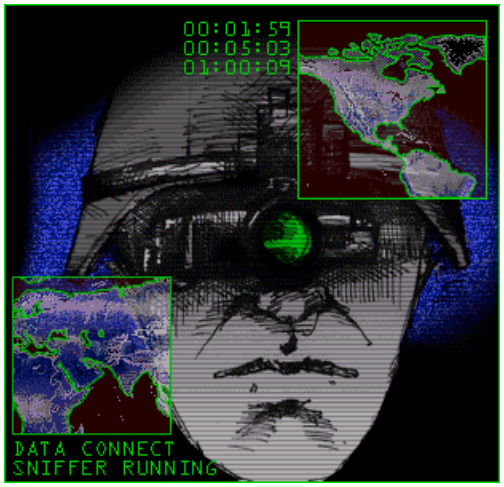
THE CENTER FOR ADVANCED STUDIES
IN SCIENCE AND TECHNOLOGY POLICY

Deconstructing Information Warfare



K. A. Taipale
Executive Director, Center for Advanced Studies
Senior Fellow, World Policy Institute
Adjunct Professor of Law, NYLS

Presented to the:
Committee on Policy Consequences and Legal/Ethical Implications of Offensive Information Warfare
The National Academies, Washington, DC, Oct. 30, 2006

Presentation overview

- Need for doctrine: convergence, divergence, 4GWF
- Laws governing state conduct
- What is “offensive information operations and cyberattack”?
  - What is IW? How is it employed? Subject to what controls?
- Conclusion - need for doctrinal framework that accounts for globalization/interdependence, US offensive power and defensive vulnerabilities, and includes private sector and NGOs
- Some policy suggestions …

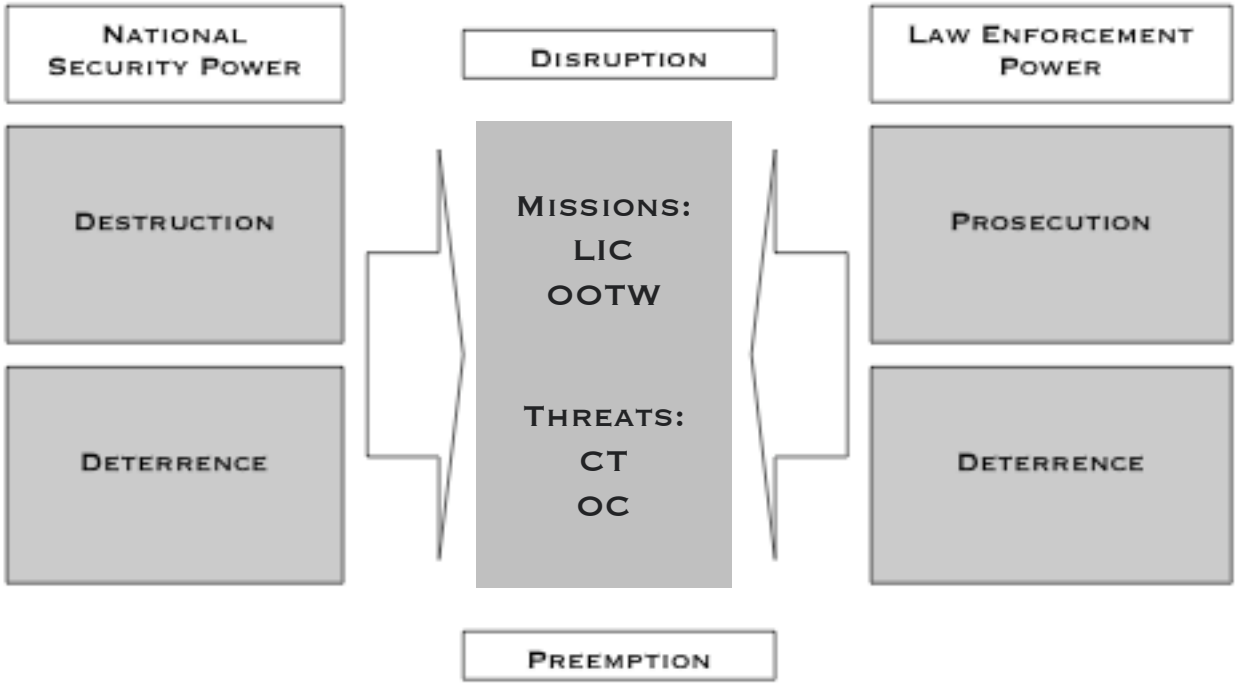
Overview of "IW"

- Threshold issue: tactical weapon system or strategic domain?
  - ICT as tool, target, or place of warfare
  - Organizational issues (STRATCOM, JFCCNW, USAF, NSA, CIA)
- Instrumental use: Deny, disrupt, degrade, destroy, (alter) information or systems (~penetrate, defend)
- OIO targets: information, channels (systems), and actors
- Target ICT qua information appliance or as control mechanism
- Attack mode: physical, syntactic (data/logic), semantic attacks

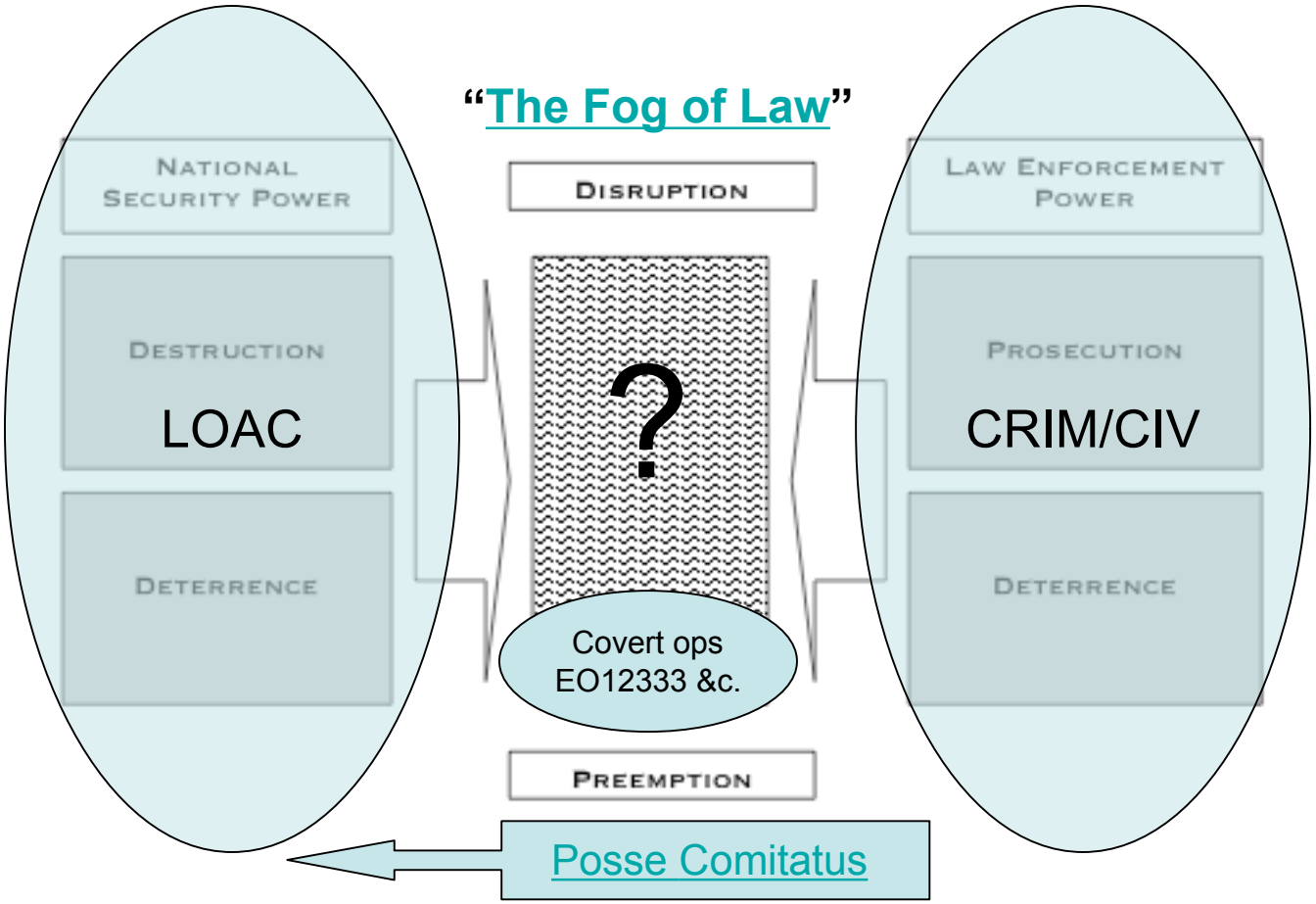
POV

- Independent, nonpartisan research
- Focused on information, technology, national and global security
- Cybercrime, counterterrorism, global information society
- Recent invited presentations on related issues
  - Information and identity management (DOD)
  - Identity and security (Harvard Law School, NAS/NRC)
  - Intelligence production (IC agency)
  - Information sharing (Markle Task Force, DHS)
  - Analysis and data-mining (NAS/NRC)
  - Foreign Intelligence Surveillance (HPSCI)
  - IO and CT (Yale Law School, BANTLE)
  - Information Warfare (NAS, current research project)

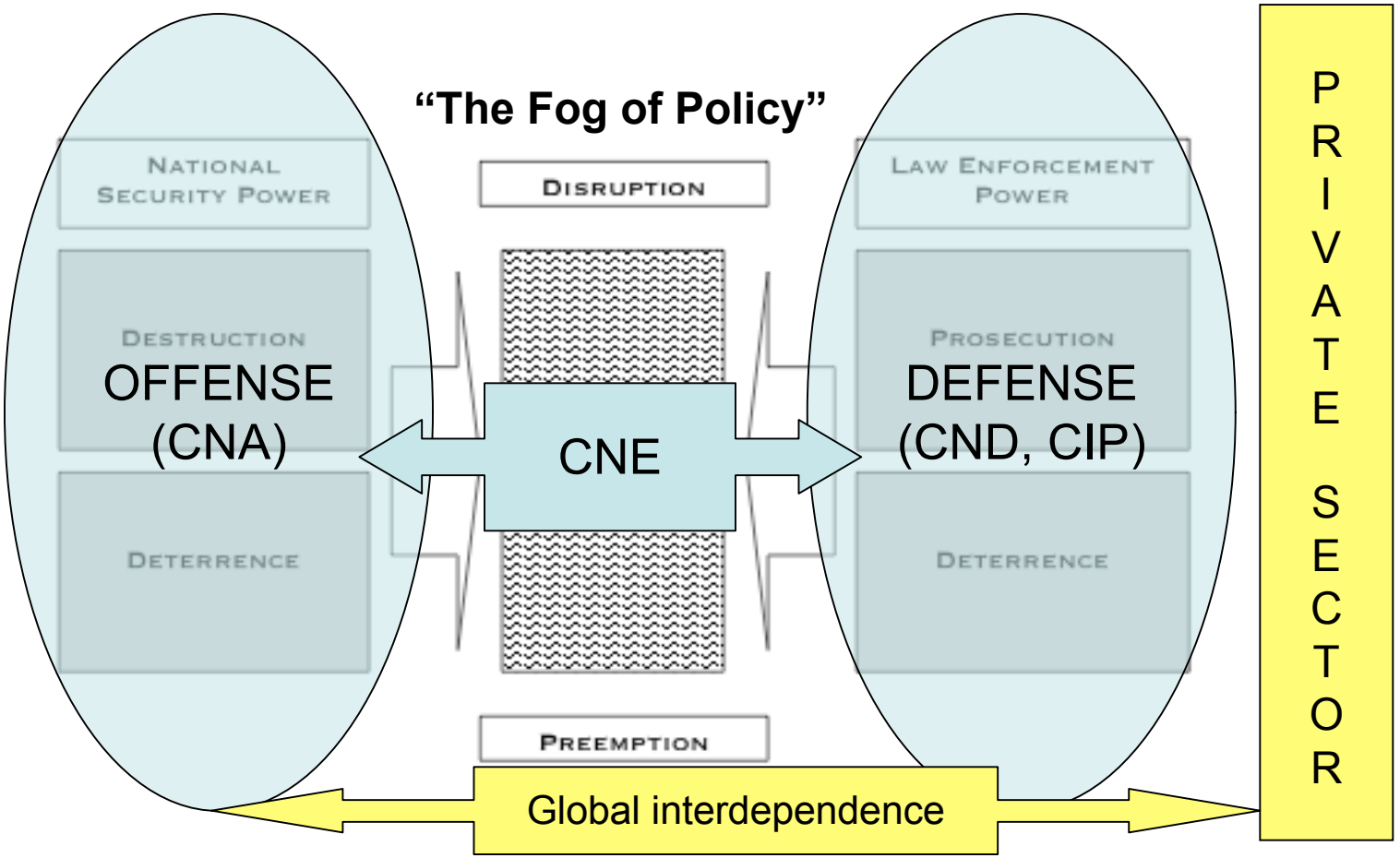
Need for overarching doctrine: converging missions and threats



Need for overarching doctrine: doctrinal vacuum



Information operations



Why “Laws of War”

- Warfighting is the use of force to make the enemy do one’s will
- “Laws of war” distinguish and protect acts [of force] that would be criminal if performed in time of peace (murder, assault, etc.)
- Non-compliance is a war crime (ICJ, Tribunals, NGOs, etc.)
- The laws of war guide the selection of methods, of weaponry, and of targets
- Following the outlawing of “aggressive war” (Kellogg-Briand 1928, UN Charter 1945) the customary laws of war have been increasingly “codified” as international “laws of armed conflict”
  - Hague/LOAC - how to initiate and conduct war
  - Geneva Conventions - how to protect combatants & noncombatants

Evolution of warfare (cumulative)

	Paradigm	COG	Leverage	
1GWF	agrarian (classical)	manpower	massed formations	Napoleonic
2GWF	Industrial (premodern)	assets	massed firepower	US Army "steel on target"
3GWF	nonlinear (modern)	control	maneuver	USMC "keep moving"
4GWF	chaotic (pomo)	moral[e]	information	SOF "hearts and minds"

4GW Warfare

- *"[The] goal [is] collapsing the enemy internally rather than physically destroying him. Targets will include such things as the population's support for the war and the enemy's culture. …. the distinction between war and peace will be blurred to the vanishing point … between "civilian" and "military" may disappear."*

  – The Changing Face of War: Into the Fourth Generation
  Col. William S. Lind, et al., Marine Corps Gazette (October 1989)

Russian POV

- *"We are approaching a stage of development when no one is a soldier anymore but everyone is a participant in combat action. The task now is not to inflict losses in men and materiel but to thwart an enemy's plans, demoralize it, undermine its worldview, and destroy its intrinsic values."*
  - *Lessons from the War in Iraq*

    Maj. Gen. G.A. Berezkin Deputy Head of the Russian Federation Defense Ministry Center of Military-Technical Information Studies, Military Thought (May 1, 2003)

Chinese POV

- *"The new principles of war are no longer 'using armed force to compel the enemy to submit to one's will,' but rather are 'using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests.'"*

  – UNRESTRICTED WARFARE
  Col. Qiao Liang and Col. Wang Xiangsui
  (Beijing: PLA Literature and Arts Publishing House, February 1999)

Al Qa'ida: information and war

Tactical: "All that we have to do is to send two Mujahedin to the farthest point East to raise a piece of cloth on which is written al-Qa'ida in order to make the generals race there to cause America to suffer human economic and political losses without their achieving for it anything of note ..."

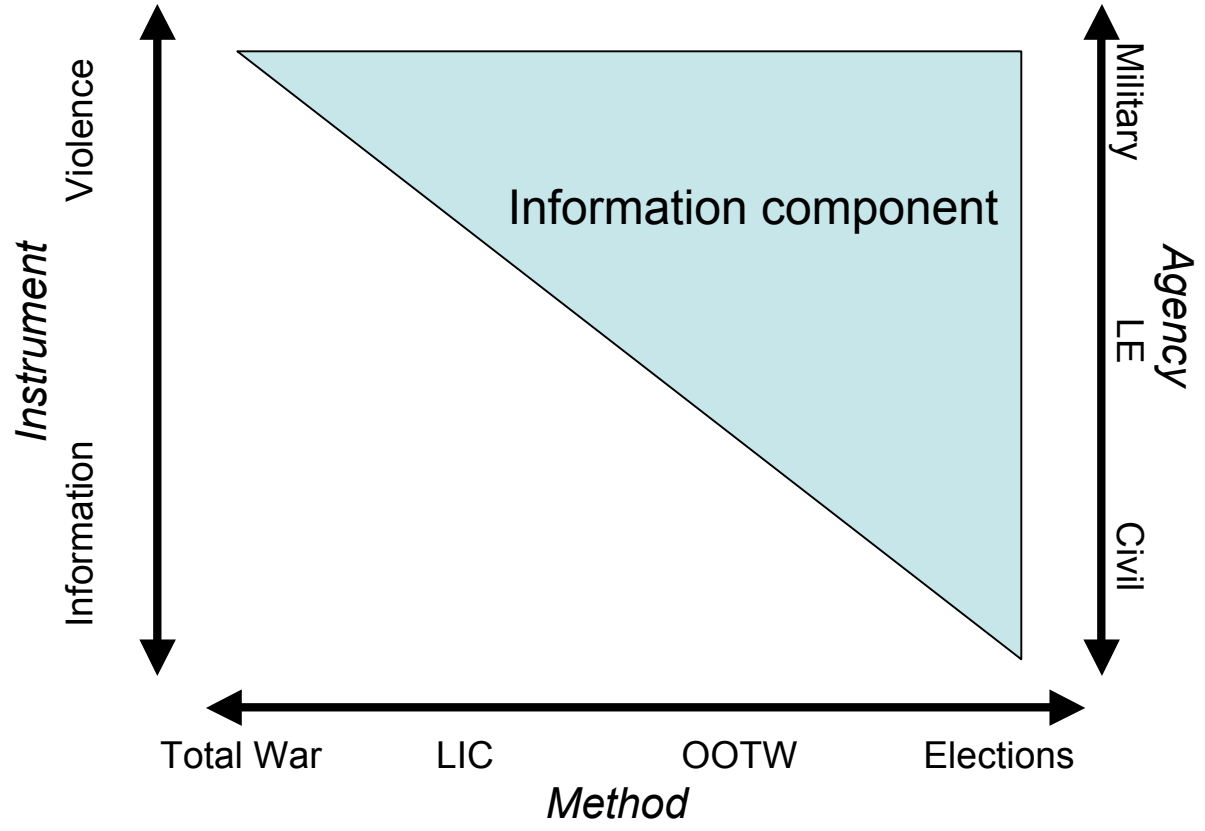
-- Osama bin Laden (2004) (Wash. Post. 11.01.04)

Strategic: "It is obvious that the media war in this century is one of the strongest methods; in fact, its ratio may reach 90% of the total preparation for the battles."

-- Osama bin Laden (2002) (AFGP-2002-600321)

Information in conflict resolution

Cliché, but war is [politics] by other means



Provides opportunity for IW and IO

- Information warfare -- information operations conducted during time of crisis or conflict to achieve or promote specific objectives over specific adversary
- Information operations (IO) -- actions taken to affect adversary information and information systems while defending one's own information and information systems
- The ultimate target for OIO is human (?) decision making
- Joint Publ. 3-13, Joint Doctrine for Information Operations (1998)

"Offensive information operations and cyberattack"

- JP 3-13 Joint Doctrine for Information Operations (2006):
  - Eliminates information warfare as a term from joint IO doctrine
  - Discontinues use of the terms 'offensive IO' and 'defensive IO'
  - Defines IO core capabilities: PSYOPS, MILDEC, OPSEC, EW, CNO
- Computer Network Operations (CNO) ("attack, deceive, degrade, disrupt, deny, exploit, defend electronic information and infrastructure")
  - Computer Network Attack (CNA) (deny, disrupt, delay, destroy)
  - Computer Network Exploitation (CNE) (collect, monitor, or falsify)
  - Computer Network Defense (CND, CIP) (protect, detect, restore, respond?)
- NSPD 16 *[Guidelines for Offensive Cyber-WF]* (2002) (C)
- DOD Information Operations Roadmap (2003) (partially C)

Computer Network Exploitation

- Surveillance/collection (CNE-Intel)
  - Fourth Amendment (USP - Markle "authorized purpose")
  - FISA, Title III, ECPA
  - Need *e-Terry* (*see* Whispering Wires) for electronic surveillance?
- Manipulation (CNE-Falsify) (OIO)
  - CCAA §1030, Convention on Cybercrime, FORN domestic law
  - Blowback/leakage (Smith-Mundt Act, Zorinsky Amendments)
  - Need FISC-like OIO warrants to attack sub-national enemies?
- Covert operations responsibilities (DOD/STRATCOM, CIA)
  - EO 12,333, National Security Act 1945, NSPD 16?
  - Compare "exploitation" (IC) v. IPB (DOD)
- Deconfliction issues

Is OIO "war" and does it matter?

- Without some "legal" sanction, OIOs are either war crimes or cybercrimes
- Thus, some authorizing doctrine (law, custom, norm, or exception) needs to be developed for lawful state action
- Cf. covert action (disavowed illegal acts)
- The issue is legal authority and political legitimacy to use OIO
- Leads to three committee policy questions (prospectus):
  1. When is enemy IO a predicate for response?
  2. When is IO a legitimate weapon of preemption?
  3. In either case, what rules govern its use?

Potential guidelines for analysis

- Analogize from two “kinds” of cybercrime
  - Unauthorized access to information (espionage and surveillance)
    - CNE(I) = Intel and law enforcement analogue
  - Interference with integrity of data or function of system (~force)
    - CNA, CNE(F) = military analogue (~ exploit v. prep)
- Further, distinguish by targeting purpose (OO, OD):
  - Strategic C2W - aimed at enemy’s political competency (leadership/population)
  - Tactical C2W - aimed at enemy’s warfighting competency (leadership/military)
  - Operational - prevent action in specific engagement
- Finally, evaluate effects (scope, duration, intensity, damage) (~Schmitt analysis)

A caution re “interference”

- Syntactic attack (data or logic)
  - Malware w/ sufficient damage can = force
- But, exceeding “TOS”?
  - Exceeding authorized access
  - Spamming
- Or, overwhelming capacity of system to respond?
  - DoS/DDoS
    - SYN, UDP, and ICMP flood attacks (unauth access to target)
    - Zombies and botnets (unauth access to distributed attackers)
    - Hacktivism? (each request “authorized”) (disturbing the peace?)
- Cf., financial “terrorism” (the curious case of Mr. Soros)

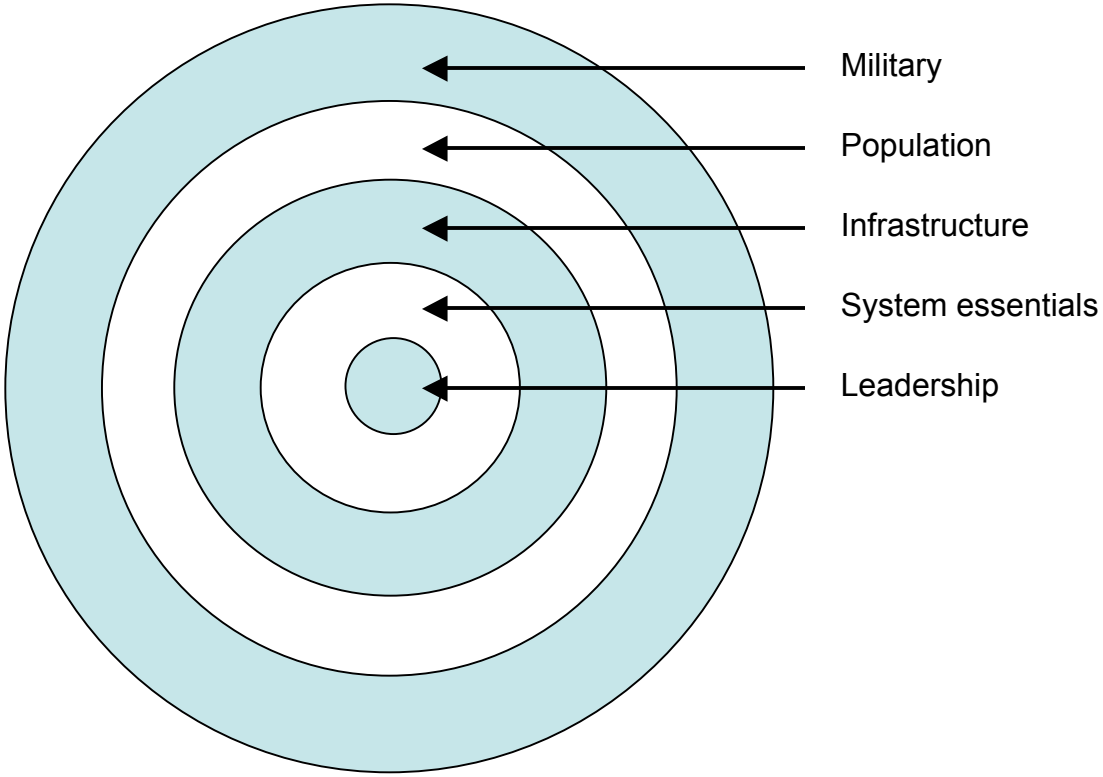
Some lessons from cybercrime trends

- From access to syntactic and toward semantic attack
  - Unauthorized access or exceeding authorized access
  - Syntactic attack (data or logic) interferes with function
  - Semantic attack (meaning) interferes with outcomes
- Collapsing perimeter of defense
  - Firewall, code scanners, application monitoring, recovery
  - Defend in depth
  - Deterrence yields to resilience, recovery
  - Active: honeypots (trap) v. strikeback (*cf*. nuisance v. trespass)
- Need to understand defense in depth when considering OIO

Three methods of warfighting

- Destroy enemy absolutely
  - kill everybody
  - 1GWF - (~obsolete for developed powers?)
- Make noncompliance too costly politically, economically, or militarily
  - impose "pain"
  - 2GWF - break things
- impose strategic or operational paralysis
  - directly or indirectly constrain enemy's ability to make or implement decisions adverse to your interests
  - 3GWF - cut off options physically
  - 4GWF - cut off options politically

Targeting: Warden's five rings



John A. Warden III, Air Theory for the Twenty-first Century (1989)

Operational OIO objectives: prevent *actions*

- Scale attack to unit of engagement (individual up to NCA)
- Attack/destroy enemy's *motivations* and *capabilities*
  - Target institutional structures that sustain enemy's cohesion
  - Target capabilities that enable enemy to act or resist
  - Undermine internal and external support
- By attacking/denying/altering:
  - *organizational* information flows
  - *operational* information flows
  - *external* information flows
- *Evaluate (and deconflict) advantage: to deny, deceive, destroy, or exploit, that is the question.*

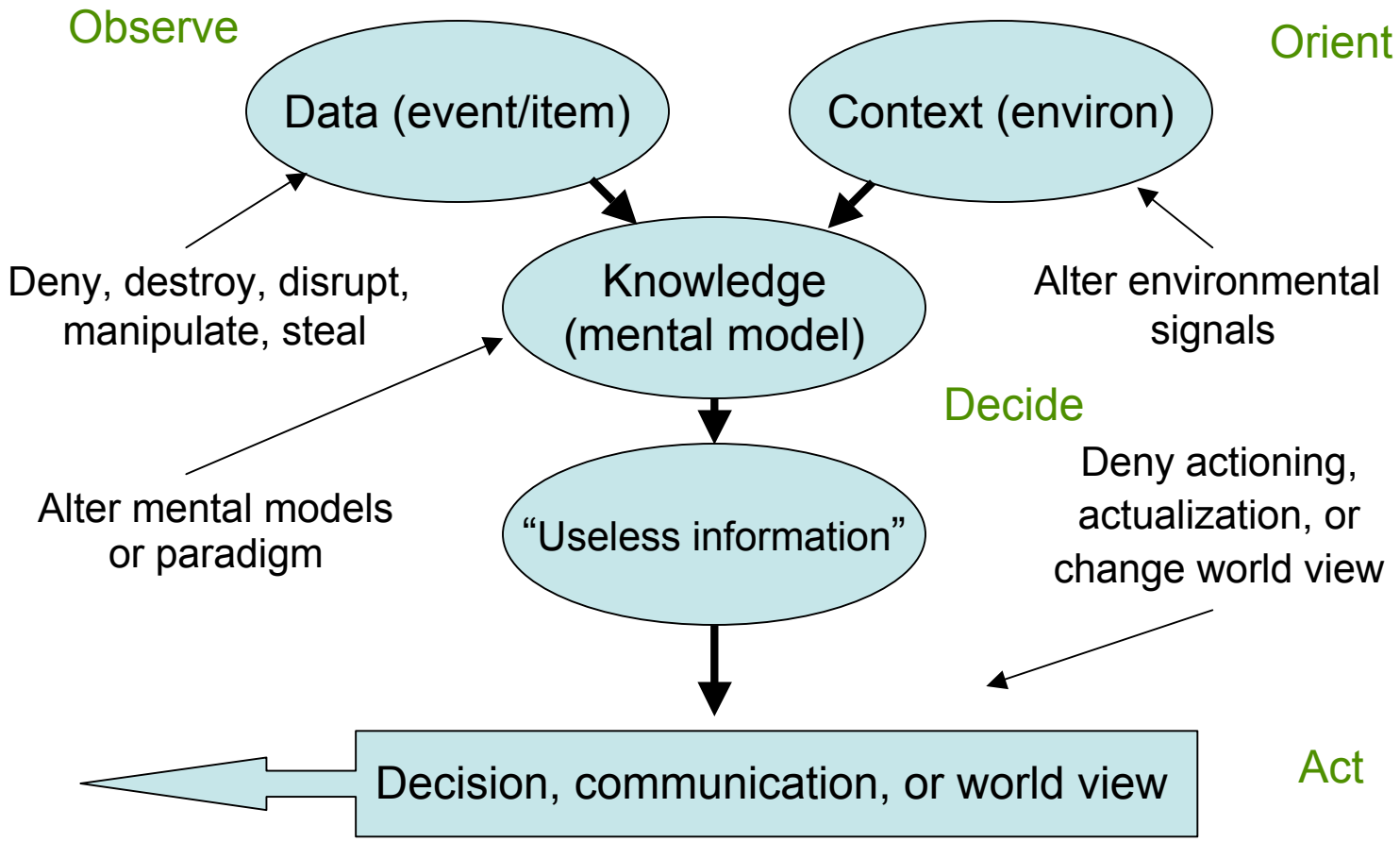
Cyberattack

- Target categories (Denning taxonomy 2005, 1999)
  - Data/content (information) (deny, corrupt, discredit)
  - Channels/media (systems) (block, delay, divert)
  - Actors ("turn", discredit, or deny freedom of action)
    - Leadership, commanders
    - Supporters (finance, supplier), sympathizers, soldiers
    - Population (effects directly related to political power)
    - International opinion ("kill faster" and the news cycle)
    - Opposition (support for and effect on)
- Objective: reorient the usefulness of information and systems to support your mission at the expense of the opponent's

Target: Information content

- Public diplomacy, strategic influence, PSYOPS-1 (present your POV)
- NSD-77 (1983), PDD-68 (1999) (C), and NSPD-16 (2002) (C)
- CNE (attack information integrity) PSYOPS-2 (corrupt their POV)
  - Manipulate input or sensors (environmental signals)
  - Manipulate, destroy, alter data within system (elements)
  - Manipulate logic (syntactic)
  - Manipulate outcome (semantic)
- Statutory restrictions/issues
  - DOD domestic info ops (Posse Comitatus) (~LE)
  - Military (battlespace prep) v. IC (exploitation) (NSA1947, EO12333)
  - domestic influence (blowback) (Smith-Mundt Act) (*but see* IOR)

OIO to disrupt OODA loop (C2W)



Target: Information channels (systems)

- CNA (CW) (conflicts w/ US, Int'l, and FORN cybercrime laws)
  - Delay (DDoS)
  - Interrupt (router attacks)
  - Distort/redirect (DNS hacks)
  - Malware (virus, trojan, logic bomb)
  - Google bombing (hacktivism) or other "engineering"? (blowback)
- Filtering/censoring (shape info environment to influence behavior/decision making)
  - Content categories vs. constative content or flow
  - "Wholesale" (not individualized) vs. "retail" (targeted)
- Complicating factors: interdependence, distinction/segregation, ownership and divergent interests (private sector)

When targeting system functionality: distinguish instrumental effects

- Primary effects: ICT qua information appliance
  - C2W (leadership, military)
  - Political control mechanisms? (Belgrade TV)
  - Political support (propaganda and counter propaganda)
- Secondary effects: ICT as control mechanisms for military or civil infrastructure or asset (SCADA, etc.)
  - Military objective/military advantage? (Gen. Conv. Art. 51(2))
  - Can't target "national will"? (*e.g.,* Serbian bridges and HRW)
  - Can you target "lifestyle"?
    - *Cf.,* "bomb you into the stone age" w/ "shut off your MTV"

Target: Information actors

- Select out, monitor, discredit or support individuals or groups (based on destabilizing effect)
- Leadership, military, population
  - increase dissension and friction, engender internal competition, undermine trust, exploit ideological breaks in leadership
  - subvert authority of leadership and senior commanders, confuse, humiliate, demoralize, and embarrass rank-and-file (personalized?)
  - Facilitate both misunderstanding and understanding of US intentions and capacity
- Provide alternatives, exits, and incentives
- E.g., Iraqi generals' cell phones, "diddling" with Milosovic

Important IW Caveat #1

- Can it be done?
  - Distributed systems
  - Redundancy/resilience/recovery
- Methods of attack (~CC)
  - Insider (human asset)
  - Social engineering (business process)
  - Vulnerability (requires technical or business process knowledge)
    - Disclosure by exploit ends opportunity
    - Patching between mapping and attack
    - Reliability - known effect? Testing? Battle damage assessment?
- Attribution/identification ~ adversary characterization
- Judging effects
  - Precision or indiscriminate weapon? *E.g.*, Iraqi banking (EU)
  - Battle damage assessment and confidence

Important IW Caveat #2

- Should it be done?
  - Offensive US strength
  - Defensive US vulnerability (more to lose)
- Use (or reserving right to) legitimizes use by others
- Interdependencies - global, multinational, national
- If not, then what arms control paradigm?
  - Characteristics of IW making control difficult:
    - Production - dual use
    - Capabilities - ubiquitous skills
    - Verification - low observability
    - Control - industry dynamics
  - *Cf*. w/ nuclear weapons, bioweapons, other
  - Offense is zero-sum yang of defense? (*cf*. "take down" w/ "bring up")

But, if you are going to do it:
"Fight the Net" and prep the battlespace (IOR)

- Need to understand opponent's organizational, operational, and external and internal information flows, business process models, and systems (~their '*network*')
- Need to map systems, process and destabilizing strategies
  - Target nodes/systems w/ high cohesion or "betweenness" (CNA)
  - Monitor nodes/systems with high information flow (CNE-I)
  - Introduce corrupt/destabilizing information (CNE-F)
  - Support nodes/systems with destabilizing effects (OPCOM)
- Need to target conditions enabling enemy opposition
- Need to Intel Prep Battlespace (IPB):
  - IOR [CNA-SYSMAP] PSYOPS-HFA, NSPD 16 , STRATCOM

Rival Interests

- Compare to US capabilities
  - *Symmetric warfare* (equal power, equal goals) ("USSR"),
  - *Dissymmetric warfare* (unequal power, equal goals) (Russia, China),
  - *Asymmetric warfare* (unequal power, unequal goals) (al Qa'ida)
- Interest in regulation
  - US argues no need for special rules (depend on LE/CC for defense) (OIO is already being doctrinalized in US, NATO, EU)
  - Russia argues for rules (1996 on) because it can't/doesn't want "arms race" (~reserves right of nuclear response?)
  - China thinks rules are to US advantage and will be broken so seeks its own advantage, "Unrestricted Warfare"
  - Note that, regardless, non-state transnational threats (CT/OC) require "special rules" combining NatSec capabilities w/ LE controls

The Laws of War

- The Hague Conventions (1899-1956)
  - Military necessity (objective, advantage)
  - Proportionality (weigh collateral damage)
  - Humanity (not indiscriminate, wanton, or cruel)
  - Chivalry (~ no perfidy but MILDEC "misinformation" - "MS SP")
- UN Charter outlaws "use of force" (art. 2) except in response to "armed attack" (self defense) (art. 51) (*Cf.,* preemption w/ anticipatory defense) or pursuant to Security Council (art. 39)
- Geneva Conventions Protocol 1 (1977) Article 51(2):
  - Targets "limited to military objectives"
  - Where attack "offers a definite military advantage"
  - Note: the US has not ratified Protocol 1 because it shifts the burden to segregate/discriminate civilians to the attacker from the defender

Jus ad bellum (predicate)

- Transition to "just war"
  - Right purpose
  - Duly constituted authority
  - Last resort
- Right of self defense, incl. anticipatory defense (*cf*., preemption)
- Paradox of IO as "armed attack" and retaliation
- Active defense -
  - issues of identification and attribution, characterization, assessment, neutrals, and proportionality
  - retorsion (tit-for-tat short of "force") v. retaliation (use of force)

Jus in bello (constraints)

- Conducting "just war"
  - Noncombatant immunity (~military objective)
  - Proportionality (collateral damage)
  - More good than harm (~military advantage)
- Recognizes collateral damage but seeks to limit
- Defender required to segregate, attacker required to discriminate
- Targeting "national will" prohibited? (mil obj / mil adv?)
  - Art. 54 ("objects indispensable to survival of civilian pop")
  - Art. 55 ("environment")
  - Art. 56 ("dangerous forces") (cw: direct or knock-on)
- *Cf.* al Qa'ida justifications (*jihad al-dafaa*) (inc. attacking civilians)
  - See "Killing in the Name of Islam" MEPC J. V.X n.2 (2002)

Often ignored real world policy constraints

- Interdependence (globalization)
  - *E.g.,* Iraq banking system intertwined w/ EU banking system
- Private actors
  - Infrastructure control and ownership
  - Multinational interests (vs. national interest)
  - Control issues (distributed, global industry)
- Ruling elites have stake in maintaining reliability of existing infrastructure (?)
  - *E.g.,* if Chinese elite interests control export industries, do they want to crash the US/Intl. banking system?
  - But *cf.,* al Qa'ida *et al.*
  - And other anti-globalization forces, etc.

Conclusion

- Need for doctrinal framework that accounts for
  - globalization/interdependence
  - US offensive power and defensive vulnerabilities (*I.e.,* the effects imbalance), and
  - includes private sector and NGOs
- US will need/want political legitimacy through *authorizing* and *control* mechanisms (policy, legal and technical) for OIO
- BL: US may have more to lose than gain from unrestricted OIO

Policy prescriptions

- IMHO:
  - renounce first use of strategic OIO,
  - develop multilateral monitoring and authorizing regime,
  - permit collective OIO and “info sanctions” (UNSC?),
  - pursue international cybercrime convention and legal harmonization,
  - deal with unauthorized access as crime or espionage, consider attacks on functionality as “use of force” (subject to Schmitt or like analysis re effects)
- But continue to prep the battlespace

http://taipale.info

</end>