First Battles in Cyberspace:
New Paradigm for 21st Century Warfare?

Dr. Dan Kuehl
(and Dr. Robert Miller)
IRM College, National Defense University
Our Opinions: Not the USG, DOD, nor NDU!
IQPC Cyber Warfare 2009

Definitions

- "Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communications technologies (ICT)"
- Cyberpower: the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power."
- Cyberstrategy: the development and employment of strategic capabilities [resources as well as operational concepts] to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power in support of national security strategy
  - Kuehl , "Cyberspace-Cyberpower: Defining the Problem" in NDU/CTNSP project ("Cyberpower & National Security")
- Cyber Operations are"the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid" [our "base" in cyberspace]
  - VCJCS Memo 25 September 2008

First Battles' Thesis

- Traditional Warfare: first defeats-even disasters- often did not equal final defeat; strategic "space" allowed for recovery
  - Geographic and Temporal ("land/distance & time")
    - Russia, 1941-44
    - Pacific, 1941-44
    - Battles for operational superiority:
    - Radar, Airspace over Western Europe, Battle of Atlantic
- Cyberwarfare: defeat in the first cyberbattle may be the defining condition for victory
  - "Victory" in Clausewitzian terms, ie./ political objectives, not solely/narrowly military

First Battles: Land

- Kasserine Pass, Feb 1943
  - US vs Rommel/Afrika Korps
    - US Losses:, 10,000 men, 1,000 vehicles
    - German losses: 2,000 men, 34 tanks
- To Paris, July-Aug 1944
  - Allies vs. fleeing Wehrmacht
    - Allied losses: 2,000KIA (Paris)
    - German losses: 14,000 KIA, 50,000 POW; (Paris)
- Time gap: 18 months

First Battles: Sea

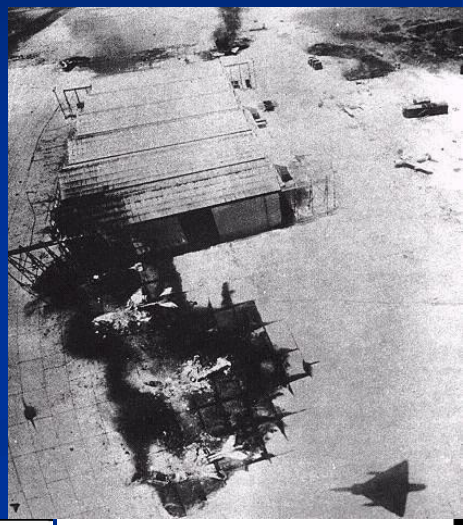
- Coral Sea: May 1942; Eastern Solomons: Aug 1942; Santa Cruz Islands: Oct 1942 (post Pearl Harbor, minus Midway)
  - US/Japan carrier battles
    - USN Losses: 2 fleet carriers sunk, 2 badly damaged
    - IJN losses: 2 light carriers sunk, 2 fleet carriers damaged
- Leyte Gulf: Oct 1944
  - USN losses: 6 ships sunk (3 light carriers)
  - IJN losses: 27 ships sunk (4 carriers, 3 battleships)
- Time gap: two years
- Next year: Hiroshima, Surrender

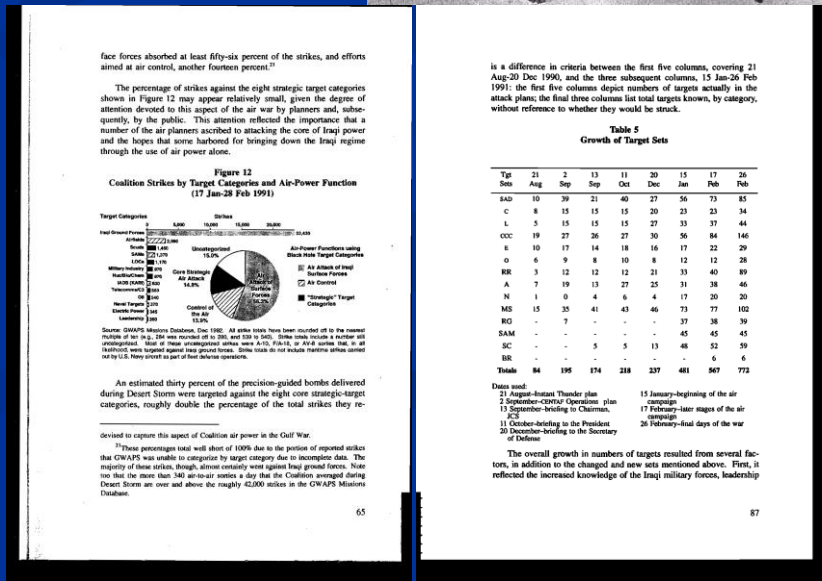
First Battles: Air

- 8AF vs. Luftwaffe
  - Unescorted bomber attacks
  - Schweinfurt/Regensburg, Aug and Oct 1943
    - US losses: 120+ bombers
    - German losses: 80+ fighters
  - End of the War
    - 2000+ bombers (day and night)
    - Cities in ruins, 500,000+ dead, industry in shambles
    - Surrender
  - Time gap: Year +

Transition Phase

- Desert Storm and "Parallel Warfare" (see 1967 IAF vs Egypt…no strategic space)
- Simultaneous aerial attack on key elements of C3
- Attacks were kinetic…but jump ahead two decades: would they need to be NOW?!





face forces absorbed at least fifty-six percent of the strikes, and efforts aimed at air control, another fourteen percent.[73]

The percentage of strikes against the eight strategic target categories shown in Figure 12 may appear relatively small, given the degree of attention devoted to this aspect of the air war by planners and, subsequently, by the public. This attention reflected the importance that a number of the air planners ascribed to attacking the core of Iraqi power and the hopes that some harbored for bringing down the Iraqi regime through the use of air power alone.

Figure 12
Coalition Strikes by Target Categories and Air-Power Function
(17 Jan-28 Feb 1991)

An estimated thirty percent of the precision-guided bombs delivered during Desert Storm were targeted against the eight core strategic-target categories, roughly double the percentage of the total strikes they re-

devised to capture this aspect of Coalition air power in the Gulf War.

[73]These percentages total well short of 100% due to the portion of reported strikes that GWAPS was unable to categorize by target category due to incomplete data. The majority of these strikes, though, almost certainly went against Iraqi ground forces. Note too that the more than 340 air-to-air sorties a day that the Coalition averaged during Desert Storm are over and above the roughly 42,000 strikes in the GWAPS Missions Database.

65

is a difference in criteria between the first five columns, covering 21 Aug-20 Dec 1990, and the three subsequent columns, 15 Jan-26 Feb 1991: the first five columns depict numbers of targets actually in the attack plans; the final three columns list total targets known, by category, without reference to whether they would be struck.

Table 5
Growth of Target Sets

Tgt Sets	21 Aug	2 Sep	13 Sep	11 Oct	20 Dec	15 Jan	17 Feb	26 Feb
SAD	10	39	21	40	27	56	73	85
C	8	15	15	15	20	23	23	34
L	5	15	15	15	27	33	37	44
CCC	19	27	26	27	30	56	84	146
E	10	17	14	18	16	17	22	29
O	6	9	8	10	8	12	12	28
RR	3	12	12	12	21	33	40	89
A	7	19	13	27	25	31	38	46
N	1	0	4	6	4	17	20	20
MS	15	35	41	43	46	73	77	102
RG	-	7	-	-	-	37	38	39
SAM	-	-	-	-	-	45	45	45
SC	-	-	5	5	13	48	52	59
BR	-	-	-	-	-	-	6	6
Totals	**84**	**195**	**174**	**218**	**237**	**481**	**567**	**772**

Dates used:
21 August–Instant Thunder plan
2 September–CENTAF Operations plan
13 September–briefing to Chairman, JCS
11 October–briefing to the President
20 December–briefing to the Secretary of Defense
15 January–beginning of the air campaign
17 February–later stages of the air campaign
26 February–final days of the war

The overall growth in numbers of targets resulted from several factors, in addition to the changed and new sets mentioned above. First, it reflected the increased knowledge of the Iraqi military forces, leadership

87

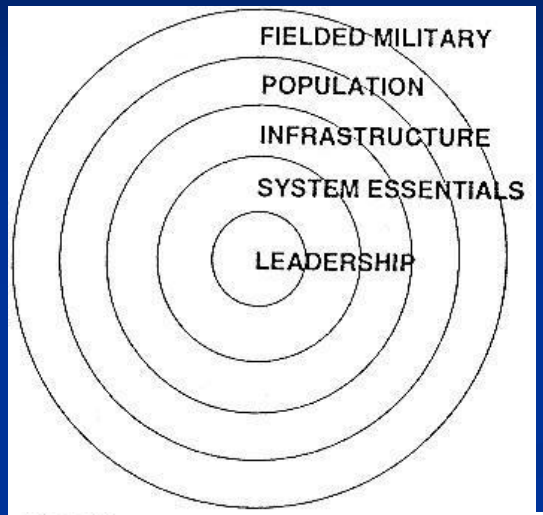
Dave Deptula, "Parallel Warfare", 1996
GWAPS, 1993

Instant Thunder 1990

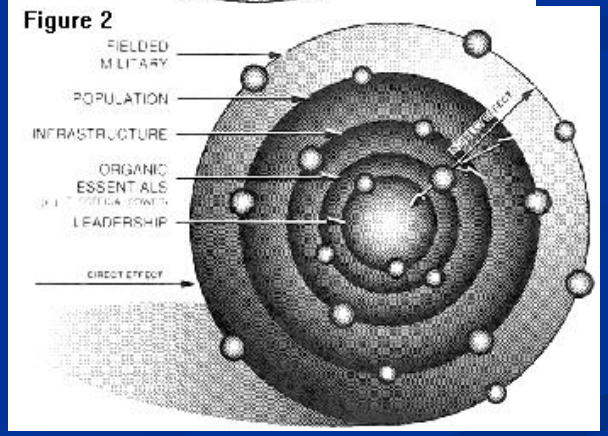
- **ESSENTIAL TARGET SETS**

– Strategic Air Defense
  – Render Iraq defenseless and minimize threat to friendly forces
– Strategic Offense Capability
  – Reduce threat to adjacent states ... now and in the future
– Hussein Regime
  – The most important center of gravity
– Telecommunications and C3
  – Rupture Hussein's link to people and military
– Electricity
  – Cripple production and create confusion
– Oil (refined products)
  – Paralyze domestic and military internal movement
– Railroads
  – Complicate movement of goods and services
– Nuclear/Biological/Chemical Research Facility
  – Reduce long-term international threat
– Military Research, Production and Storage
  – Limit offensive capability – short and long-term

http://www.washingtonpost.com/wp-srv/inatl/longterm/fogofwar/docinstant.htm



John Warden, *The Air Campaign*
1988, NDU Press



John Warden, "The Enemy as a System"
Airpower Journal, Spring 1995
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm

Desert Storm 1991

- **JFACC Air Campaign Objectives**
- Isolate and incapacitate the Iraqi regime:
  - Leadership command facilities.
  - Crucial aspects of electricity production facilities that power military and military-related industrial systems.
  - Telecommunications and C3 systems.
- Gain and maintain air supremacy to permit unhindered air operations:
  - Strategic IADS, including radar sites, SAMs, and IADS control centers.
  - Air forces and airfields.
- Destroy NBC warfare capability:
  - Known NBC research, production, and storage facilities.
- Eliminate Iraq's offensive military capability by destroying major parts of key military production, infrastructure, and power projection capabilities:
  - Military production and storage sites.
  - Scud missiles and launchers, production and storage facilities.
  - Oil refining and distribution facilities, as opposed to long-term production capabilities.
  - Naval forces and port facilities.
- Render the Iraqi army and its mechanized equipment in Kuwait ineffective, causing its collapse:
  - Railroads and bridges connecting military forces to means of support.
  - Army units to include RGFC in the KTO.
    - Source: *Conduct of the Persian Gulf War*, Chapter 6: "The Air Campaign" http://es.rice.edu/projects/Poli378/Gulf/gwtxt_ch6.html

- ***Telecommunications and Command, Control, and Communication Nodes***

  The ability to issue orders to military and security forces, receive reports on the status of operations, and communicate with senior political and military leaders was crucial to Saddam Hussein's deployment and use of his forces. To challenge his C3, the Coalition bombed microwave relay towers, telephone exchanges, switching rooms, fiber optic nodes, and bridges that carried coaxial communications cables. These national communications could be reestablished and so, required persistent restrikes. These either silenced them or forced the Iraqi leadership to use backup systems vulnerable to eavesdropping that produced valuable intelligence, according to DIA assessments, particularly in the period before the ground campaign. More than half of Iraq's military landline communications passed through major switching facilities in Baghdad. Civil TV and radio facilities could be used easily for C3 backup for military purposes. The Saddam Hussein regime also controlled TV and radio and used them as the principal media for Iraqi propaganda. Thus, these installations also were struck.

(Anything here that has NOT been discussed In any Cyberwar article ever written!?)

"We have built our future upon a capability that we have not learned how to protect."

George Tenet
Former Director of Central Intelligence

The New National/Global Security Environment

- "Global Asymmetric Engagement/Asymmetric Counterforce'
  - Cyberwarfare vs information & networks; operating in the global commons
- Asymmetric warfare & the "revolution in military affairs" = others are looking for OUR weaknesses
  - Information-dependent military operations
  - Critical infrastructure-dependent national societies
  - Inter-connected global economies
- Have we the organizations, doctrines, personnel needed to survive and win the First Battle in Cyberspace?

Cyber-Attacks-- 1

- Asymmetric Advantages of Attack
  - Cheap
  - Defense is Disproportionately Expensive, Difficult
  - Plausible Deniability & Masking Effects
- "Weapon of Mass/Precision Disruption"
  - The entire grid vs one substation
- Chaos May Be More Effective Than Carnage
  - May be narrowly-focused chaos

Cyber-Attacks-- 2

- Strategic as Well as Tactical/Operational Goals, Impacts
  - Does not mean "national collapse"
- Could Be Combined With Limited Kinetic Attacks (Special Ops) to broaden impact, create synergies and exploit effects
- Would Try to Exploit "Virtual Seams" Between Functional/Organizational Entities
- Manipulation more dangerous than denial

Critical Infrastructure Industry	Direct Percent of GDP	Effective Percent of GDP	Dependent Percent of GDP
Electric Power	1.5	3.4	72
Oil and Gas Fuel	1.0	3.0	71
Telecom & Internet	2.6	4.9	62
Banking and Finance	5.7	8.6	59
Water and Sanitation	< 1	< 1	40
Chemical Industries	1.7	4.1	33
Air Transport	0.5	2.0	24
Ground Transport	2.1	4.0	62*
Health Care	6.7	15.4	16
Police and Fire	< 1	< 1	10
Electronics Industry	1.4	4.8	5
Automotive Industry	1.1	3.2	4
Defense Industries	0.4	1.2	2

Scott Borg: Cyber Consequences Unit http://www.usccu.us/

Potential Cyber Attack Objectives

- Disrupt enemy infrastructure, logistics and supply chains
- Distract, confuse, and disable enemy C4ISR
  - OODA-Loop effects
- Impair the movement of military forces
- Deny similar capabilities to the enemy
- Create opportunities for strategic attacks on enemy infrastructures
- Weaken, distract and disorient social cohesion and political will of both military forces and civil populace
- Shape global perceptions of the conflict
- Time-Gap: potentially NANOSECONDS!

Bob Miller & Irv Lachow, "Strategic Fragility", http://www.ndu.edu/CTNSP/defense_horizons/DH59.pdf

Information/Infrastructure Operations (I2O)

- Combined with other types of operations.
- Largely, but not entirely, fought in cyberspace.
  - Special operations and limited kinetic efforts are also likely.
- Strategic as well as operational/tactical goals.
- Important asymmetric advantages to the weaker party.
- Important advantages to the first mover. Combined with the relative ease of initiating such operations, this will provide powerful incentives to a hostile (or merely nervous) potential adversary to initiate actions.
- No real way to protect against I20 efforts, but they can be limited through resilience strategies and, perhaps, be deterred by the development of retaliatory capabilities.
- Significant victory in the I20 realm may decide war aims.

Bob Miller & Dan Kuehl, "Cyberspace and the First Battle in 21st Century Warfare"

Cyberwarfare Posture

- Add Cyberspace threats to exercises
- Greater buy-in from CJCS, Services, COCOMs
  - Operational community needs to see its reality
- Adequate personnel force for cyber defense
- Info Assurance across system life-cycle
- DOD: assume tasking to respond to cyber attacks on government & infrastructure

DSB 2007 "Challenges to Mil Ops in Support of National Interests"

President Obama & Cyber

Protect Our Information Networks

Barack Obama and Joe Biden -- working with private industry, the research community and our citizens -- will lead an effort to build a trustworthy and accountable cyber infrastructure that is resilient, protects America's competitive advantage, and advances our national and homeland security. They will:

Strengthen Federal Leadership on Cyber Security: Declare the cyber infrastructure a strategic asset and establish the position of national cyber advisor who will report directly to the president and will be responsible for coordinating federal agency efforts and development of national cyber policy.

Initiate a Safe Computing R&D Effort and Harden our Nation's Cyber Infrastructure: Support an initiative to develop next-generation secure computers and networking for national security applications. Work with industry and academia to develop and deploy a new generation of secure hardware and software for our critical cyber infrastructure.

Protect the IT Infrastructure That Keeps America's Economy Safe: Work with the private sector to establish tough new standards for cyber security and physical resilience.

Prevent Corporate Cyber-Espionage: Work with industry to develop the systems necessary to protect our nation's trade secrets and our research and development. Innovations in software, engineering, pharmaceuticals and other fields are being stolen online from U.S. businesses at an alarming rate.

Develop a Cyber Crime Strategy to Minimize the Opportunities for Criminal Profit: Shut down the mechanisms used to transmit criminal profits by shutting down untraceable Internet payment schemes. Initiate a grant and training program to provide federal, state, and local law enforcement agencies the tools they need to detect and prosecute cyber crime.

Mandate Standards for Securing Personal Data and Require Companies to Disclose Personal Information Data Breaches: Partner with industry and our citizens to secure personal data stored on government and private systems. Institute a common standard for securing such data across industries and protect the rights of individuals in the information age.

Defense

Protect the U.S in Cyberspace: The Obama-Biden Administration cooperate with our allies and the private sector to identify and protect against emerging cyber-threats.

http://www.whitehouse.gov/search/?keywords=cyber

Advice for Obama Admin

- Three Suggestions
  - Do not treat cyberspace in isolation from information environment (See DepSecDef Memo of May 07)
    - Need comprehensive Cyberstrategy as a segment of an even more comprehensive National Info Strategy
      - "Comprehensive National Cybersecurity Initiative" (CNCI) is vital but not enough by itself
  - Grow the Partnership
    - Public Sector: Interagency/Government (all levels), Military, Congress, Intel, Agencies, etc
    - Private Sector: Industry/Business, Academia, Society
    - International partners and players
  - Build the "3Cs" (next slide)

Information Strategy: "3Cs"

- Builds on "3Cs"
  - Build, enhance, support Connectivity
    - Physical: networks, infrastructures, Information-Communication Technology (ICT) based on Cyberspace
    - Human: one-one, one-many, many-many (enabled by ICT)
  - Build/Use institutions that create Content
  - Measure Cognitive impact
    - USE of Cyber/Info for success (military, economic, diplo, etc)
  - Get the REAL experts (ie. Business-Private Sector)
    - Obama Cyber policy seems to get this
- All Three require partnerships beyond government, military, and especially the private sector to include non-US, and they require a long-term view…this isn't years, it's decades
- **All Three depend on and use Cyberspace: key to future national security!**

Dr Dan Kuehl
kuehld@ndu.edu 202-685 2257

http://www.ndu.edu/irmc/programs/index.html

Programs/Certifications for/in…
Chief Information Officers
Information Assurance
Organizational Transformation…

…and **Information Strategists**