single hop**
- **Unlike commercial systems, not always opportunity to survey operational environment and then fine tune in the field during deployment**
- **Need tools for early performance prediction**
  - These not well enough developed to avoid deployment surprises
  - Difficult to achieve trial-and-error cycles early in the engineering process.
- **Difficult to extrapolate performance in one environment to performance in another environment, because of the many non-linear inter-relationships among network parameters.**
  - Scalability: knowing how a system works with 10 nodes does not guarantee knowing how it will work with 20.
  - if a system works in a desert, we cannot always confidently predict that it will also work in an urban environment.



Crucial Difference 3: Multiple Heterogeneous Networks

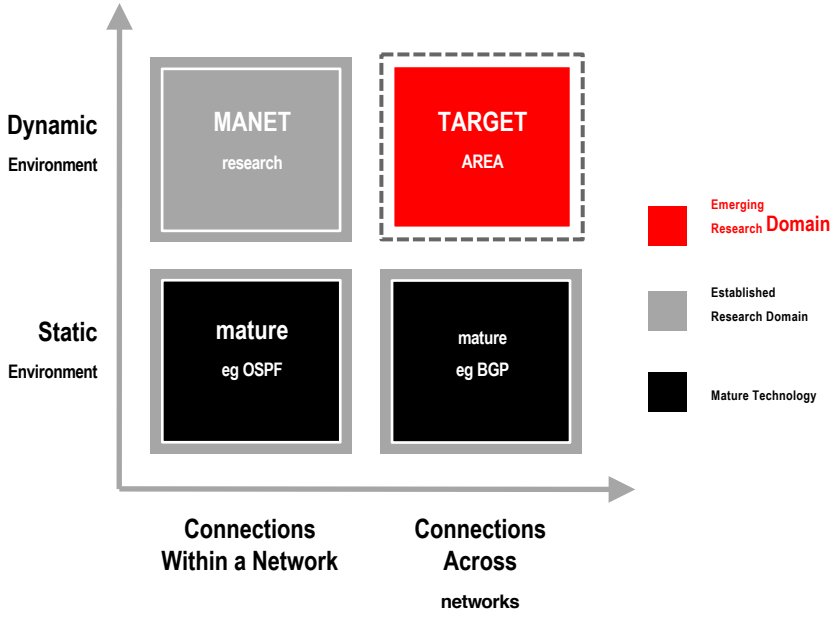
- **Commercial networks have tended to be homogeneous**
- **Military is planning not only multi-hop networks, but multiple *variants* of multi-hop networks *in simultaneous use,* in same geographic area**
- **Connecting various echelons of ground units to themselves and one another, to airborne platforms, & satellites**
- **Wide range of communications technologies may be in play at the same time**



Crucial Difference 3: Multiple Heterogeneous Networks

Protocols

- **Protocols used to connect users *within* a network often different than the protocols used to connect different networks together**
- **Most research on mobile networks to date has focused on protocols for connecting within networks**
- **Need & opportunity for research into protocols that efficiently connect different networks, particularly in dynamic environments.**



(OSPF = Open Shortest Path First)
(BGP = Border Gateway Protocol)
(MANETs = Mobile Ad Hoc Networks)

Crucial Difference 3: Multiple Heterogeneous Networks

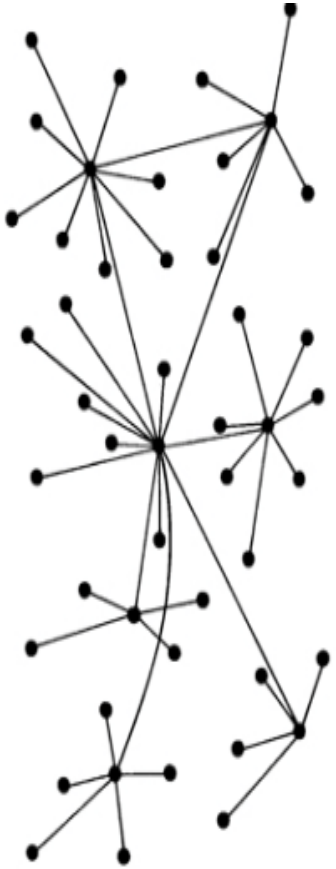
Network Management

- **Network management of complex tactical networks not fully developed**
- **Most work to date focused on managing a single network in an almost static environment (& still room for improvement)**
- **Larger challenge: more "holistic" network management approach to ensure that rapidly changing networks operate cohesively together to support combatant commanders' intentions.**
  - Will need well-defined interfaces to constituent network managers and may work on a slower timescale and on a larger aggregation of resources (analogous to standard military chain of command)
  - Simplifying and connecting network management approaches will
    - » Improve network performance, esp. in a fluidly changing environment
    - » Reduce the needed number of network operators & level of expertise required of them

Crucial Difference 3: Multiple Heterogeneous Networks

Decentralization of Services

- **Networks in commercial space often dependent on centralized services**
- **Tactical users often disconnected from centralized services for long periods of time**
- **When time-critical information sharing a primary requirement, need more distributed approach to data transport and reliability**
- **Existing paradigms**
  - Multicast application technology
  - Disruption-tolerant transport
  - Dynamic routing
- **These are often not optimized or well understood at an architectural level for effective DoD deployment**
- **Another way to address the same issue is to develop applications (*e.g.*, chat) that do not rely on a central server.**
- **Such techniques are being used extensively in early prototypes but more work is needed before they are widely deployed.**



Crucial Difference 3: Multiple Heterogeneous Networks

Exploitation of Heterogeneity

- **Collections of heterogeneous networks not only pose important challenges, but can also offer significant benefits**
  - Heterogeneity can provide added system robustness in severe & changing propagation environments and under intentional attacks
  - Having heterogeneous network connections may increase the reliability of delivery
  - Mass transit analogy
    - » Stalled trains don't affect buses
    - » Auto accidents don't affect subway trains
- **There are protocols for sending a piece of data reliably to one user, but for multiple users in difficult environments it's much harder**
  - e.g. in MANET environment, users may be temporarily disconnected
  - Protocols that will provide very high reliability will have reactions to link errors and routing drops in very different ways then current Internet protocols.
  - In the case of sending data to many users simultaneously (e.g., a map to a whole platoon), techniques for doing so reliably are even less mature

Crucial Difference 4: Complex & Contested Electromagnetic Environment

Hostile Action

- **Military must contend with jamming and other hostile electronic attack**
- **Not all military communications will need to be robust against disruption all the time**
- **But there needs to be a hardened core of capability that can provide critical services even under the most severe conditions**
- **Systems that are robust today are not guaranteed to be so in the future, as adversary capabilities will continue to grow with technological advances**
- **To counteract this growth in hostile electronic attack capability, new techniques need to be developed in key areas**
- **One such area is airborne command and control, since aerial platforms are often an easy target for enemy jammers**

http://www.cellphone-jammer.org/270w-high-power-full-band-4g-cell-phone-signal-jammer-p-697.html

Inexpensive Jammer available from China that can be ordered over the Internet.

Crucial Difference 4: Complex & Contested Electromagnetic Environment

Contested Spectrum

- **Spectrum a valuable resource**
  - U.S. 700-800 MHz auction 2008: $19.1B for 62MHz, or $1.02/Mhz/capita
  - Germany 700-800 MHz auction 2008: €3.58B for 60 MHz, or €0.73/Mhz/capita
- **This is obviously an issue for commercial space, too**
- **But U.S. DoD has *lost* ~300 MHz of spectrum previously reserved for military use since 1992, with more to come!**
- **Key capability: measure the current spectral environment and make this information available rapidly to both radios and network planners.**
  - This differs from most current systems, which do not have real-time feedback and rely solely on static pre-planned frequency allocations that are often not fully used
- **DoD needs a holistic management approach for all systems that use or depend on spectrum availability.**
  - Currently radios, jammers, radars, and sensors are all managed separately
  - They often have some technical similarities and must operate in the same geographic area.
  - Broader spectrum approach that accounts for these different users and shares functions and information among the different systems will help alleviate spectral congestion
  - Examples of potential sharing range from sharing the spectrum (by e.g., frequency, space, time, power) to sharing physical space to sharing components (even conceivably RF power amplifiers)

Crucial Difference 4: Complex & Contested Electromagnetic Environment

Contested Spectrum

- **There may be synergy with the commercial sector in some of the necessary improvement areas:**
  - Using spectrum efficiently
  - Measuring usage
  - Dynamically adapting frequency bands
  - Sharing resources across all emitters
  - Refreshing the hardened core of critical capabilities
  - New technologies such as Cognitive radios, Dynamic Spectrum Access, Steerable antennas

- **But many of the operating conditions are unique to the military (e.g., jamming) & will not be addressed by commercial entities.**

Facets of Assured Communications

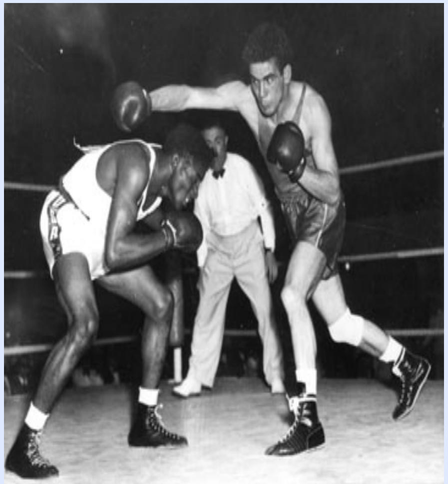
PROTECTED

- ***Guards*** **against a punch**

http://www.fightproducts.com/about-headgear.htm

FLEXIBLE & AGILE

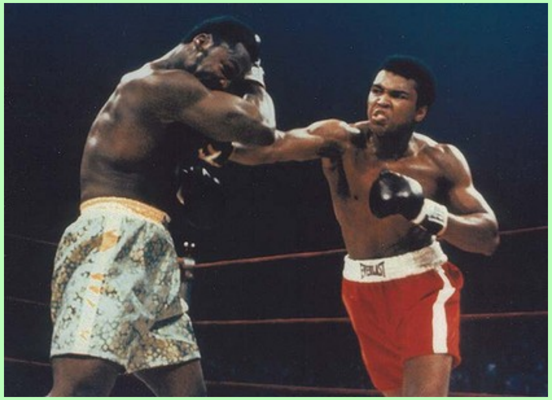
- **Can *duck* a punch**



Floyd Patterson, 1952 Olympics
http://www.canoe.ca/2000GamesGalleryPreviousImages/1952_boxing.jpg

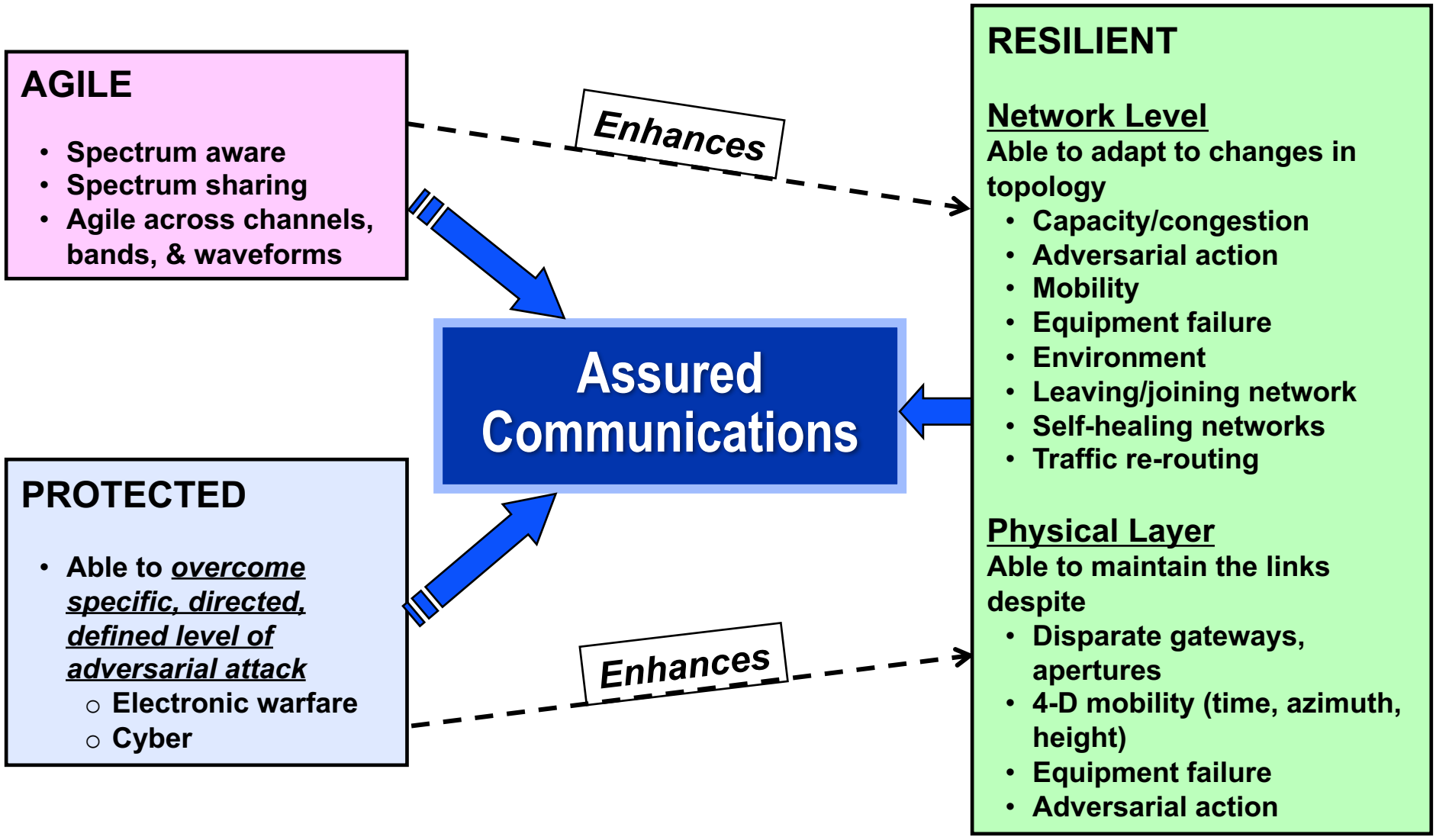
RESILIENT

- **Can *take* a punch**



Frazier vs. Ali, Manila, 1975
http://images.smh.com.au/2012/03/30/3176136/ipad-art-wide-Manilla-420x0.jpg

Facets of Assured Communications



Examples of Required Advances

AGILE

- Smart antennas
  - 3D Beamforming
  - Adaptive Nulling
  - Massive MIMO
- RF front ends
  - Multiband duplexers & diplexers
  - Greater dynamic range
  - More efficient power amplifiers
- Cognitive radios that can adjust their transmission parameters in order to identify and manage available spectrum, perhaps predictively

PROTECTED

- Similar advances as required for *Agile*
- Convergence of Electronic Warfare and Cyberdefense with Communications
  - Multifunction waveforms, such that the communications waveform of the friendly force can be used in jamming the communications of adversary forces

Enhances

Enhances

Assured Communications

RESILIENT

- Improved management of heterogeneous networks
  - multi-path routing and network coding;
  - rapid network adaptation in the presence of sudden changes in the electromagnetic environment.
- Better network interfaces and control
  - common status reporting, link selection, anomaly detection, etc.;
  - collective reporting of and efficient dissemination of the characteristics of the radio environment.
- Isolation of compromised subnets upon detection and reconstitution of compromised networks

Bottom Line

- Success in complex missions depends on agile organizations with assured communications
- There is a complex interplay between enterprise approach and communications capability
- While more agile organizations—those that can select an appropriate enterprise approach in the face of dynamic situations and in light of their own communications technology—can make up for communications shortfalls to an extent, there is no substituted for assured communications capabilities.
- DoD-Specific research is still required!

BACKUP/OTHER

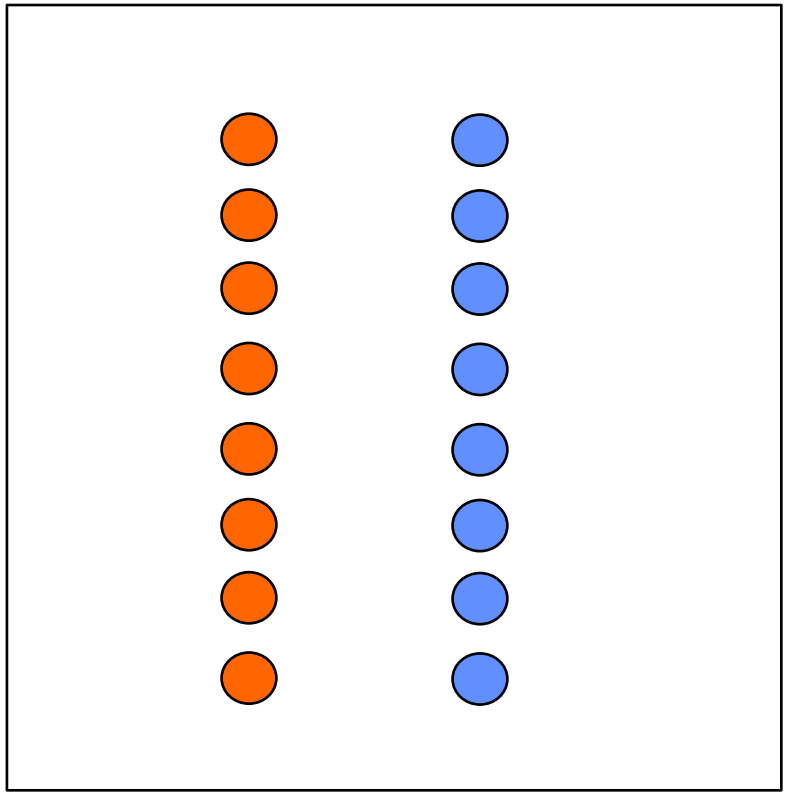
C2 Failures—Bottom Line

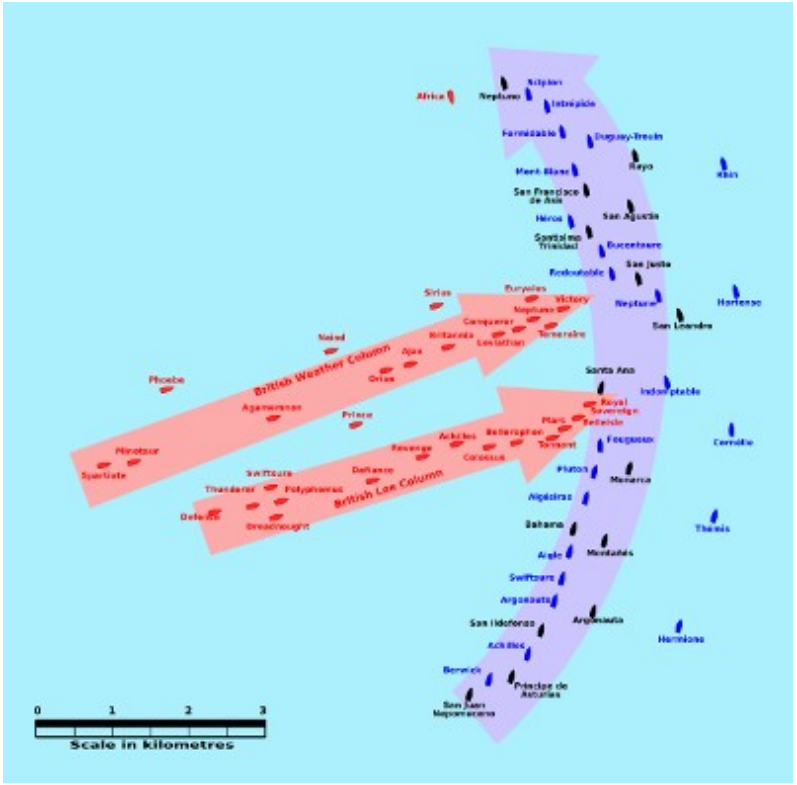
"What we've got here, is failure to communicate"

http://media.beta.photobucket.com/user/boro_01/media/Cool_Hand_Luke_Martin.jpg.html?filters[term]=strother%20martin&filters[primary]=images&o=1

Strother Martin as "The Captain," *Cool Hand Luke*, (Warner Brothers, 1967)

Nelson Victory at Trafalgar, 1805





http://files.abovetopsecret.com/uploads/ats52850_606px-Trafalgar_1200hr_svg.jpg

Prevailing Tactics

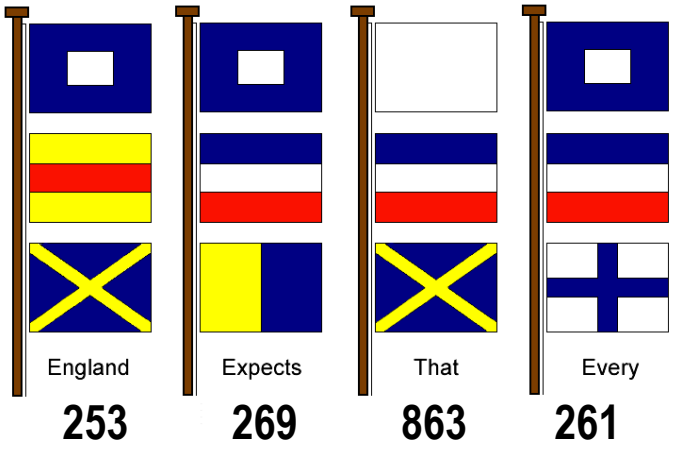
- Relatively controlled engagement
- Facilitated communications (signaling flags)
- Either side could break off & limit losses
- Often led to inconclusive results.

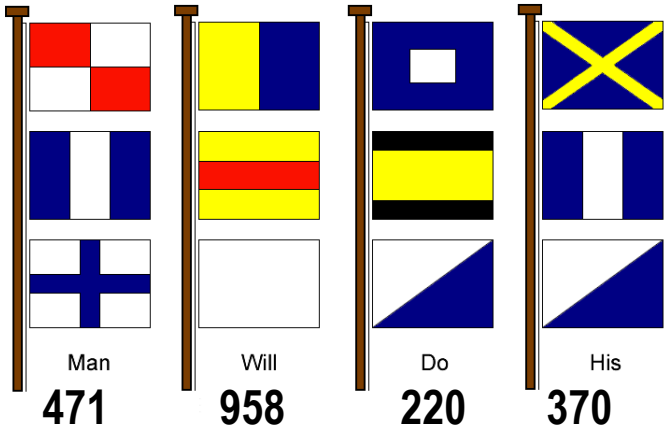
Nelson's Tactics

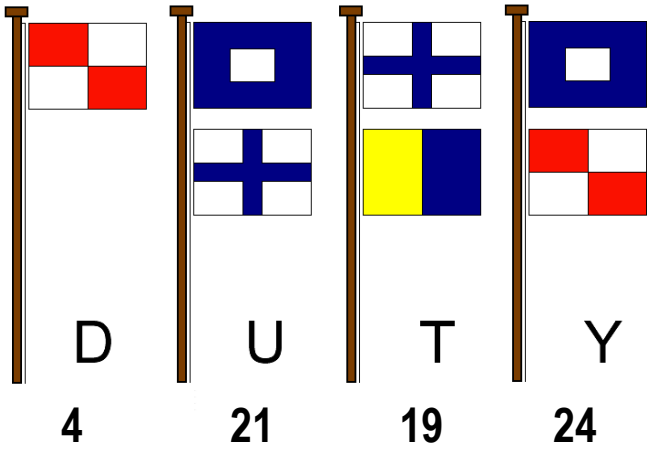
- Cut enemy line and isolate pieces
- Force decisive battle
- Disrupt enemy communications
- However, also disrupt own communications

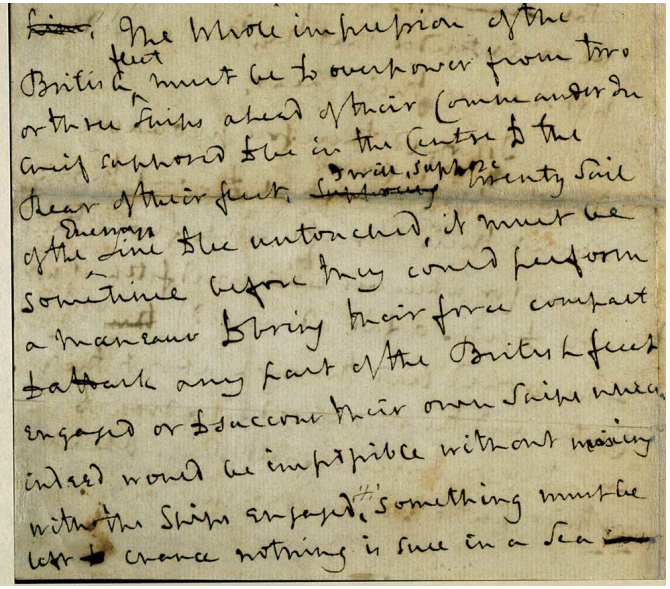
Nelson Victory at Trafalgar, 1805

- Reduced the need for communications and coordination
- Shared intent
- Trust
- Individual initiative









Nelson's Trafalgar Memorandum, 1805

- Brief and clear statement of intent that did not attempt to anticipate every eventuality in detail.

http://www.tallmodelships.com/pictures/big/hms-victoryC-model-ship59.jpg

Nelson Chequer