

INFORMATION OPERATIONS THEORY

Sun Tzu "To subdue the enemy without fighting is the acme of skill"

T.S Eliot "Where is the knowledge we have lost in information?"

Information Operations

- DEFINITIONS
- CURRENT ENVIRONMENT (DoD)
- HISTORICAL PRECEDENT (PSYOPS)
- IO BASICS
- ENCRYPTION

Operations and Warfare

- INFORMATION OPERATIONS
- Information Security
- Information Superiority
- Information Awareness
- Information Readiness
- OOTW -- Operations Other Than War

INFORMATION WARFARE

Asymmetrical Warfare

Net-Centric Warfare (NCW)

Fourth Generation Warfare

“ASYMMETRY”

A Polymorphic Term

- Cultural Asymmetry
- Asymmetrical Ciphers (One-Way Encryption)
- Asymmetrical Information Sharing

BIBLIOGRAPHY

Lord, Carnes, and Barnett, K.R., ed., Political Warfare and Psychological Operations, National Strategy Information Center, 1988

Frank R. Barnett, B. Hugh Tovar, Richard H. Shultz, Special Operations in US Strategy, National Defense University Press (with National Strategy Information Center)gg 1984

Martin C. Libicki, Conquest in Cyberspace - National Security and Information Warfare, Cambridge University Press, New York, NY, 2007

Melanie Gutjahr, The Intelligence Archipelago, Joint Military Intelligence College, Washington D.C. 2005

Patrick D. Allen, Information Operations Planning, Artech House, Norwood, MA, 2007

Information Warfare: Definition

Libicki:

"The use of information to attack information"

". . . fundamentally about information and the use to which information is put - making better decisions"

"Information warfare remains largely theoretical"

"The control of information about information warfare is itself an aspect of information warfare."

Patrick D. Allen's List of "Sample IO Desired Effects Compiled From Various Sources":

- Access
- Cascading Network Failure
- Control
- Coordination Failure
- Create Information Vacuum
- Decapitate
- Deceive
- Decision Paralysis
- Defeat
- Degrade
- Delay
- Deny
- Destroy
- Desynchronize
- Deter
- Diminish
- Dislocate
- Disrupt
- Divert
- Exploit
- Halt
- Harass
- Influence
- Inform
- Interrupted
- Lose Confidence in Information
- Lose Confidence in Network
- Manipulate
- Mislead
- Negate
- Neutralize
- Operational Failure
- Paralysis
- Penetrate
- Prevent
- Protect
- Read
- Safeguard
- Shape
- Shock
- Stimulate
- Stop

Libicki: "Information GLUT" (Information Overload)

"The efflorescence of information content and conduits tends to complicate the three basic goals of information warfare: denial of service, interception (exploitation), and corruption of information files and flows."(p105)

Information Overload Results in:

- A)-top-down command (separation of focus requires layers of analysis, micromanaging)
- B)-not enough time to Process = delegation of responsibility
- C)Consultants, Specialists

"Can more information technology cure the ills brought about by information technology?"(115)

Allen on a DEDICATED Information Domain:

"In this stage of the Information Age, the U.S. military is grappling with whether or not it needs to define the information sphere as a domain, similar to the air, land, sea, and outer space domains that already exist. A few notable people refer to this area an "information domain," while others call it the "cyberspace domain," and still others refer to various elements of this area as either the "cognitive domain" or the "information environment." We believe that "information sphere" should be the preferred term . . ."

Allen's Proposed DoD INFORMATION DOMAIN:

"The space defined by relationships among actors, information, and information systems that form a sphere of interest and influence in or through which information-related activities, functions, and operations are undertaken to accomplish missions and exercise control over an opponent in order to achieve desired effects."

Actor: "sender, liaison, modifier, transferor, or recipient, intended or unintended"

Information: "The data and content being passed among actors via information systems"

Information Systems: "any communications, information storage, or information perceiving system, including couriers"

INFORMATION OPERATIONS ROADMAP -- Rumsfeld, 2003



Information Operations Roadmap

E. ENHANCING IO CORE CAPABILITIES (U)

1. *Computer Network Defense (U)*.....
2. *Computer Network Attack (U)*
3. *Electronic Warfare (U)*.....
4. *Psychological Operations (U)*.....
5. *Operations Security (U)*.....
6. *Military Deception (U)*.....

~~SECRET~~/NOFORN

- Number of events is increasing. The number of detected events on DoD networks continues to grow while [REDACTED]
- Exercises demonstrate our vulnerabilities. Exercise ELIGIBLE RECEIVER 03 demonstrated gross vulnerabilities resulting from [REDACTED]
- [REDACTED]
- Latest tools are not available. [REDACTED]
- Near and long-term threats. [REDACTED]

IO ROADMAP

- (U) Three integrated IO functions. The Department's concept of IO should emphasize full spectrum IO that makes a potent contribution to effects based operations across the full range of military operations during peace, crisis and war. The concept includes three integrated IO functions of overriding importance:
 - (U) Deter, discourage, dissuade and direct an adversary, thereby disrupting his unity of command and purpose while preserving our own.
 - (U) Protect our plans and misdirect theirs, thereby allowing our forces to mass their effects to maximum advantage while the adversary expends his resources to little effect.
 - (U) Control adversarial communications and networks and protect ours, thereby crippling the enemy's ability to direct an organized defense while preserving effective command and control of our forces.

~~SECRET//NOFORN~~

IO ROADMAP

(U) *Current Situation.*

- ~~(S)~~ Networks are growing faster than we can defend them. [REDACTED] As a result, greater vulnerability results from enterprise expansion. Specifically:
 - ~~(S)~~ Unprotected networks surrender asymmetric advantage. DoD has focused attention on improving the security of its networks, but the Department's [REDACTED]
 - ~~(S)~~ Attack sophistication is increasing. The sophistication and capability of both hackers and nation-states to degrade system and network operations are rapidly increasing. [REDACTED]

IO ROADMAP

(U) *Current Situation.*

- ~~(S)~~ Inadequate policy. A review of existing policy for IO found that policy lags behind operations.
 - (U) There is not a consensus on how to define IO or its contribution to warfighting.
 - (U) Computer Network Defense (CND) lacks up to date policy and legal guidance (including newly acquired authorities provided by the Patriot and Homeland Security Acts) to guide responses to intrusions or attacks on DoD networks.
 - ~~(S)~~ [REDACTED] that would guide development of desired capabilities, specific weapons development and employment, interagency coordination, and declaratory policy.
 - (U) EW policy is outdated. DoD's overarching policy was published in 1994 after the first Gulf War. The DoD directive is not consistent with the approach or recommendations of this report. It needs to be updated to stress EW as an integral part of Information Operations with important linkages to Computer Network Operations and other IO core capabilities.

IO ROADMAP

2. Relationship of Public Diplomacy and Public Affairs to IO (U)

(U) DPG Tasking.

- (U) USD(P), in coordination with ASD(PA) will analyze and make recommendations on those policy, strategy and legal issues affected by and related to the proper role for public diplomacy and public affairs in relation to IO. Particular emphasis will be given to examining the appropriate relationship of PSYOP to public affairs as they relate to USG communications strategies for both adversaries and non-adversaries. The analysis will include recommendations on policies, requirements, resources, training and education to support a transformed communications capability in support of military operations in the global information environment.

IO ROADMAP: GOALS

CND: Computer Network Defense

“Desired Outcome: A robust, layered defense across DoD enhanced through global and enclave situational awareness with the centralized capability to rapidly characterize, attribute and respond to attacks.”

“This strategy should be based on the premise that the Department will “fight the net” as it would a weapons system.”

IO ROADMAP: GOALS

CNA: Computer Network Attack

“A comprehensive interagency process is underway to evaluate the use of offensive cyber tools and develop national policy.”

“Desired Outcome: Forces trained with well-tested and reliable CNA weapons that are aligned with appropriate target sets and integrated with other IO capabilities and weapon systems.”

CNA: LEGAL ISSUES

"... what level of data or operating system manipulation constitutes an attack. This distinction is necessary to clarify which actions can be appropriately taken in self-defense and whether an action is an attack or an intelligence collection operation."

"A legal regime for handling the difficulty of distinguishing between domestic and foreign sources of attack in cyberspace is required. It should capitalize on newly acquired authorities provided by the Patriot and Homeland Security Acts."

"Legal review should determine if appropriate authorities permit attack through unwitting hosts (merely transiting or controlling the host in order to launch the attack) if the action elicits an attack against the host computer system."

"Legal Review should determine what level of certainty about the origin of an attack is required before the U.S. can respond in kind."

IO ROADMAP: GOALS

EW: Electronic Warfare

"Examples include the non-kinetic disruption of WMD facilities and disabling/disruption of missiles prior to launch."

"Desired Outcome: Achieve "Dial an Option" Electronic Attack capabilities that deny adversary situational awareness, disrupt command and control and develop targeting solutions to defeat weapons while protecting our against the same."

IO ROADMAP: GOALS

PSYOPS: Psychological Warfare

"Over the last decade, numerous studies have documented the deterioration of the PSYOP capabilities and recommended remedial action. Although not officially categorized as such, PSYOP has long been recognized as a low-density, high-demand asset, which is particularly valued in the war on terrorism.

...

"Desired outcome: A PSYOP force ready to conduct sophisticated target-audience analysis and modify behavior with multi-media PSYOP campaigns featuring commercial-quality products that can be rapidly disseminated through the Combatant Commanders area of operations."

PSYOPS: Details

9. (U) Increase Psychological Operations Capabilities.

(S) Over the last decade, numerous studies have documented the deterioration of PSYOP capabilities and have recommended remedial action. Well-documented PSYOP limitations persist. These include: the [REDACTED]

[REDACTED] insufficient numbers of experienced and well equipped PSYOP personnel; and a limited ability to disseminate products into denied areas. SOCOM and Army PSYOP force enhancement efforts are already underway per IO Roadmap recommendations in the last program review, and they should continue. In addition:

(U) SOCOM should create a Joint PSYOP Support Element to coordinate Combatant Command programs and products with the Joint Staff and OSD to provide rapidly produced, commercial-quality PSYOP product prototypes consistent with overall U.S Government themes and messages.

(U) SOCOM's ongoing PSYOP Advanced Concept Technology Demonstration and modernization efforts should permit the timely, long-range dissemination of products with various PSYOP delivery systems. This includes satellite, radio and television, cellular phones and other wireless devices, the Internet and upgrades to traditional delivery systems such as leaflets and loudspeakers that are highly responsive to maneuver commanders.

PSYOPS: Details

- ~~(S)~~ Coordinating information activities. Major DoD “information activities” include public affairs, military support to public diplomacy and PSYOP. The State Department maintains the lead for public diplomacy, the [REDACTED] and the International Broadcasting Board of Governors maintains the lead for broadcasting USG messages overseas, often with DoD in a supporting role. DoD has consistently maintained that the information activities of all these agencies must be integrated and coordinated to ensure the promulgation of consistent themes and messages.
 - (U) Historically PSYOP is the IO area considered most in need of coordination and deconfliction with public affairs and public diplomacy. In particular, attention is typically paid to the need to carefully segregate PSYOP from public affairs for fear that PSYOP tactics and techniques would undermine the credibility of public affairs efforts.
 - (U) Department of State practitioners of public diplomacy have historically expressed similar reservations about PSYOP.

PSYOPS: Details

- ~~(S)~~ Coordinating information activities. Major DoD “information activities” include public affairs, military support to public diplomacy and PSYOP. The State Department maintains the lead for public diplomacy, the [REDACTED] and the International Broadcasting Board of Governors maintains the lead for broadcasting USG messages overseas, often with DoD in a supporting role. DoD has consistently maintained that the information activities of all these agencies must be integrated and coordinated to ensure the promulgation of consistent themes and messages.
 - (U) Historically PSYOP is the IO area considered most in need of coordination and deconfliction with public affairs and public diplomacy. In particular, attention is typically paid to the need to carefully segregate PSYOP from public affairs for fear that PSYOP tactics and techniques would undermine the credibility of public affairs efforts.
 - (U) Department of State practitioners of public diplomacy have historically expressed similar reservations about PSYOP.

PSYOPS: Details

- (U) PSYOP equipment capabilities require 21st Century technology. This modernization would permit the long-range dissemination of PSYOP messages via new information venues such as satellites, the Internet, personal digital assistants and cell phones:
 - (U) PSYOP ACTD. Commencing in FY04, SOCOM initiates an Advanced Concept Technology Demonstration (ACTD) to address dissemination of PSYOP products into denied areas. The ACTD should examine a range of technologies including a network of unmanned aerial vehicles and miniaturized, scatterable public address systems for satellite rebroadcast in denied areas. It should also consider various message delivery systems, to include satellite radio and television, cellular phones and other wireless devices and the Internet.
 - (~~FOUO~~) PSYOP recapitalization. PDM-1 provided funding across the FYDP to modernize the family of loudspeakers and acquire and improve leaflet delivery systems. This includes wind-supported air delivery systems and precision guided canister bombs. Loudspeakers will incorporate technologies that improve range,

PSYOPS: Details

- ~~(S)~~ The study also noted that PSYOP capabilities had not kept up with requirements, but did not endorse assigning the PSYOP mission to STRATCOM. The study recommended SOCOM retain the PSYOP mission, but STRATCOM should coordinate with SOCOM to ensure full integration of PSYOP as a core capability of IO.

(U) Recommendation: Create a Joint PSYOP Support Element (#48).

- ~~(S)~~ DPG 04 directed the creation of a “strategic” PSYOP unit. The title of this unit was changed to reflect IO Roadmap recommendations on the proper relationship of PSYOP to public diplomacy and public affairs (see previous section on this topic). However, the intent remains the same, which is that the Joint PSYOP Support Element should:

PSYOPS: Details

(U) Recommendation: Support active public affairs programs that influence foreign audiences (#8).

- ~~(FOUO)~~ Clear boundaries for PSYOP should be complemented by a more proactive public affairs effort that expands to include a broader set of select foreign media and audiences. PDM-1 provided \$161M to ASD(PA) over the Future Years Defense Plan (FYDP) to implement this intent. These funds will enable ASD(PA) to:
 - (U) Develop a global web site supporting U.S. strategic communications objectives. Content should be primarily from third parties with greater credibility to foreign audiences than U.S. officials.
 - (U) Identify and disseminate the views of third party advocates that support U.S. positions. These sources may not articulate the U.S. position the way that the USG would, but they may nonetheless have a positive influence.

PSYOPS: Details

- (U) Impact of the global village. The increasing ability of people in most parts of the globe to access international information sources makes targeting particular audiences more difficult. Today the distinction between foreign and domestic audiences becomes more a question of USG intent rather than information dissemination practices:
 - (U) PSYOP is restricted by both DoD policy and executive order from targeting American audiences, our military personnel and news agencies or outlets.
 - (U) However, information intended for foreign audiences, including public diplomacy and PSYOP, increasingly is consumed by our domestic audience and vice-versa.
 - (U) PSYOP messages disseminated to any audience except individual decision-makers (and perhaps even then) will often be replayed by the news media for much larger audiences, including the American public.

IO ROADMAP: GOALS

OPSEC: Operational Security

"Desired Outcome; All plans are built, and operations executed, with priority attention to operations security."

More Red Teaming

IO ROADMAP: GOALS

MILDEC: Military Deception

"The value of military deception, like OPSEC, is intuitive."

Standard case: WWII -- invasion at Normandy instead of falsely advertised Calais.

INTELLIGENCE COMMUNITY

- * Independent Agencies

- o Central Intelligence Agency (CIA)

- * United States Department of Defense

- o Secretary of Defense, through the Counterintelligence Field Activity (CIFA)

- o Air Force Intelligence, Surveillance and Reconnaissance Agency (AF ISR)AIA

- o Army Intelligence

- o Defense Intelligence Agency (DIA)

- o Marine Corps Intelligence Activity

- o National Geospatial-Intelligence Agency (NGA)

- o National Reconnaissance Office (NRO)

- o National Security Agency (NSA)

- o Office of Naval Intelligence (ONI)

- * United States Department of Energy

- o Office of Intelligence

- * United States Department of Homeland Security

- o Coast Guard Intelligence

- o Office of Intelligence and Analysis

- * United States Department of Justice

- o Federal Bureau of Investigation (FBI)

- o Drug Enforcement Administration(DEA)

- * United States Department of State

- o Bureau of Intelligence and Research (INR)

- * United States Department of the Treasury

- o Office of Intelligence and Analysis

INTELLIGENCE COMMUNITY

HOW to organize the collection and sharing of information at a national level has, since its initial creation in 1947 (National Security Act), consistently been a subject of debate.

Congressional Oversight Committees have repeatedly sought and suggested a more integrated approach.

DoD fights to retain control and retains the vast majority of resources allocated to INFORMATION GATHERING which determines HOW the U.S. collaborates with other nations.

Intelligence Reform and Terrorism Prevention Act 2004

"must be seen as the start of Community reform in the 21st Century, not the endgame." (Gutjahr, p185)

-redefines "National Intelligence" (WMD as separate, specific, category of information) -- any information gathered that pertains to more than one organization and relates to U.S. Interests.

-creation of Director of National Intelligence (role formerly held by the Director of Central Intelligence) "full range of management, budgetary and personnel responsibilities needed to make the entire U.S. intelligence Community operate as a coherent whole."

-National Counterterrorism Center, National Counterproliferation Center, with possibility for more

Problems (according to Gutjahr):

-An Oversight: no new Congressional OVERSIGHT committees (also failed to streamline oversight)

-CIA and DoD still use incompatible information systems (CIASource vs. SIPRNet)

IC and IT

Notes From INTELLIGENCE ARCHIPELAGO by Melanie M.H Gutjahr

-Gutjahr: We require "a more agile, streamlined, fluid, cooperative and collaborative Inteligence Commmunity"

quoting John F. Lehman, 9/11 commissioner and former sec of navy:
"There are no protocols for the Intelligence Community for sharing. This is an IT problem. It's a deep, embedded, funcitonal problem throughout the Community for common protocols for information."

-Gutjahr: "The Community must now endeavor to collect against loosely affiliated, networked adversaries using commercial off-the-shelf communciations equipment and encryption devices."

-CIA uses CIASource. DoD uses SIPRNet. These are NOT cross compatible . . .

Term: HORIZONTAL Integration (AGILE / EXTREME Programming)

Major Conceptual Stumbling Blocks / Disagreements

- Acceptance of PSYOPS and IO as Overarching
All aspects of Logistics
- Understanding of "operations" as opposed to
"warfare" to allow for "friendly" conquest.

Historical Precedent

The origin of INFORMATION THEORY coincided with the origin of the CIA and NSA:

Claude Shannon: 1948 "A Mathematical Theory of Communication"

(How to encode messages and prevent information loss/uncertainty)

The CIA and NSA were created one year earlier, in 1947 (National Security Act)

Historical Precedent

Even before the CIA there was PSYOPS:

Alfred H. Paddock, Jr., "U.S Army Special Warfare: It's Origins" National Defense University Press, 1982:

On the man behind the WWII Office of Strategic Services (precursor to the CIA) -> ("WILD" Bill Donovan)

"Donovan's concept of psychological warfare was all-encompassing. The first stage would be 'intelligence penetration,' with the results processed by R&A [Research and Analysis], available for strategic planning and propaganda. Donovan called propaganda the 'arrow of initial penetration' and believed that it would be the first phase in operations against an enemy. The next phase would be special operations, in the form of sabotage and subversion, followed by commando-like raids, guerilla actions, and behind-the-lines resistance movements. All of this represented the softening-up process, prior to invasion by friendly armed forces. Donovans' visionary dream was to unify these functions in support of conventional operations, thereby forging 'a new instrument of war.'

Theoretical Goal of IO

From Libicki:

Quoting Ryan Henry and C. Edward Peartree "Military Theory and Information Warfare" Parameters, 1998:

"The more radical of the theorists predict that information warfare will not only provide dominant awareness of the battlespace; it will also allow us to manipulate, exploit, or disable enemy information systems electronically. The intent here evidently is to knock an enemy senseless - literally - and leave him at the mercy not only of conventional kinetic attack, but of psychological operations aimed at controlling his perceptions and decision-making abilities. Public opinion is to be shaped, leaders will be cut off from citizens, and the mind of the enemy will be directly penetrated and his strategy defeated. In the ideal case, all this will occur bloodlessly, fulfilling Sun Tzu's goal of victory without battle. At least that's the theory."(p38)

PSYOPS and IO

PSYOPS and IO are very closely related (not just one element . . .)

Lessons can be learned from the HISTORICAL BACKGROUND of Psychological Operations as it resonates with the current "Roadmap"

PSYOPS is another abstract instrument of war that had a major organizational re-evaluation begun in the 1980's . . .

Psyops: Considered by some to be the most effective non-lethal weapon at the disposal of SOCOM [special operations command]

Paddock in the 80's: "There is no US national-level organization for PSYOP" we need to treat it as a "weapons system" not as an "afterthought"

What is PSYOP?

Vagueness of Definition due to Breadth of Application

Lord: "a psychological-political component is inherent in every use of the diplomatic, economic, and military instruments of national power"

Richard Stilwell: "the nonintrinsic instruments of national power"

Alfred H Paddock Jr: "unconventional warfare"

What is PSYOP?

Paddock Elaborates (in the 80's):

"may be defined broadly as the planned use of communications to influence human attitudes and behavior. It consists of political, military, and ideological actions conducted to create in target groups behavior, emotions, and attitudes that support the attainment of national objectives. If used properly, PSYOP will normally precede, accompany, and follow all applications of force. This will be carried out under the broader umbrella of US national policy, and the military component of the overall psychological operations effort should be coordinated fully and carefully with other agencies of government."

What is PSYOP?

Barry Zorthian: "We obviously have a semantic problem that's never been solved. We're not always in agreement on the meaning terms such as psywar, communications, psychological operations, media relations, political operations. They cover a vast amount of ground. If we put aside combat psychological operations and look at the rest of it as the political dimension - the communications dimension - of a national effort, whether in a context of conventional or low-intensity combat or even in 'violent peacetime,' then perhaps we can all get together and be talking about the same thing." (PWPO p73)

What is PSYOP?

Barry Zorthian: "You cannot compartmentalize communication. Communication with the media has to be consistent with communication to the enemy, to third parties, to the rest of the world. PSYOP and communication with the media are part of the same whole." p74

Codevilla: "our policymakers have not been competent at making foreign policy and military strategy."

Abram Shulsky : "One can't have, as Dr. Codevilla says, a two-track policy, one track secret and one public, without there being a real strategy somewhere in the background relating the two." (PWPO p106)

More Definitions

Political Warfare:

Angelo M. Codevilla: "the forceful political expression of policy." PWSOp77

"the marshaling of human support, or opposition, in order to achieve victory in war or in unbloody conflicts as serious as war."

More Definitions

Codevilla on Gray Propaganda:

Radio Free Europe, Voice of America, etc. with gov funds "on behalf of something bigger than the US government" -- "Outside of a responsible policy process"

and Black Propaganda:

Church and Pike Committees of 1970's discovered many instances.

e.g. spread info about sexual misdeeds of Indonesia's leftist dictator, SUKARNO, then spreading them about the world through channels **not attributable to US.**

IO Foretold in PSYOP debate

An OBSERVATION from Codevilla:

"Soon it will be possible to beam, not broadcast, radio and television signals anywhere in the world. In other words, it will be possible for one people to take part in another's domestic political discussion. But what messages do we wish to send? And to what end?"p99

IO Foretold in PSYOP debate

An OBSERVATION from FRANK BARNETT
"12 Steps to Reviving American Psyop" (in PWPO)

" Just as the hardware of missiles can be
modernized, so can the software of PSYWAR"
p216

IO Foretold in PSYOP debate

Robert Kingston:

"PSYOP could be the essence and the core of insurgency and couterinsurgency operations." p143

"PSYOP planning and operations should blanket all phases of political-military operations, starting with international tension and going through all pre-conflict, conflict, and post-conflict phases." "I don't believe we fully understand the potential for peacetime overt psychological operations."

PYSOPS Problems = IO Problems

The IMPORTANCE of PSYOPS has been REPEATEDLY LOST / Forgotten /
Misunderstood:

lord: "Precisely because the instruments of psychological-political conflict are not altogether disctinctive, this arena requires fully integrated planning and coordinated operations throughout virtually the entire national security bureacracy. This coordination has always proven difficult for the US government . . . " (p27)

-- lack of support in military and state dep't points to CIA -- but
unable to cooperate.

-- need collective goal of DISSEMINATION as well as of
COLLECTION

--in other words, we lack cohesive analysis of the MESSAGES we
send and cohesive analysis of the MESSAGES we receive.

"the very identification of PSYOP as a special forces mission has
tended to isolate it from normal military activies and bring under a
certain suspicion, which its "black" connotations have further
strengthened."p28

“WARFARE”

FINALLY:

Is it just "warfare?" == Lord: "Psychological-Political operations need not be directed only to adversaries; indeed, not only neutral but also allied and semi-allied nations potentially constitute highly important targets, since the weakening of US alliance structures is a key strategic objective of the political warfare activities of the Soviet Union. And, of course, psychological-political operations need not be undertaken only in a context of military conflict. On the other hand, to divorce psychological-political operations entirely from the arena of international conflict and national strategy - a natural tendency in the United States and other Western democracies, for cultural as well as bureaucratic reasons = runs the risk of cutting them adrift from any tangible national purpose and destroying their effectiveness." p17

Related to Libicki's notion of "FRIENDLY CONQUEST IN CYBERSPACE"

HACKER ARMIES

"South Korea's Defense Ministry claims North Korea may have trained as many as 600 computer hackers to launch cyber-attacks against the United States and South Korea. Although computers are a rarity and Internet access in North Korea is almost non-existent, the Defense Ministry maintains North Korea information warfare capabilities had reached the level of advanced countries." Gutjahr p106

How does one distinguish between random hackers and ones hired by a Nation?

The Threat of IT

Gutjahr: Quoting Aris A. Pappas senior community management staff officer:

"Technology is no longer a U.S. monopoly. We are now facing the same reality that confronted the Soviets: technology is, and has always been, ideologically neutral. It benefits anyone with access and means. This simple fact now represent an enormous challenge to US intelligence."

... Whereas satellite imagery and signal and comm intercepts provided the US an "information edge" it is no longer so.

Pappas and Simon: "The IC will encounter surprises from both the use of known technology in unexpected ways and the innovative application of a combination of new technologies."

Quoting Hayden before Joint Intelligence Community in 2004:

"The volume, variety and velocity of human communications make our mission more difficult each day. A SIGINT agency has to look like its target. We have to master whatever technology the target is using . . . We had acted successfully against a resource-poor, oligarchic, technologically inferior, and overly bureaucratic nation state. Now we had to keep pace with a global telecommunication revolution, probably the most dramatic revolution in human communications since Gutenberg's invention of movable type."

The Threat of IT

Gutjahr, quoting G. Tenet at Senate Armed Services Committee:

"America stood out as an object for admiration, envy, and blame. This created a kind of cultural asymmetry. To us, Afghanistan seemed very far away. To members of al-Qa'ida, America seemed very close. In a sense, they were more globalized than we were." (p109)

SECURITY and CONNECTIVITY

From Gutjahr:

Thomas P.M. Barnett:
Disconnectedness Defines Danger

- The CORE (Globalized World)
- The GAP (non-Globalized)
- Increase SECURITY by increasing
CONNECTIVITY

FRIENDLY CONQUEST

Martin Libicki:

"Lost in this clamor about the threat from hackers is another route to conquest in cyberspace, not through disruption and destruction but through seduction leading to asymmetric dependence. The seducer, for instance, could have an information system attractive enough to entice other individuals or institutions to interact with it by, for instance, exchanging information or being granted access."(p3)

Learning from Microsoft = Determine the
STANDARDS of information sharing . . .

FRIENDLY CONQUEST

Martin Libicki:

"Hostile conquest is more often expressed not as control but as denial - the demonstrated ability to take from the victim full use of its own infrastructure."(p125).

FRIENDLY CONQUEST

(see Joseph Nye on "SOFT POWER")

- voluntary transactions (at first)

- leads to unwarranted influence of conquerer's systems

- asymmetrical coalition (builder of system vs. user)

- information is special for coalition development:

 - it's cheap/free

 - a question of ACCESS THROUGH and OF cyberspace

 - web makes it easier, cost effective, offers a steady stream (like

Microsofts .Net initiative)

- using common solutions = seeing common problems

- i.e. why learn two ways of doing same thing?

FRIENDLY CONQUEST

DoD's GLOBAL INFORMATION GRID
could be used in this way by following the
Microsoft model of controlling information by
controlling the FORMAT of information --
building a DOMINANT system and spreading
COMPATIBILITY.

FRIENDLY CONQUEST

Geospatial Data's Potential for Friendly Conquest?

- To map something is, in a deep sense, to own it (Libicki, p170)
- A good BARGAINING chip
- Maps as whiteboards for collaboration.

FRIENDLY CONQUEST

That Joseph Nye Quote:

From Gutjahr (p125): Joseph S. Nye, Jr. Chairman of the National Intelligence Council, in 1995:

"Knowledge, more than ever before, is power. The one country that can best lead the information revolution will be more powerful than any other. For the foreseeable future, that country is the United States."

Information and Information Systems

Layers of Computer Information and Systems:

Physical (hardware, infrastructure, wires)

Syntactic (format, instruction, control -- the rules)

Semantic (human-understood info -- versions of reality, images, videos)

->*complexity helps blur the boundary between commands (syntactic) and info (semantic)

e.g.: system commands hidden in images . . .

Information Systems

Libicki:

"The advent of a true semantic layer is likely to create more avenues for friendly conquest. The influence accrues to whoever wins the right to define the words that refer to the real world - that is, what they encompass and exclude A developed pragmatic layer, should it occur, would offer even more impetus for friendly conquest by reinforcing the role of semantic exchange." (p255)

Misinformation and Disinformation

Libicki:

KINDS OF NOISE

Misinformation -> believing what is not true

Disinformation -> being unable to believe what is true (p50)

Notice this USER-based definition as opposed to the state department (where it is based on INTENT)

State Department definition:

<http://usinfo.state.gov/media/Archive/2005/Jan/26-288268.html>

based on INTENT

See -> IO_ROADMAP -> Targeting Audiences

Humans: A PRIORI logic (we find it hard to believe based on presupposition)

Computers: Once something is IN the system, it is LEGITIMATE (even if beyond reason)

NOISE

WHAT are basic methods of attack?

- Add NOISE to a signal:

- Extra Information to WASH OUT important info

Defense through Redundancy

- Trellis Encoding

- Hopfield Net (node based, like neurons)

- Fourier Transforms

Defense through Filtering

- Knowing how much noise is coming

- Knowing how much to let through

- (human filtering of tabloids, for instance)

NOISE TOLERANCE

CASTLES vs AGORAS

DEFENSE: Noise TOLERANCE (car manufacturing vs. wall street)

The case to OPEN up strongly protected networks like SIPRnet and NIPRnet (btw: the I-love-you virus got through to SIPRNet)

- Outsourced Experts
- Collaboration info sharing
- knowledge circulation
- multimedia, software, simulation

. . . all require interconnectedness

"Those who can keep their enemies in the castle own the agora"(P71)
-- "induce the adversary to close itself off" -- and thereby lose the advantage of a more open system.

How much noise can an information conduit withstand before it is totally destroyed (p56)

GETTING IN

- seduce a spy (KGB nuclear spies)
- remote maintenance port (air-duct)
- pre-built backdoors (the Swiss did it)
- wifi mining
- wiretapping

ONCE IN

SPYING (eavesdropping)
DENIAL OF SERVICE (flooding)
CORRUPTION (inserting anomalies)
DISTRACTION (false alarms)

PING ECHO FLOOD SAG

- how does enemy react to information injection?
(does it limit AGILITY or INTEGRATION?)
 - how intolerant of info overload?
-

- Collect Decision-Making Info
- Plant Surveillance
- Insert irrelevant info
- Measure response

NO FORCED ENTRY

rather, exploitation of vulnerabilities

- exception: flooding attacks (crowding ports)
- As such, IO is critically tied to DECEPTION
 - Seeks to cause MISCHIEF (Friendly Fire, Collateral Damage)
 - "The future of information systems security has far more to do with the future of information systems vulnerabilities than with information weapons."(p40)
 - "not a precision instrument . . . effects of attack are based on system's construction and its entry points."

PROBLEMS with IO

UNPREDICTABILITY:

“It is very difficult to prepare strategically -- unlike chess, Nth order decisions are made on an ever-changing board. IO addresses the very ability to make decisions.”

-To understand vulnerabilities of a system, "One would need to know how humans would react to failures in their machines = what trust would they put in them, what measures would they take in the fact of induced doubt, how redundant would machines be made, how quickly can they learn that something is wrong, and so on. There is almost no empirical data on act of information warfare in wartime, and only scattered information on broader systemic relationships between computer-based information and the decisions they inform."(p92)

-WHAT will be attacked is something we have overlooked -- a faulty detail. We simply don't know how the system will respond.

-System Architecture can change "in between moves"

PROBLEMS with IO Strategy

OTHER PROBLEMATIC PRACTICALITIES:

- "Reducing the control that an adversary possesses renders war-limitation, as opposed to warfighting, strategies HARDER, not easier, to carry out" (p97)
- Perversity is easy ("polluting an information source leads others to discard it and therefore alleviates . . . the opponents information glut" p122)
- "Frustrates normal command and control" -- leaks, keystroke oversight . . .
- collateral damage "the affected system may be controlling or influencing processes and services of which the attacker is unaware" (p99)
- "such uncertainty makes integration into combined arms a hairy bear of a problem" (p99)

Information Security Bullet Points

- easy to be misinformed about Information Systems
 - probing itself can:
alert owners, mask action, cause lack of confidence
in a system, reveal weakness of response
- different in war than in peace (level of security,
focus of operation)

IO COLLATERAL DAMAGE

"The more the world's economy becomes globalized, the harder it is to predict the ripples from any one act of mischief."(p259)

Terrorists and the Internet

Jihad 2.0 (by Nadya Labi) -- Terrorists Use of the Internet:
Recruiting, Distribution, Command / Control
the internet is "a vast recruiting ground - in effect, a new borderless
Afghanistan" (Libicki quoting Nadya Labi, Jihad 2.0)

Terrorist presence on internet has "assumed evanescent qualities . . . all
in all, what makes the Jihadist terrorists so difficult to confront in
cyberspace is that they have not attempted to conquer it in any way,
shape, or form. They defend nowhere, the better to appear
anywhere."(p262)

Terrorism and FRAUD (from Gutjahr, p105) quoting Ronald Noble
"Interpol believes there is a significant link between counterfeiting
and terrorism in locations where there are entrenched terrorist
groups."

Encryption as a Weapon

Encryption as a WEAPON- 1990s (from THE CODE BOOK, by Simon Singh)

1998 -- 33 nations sign the Wassenaar Arrangement limiting arms exports, which also covers powerful encryption technologies.

1993 Pat Zimmerman becomes subject of grand jury investigation

PGP (Pretty Good Privacy)
<http://www.pgpi.org/pgpi/>

IDEA, PGP (Pretty Good Privacy) fueled by Business interests,
International Law

Methods of Decryption

METHODS OF DECRYPTION:

Traffic Analysis (who is sending how much information to whom)

Trojan Horse (seems like a legit Encryption but not really . . . actually records key and sends it along to designer of the virus)

Tempest Attack -- detects electromagnetic signals emitted by electronics on a computer's display unit (prevented with shielding materials -- need a license in the US to buy the material)

Backdoor -- something which allows designers to decrypt user's messages

e.g. Crypto AG (Swiss Company) -- how US caught assassins of former prime minister

History of Encryption

History of ENCRYPTION

From THE CODE BOOK, by Simon Singh (Fermat's Enigma guy)

1960's ARPA -- DOD's Advanced Research Projects Agency -- "tried to find a way of connecting military computers across vast distances" p254 for "robustness" and backup plans.

1969 - ARPANet (in 1982 it became the Internet)

1973 America's National Bureau of Standards formally requests proposals for a standard encryption system that would allow business to speak secretly unto business p248

LUCIFER (IBM) BY HORST FEISTEL (NSA had wanted "monopoly on cryptographic research")

GREATEST problem in cryptography was KEY DISTRIBUTION
US gov keys managed by COMSEC (communications security)

History of Encryption

1975: Whitfield Diffie, Martin Hellman, Ralph Merkle conceptualizes Asymmetrical cyphers

ONE WAY FUNCTION ($Y^x \pmod{P}$)

PUBLIC KEY CRYPTOGRAPHY or NONSECRET ENCRYPTION

RSA (Rivest, Shamir, Adleman) -- ASYMMETRICAL cyphers ("a one-way function that can be reversed only if the receiver has some special information" p273)

- process of descrambling is not just opposite of scrambling
- even the encrypting party cannot decrypt the message . . .
- "padlock" analogy (anyone can lock the message, but only one can unlock)

Large Prime Numbers multiplied to N (10 to the 308)

Will someone find a quick way to factor N to two PRIME numbers? Not yet.

*Actually invented at Government Communications HQ in Britain by James Ellis . . .

History of Encryption

Singh's examples of ASYMMETRICAL cipher (quoted verbatim):

1- Alice must create a public key, which she would then publish so that Bob (and everybody else) can use it to encrypt messages to her. Because the public key is a one-way function, it must be virtually impossible for anybody to reverse it and decrypt Alice's messages.

2- However, Alice needs to decrypt the messages being sent to her. She must therefore have a private key, some special piece of information, which allows her to reverse the effect of the public key. Therefore, Alice (and Alice alone) has the power to decrypt any messages sent to her. (p274)

Conclusion

Conclusion:

If anyone asks, I am not really studying this phenomenon.