AIR WAR COLLEGE

AIR UNIVERSITY

FUTURE OPERATING CONCEPT – JOINT COMPUTER NETWORK OPERATIONS

by

Robert Burris, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

17 February 2010

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government and is not to be reproduced or published without the permission of the Air War College Studies Directorate.

Table of Contents

Page

Illustrations

Page

General

> The *Capstone Concept for Joint Operations* describes how the joint force will operate in an uncertain, complex, and changing future characterized by persistent conflict…Military success in the future rarely will be the product of radically new ideas, but instead will typically result from adapting these enduring truths to new requirements, conditions and capabilities.
>
> M.G. Mullen, Admiral, CJCS

The conduct of operations in Cyberspace[1] represents the adaptation of enduring truths to emerging threats[2] prescribed by CJCS and relies on a strategy of achieving information superiority[3] in the battlespace. Information Operations (Info-Ops) provides the framework for success by translating superior decision making into a competitive advantage[4] for the Joint Force Commander (JFC). The key principles of joint information operations are the synergy of three categories of Info-Ops capabilities; core, supported, and related "to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own"[5].

The core Info-Ops capabilities available are electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operational security (OPSEC). Each core capability is independently focused on achieving critical operational effects or preventing the adversary from accomplishing its desired effects by integrating with supported and related capabilities[6].

The supporting Info-Ops capabilities are counter intelligence (CI), physical attack (kinetic), physical security, information assurance (IA), and combat camera (COMCAM). Each capability seeks to provide friendly forces the information advantage through active defense of decision makers from attacks. Further, they target effects at adversary decision making through active influence and degradation campaigns against their perceptions and behavior in the battlespace[7].

The related Info-Ops capabilities are public affairs (PA), civil-military operations (CMO), and defense support to public diplomacy. Each related capability offers flexible options for influencing adversary perceptions and decision-making in peacetime, crisis build-up, and during hostilities. They demonstrate resolve and communicate national interests toward tangible (physical, psychological) effects supporting objectives and influence of foreign perceptions[8].

To be effective, all three categories of Info-Ops capabilities must be part of forces and capabilities being prepared, planned, and executed synergistically toward effects on adversary decision makers, fielded forces, information and systems, and external audiences[9]. The active defense of friendly capabilities requires reciprocal preparation, planning, and execution within the theater, and other impacted audiences consistent with JFC's intent. These comprise the dimensions of the joint information environment when applying Info-Ops forces[10].

The joint information environment aggregates decision makers (civil and military), organizations (national, international), and the resources (materials, systems) that collect, process or act on information across all domains[11]. In this environment, the O-O-D-A[12] loop frames the interaction between humans and automated systems for decision making[13]. This interaction occurs across the full spectrum of conflict and is relevant in all instruments of power as categorized in one of three interrelated dimensions; physical, informational, and cognitive[14].

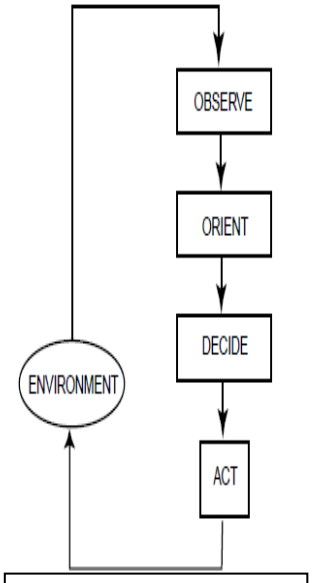

Figure 1

The physical dimension, where physical platforms and communications networks traverse wired and wireless infrastructures with supporting technologies to connect individuals, groups, and organizations for operational C2 purposes[15]. The informational dimension is where content and flow of C2 information is collected, processed, stored, disseminated, and displayed. The residence of the application of military force datasets and commander's intent impact protection required of this dimension. The cognitive dimension is where humans think, perceive, visualize, decide, and includes decision makers and target audience.

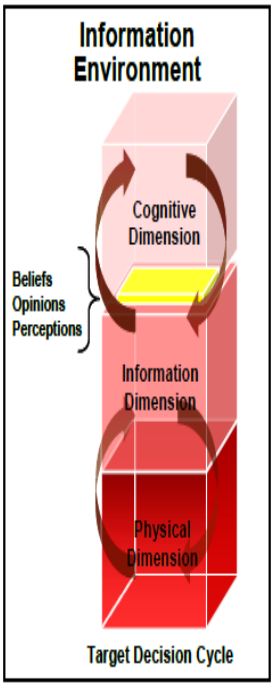

Figure 2

The factors of leadership, morale, unit cohesion, and situational awareness coupled with public opinion, public information, media perceptions and rumors are influenced in this dimension therefore battles and campaigns may be won or lost here making this the most important dimension[16]. The technological advances that afforded the exponential surge (sources, outlets, speed) of capabilities in both physical and informational dimensions have not translated to the cognitive dimension where content and context shape the qualitative value of information relative to its purpose[17]. The success of Info-Ops ultimately is determined by the ability to improve and maintain quality of friendly information while degrading the adversaries such that friendly forces are able to exploit the difference in speeds of the relative O-O-D-A loops.

The JFC's ability to apply the principles of Info-Ops, specifically CNO, to deliberately affect or defend the joint information environment relative to decision making is biased by five key assumptions[18]. First, quality of information of value to decision makers is subject to influence

from geography, language, culture, religion, organization, experience, or personality. Second, decisions are made based on information available at that time. Third, the relevant aspects of the information environment and processes used to make decisions are understandable. Fourth, it is possible to affect the information environment of decision makers through psychological, electronic, or physical means. Finally, the effectiveness of actions relative to an objective is measurable[19].

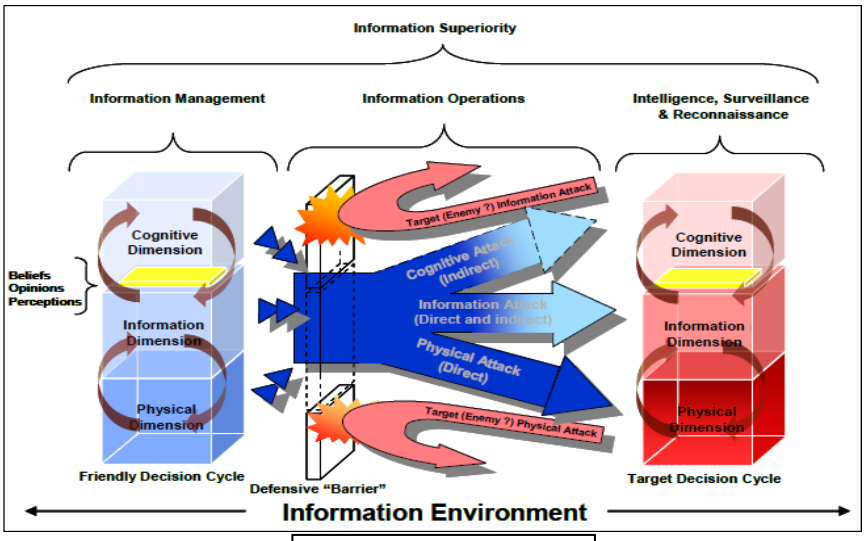

Figure 3

The constraint in "targeting" with these principles against the critical psychological, electrical, and physical elements in the information environment is consistency with national security policy and strategic objectives. In sum, CNO will target decision makers by affecting the human thinking processes, knowledge and understanding of the situation in three distinct ways. First, by taking those actions that add, modify, or remove information. Second, by taking actions that affects the collection, communication, processes, and storage of information. Third, to influence the way information is received, processed, interpreted, and used by decision makers[20]. These capabilities have simultaneous application in offensive and defensive situations

to destroy, disrupt, degrade, deny, deceive, exploit, influence, protect, detect, restore, and respond[21] when fully integrated in mission planning and execution.

The adaptation of the principles of Info-Ops to joint warfighting in cyberspace represents the launching point for this future operating concept. The acceptance of the unifying application of Info-Ops core, supporting, and related capabilities in concert with doctrinal prescriptions explores joint operations in the cyber domain with focus on computer network operations.

The thesis, then, is that the synergistic effect of jointly integrated computer network operations (CNO) provides the JFC with the opportunity to exploit vulnerabilities across the full spectrum of conflict through mission essential functions uniquely enabled by the cyber domain. The globally inter-connected fusion of terrestrial, airborne, and space based capabilities[22] spawned CNO resulting from increasing use of communications and computers networked with information technology based infrastructure[23] by civil-military institutions. The NMS-CO[24] codified this adaptation of warfare and the need for agility "within and through" cyberspace as a key tenant of "net-centric warfare"[25]. Cyberspace[26] is characterized by "use of electronics and electromagnetic spectrum" as a means to store, modify, and exchange information acting as the conduit between the physical and cognitive dimensions of the information environment. In concert primarily with EW, CNO can be employed to "attack, deceive, degrade, disrupt, deny, exploit, and defend" operations in the cyber domain.

To comprehend this complex but evolving capability, CNO is segmented into three components; computer network attack (CNA), computer network defense (CND), and computer network exploitation (CNE)[27]. CNA's ability to "disrupt, deny, degrade, or destroy the information in computers and their associated networks or the computers and networks

themselves" is the means of attack through cyberspace[28] or the cyber domain. CND's focus to "protect, monitor, analyze, detect, and respond to unauthorized activity, internal and external, on DoD information systems and networks" are applied to defend[29] enabled by OPSEC. CNE "gathers data from target or adversary information systems or networks" in concert with EW for intelligence exploitation converges with the electromagnetic spectrum[30].

Figure 4

The significance of CNO gains prominence as a warfighting capability as the range of computers and associated networks operating in cyber domain broadens. The emerging 21st century warfare[31] environment enables unsophisticated military and terrorist groups to successfully C2 against superior conventional forces through proliferation of technology. The mission essential functions of CNO to attack, defend, and exploit vulnerabilities from increased reliance on cyberspace while the identification and protection from the same to friendly information systems requires power projection from an adaptable cyber force[32].

Purpose

America is under widespread attack in cyberspace. Unlike in the air, land, and sea domains, we lack dominance in cyberspace and could grow increasingly vulnerable if we do not fundamentally change how we view this battle space.

Gen James E. Cartwright, USMC
Former Commander, US Strategic Command

This concept will guide the preparation, planning, and execution of joint Info-Ops[33] with the goal of information superiority. The aggregation of decision maker, data, and systems that collect, process, disseminate, or act exists in a new medium, a virtual reality of the battlespace enabled by Web 2.0[34]. The concept of "net-centric" warfare envisioned linkage between "sensor and shooter" links to expedite O-O-D-A loop[35] reaction time, this "new media" fuses technological and social exchanges in the battlespace.

Figure 5

The transformation into a socio-technological platform changed C2 architecture to a 3D framework of asymmetric collaboration in the "multiverse"[36]. The ability to preview adversary and friendly forces "…includes aspects of the physical world, objects, actors, interfaces, and networks that construct and interact with virtual environment[37]"avoids the constraints of "time, space, and distance" applied to conventional platforms with the persistence uniquely attributed to operating virtually. This shift to a multi-dimensional framework is much more than a technological renaissance. The significance of increased situational awareness permeated strategic thinking since Clausewitz's era; the enabling ability of distributed decision making with cross-domain freedom of action creates effects at operational speed with "new battle-changing opportunities for engagement"[38].

Time Horizon, Assumptions, and Risks

This future operating concept outlines CNO as an integrated Info-Ops capability with a time horizon represented in the near term (3 – 5 years) and long term (5 – 10 years). The key assumptions complement the other instruments of power as prescribed by national security strategy and rely on the unified employment of the other core, supporting, and related Info-Ops capabilities to meet JFC objectives. The risks associated from operational, legal, and technical aspects are consistent with full spectrum engagement of US and coalition operations.

Description of the Military Problem

> *Know the enemy and know yourself; in a hundred battles you will never be in peril. When you are ignorant of the enemy, but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and yourself, you are certain in every battle to be in peril.*
>
> Sun Tzu

The objective "to gain and maintain information superiority"[39] recognizes information as a strategic asset aggregated in cyberspace with accessible dimensions as the future challenge. Threats and opportunities span "geopolitical boundaries integrated into critical infrastructures of commerce, governance, and national security[40]" and range from regular to irregular conflict, humanitarian relief and reconstruction all requiring "sustained engagement in the global commons"[41]. Whether state sponsored or ideological in nature, threats to prosperity and security are enabled through cyberspace toward the US strategic advantage and against the sources of strength and national sovereignty. These threats may take the form of explosive vests in a central market, a beheading captured in streaming video, precise cyber/space/missile strikes, or

weapons of mass destruction "characterized by interdependence, uncertainty, complexity, and continual change "[42] propagated through the cyber domain.

The joint force needs agility in this "new reality" of conflict with geopolitical and socioeconomic implications brought about by adaptive human's intent on disrupting political stability and exploiting the free access to the "global commons"[43]. The ability to forecast operations rely on historical trends, context, and the perceived implications on future political tensions while "balance of power" and ideological (secular, religious) divides remain polarized. Technological advancements amplify "fog and friction" in conflict to "distort, cloak, and twist the course of events" to an infinite number of incidents that overload information stores to create misperceptions and faulty assumptions affecting human perceptions[44].

The technological changes that shaped an exponential linkage between energy, financial, political, strategic, and operational domains converged with capabilities used by the joint force generating susceptibility to the perceptions and will of decision makers and populations[45]. The NMS-CO[46] submits "cyberspace superiority" to counter this by integrating "military, intelligence, and business operations to defend critical infrastructure, the homeland, or other vital interests" despite the obstacles.

The first obstacle for CNO to overcome is establishing freedom of movement in the cyber domain. The situational awareness required is plagued by a constant state of change both in the variants of rate and depth of change within heterogeneous networks. The transitory nature of potential targets affects offensive and defensive countermeasures as new defenses are established and targets diminish from the battlespace[47]. Second, defensive countermeasures are challenged by myriad of dichotomies based on distributed operations collaborating across "global

commons" from a hybrid of network connections of commercial, government, agencies with separate and independent security protocols[48].

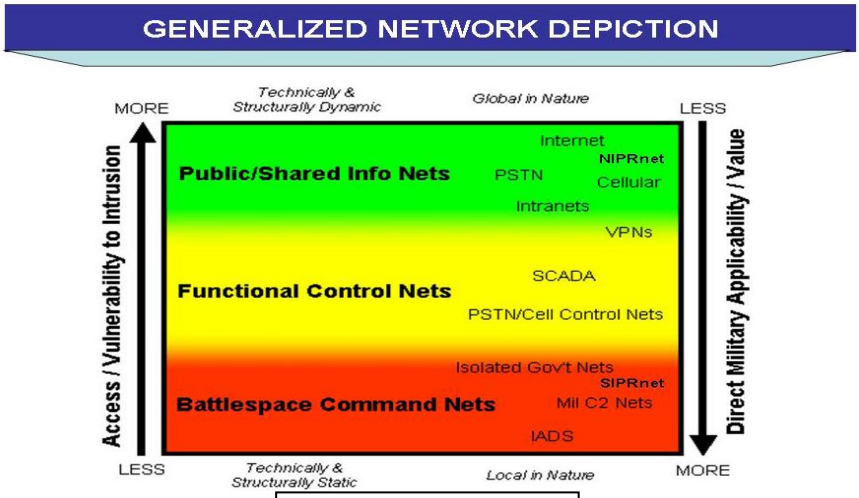

Figure 6

Third, offensive measures require access to networks, including isolated and secure nodes/segments. These "open networks" are fraught with legal, intelligence, and potential IP collateral damage[49] making conventional targeting the path of least resistance. This further complicates non-kinetic options where geo-political interests require multilateral authorization. Finally, the ability to execute within a compressed decision cycle represented in microseconds vice hours/days. Fleeting, time-sensitive targets directly affect the IPOE and dictates pre-planned/pre-coordinated authority commensurate with the "global commons".

Synopsis

This concept recognizes the cyber domain as a merger of interdependent information technologies, infrastructures, and networks whose proliferation and exponential increase of reliance for military, intelligence, and business enterprise cross geopolitical boundaries. CNO in these "global commons" is framed around three major components. First, the cornerstone of

effective CNO is the assurance that operations are unimpeded by friendly or adversary activities--"freedom of movement"[50]. This component is based on two key enablers; situational awareness and "active defense"[51]. Situational awareness includes friendly, adversary, and "witting/unwitting 3rd party"[52]nations that are participating actors coupled with active network defense posture of all relevant nodes, segments applicable as "cross-domain"[53] entries to the battlespace. Second, to sustain maneuver, offensive and defensive "counter-cyber operations" integrates the planning, and employment of capabilities through effective tools, techniques, and procedures to plan, administer, and monitor ongoing operations. These "counter-cyber" methods afford the JFC with the ability to respond to threats, outages, or other impacts to the battlespace while maintaining their availability, integrity, confidentiality, and non-repudiation[54]. Finally, the characteristics of the cyber domain reflect "vastness, complexity, volatility, and rapid evolution"[55]with compressed decision cycle in derivatives of seconds placing a premium on sustained IPOE.

This strategic environment encompasses critical infrastructure, the conduct of commerce, governance, and national security thus establishes the need for a cohesive set of imperatives for successful operations. The NMS-CO outlines ten such imperatives[56] to apply and integrate into military functions. The most important for CNO to consider are: that offensive and defensive operations are strongest when mutually supporting, thorough integration (organizations, capabilities, technologies, etc.) minimizes operational seams and expands resources, collaborative information sharing must occur rapidly, securely, and systematically between stakeholders, the ability to operate through degradation focused on the mission essential functions, capability to C2 across the full spectrum of conflict synchronized on awareness of generating effects, and to establish and enforce configuration management standards.

Application and Integration of Military Functions

America retains both the powers of "intimidation and inspiration." We will continue to play a leading role in protecting the values that grew out of the wisdom and vision of our nation's original architects. We must be under no illusions about the threats to our shared values, but we must also recognize the military as only one, albeit critical aspect of America's strength. This strength must specifically recognize the need to adapt to the security challenges we face, whether or not the enemy chooses to fight us in the manner that we would prefer. America's military cannot be dominant yet irrelevant to our policy makers' requirements.

To gain and maintain superiority in this environment, the ability to integrate attack, defend, and exploit[57] missions and operations are a critical capability for the JFC. To achieve and maintain superiority in cyberspace begins with assurance of friendly use of cyberspace while denying the same to an adversary—"freedom of movement". The attainment and sustainment of this ability to maneuver must be integrated across all domains and synchronized with the other core Info-Ops capabilities specifically with IPOE oriented toward exploitation activities. The advantages of situational awareness irrespective of constraints of time and space provide broad maneuver ability to friendly forces while constraining adversary access and exposing their operations to precision strikes on "key nodes and forces" in cyberspace[58]. Any success in achieving superiority in cyberspace is organized around three guiding principles; ensure availability of the domain to cyber forces, establish C2 of the domain through cyber forces, and enable operations for military, intelligence, business across air, land, sea, space, and cyber domain. These parameters transcend the constraints of time and space enabling degrees of persistence unparalleled with traditional platforms operating in the conventional domains.

To ensure the cyberspace domain is available to conduct operations, CNO will administer, operate, and monitor all networks contributing to operations with the ability to respond to threats and events that could affect freedom of movement. The situational awareness derived from the fusion of terrestrial, airborne, space based platforms, and networks prepare the

battlespace and leverage the inherent defensive countermeasures on their initialization. To C2 this aggregation of networks in the operational environment requires active defensive and offensive "stratagems" (see appendix I) to maintain freedom of movement.

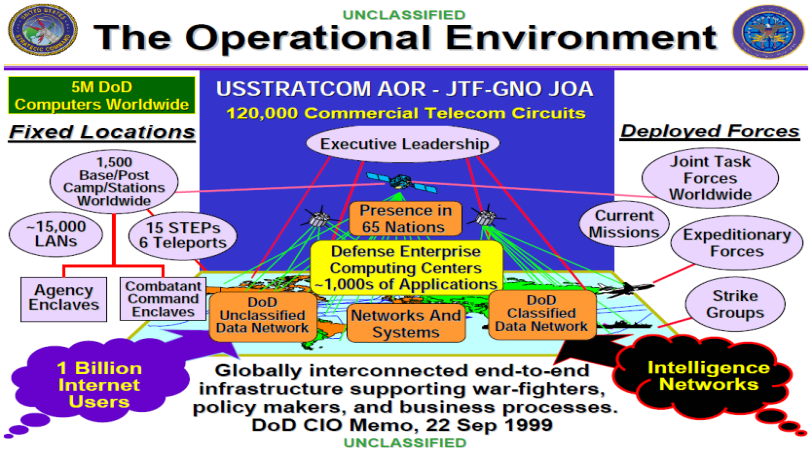

Figure 7

Defensive operations reinforce the freedom for cyber forces to maneuver through active defense of the electromagnetic spectrum, networks, and associated critical supporting infrastructure. This includes physical force protection and computer network defense focused on preventative measures for access control, destruction, and exploitation intentions. These defensive measures "focus on creating and maintaining cyberspace, while defensive operations seek to protect it—physically, logically, and electronically—from specific threats" and may overlap with other measures such as electronic protection, OPSEC, and the ability to "attack" adversary systems for strictly defensive purposes. Offensive operations maintain superiority through the capability of targeting any portion of the information environment ranging from particular physical nodes and links to the actual data resident to deny, degrade, disrupt, destroy, alter, or otherwise adversely affect an adversary's ability to use cyberspace.

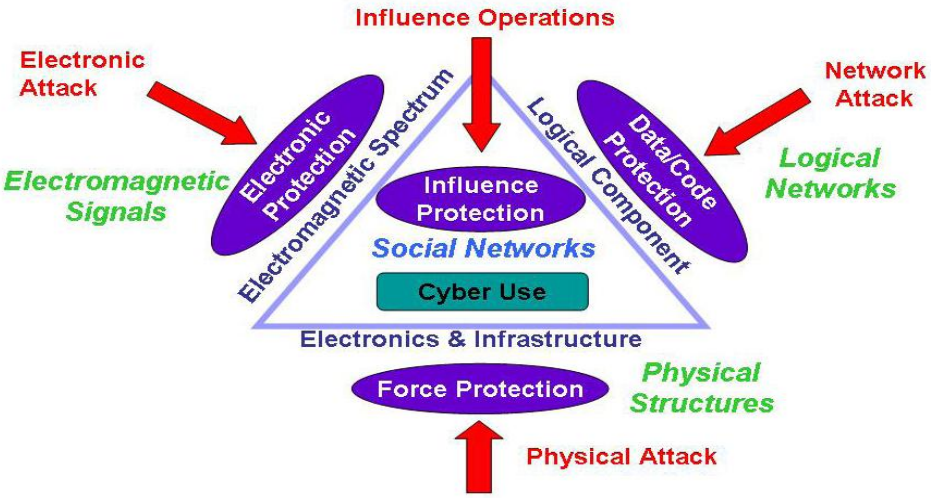

Figure 8

Specifically, CNO includes the capability to: (1) attack and disrupt enemy computer networks; (2) defend our own military information systems; and (3) exploit enemy computer networks through intelligence collection through use of computer code and applications to destroy networks and penetrate enemy computers to steal or manipulate data, and take down enemy C2 systems as in appendix III. The diverse means of communicating and differing levels of interconnectivity among nodal segments, traverse geo-political boundaries with multiple points for isolation requires three distinct modules that contribute to the joint force's ability of maneuver; CNA, CND, and CNE[59].

CNA is intended to disrupt or destroy information resident in computers and computer networks. As a distinguishing feature, CNA normally relies on a data stream used as a weapon to execute an attack. For example, sending a digital signal through a network to instruct a controller to shut off the power flow is CNA, while sending a high voltage surge through the electrical power cable to short out the power supply is considered EW. (Note: a digital stream of code or pulse of EM energy can create false images in adversary computers)[59].

CND is defensive measures to protect information, computers, and networks from disruption or destruction. CND includes actions taken to monitor, detect, and respond to unauthorized computer activity. Responses to cyber attack against U.S. forces may include use of passive information assurance tools, such as firewalls or data encryption, or may include more intrusive actions, such as monitoring adversary computers to determine their capabilities before they can attempt an attack. Legal determination of what level of intrusion or data manipulation constitutes an attack is necessary to categorize for intelligence collection operation, and actions appropriate in self-defense[59].

CNE is not yet clearly defined within DOD but before a crisis develops it seeks to prepare the battlespace through IPOE and extensive planning activities. This involves intelligence collection that is usually performed through network tools (see appendix II) that penetrate adversary systems to gain information about system vulnerabilities, or to make unauthorized copies of important files. The tools are similar to those used for computer attack, but configured for intelligence collection rather than system disruption[59].

In each case, these modules require a template for the use of "cyberwarfare" platforms through maneuvers, or "cybercraft", to achieve desired effects. The tools/tactics, techniques, and procedures (TTPs) in appendix II represent as series of mission essential tasks considered necessary capabilities to be employed across the range of operations.

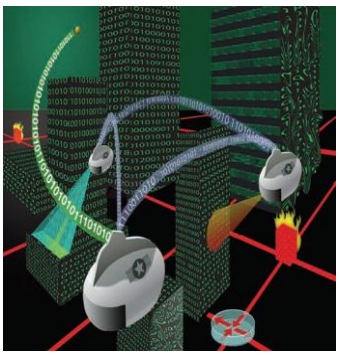

Figure 9

Necessary Capabilities

We must change the paradigm in which we talk and think about the network: we must "fight" rather than "manage" the network and operators must see themselves as engaged at all times, ensuring the health and operation of this critical weapons system

- Secretary of Defense Donald Rumsfeld

NetOps is the operational construct that the Commander, US Strategic Command (CDRUSSTRATCOM) will use to operate and defend the Global Information Grid.

- USSSTRATCOM, Joint CONOPS for GIG NetOps, 15 Aug 2005

The global reach of cyberspace operations requires collaborative planning and assessment at the strategic and theater level to integrate actions across the joint information environment. The "varying degrees of range, maneuver, and lethality"[60] of operations in the cyber domain may occur in and from states, cooperative or failed, against target state or non-state actors.

The freedom of movement in this environment begins with gaining and maintaining access to the battlespace through kinetic (physical) or non-kinetic (electronic) means. Both have definitive ROE implications due to geopolitical boundaries of US, allies, and third party countries infrastructure and requires comprehensive understanding of the adversary use of the domain. The nature of targeting options revealed from IPOE will identify the relative nodes and segments susceptible to Title 10[61] and Title 50[62] tools to access the physical and logical maneuver space (see appendix III). The awareness of the infrastructure components, electronic systems, and the electromagnetic spectrum also reveal security protocols that are critical to discovery of "faults in the code or logic" subject to exploitation. The identification of an alteration to this fracture point upon being flagged from a "defensive" posture will require adversary modification followed by adaptation by the "cyber weapon" being employed to maintain maneuver ability.

The ability to recognize and isolate this non-kinetic attack requires quick reaction by cyber forces to reconstitute and regenerate decisively. The capability to act and react faster than the adversary seeks to exploit or capitalize on the "ability to O-O-D-A" more effectively as a means of competitive advantage that comes from decision superiority. The attributes of decision superiority as described in Joint Vision 2020 as "better decisions arrive and implement faster than opponents, or in a non-combat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish the mission". The proliferation of technology has a reciprocal dependence on information centric processes to manage the battlespace. They synchronize the distributive operations of information technology systems and processes to "gather, manipulate, and disseminate" information in and through the information environment that synthesizes movement of forces under a broad span of control.

The C2 of cyber forces occur with greater speed, range, and flexibility of traditional forces. These forces present through OPCON and TACON not uniquely, however coordination across multiple geopolitical AORs in simultaneous operations produce strategic/operational/tactical effects is unique to cyber. The boundaries of these operations transcend global and geographic theaters, thus coordination, prioritization, and/or restrictions are paramount to success. A flexible C2 structure must be sufficiently robust to fuse global, theater, and non-DoD agency forces to synchronize distributed operations across the spectrum of conflict. The unity of effort and purpose for global C2 is critical to construct integrated operations of cross-domain effects in cross-theater campaigns.

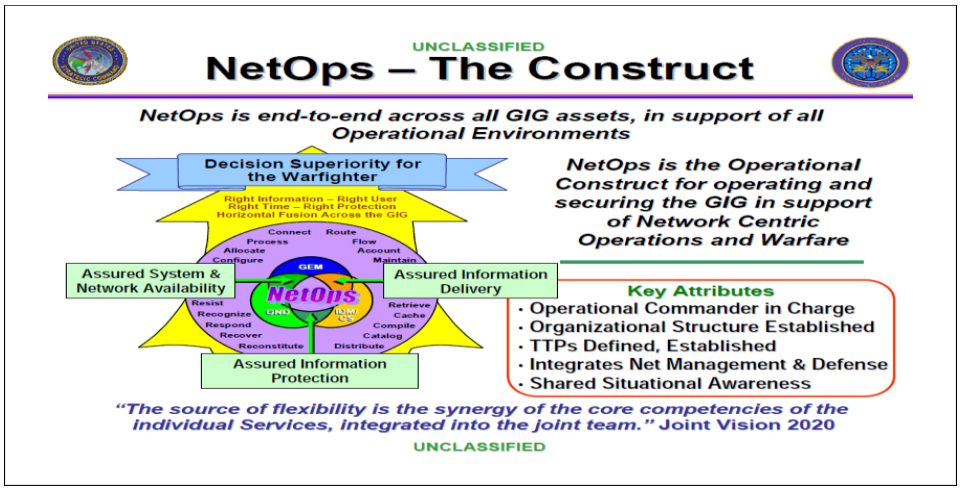

Figure 10

USSTRATCOM integrates space, global strike, ISR, network warfare, and missile defense into functional commands[63] with JTF-GNO for operations in the cyber domain. The measures and counter-measures applied by JTF-GNO provide the "essential tasks, situational awareness, and C2" that synchronizes effects of "assured systems and network availability, assured information protection and defense required for unified information campaign". The OPCON over service network operations components and TACON from respective emergency/incident response centers yields an event based C2 structure that aggregates and segments "pertinent theater, operational, and tactical system and network views" of the battlespace. These operations are "highly dynamic and maneuverable with transitions between F2T2EA phases nearly instantaneously." Integrating effects based operations that contribute to information and decision based superiority require the ability to leverage this strategic reach afforded by the cyber domain.

Spatial and Temporal Dimensions

Operations in the cyber domain are "continuous, cyclic, and iterative" and distinctly different from conventional platforms in traditional domains. In reality these operations are planned and executed with on-going IPOE and targeting across the EMS, electronic information systems and networks vulnerable to threats. Offensively, operations are undertaken to exploit vulnerabilities while simultaneously defensive actions "secure" them virtually. Further, as the avenues for exploitation broaden, they are subject to altering "data at rest" that previously required kinetic access. The continued proliferation and sophistication of "wireless" platforms complicates CNO by increasing the pathways to data stores used for C2 as the battlespace moves across the EMS requiring the conjunctive employment of EW capabilities.

The speed of operations accelerated OPSTEMPO and compressed the O-O-D-A loop to maneuvers represented in milliseconds. The effects in the cyberspace can cross strategic, operational, and tactical levels across multiple domains simultaneously. The ripple effects, intended and unintended, may traverse joint, coalition, and civil infrastructures along with friendly domains. The unique attributes and speeds of exploitation require commensurate response in decision making to match the dynamic climate cyberspace. This reveals a cycle of adaptation in tools and weapons for specific targets that emerge as a result of exploitation as new paths emerge from the 'low cost of entry". Operations in this venue have unique maneuver ability through the use of "logic" or "code" (see appendix III) to gain and react through access by the forces in cyberspace. The "branches and sequels" continue in this domain until the mission is complete or the counter operations are halted.

Conclusion

> *More therefore than all plans and schemes based on material factors, the art of battle consists in maintaining and strengthening the psychological cohesion of one's own troops while at the same time disrupting that of the enemy's. The psychological factor is therefore all-important*
>
> General Andre Beaufre

The widespread recognition that successful joint operations, now and in the future, relies on the fusion and synergy of space, air, land, and sea domains with the cyber domain is critical. The "stovepipe" models of each independent domain wielding their respective platforms as a contributing instrument of power have succumbed to the pronounced acknowledgement that operations in the cyber domain are not mere enablers to successful operations, rather they are precursors to dominating the battlespace though information superiority. This future operating concept serves to broadly outline capabilities the JFC can employ to seize the initiative in and through the cyberspace. CNO, when jointly employed with the other core, supporting, and related Info-Ops capabilities provides significant advantage through "attack, deceive, disrupt, deny, exploit, and defend" maneuvers aimed at decision superiority uniquely enabled by the cyber domain.

Appendix I – Anatomy of Cyberspace Operation[64]:

Cyberspace operations are being conducted every day—some aspects of planning and execution are constantly ongoing. As Figure 2-3 shows, a key distinction is not only between planning and execution, but also between offensive and defensive thinking. As they work through the steps depicted in this figure, cyberspace operators also continuously work through the intelligence process and the targeting cycle described in joint doctrine.

Execution in cyberspace comprises two types of thought: offensive and defensive. For example, we engage in offensive operations to attack a vulnerability gained through access. We engage in defensive actions to close a vulnerability resulting from an adversary's access. Therefore, access is the "on ramp" for both sides' offensive actions. We protect access through a variety of means, such as password protection, firewalls, closed networks, or certificates—all of these predicated on the vigilance of individual network users.

In the cyberspace domain, ISR and offensive activities fall into a minimum of ten broad categories.

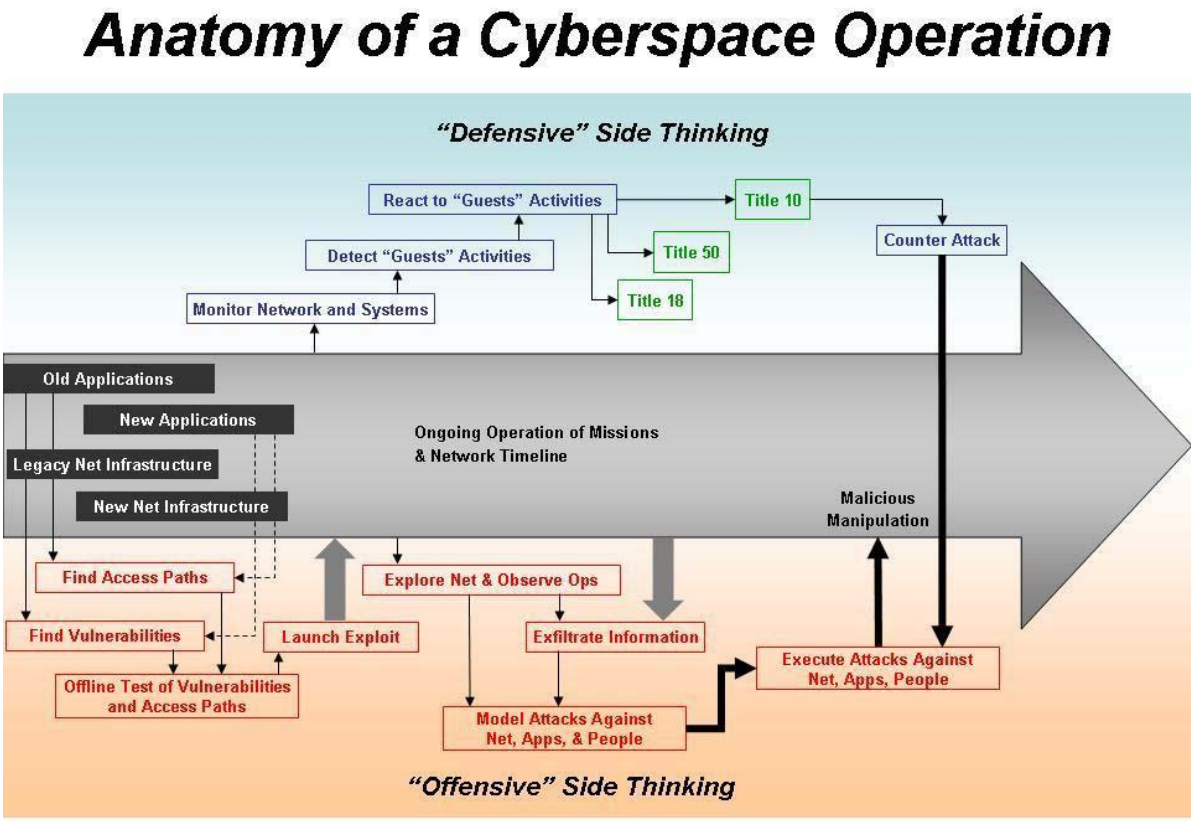

Figure 2-3. Anatomy of a Cyberspace Operation

- Determine the detailed layout and architecture of the adversary's cyberspace operations.
- Determine access paths.
- Determine vulnerabilities
- Test these vulnerabilities and access paths offline.
- Launch exploitation.
- Explore network and observe operations.
- Exfiltrate information.
- Model attacks against networks and applications.
- Execute attacks against networks and applications.
- Assess attack.

A critical task is to identify vulnerabilities within the applications or network infrastructure systems and access paths to those vulnerabilities. Vulnerabilities within infrastructure components and many applications can be identified because these applications are commercially available and can be purchased on the open market. Access paths are often revealed through technology, but many social engineering schemes are simpler to execute. In any case, it is not difficult for adversaries to obtain copies of some of the basic components that operate on anyone's network.

Intruders can, at their leisure, test and analyze commercially-available products to develop means of exploitation. These intruders can then extract information from a network. Once intruders extract mission-relevant data, they can analyze it offline for further vulnerabilities. At a time of their choosing, they can activate these various means of attack or intrusion to manipulate both data and application processes.

Defense against surreptitious activity involves three steps:
- Monitoring networks and systems.
- Detecting intrusions and other activities.
- Reacting to (restoring) intrusions and other activities.

Establishing situational awareness of activity on the network is the first priority. This is obtained by monitoring network traffic and observing standard as well as unusual information flows or system processing. If monitoring is adequate, this will reveal the presence of unwelcome activity within the network.

Appendix II – Tools, Tactics, Techniques, and Procedures:

1. **Types of Cyberwarfare[65] Techniques**

• Attacking Critical Infrastructure - many components of the national critical infrastructure (electricity, water, fuel, communications, transportation) are vulnerable to concerted electronic attacks; such attacks pose serious domestic disasters, including financial meltdown, flooding, chaos, and mass casualties
• Disruption in the Field/Denial of Service - individuals can block, intercept, or pollute vital lines of communication; this form of attack is of particular importance to the military which relies heavily upon electronic communications, transmitted via computers and satellites, to coordinate activities; such attacks can be carried out by flooding a site with e-mail or overwhelming it with requests for information which block others' access to the site and/or cause the site to crash
• Gathering Secret Data - classified and sensitive information which is not handled securely can be intercepted and/or tampered, i.e. computer network espionage
• Disinformation Campaigns - the Internet is a popular tool for finding news, and can be utilized to spread mis- and dis-information to affect a population's beliefs or psychology; additionally, the Internet can be used as an open forum and platform for rhetoric to incite sympathizers
• Web Vandalism - the deactivating and/or defacing of Web pages; hackers break into a website's files and alter them by posting obscenities or generally changing the content of the site that is viewed on the World Wide Web

2. Potential Cyberwarfare Weapons[66] Procedures

• Computer Viruses - can be fed into a computer either remotely or by "mercenary" technicians
• Logic Bombs - a type of computer virus which can lie dormant for years, until, upon receiving a particular signal, is awoken and begins attacking the host system
• Chipping - a plan (originally proposed by the CIA, according to some sources) to slip booby-trapped computer chips into critical systems sold by foreign contractors to potentially hostile third parties and/or recalcitrant allies
• Worms - self-replicate ad infinitum, eating up a system's resources
• Trojan Horses - a malevolent code inserted into legitimate programming in order to perform disguised functions
• Back Doors and Trap Doors - a mechanism built into a system by the designer, in order to provide the manufacturer or others the ability to "sneak back into the system" at a later date by circumventing the need for access privileges

3. Cyberwarfare Tools[67]

• Social Engineering
• Hacking
• Denial-of-Service attacks
• Eavesdropping
• Dumpster Diving
• Identity Theft
• Sabotage
• Insertion of rogue code
• Industrial Espionage
•Stealing intellectual property and confidential information
• Physical Theft

• Insertion of misinformation
• Perception Management

4. Cyberwarfare Tactics[68]

• Eavesdropping on the opponent's/target's computer networks and communications
• Interrupting transmission of messages across adversary's communications lines
• Intercepting and altering messages being transmitted between management and operations
• Mapping the opponent's network
• Scanning the opponent's networks for vulnerabilities
• Providing misinformation to confuse the opponent
• Planting fast acting rogue code on the opponent's system (i.e. viruses, worms, etc.)
• Using known vulnerabilities in software to gain access to the opponent's system
• Planting bad data or code to surreptitiously undermine the opponent's systems or data
• Launching denial-of-service attacks against the opponent
• Ensure accurate reporting of happenings, i.e. report only facts
• Monitoring own systems for intrusions, eavesdropping, mapping, and scanning
• Analyze the opponent's patterns of attack for pre-empting future actions and attacks
• Attacking from bogus, anonymous, or innocent sources/servers
• Penetrating computer networks
• Reconfiguring the opponent's firewall
• Planting spies in opponent's operations (i.e. insiders, disenfranchised employees, contractors)
• Monitoring own transactions for spies
• Having imaged backups of computing software and environment to allow fast recovery
• Ensuring backup hardware and power supply are on hand
• Develop efficient command and control systems
• Ensure all members know their area of responsibility and boundaries for decision-making
• Ensure all members know the procedures and rules
• Ensure all members have an in-depth knowledge of their tools and tactics
• Debrief regularly

Appendix III – Cyber Attack Classes[69], Categories and Methods[70]:

1. Classes

Attack	Description
Passive	Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capture of authentication information (e.g., passwords). Passive intercept of network operations can give adversaries indications and warnings of impending actions. Passive attacks can result in disclosure of information or data files to an attacker without the consent or knowledge of the user. Examples include the disclosure of personal information such as credit card numbers and medical files.
Active	Active attacks include attempts to circumvent or break protection features, introduce malicious code, or steal or modify information. These attacks may be mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks can result in the disclosure or dissemination of data files, denial of service, or modification of data.
Close-In	Close-in attack consists of a regular type individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close physical proximity is achieved through surreptitious entry, open access, or both.
Insider	Insider attacks can be malicious or nonmalicious. Malicious insiders intentionally eavesdrop, steal or damage information, use information in a fraudulent manner, or deny access to other authorized users. Nonmalicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as “getting the job done.”
Distribution	Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks can introduce malicious code into a product, such as a back door to gain unauthorized access to information or a system function at a later date.

2. Categories and Methods

Attack	Description
Denial Of Service (DoS) Attacks	
Flooding	Sending extraneous data or replies to block a host services
SYN/RST Flooding	Exploiting limited cache in IP stack to block connections
Smurfing	Using the IP broadcast system and IP spoofing to multiply floods
Out Of Band/Fragment Attacks	Exploiting vulnerabilities in IP stack kernel implementations
Nuking	Using forged messages to reset active connections
Specific DoS	Generating requests that block one specific vulnerable service
Malicious Software Attacks	
Logical Bomb	Program designed to cause damage under certain conditions
Backdoor	Program feature allowing remote execution of arbitrary commands
Worm	Program that spawns and spreads copies of itself
Virus	Code that self-reproduces in existing applications
Trojan	Program-in-a-program that executes arbitrary commands
Exploiting Vulnerabilities	
Access Permissions	Exploiting read/write access to system files
Brute Force	Trying default or weak login/password combinations
Overflow	Writing arbitrary code behind the end of a buffer and executing it
Race Condition	Exploiting temporary insecure conditions in programs
IP Packet Manipulation	
Port Spoofing	Using commonly used source ports to avoid filtering rules
Tiny Fragments	Using small packets to bypass firewall protocol/port/size checks
Blind IP Spoofing	Changing source IP to access password-less services
Nameserver ID "Snoofing"	Blind spoofing with calculated false ID numbers NS-caches
Sequence Number Guessing	Calculating TCP SEQ/ACK numbers to spoof a trusted host
Remote Session Hijacking	Using spoofing to intercept and redirect connections
Insider Attacks	
"Backdoor" Daemons	Opening a port for further remote access
Log Manipulation	Removing traces of attacks and unauthorized access
Cloaking	Replace system files with trojans to hide unauthorized access
Sniffing	Monitor network data to find sensitive data e.g. passwords
Non-Blind Spoofing	Monitor network to hijack active or make forged connections

Appendix IV - Bibliographies:

1. Air Force Concept of Operations for Information Operations (AF IO CONOPS), 6 Feb 2004.
2. Air Force Doctrine Document (AFDD) 2-5. Information Operations, 11 January 2005.
3. Air Force Doctrine Document (AFDD) 2-11 (DRAFT) Cyberspace Operations, 2008.
4. Air Force Scientific Advisory Board, Implications of Cyberwarfare, Vol 1, August 2007
5. Air Force Policy Directive 10-28. Air Force Concept Development, 15 September 2003.
6. Air Force Concept of Cyberwarfare, November 2007
7. Defense in Depth. IATF Report. Washington, DC: Information Assurance Technical Forum, 2002.
8. Department of the Army, Information Operations Primer, Department of Military Strategy, Planning, and Operations U.S. Army War College Carlisle Barracks, PA November 2008
9. Department of the Army, Field Manual 3-13 Section IV, Global Security.Org, last accessed November 2009
10. DoD, The National Military Strategy for Cyberspace Operations, December 2006
11. Department of Defense Directive O-3600.1. Information Operations, 14 August 2006.
12. DoD Information Operations Roadmap (IO Roadmap). 30 October 2003.
13. Joint Publication 3-0 (JP 3-0). Joint Operations, 17 September 2006.
14. Joint Publication 3-13 (JP 3-13). Information Operations, 13 February 2006.
15. Joint Publication 3-13 (JP 3-13). Information Operations (second draft), 14 December 2004.
16. Brown, Christopher DEVELOPING A RELIABLE METHODOLOGY FOR ASSESSING THE COMPUTER NETWORK OPERATIONS THREAT OF NORTH KOREA Naval Postgraduate School Monterey, CA, September 2005
17. Courville, Shane AIR FORCE AND THE CYBERSPACE MISSION DEFENDING THE AIR FORCE'S COMPUTER NETWORK IN THE FUTURE, Center for Strategy and Technology Air War College Air University Maxwell Air Force Base, Alabama December 2007
18. Dull, David, IMPLEMENTING NETWORK-CENTRIC OPERATIONS IN JOINT TASK FORCES: CHANGES IN JOINT DOCTRINE, U.S. Army Command and General Staff College, June 2006
19. Gardiner, Von , NETWORKS—THE AIR FORCE'S NEWEST WEAPON SYSTEMS, Air War College, Air University-Maxwell AFB, AL February 2006
20. Grant, Rebecca, Victory In Cyberspace, Air Force Association, October 2007
21. Glebocki, Joseph Jr., DoD Computer Network Operations Time to Hit the Send Button, U.S. Army War College, Carlisle Barracks, PA, March 2008
22. Hunt, Carl, Net-Centricity and Global NetOps, USSTRATCOM-JTF GNO, March 2006
23. Kamphausen, Roy and Lai, David and Scobell, Andrew, BEYOND THE STRAIT: PLA MISSIONS OTHER THAN TAIWAN, Strategic Studies Institute, U.S. Army War College Carlisle, PA, April 2009
24. Krekel ,Bryan, Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, Northrop Grummon-Prepared for The US-China Economic and Security Review Commission, October 2009

25. Orr, George, Combat Operations C3I Fundamentals and Interactions, Airpower Research Institute Air University Press Maxwell Air Force Base, Al , July 1983
26. Patterson, Jason and Smith, Matthew, Developing A Reliable Methodology for Assessing the Computer Network Operations Threat of Iran, Naval Postgraduate School Monterey, CA, September 2005
27. Quick, Chris, Integration of Information Operations in Combat, Naval Postgraduate School Monterey, CA, December 2008
28. Radice, Richard, DOMINATING CYBERSPACE, U.S. Army War College, Carlisle Barracks, PA, March 2007
29. Rid, Thomas WEB SPECIAL:War 2.0, Hoover Institution – Stanford University, February 2007 http://www.hoover.org/publications/policyreview/5956806.html
30. Rollins, John, CRS Report to Congress – Terrorist Capabilities for Cyberattack: Overview and Policy Issues, January 2007
31. Scurlock, Antonio , STRATEGIC PLANNING TO CONDUCT JOINT FORCE NETWORK OPERATIONS: A CONTENT ANALYSIS OF NETOPS ORGANIZATIONS STRATEGIC PLANS , Naval Postgraduate School Monterey, CA , March 2007
32. Sevy, Bradley Using Covert Means To Establish Cybercraft Command And Control, Air Force Institute of Technology Air University Wright-Patterson Air Force Base, Ohio, March 2009
33. Schmitt, John F. A Practical Guide for Developing and Writing Military Concepts. Defense Adaptive Red Team Working Paper #02-4. McLean, VA: Hick & Associates, Inc., December 2002.
34. Silbaugh, Eric, NETWORK-CENTRIC OPERATIONS – PROMISE, CHIMERA, AND ACHILLES' HEEL: CHALLENGES AND PITFALLS FOR NETWORKS AND INFORMATION INFRASTRUCTURE, Air University Air Command and Staff College, April 2005
35. Stein, George J. "Information Warfare," in Cyberwar: Security, Strategy and Conflict in the Information Age, ed. Alan D. Campen et al. Fairfax, VA: AFCEA International Press, May 1996.
36. Stein, George, "The 21st Century Air Force:An Integrating Imperative", Air University-Air War College Maxwell AFB, AL July 2009
37. Stytz , Martin and Banks, Sheila, ISSUES AND REQUIREMENTS FOR CYBERSECURITY IN NETWORK CENTRIC WARFARE, Air Force Research Laboratory,Wright Patterson AFB,OH, June 2004
38. Thomas, Timothy, China's Electgronic Long Range Reconnaissance, Military Review November – December 2008
39. Upton, Oren, Asserting National Sovereignty in Cyberspace: The Case for Internet Border Inspection, Naval Postgraduate School Monterey, CA , June 2003
40. Wentz ,Larry and Barry,Charles, Military Perspectives on Cyberpower CENTER FOR TECHNOLOGY AND NATIONAL SECURITY POLICY NATIONAL DEFENSE UNIVERSITY WASHINGTON, DC, July 2009
41. Wilson, Clay, CRS Report to Congress – Information Operations, Electronic Warfare, and Cyberwar: Capability and Policy Related Issues, March 2007
42. Williamson, Jennie, Information Operations: Computer Network Attack in the 21st Century, U.S. Army War College, Carlisle Barracks, PA, April 2002

43. Woolley Pamela, Defining Cyberspace as a United States Air Force Mission, Air Force Institute of Technology Air University Wright-Patterson Air Force Base, Ohio, June 2006
44. Wrona, Jacqueline-Marie, From Sticks and Stones to Zeros and Ones: The Development of Computer Network Operations as an Element of Warfare A Study of the Palestinian-Israeli Cyberconflict and what the United States Can Learn from the "Interfada", Naval Postgraduate School Monterey, CA , September 2005
45. US Department of Defense. Joint Net-Centric Campaign Plan, Washington, DC: Joint Chiefs of Staff, October 2006. http://www.jcs.mil/j6/c4campaignplan/JNO_Campaign_Plan.pdf
46. US Department of Defense, Joint Information Operations Force, Washington, DC: Chairman of the Joint Chiefs of Staff March 2009
47. US Department of Defense, Universal Joint Task List, Washington, DC: Chairman of the Joint Chiefs of Staff, January 2009
48. US Department of Defense. Joint Vision 2020 (JV 2020). Washington, DC: Chairman of the Joint Chiefs of Staff, June 2000.
49. US Department of Defense. National Defense Strategy of the United States of America. Washington, DC: Office of the Secretary of Defense, March 2005.
50. US Department of Defense. National Military Strategy for Operations in Cyberspace. Washington, DC: Chairman of the Joint Chiefs of Staff, 2006.
51. US Department of Defense. Capstone Concept for Joint Operations ver 3, January 2009
52. US Department of Defense, A Network-Centric Operations Case Study: US/UK Coalition Combat Operations during Operation Iraqi Freedom, Force Transformation, March 2005
53. US Joint Forces Command, Joint Operating Environment 2008, November 2008https://us.jfcom.mil/sites/J5/j59/default.aspx

Appendix V - Endnotes:

[1] National Military Strategy for Cyberspace Operations defines cyberspace a, "a domain characterized by electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated infrastructures", page ix
[2] Capstone Concept for Joint Operations, states "Defending national interests…threats could range from direct aggression to less openly belligerent actions that nonetheless threaten vital national interests", page 9
[3] JP 3-13, Information superiority definition "information superiority is described as the operational advantage gained by the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same"., page I-5
[4] JP 3-13 page I-1, para 1
[5] DoD 3600.1 page 1, para 3
[6] Ibid, page 2, para 4.2
[7] Ibid, page 2, para 4.1, 4.2
[8] Ibid, page 2, para 4.1.1
[9] JP 3-13, I-1, para 1
[10] Ibid
[11] Ibid, para 2
[12] Orr, Combat Operations C3I Fundamentals and Interactions, page 35
[13] IJP 3-1, para 2
[14] Ibid, para 2
[15] Ibid, para 3
[16] Ibid, para 4
[17] Ibid, para 4c
[18] Ibid, page I-8, c1
[19] Ibid, page I-8, c1-5
[20] Ibid, page, I-9, para 1-2
[21] Ibid, para 3
[22] AF Concept of Cyberwarfare, page 3, para 2
[23] Ibid II-4, para f-1
[24] NMS-CO is National Military Strategy for Cyberspace Operations
[25] AF Concept of Cyberwarfare, page 4
[26] Ibid, page 1
[27] Ibid, para f-1
[28] Ibid, page II-5, para
[29] Ibid, para 2
[30] Ibid, para 3
[31] Stein, George, The 21st Century Air Force, page 2 para 1
[32] Ibid, para 2
[33] USA Information Operations Primer, page 59
[34] Rid, Thomas, Web 2.0, page 3 items 1 – 7
[35] Orr, Combat Operations C3I Fundamentals and Interactions, page 99 para 1

[36] Metaverse Roadmap Pathways to the 3D Web, page 4
[37] ibid
[38] Concept of Cyberwarfare, page ii, para 2
[39] JP 3-13, page i-6
[40] National Military Strategy for Cyberspace Operations, page 1
[41] JFCOM Joint Operating Environment (JOE), page 3
[42] National Military Strategy for Cyberspace Operations, page 1
[43] ibid
[44] ibid
[45] ibid
[46]National Military Strategy for Cyberspace Operations, 2006
[47] AF Concept of Cyber Warfare, description of counter cyber operations and freedom of movement, page 5
[48] ibid
[49] AF Cyberspace Operatiions 2-11, page 12 para 4
[50] Ibid, page 9 parae 4
[51] Ibid, page 8
[52] ibid
[53] ibid
[54] ibid
[55] Ibid, page 9
[56] NMS-CO issues ten strategic imperatives to take account of to operate successfully in the domain, page 10
[57] Ibid, page 11
[58] Ibid, page 17
[59] Clay Wilson, CRS Report to Congress, page 5
[60] AFDD 2-11, page 20 para 2
[61] AFDD 2-5, page 20 states that Military forces under a combatant commander derive authority to conduct NetA from the laws contained in Title 10 of the U.S. Code (U.S.C.).
[62] AFDD 2-5, page 20 states that Intelligence forces in the national intelligence community derive authority to conduct network exploitation and many NS operations from laws contained in U.S.C. Title 50.
[63] Cyberspace Operations primer, page 89
[64] Cyberspace Operations AFDD 2-11, pages 35-36
[65] "Types of Cyberwarfare" according to "Special Focus: Cyberwarfare," The Center for the Study of Technology and Society, 22
[66] "Potential Infowar Weapons" according to Yael Shahar in "Information Warfare: The Perfect Terrorist Weapon," February 1997
[67] Armstrong, Helen and Davey, John "Educational Exercises in Information Warfare – Information Plunder and Pillage," Submitted to NCISSE 2001, May 22-24, 2001, 5th Annual Colloquium for Informatioin Systems Security Education, George Mason University
[68] Ibid. Armstrong and Davey provide these examples as possible tactics used in cyberwarfare.
[69] Information Assurance Technical Forum, Defense in Depth. (Washington, DC: Government Printing Office, 2002), 5.

[70] Fadia,Ankit Network Security: A Hackers Perspective (Cincinnati, OH: Premier Press, 2003), 165-230