THE UNITED STATES NAVAL WAR COLLEGE

JOINT MILITARY OPERATIONS DEPARTMENT

War in the Information Age: A Primer for Information Operations and Cyberspace Operations in 21st Century Warfare

Richard M. Crowell

Revised
12 January 2016

THIS PAGE INTENTIONALLY BLANK

War in the Information Age:
A Primer for Information Operations and Cyberspace Operations in 21st Century Warfare

Land, Maritime, Air, Space, and Cyber domains[1]

By

Richard M. Crowell

Fourth Edition

12 January 2016

(This is a revised edition of my original Primer written in January 2010. Revisions are intended to keep abreast of the changing terminology, provide clarification of proceedings as information becomes known, and to offer contemporary examples of events in the fast pace world of information operations and cyberspace operations. This version has an increased emphasis on information operations. The views expressed in this paper are those of the author and do not reflect the official policy or position of the Naval War College, Department of the Navy, Department of Defense, or the U. S. Government.)

THIS PAGE INTENTIONALLY BLANK

Contents

Common Abbreviations

CCDR – Combatant Commander

CCMD – Combatant Command

CCMD CPT – Combatant Command Cyber Protection Team

C2 – Command and Control

CCMF – Cyber Combat Mission Force

C/NMT – Cyber National Mission Team

C/NST – Cyber National Support Team

CNDSP – Computer Network Defense Service Provider (Program)

CO – Cyberspace Operations

CSE – Cyber Support Element

CST – Combat Support Team

CPT – Cyber Protection Team

CMT – Combat Mission team

DCO-IDM – Defensive Cyberspace Operations–Internal Defensive Measures

DCO-RA – Defensive Cyberspace Operations–Response Actions

DDoS – Distributed Denial of Service

DISA – Defense Information Systems Agency

DNC – DISA Network Center

DoDIN – Department of Defense Information Network

IO – Information Operations

IW – Information Warfare

JCC – Joint Cyber Center

JFC – Joint Force Commander

JFCCC – Joint Force Cyber Component Commander

JIE EOC – Joint Information Environment Enterprise Operations Center

JIE GEOC – Joint Information Global Environment Enterprise Operations Center

NMT – National Mission Team

NST – National Support Team

RNOSC – Regional Network Operations Security Center

SVC NSOC – Network Operations and Security Center

TNCC – Theater Net Ops Control Center

List of Illustrations

THIS PAGE INTENTIONALLY BLANK

Information warfare consists of those actions intended to protect, exploit, corrupt, deny, or destroy information, or information resources in order to achieve a significant advantage, objectives, or victory over an adversary.

– Winn Schwartau, InfoWarCon 2009, Washington, DC

Introduction

Traditionally, warfare has been waged in physical domains that can be seen and touched by those who conduct operations in them.[2] Until recently, there were four domains – land, maritime, air, and space. Human use of the interconnected electronics to move digitized information through the electromagnetic spectrum has brought forth a fifth domain – cyberspace. Information in the form of content and code is what moves through cyberspace and is increasingly used as force to compel action. Information content is sent around the world in micro seconds and when displayed on various electronics it influences people to act. Code is the computer software that runs electronics and moves the content; it can force electronics to act independently of the owner's intent. How these forces are used in support of military objectives and political ends are important aspects of twenty–first century conflict. All warfighters must learn to operate in cyberspace and be able to fight and win with information as a weapon.

This paper will describe the role of information operations (IO) and cyberspace operations (CO) in information age warfare and depict their relationship to the 21st century concept of hybrid warfare. It presents the framework of operational art, specifically operational factors and joint functions as a tool for understanding IO and CO and integrating them into plans and operations.[3] Questions are posed throughout the monograph aimed at helping operational commanders and planners frame their thoughts on future conflict. Additionally, this work postulates that cyberspace is a near perfect domain in which to create surprise and dilemmas for one's adversary; largely because of the speed of movement and depth of penetration into society it provides information.

Information Warfare Circa 1981

During the Cold War, the USSR was at least a decade behind the U. S. in computer technology. To fill that void, the Soviets developed an aggressive program to steal U. S. and Western science and technology. In 1981 French President Francois Mitterrand passed vital information to U. S. President Ronald Reagan. The case was designated *Farewell* by the French Direction de la Surveillance du Territoire (DST), and later became known as the *Farewell Dossier*.

Some of the most useful information gained from the *Farewell Dossier* was the KGB's 'shopping list' for their desired technology. In his book, *At the Abyss, an Insider's History of the Cold War*, Thomas C. Reed, a former Secretary of the United States Air Force[4] and Director of the National Reconnaissance Office,[5] recounts the story of early computer warfare which was prompted by the Soviet Union's desire to more efficiently control some of its industrial control systems for its oil and gas production.

> The production and transportation of oil and gas was at the top of the Soviet wish list. A new trans-Siberian pipeline was to deliver natural gas from the Urengoi gas fields in Siberia across Kazakhstan, Russia, and Eastern Europe,

> into the hard currency markets of the West. To automate the operation of valves, compressors, and storage facilities in such an immense undertaking, the Soviets needed sophisticated control systems. They bought early model computers on the open market, but when Russian pipeline authorities approached the U. S. for the necessary software, they were turned down. Undaunted, the Soviets looked elsewhere; a KGB operative was sent to penetrate a Canadian software supplier in an attempt to steal the needed codes. U. S. Intelligence, tipped by *Farewell*, responded and – in cooperation with some outraged Canadians – "improved" the software before sending it on.
>
> Once in the Soviet Union, computers and software, working together, ran the pipeline beautifully – for a while. But that tranquility was deceptive. Buried in the stolen Canadian goods – the software operating this whole new pipeline system – was a Trojan Horse. (An expression describing a few lines of software, buried in the normal operating system, that will cause that system to go berserk at some future date (Halloween?) or upon the receipt of some outside message.) In order to disrupt the Soviet gas supply, its hard currency earnings from the West, and the internal Russian economy, the pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to the pipeline joints and welds. The result was the most monumental non-nuclear explosion and fire ever seen from space. At the White House, we received warning from our infrared satellites of some bizarre event out in the middle of Soviet nowhere. NORAD feared a missile liftoff from a place where no rockets were known to be based. Or perhaps it was the detonation of a small nuclear device. The Air Force chief of intelligence rated it at three kilotons, but was puzzled by the silence of the Vela satellites. They had detected no electromagnetic pulse, characteristic of nuclear detonation.[6]

In his 2012 article *Cyber Security: A Pre-History*, Michael Warner, the command historian for U. S. Cyber Command states, "The sourcing for these claims are unclear, and it is not yet possible to know the truth of the matter from publicly available records, but it bears noting that the Soviets independently made similar claims on their own."[7] Warner goes on to cite Lieutenant General Nikolai Brusnitsin, former Deputy Chairman of the State Technical Commission of the USSR, "In 1990 the Ministry of Defense publicly accused US intelligence of implanting not only 'units' that would beam data out of computers acquired by the USSR, but also 'viruses' and 'gimmicks which render a computer totally inoperative'."[8]

Whether or not Reed's assertions are wholly true both sides in the Cold War clearly displayed intent to manipulate early networked computer controls in support of military objectives and political ends. The pipline event did not utilize the modern method of inserting malicious software (malware) via the Internet, but clearly demonstrated a desire to manipulate supervisory control and data acquisition (SCADA) systems. SCADA are real time industrial process control systems that use computers and software to monitor and control systems from nuclear power plants and electric power grids to railroad switching terminals and drinking water and sewage treatment facilities. Given advances in computers and information networks since the 1980s, one can easily envision the burgeoning risks of the growing dependence corporations, governments, and militaries have on information–communications technologies (ICT).

Twenty-first Century

On August 17, 2009 the Sayano-Shushenskaya hydroelectric dam suffered a catastrophic explosion due to an *accidental* SCADA input. The explosion of one of the dam's ten turbine generators (weighing over 1,000 tons) destroyed nine of ten generators, flooded engine and turbine rooms and killed dozens. While the SCADA input was done unintentionally, this incident demonstrates how deliberate inputs via the Internet could be designed to physically degrade and destroy critical infrastructure, and kill humans. In discussing the incident General Keith Alexander, USA, then, Commander U. S. Cyber Command stated,

> One of the dam's ten 650-megawatt hydro turbine generators, weighing more than 1,000 tons, was being serviced and, by mistake, **was remotely restarted by a computer operator 500 miles away**. The generator began spinning and rose 50 feet into the air before exploding. The flood caused by the accident killed 75 people and destroyed eight of the remaining nine turbines. A similar deliberate attack remains a huge problem… [The] **destruction by cyber-attacks was outranked only by nuclear bombs or other weapons of mass destruction**.[9] [Emphasis added]

In addition to direct SCADA inputs, malware in the form of worms are increasingly concerning for those who rely on cyberspsce for government, military, corporate, and civilian activities. "Worms are computer programs that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively."[10] One of the most significant examples of this type of malware is named Stuxnet. The computer worm emerged in 2010 to physically alter and destroy some of Iran's nuclear processing equipment. Stuxnet (code) affected both human and automated decision making in that it made the equipment produce substandard material and destroy machinery while giving signals (content) to the human operators that all was working well.

Additionally, chaos can be created with the insertion of malware into civilian or military command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) systems or a power company's SCADA system. This could degrade, deny or destroy a power grid supporting military command and control (C2) systems, resulting in an impotent military. A similar attack against a civilian power grid during extreme cold weather could result in a significant loss of life and perhaps more importantly a loss of confidence in the government. Would this be an information operation or a cyberspace operation? An attack of this type would certainly send a message. Could this be a weapon of mass destruction or effect (WMD/E)[†]?[11] Would the above merging of means and modes be classified as hybrid warfare? What actions would the U. S. Department of Defense take? Which command would respond? More importantly, how does the commander need to think about warfare in the information age?

[†] A weapon of mass destruction (WMD) is defined as chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties and exclude the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon. (U. S. Department of Defense Dictionary of Military and Associated Terms (Joint Publication 1-02), 8 November 2010, As Amended Through 15 April 2013, 302). Weapons of mass effect (WME) are weapons capable of inflicting grave destructive, psychological and/or economic damage to the United States. (Homeland Security Advisory Council Weapons of Mass Effect Task Force on Preventing the Entry of Weapons of Mass Effect Into the United States, January 10, 2006, 3)

The Information Environment, Information Operations, and Cyberspace

National security is being redefined by cyberspace. In addition to opportunities, DOD faces significant cyberspace challenges
– DoD Strategy for Operating in Cyberspace – July 2011

The information age has been described by Winn Schwartau, author of numerous books on the information age and information warfare, as "computers everywhere."[12] While much has been written about the age and its impact on modern warfare, its primary characteristic is the proliferation of human use of information-communication technology (ICT). ICT incorporates information systems and resources (hardware, software, and wetware) used by military and civilian decision makers to send, receive, control, and manipulate information necessary to enable 21st century decision making.[13]

The combining of individuals, systems, content, and resources to enable decision making forms the Information Environment (IE). The IE, a term of art, is defined in Joint Doctrine for Information Operations as, "The aggregate of individuals, organizations, and systems that collect process, disseminate, or act on information. This environment consists of three interrelated dimensions which continuously interact with individuals, organizations, and systems. These dimensions are the physical, informational, and cognitive."[14]

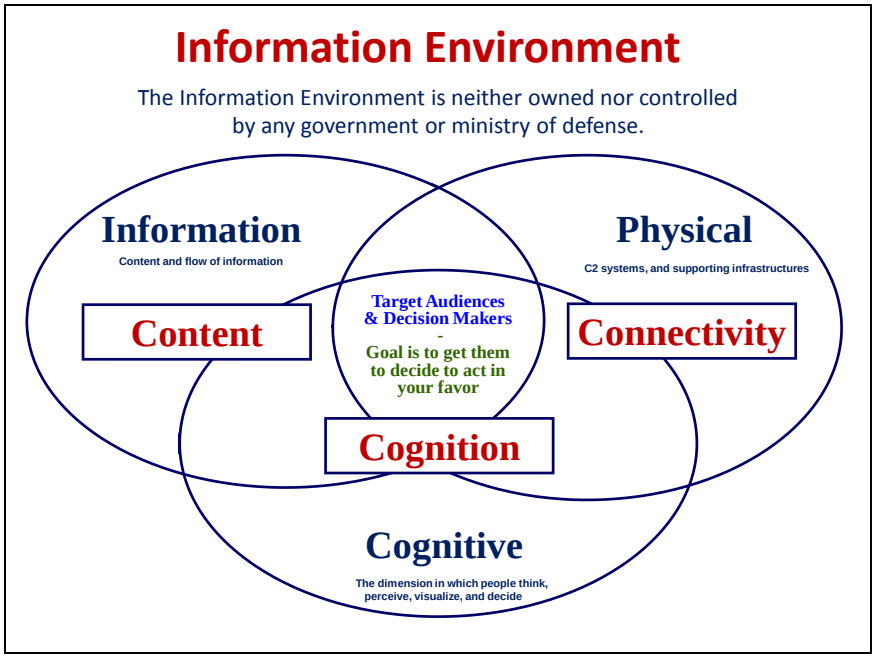


Figure 1. The Information Environment

These dimensions are inextricably linked and because of the accelerated intertwining of cyberspace and human activity in this century both information operations and cyberspace operations are increasingly used in all domains in support of both civilian and military objectives and political ends.

Information Operations

The military capability that is most often used to achieve objectives within the IE is information operations (IO). U. S. Joint Military Doctrine defines Information Operations as:

> The integrated employment, during military operations, of **information-related capabilities** in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.[15] [Emphasis added]

This 2012 definition is instructive as it moves away from previous Joint Doctrine that grouped IO into core, supporting, and related capabilities; often seen as 'stove pipes'. The use of information-related capabilities (IRCs) is important in that it is not tied to any one technology or time frame. The move to IRCs opens the door for any and all possible capabilities to be used.

There is no defined set of IRCs. Social media like Facebook™, Twitter™, and smart phone apps are some of the capabilities *du jour*, but we must understand what future IRCs will look like and how friends and foes will use the power of information to achieve objectives. To this end IO may be thought of as disseminating and protecting information and its sources of production, storage, and movement in support of objectives. To effectively use the information we must mature our ability to develop precise messages (content) and use the right IRC (connectivity) to deliver it to decision makers in order to influence them to decide in our favor.

The caveat associated with use of information-related capabilities is the old adage that "with great power comes great responsibility." With respect to content, one only has to look at the variety of images and social media postings from the front during Operations ENDURING FREEDOM (OEF) and IRAQI FREEDOM (OIF) to understand the importance of educating all service men and women on the power of information content, specifically images, in contemporary conflict. Sending content electronically to, from, and around the battlefield can be seen as using information to achieve objectives. Content can be a sword that cuts both ways. Cyberspace allows images to move globally in seconds. It also permits anyone with access to them to easily manipulate the content in support of their physical and cognitive objectives. This drives the need to view content and the code that moves it as both offensively and defensively in twenty–first century warfare.

Cyberspace

No one disputes the explosive expansion in the use of cyberspace. Around the globe, more and more people are making decisions based on information gleaned from information age methods rather than industrial age ones. The common thread with the information age methods is that they use cyberspace to move information to and from electronics, and ultimately decision makers. The number of humans utilizing cyberspace for commonplace activities (communication, news, shopping, banking, and entertainment) is rapidly accelerating. Between 2006 and 2008 use of cell phones and Internet to receive news grew from 1% to 48%, in Mumbai, India, a city of 13 million people.[16]

There are disputes, however, as to the definition of cyberspace. As understanding and use of this new domain evolves, so too does the definition. Earlier definitions focused on computers and computer usage. *The Oxford English Dictionary* defines cyberspace as the notional environment in which communications over computer networks occurs.[17] Schwartau, states, "Cyberspace is the intangible place between computers where information momentarily

exists on its route from one end of the global network to the other."[18] Later definitions have evolved to include all manner of electronic communications. Still disputed is whether or not human activity should be included in the definition of cyberspace.

It is not surprising that our technology–oriented military exclude human activity from the definition of cyberspace. The Department of Defense (DoD) Joint Doctrine defines cyberspace as, "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[19]

Because humans are the inventors of information technology, the author supports a holistic definition of cyberspace; one that includes both technology and human activity. Dr. Daniel T. Kuehl, the former Director of the Information Resource Management College at the National Defense University, provides an inclusive definition of cyberspace that shows intertwining of domains and human activities.

> Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information–communications technologies (ICT).[20]

Obviously, cyberspace would not exist without its component electronics and electromagnetic spectrum (EMS). Electronics are the computers, smart phones, weapons systems, and hardware that have components that direct electric current. Understanding the electromagnetic spectrum aids in physically defining cyberspace as the EMS is what the digitized information moves through in cyberspace.

The ability to understand cyberspace is directly related to comprehending how and why information (content and code) moves through the IE and how that information is used to influence human and automated decision making in both peace and war. While the nature of war remains unchanged, it is the character that is malleable. Today, the battle for the hearts and minds of the people around the globe is being waged in the IE with weapons that use information instead of physical force. Cyberspace, with its lack of traditional geometry, represents perhaps the most malleable of operating environments; one that is changing the character of war by enabling vast amounts of information to be moved globally to both humans and electronics, frequently compelling them to act.

DoD Cyberspace Operations

The likelihood of tactical actions in cyberspace having strategic effects has led the U. S. DoD to develop specific organizational structures for cyberspace operations. In his 2007 article, *Warfighting in Cyberspace*, then, Lieutenant General Keith Alexander, USA, Director of the National Security Agency (NSA) and Commander Joint Functional Component Commander – Network Warfare (JFCC-NW), described how the U. S. DoD is organized for operations in cyberspace:

> We have redefined our cyberspace mission area in terms of offensive–network warfare (NW) and defensive–network operations (NetOps)–and established JFCC–NW and JTF– GNO [Global Network Operations]

> to address each of those mission sets, respectively. As directed by the USSTRATCOM Commander, the Joint Functional Component Command for Network Warfare (JFCC–NW) was established to "optimize planning, execution, and force management for the assigned missions of deterring attacks against the United States, its territories, possessions, and bases, and employing appropriate forces should deterrence fail, and the associated mission of integrating and coordinating [Defense Department] CNA [computer network attack] and computer network defense as directed by headquarters USSTRATCOM." The command further defines *network warfare* as "the employment of computer network operations with the intent of denying adversaries the effective use of their own computers, information systems, and networks." This mission statement recognizes the primacy of the strike or attack aspects of computer network attacks as a military fire, not merely as an enabler for cognitive effects. USSTRATCOM has also begun to develop tactics, techniques, and procedures and other concepts designed to integrate cyberspace capabilities into cross-mission strike plans. We are developing concepts to address warfighting in cyberspace in order to assure freedom of action in cyberspace for the United States and our allies while denying adversaries and providing cyberspace enabled effects to support operations in other domains. These concepts, and the cyberspace effects that they focus on, are clearly based on the military concepts of strike, fires (supporting and suppressing), and defense. While the concepts of NW and NetOps are a good start, they represent only a small subset of the elements of military power available within or enabled by cyberspace. In order to fully engage in the development of joint doctrine within the cyberspace domain, it is also necessary to develop a definition of exactly what warfare within cyberspace – or cyberspace warfare – is.[21]

In June 2009, the DoD reorganized, consolidating under one command the network warfare and network operations discussed by General Alexander. Secretary of Defense Robert Gates directed that the Commander, U. S. Strategic Command (CDRUSSTRATCOM) establish U. S. Cyber Command (USCYBERCOM) as a subordinate unified command.[22] The 23 June 2009 establishment memorandum directed the CDRUSSTRATCOM to delegate authority to conduct specified cyberspace operations (the functions previously done by JFCC-NW and JTF-GNO) of the Unified Command Plan to the Commander USCYBERCOM. Secretary Gates stated,

> Cyberspace and its associated technologies offer unprecedented opportunities to the United States and are vital to our Nation's security and, by extension, to all aspects of military operations. Yet our increasing dependency on cyberspace, alongside a growing array of cyber threats and vulnerabilities, adds a new element of risk to our national security. To address this risk effectively and to secure freedom of action in cyberspace, the Department of Defense requires a command that possesses the required technical capability and remains focused on the integration of cyberspace operations. Further, this command must be capable of synchronizing warfighting effects across the global security environment as well as providing support to civil authorities and international partners.[23]

The information–related capability most associated with cyberspace is known as cyberspace operations (CO); the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.[24] U. S. Joint Doctrine divides CO into the concepts of Offensive Cyberspace Operations (OCO) and Defensive Cyberspace Operations (DCO). OCO are cyberspace operations intended to project power by the application of force in or through cyberspace.[25] DCO are passive and active CO intended to preserve the ability to utilize friendly cyberspace capabilities, and protect data, networks, net-centric capabilities, and other designated systems.[26] This terminology further aligns warfighting in and through cyberspace with the physical domains.

DoD further defines what must be done in cyberspace to move information to decision makers by expanding the concepts of DCO and OCO. Figure 2 delineates how the DoD Information Networks (DoDIN) global operations are defended with the subsets of DCO, DCO Internal Defense Measures (DCO–IDM) and Response Actions (DCO–RA) that support freedom of maneuver in cyberspace. OCO is seen as the capability to project power through the domains enabling the JFC to achieve objectives. The bridge between defense and offense is built on the same actions that all forces must do successfully, regardless of the domain – conducting comprehensive intelligence, surveillance, and reconnaissance (ISR) along with complete operational preparation of the environment (OPE).

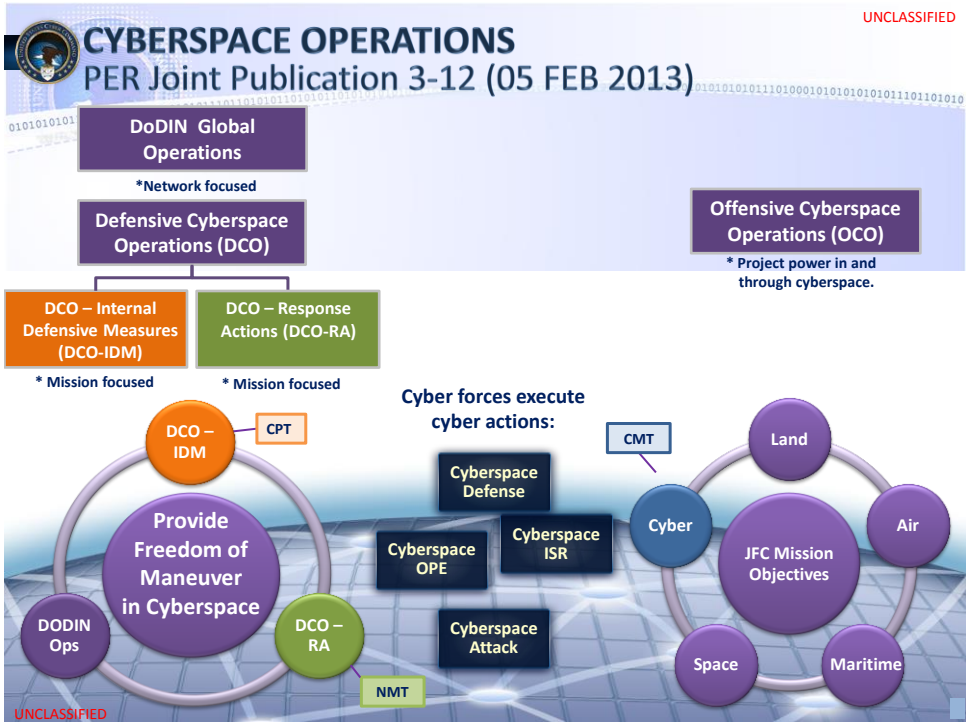


Figure 2. Cyberspace Operations per Joint Publication 3-12[27]

Operation BODYGUARD, the World War II strategic deception for the Allied invasion of Northern Europe, is a twentieth century example of using information–related capabilities of the

day in moving information to a decision maker largely via the electromagnetic spectrum.[‡] The decision maker might be a civilian or military leader, or the local populace. Today the information can be moved by radio, television, cell phone, e–mail, hacking with a structured query language (SQL) injection,[28] or a phishing scheme.[29] These and the majority of IRCs have the ability to move content through cyberspace. The relationship between IO, cyberspace, and human interaction is best described by Colonel David T. Fahrenkrug, USAF and Kuehl:

> While information operations thus includes all three dimensions of the information environment, [physical, informational, and cognitive] cyberspace comprises only a part—albeit perhaps a very large part—of the connectivity and content dimensions.[30] Cyberspace is thus shaping and changing the three dimensions of the information environment: how we create information content itself (a Web page, for example), how we share that content through new forms of connectivity (the Internet links that make that Web page accessible to over a billion people), and how human interaction and communication are affected.[31]

The Forces of Content and Code

Content as Force

Content and code moving through cyberspace are increasingly important forms of force in contemporary conflict. Content is most recognizable as words, pictures, files, et al. are converted to digital data in the form of binary code (1s and 0s) by the electronics. The digital data is placed into 'packets' and these are sent via electromagnetic radiation along the most secure and expeditious route between two points. Radio, television, voice, and data signals are sent from a transmitter to a receiver, in the same way communication of old was sent on packet ships sailing the Atlantic Ocean between England and the United States. Content whether it is presented as radio, television, a web page or any one of the myriad of social media is used to achieve both cognitive and physical objectives. Influencing human decision making by getting someone to believe something and then to act in your favor are examples of information as a cognitive force. In discussing the importance of the human mind in warfare, Clausewitz reminds us, "Naturally, moral strength must not be excluded, for psychological forces exert a decisive influence on the elements involved in war."[32]

[‡] The deception relied heavily on convincing the German decision makers of three main objectives: 1) a large force will go to Norway and threaten Germany from the North. A fictitious army was created in Scotland. The British Fourth Army sent out thousands of 'real' radio signals that were electronic deceptions; 2) the main invasion will come through the Pas de Calais, France. The First US Army Group (FUSAG) was created in the county of Kent (near Dover). Another ghost army, FUSAG with General Patton as its real commander, also sent out thousands of 'real' radio signals; 3) whatever happens in Normandy is a feint. The messages were reinforced by the truth because Dover to Calais is the shortest distance England to France, the beaches around Calais are large and flat, and it was the beginning of the shortest land route into Germany.

Most of the information was moved via radio and Morse code signals. Additionally, in the early hours of June 6th the Allies conducted an elaborate electronic deception in the form of air and sea assets emitting false targets. This presented the appearance of an armada moving towards Calais. This information was reinforced by dozens of German agents, turned by the British XX (double cross) organization, sending electronic messages back to the Abwehr, German Intelligence HQ. All of this was done to convince the German decision makers, primarily Adolph Hitler, to decide in the Allies favor.

In information age wars those who cannot compete against traditional military force have resorted to the use of information content as a weapon. Much of what is happening in contemporary conflict can be seen as a twenty–first century form of guerilla theater; the manipulation of media in pursuit of objectives and ends. In discussing the links between the content and cognition dimensions of the IE Dr. Richard Landes, the director and co-founder of the Center of Millennial Studies at Boston University, states, "[G]lobal jihad is waging a cognitive war against the West because they cannot win on the battlefield."[33] Landes coins the phrase 'Pallywood'(a conflation of the world's two largest centers of cinema production Hollywood and Bollywood with Palestinian manipulation of the media) – "the Palestinian obfuscation and outright lying in reporting news events, laid out a comprehensive framework to understand how Hamas's narrative took over the public sphere."[34]

Many state and non–state actors are adept at using content to achieve their objectives. Landes defines a three–prong approach used by Hamas [and others] to control the narrative, "Arouse protest in the West to stop Israel; feed Lawfare (law warfare) attacks that severely restrict Israel's use of weapons; demonize and delegitimize Israel in the world community [with events such as] Israel Apartheid Week and BDS [boycott, divest, and sanctions]."[35]

Code as Force

Information code (computer software) is also produced in various forms and used to influence automated decision making. Malicious software code (malware) is often written to get electronics – computers, smart phones, and other forms of hardware to act independently of the owners' intent. Stuxnet, mentioned earlier, demonstrates that when malicious code and content are combined the effects can be significant.

Two modern examples of electronics, software, and the electromagnetic spectrum (EMS) used in decision making are the Apple iPhone and the maritime Automated Information System (AIS). On global system for mobile (GSM) networks the iPhone moves information via the electromagnetic spectrum using the 850 MHz frequency for voice and 1900 MHz frequency for data.[§] The U. S. Department of Homeland Security and the U. S. Coast Guard describe AIS as a shipboard display system (e.g. radar, chart plotter, etc.) with overlaid electronic chart data that includes a mark for every significant ship within radio range; with a velocity vector (indicating speed and heading).[36] Similar to the iPhone, the AIS uses two frequencies, 161.975 MHz and 162.025 MHz, to move information to and from the electronic displays. Incidentally, AIS can be bought in Europe for approximately US$ 500 and in early 2009, Somali pirates were reported to be using AIS to identify and track their targets.[37]

Electronics and the EMS in the cyberspace domain may be better understood when viewed as an analogy for ships and the sea in the maritime domain. The human activities of planning, directing, and operating in a given domain are essential to understanding it. This is especially true for cyberspace. Increasingly more people get their information from electronics - satellite television, personal computers, smart phones, blogs, new media, or social networking sites[**].[38]

[§] Global system for mobile (GSM) technology differs from code division multiple access (CDMA) in that on true GSM networks iPhones can move voice and data simultaneously. This often causes a slower rate of data transfer. GSM has the greatest market share worldwide with approximately 80 percent. CDMA, the predominant U. S. technology has a faster data transfer rate. CDMA has approximately 20 percent of the global market.

[**] New media and social networking enable near instantaneous direct communication between individuals and groups. Both use cyberspace and electronics to move information in order to influence human decision making. New media and social networking are extremely important to understanding social interaction and decision making,

In 2007, 84% of the population of Moscow, Russia owned cell phones.[39] In that year, 45% of Muscovites used cell phones to get news.[40] By the end of 2014 61% of all Russians had access to the Internet.[41] Global Internet user penetration in 2014 reached 40%, 78% in developed countries, and 32% in developing countries.[42]

The persistent growth of electroninc connectivity means that more and more human activity will occur in and through cyberspace. These activities will include, but are not limited to, legal and illegal activities such as entertainment, navigation, banking, networked communication, identity theft, information theft, and monetary theft. Examples of the scope of global activity in cyberspace in the early 21st century include over 3.04 billion Internet users (or 42 percent of people on earth),[43] nearly seven billion mobile cellular subscriptions,[44] in excess of one billion Facebook™ users in 2014,[45] and trillions of dollars moved electronically per day via electronic funds transfers (EFT).[46]

Paralleling the rapid expansion of civilian cyberspace use is the increased use of cyberspace by modern militaries. Many militaries now rely almost exclusively on the domain to move information to decision makers – commanders and troops. Military uses of cyberspace include, but are not limited to, e-mail (unclassified and classified), chat (in various commercial formats), Video Teleconference (VTC), Global Command and Control System (GCCS), Global Transportation Network (GTN), Automated Identification Technology (AIT), In-Transit Visibility (ITV), Joint Tactical Radio System (JTRS), Blue Force Tracker (BFT), Theater Battle Management Control System (TBMCS), Link 11 and Link 16 Data Link Systems, Unmanned Aerial Systems (UAS, i.e. Global Hawk and Predator), Global Positioning System (GPS), and Joint Direct Attack Munitions (JDAM).

An example of code that can make electronics act independently of the owner's intent and destroy machines are Bots or robots; remote controlled pieces of malicious software that are inserted into one or more computers. Once a computer becomes infected by the Bot, it becomes a tool or weapon – a lasting legacy of the hacker. Typically, a small group of hackers can create and control a network of bots–a BotNet.[††] BotNets have been known to exceed 100,000 computers. A Bot herder, a hacker with oversight of the BotNet, gives a signal and his network can launch tens of millions of packets of information all aimed at the same or multiple targets. If the target is a server that runs a government website or communications node, the massive amount of information packets sent by the BotNet can simply overload the server and supporting infrastructure, shutting them down, and denying service to legitimate users. This is what is commonly termed a distributed denial of service (DDoS). What effect might new malware have on modern militaries with their near total reliance on electronics for warfighting?

Cyberspace as a Warfighting Domain and the use of Information-related Capabilities

Perhaps no nation state understands cyberspace, its potential and the integral nature of human activity within cyberspace better than China. In the late 20th century, China made the astute decision to focus on the asymmetric possibilities of cyberspace, dedicating precious resources to this mission. There have been innumerable Chinese military strategy books written on cyberspace operations, information warfare, information operations, and electronic warfare. The

---

mainly because of the potential viral nature of this type of communication; however, they are beyond the scope of this paper.

[††] BotNets are a network of remotely controlled bots.

1999 classic *Unrestricted Warfare*, written by two Chinese Colonels (Liang and Xiangsui), frames future war as 'war beyond its traditional military domain'. Importantly, the colonels describe 'domain' as a concept derived from the concept of territory and used to delineate the scope of human activities.[47] In their 'war beyond limits' treatise, the colonels state that, 'All of these things are rendering more and more obsolete the idea of confining warfare to the military domain…'.[48] Two other leaders in the Chinese movement are Shen Weiguang and Dai Qingmin. One of Shen's primary works is titled "*World War, The Third World War–Total Information Warfare*". Dai has written works on integrating network and electronic warfare. Colonels Liang and Xiangsui state, "The expansion of the domain of warfare is a necessary consequence of the ever-expanding scope of human activity, and the two are intertwined."[49] China understands the crucial intertwining of human activity with electronics and the electromagnetic spectrum and that cyberspace will play a huge role in future war.

Given the passive nature of civilian and military cyberspace use, and the distinct advantage others have in this field, America's military must develop expertise in how war is waged in cyberspace. One hurdle is our national tendency to gravitate toward technical solutions rather than abstract solutions. With the exception of the electronics, cyberspace cannot be seen or touched. Another hurdle is our natural human tendency to favor familiar (the original four domains – land, maritime, air, and space) and to approach the new domain of cyberspace with confusion and/or apprehension. Both of these hurdles must be overcome, as armed forces reluctant to evolve are destined for failure. While all the possibilities for waging war in this domain have not yet been unearthed, military leaders must be comfortable with this domain. They must understand the domain – human activity as well as technology; be familiar with the methods used to wage war in all domains; and be open and creative enough to envision new possibilities.

Understanding the Domain

A first step in understanding the domain is to view the current state of flux through the lens of the then changing 19th century maritime domain. While men had been sailing ships at sea for thousands of years, moving cargo and currency and conducting trade, communications, and logistics; the mid-19th century brought forth the first wrought iron steamship, the SS Great Britain. Some say Isambard Kingdom Brunel's invention changed the way men thought about the maritime domain. Prior to this ship, the movement of mail and priority cargo was conducted between the United States and the United Kingdom on the most reliable and secure sailing ships known as packet ships.

An 1858 New York Times article titled *The Last of the Packet Ships*, documented the transition to steam. The article lamented the downfall of New York's thriving ship building and communication industries that was brought about by the changes in shipping from wood and canvas to iron and steam. The article stated, "The obvious advantages of such an arrangement were so great that passengers and shippers gave preference to the ships that could be relied on to sail on a certain day…and their ships were as remarkable for their great speed…and their regularity of sailing."[50] The article continued, "In accomplishing this work, England has gained a greater victory than she did at the Nile or Trafalgar, and Britannia may again wave her trident in triumph."[51] The SS Great Britain and her sister ships could virtually guarantee that a passenger (and cargo to include mail) would arrive on time, well ahead of any sail powered rivals.[52] The steam ship became a reliable means of transportation that was less dependent on wind and other forces of nature. This reliability lead to coal fired, steam powered dreadnoughts

at the turn of the 20th century and eventually oil fired battleships and aircraft carriers during World War II. Even nuclear fueled submarines and aircraft carriers are steam powered.

Some felt the steam ship caused the navies of the world to think differently about warfare at sea. Did it? Did the fact that trade, commerce, communication, and military actions all happened faster by more reliable means result in war at sea somehow being new or different? How did Admiral Nelson come to think 'operationally' in the years and months prior to the Battle of Trafalgar? Was Admiral Nimitz's employment of what we now call operational art, when Nimitz conducted Operation GRANITE, the island hopping campaign in the central Pacific Ocean during World War II, different from Admiral Nelson's devices?

Nelson and Nimitz both had to balance time, space, and force along with sequencing required warfighting functions. Dr. Milan Vego tells us that, operational art exists between strategy and tactics serving as both a bridge and an interface between theory and practice.[53] This holds true for all domains, including the complex man-made domain of cyberspace. The importance of understanding operational art and a commander's ability to 'think operationally' cannot be overstressed.

21st Century Hybrid Warfare

In the 2007 document, *A Cooperative Strategy for 21st Century Seapower*, the maritime service chiefs describe some of the maritime security challenges for the new century.

> Conflicts are increasingly characterized by a hybrid blend of traditional and irregular tactics, decentralized planning and execution, and non-state actors using both simple and sophisticated technologies in innovative ways.[54]

Hybrid wars were described by General James N. Mattis, USMC and LtCol Frank Hoffman, USMC (Ret.) in 2005 as a merger of different means and modes of war.[55] These means and modes include conventional, irregular tactics, terror, crime, networked, coercion / co-option, and IRCs; they can be creatively combined to produce dilemmas for one's adversary.[‡‡] It is "multi-modal or multi-variant rather than a simple black and white characteristic of one form of warfare."[56]

In the *Origins and Development of Hybrid Warfare*, Hoffman discusses new principles appropriate to Liang and Xiangsui's "beyond-limits combined war."

- **Omni-directionality** – requires that commanders observe a potential battlefield without mental preconditions or blind spots. The designing of plans, employment measures, and combinations must use all war resources which can be mobilized. The commander is enjoined to make no distinction between what is or is not the battlefield. All the traditional domains, (ground, seas, air, and outer space) as well as politics, economics, culture, and moral factors are to be considered battlefields.

[‡‡] *Examples of means and modes:* The means to move combat power might be strategic sealift; a mode would be roll-on / roll-off (RoRo) shipping used by the Military Sealift Command. Additionally, an information–related capability (IRC) means would be an offensive cyberspace operation (OCO) in the form of a computer network attack; the mode could be a structured query language (SQL) injection, or a phishing scheme.

- **Synchrony** – enjoins on commanders to link the disaggregated nature of multiple battlefields in different domains with consideration of the temporal dimension. In other words, "conducting actions in different spaces in the same period of time" to achieve desired effects. Instead of phases with the accumulated results of multiple battles, strategic results can now be attained rapidly by simultaneous action or at designated times.

- **Asymmetry** – here the authors recognize that asymmetry manifests itself to some extent in every aspect of warfare. However, asymmetry has been sought in operational terms within traditional military dimensions. In war beyond limits, the spectrum for overlooking the normal rules is much wider.[57]

Cyberspace and hybrid warfare are natural partners. As the intertwining of domains with human activities continues to grow, so will the utilization of cyberspace operations to move code and content in pursuit of military objectives and political ends. In discussing the activities associated with hybrid war, Frank Hoffman states,

> These multimodal activities can be conducted by separate units, or even the same unit, but are generally operationally and tactically directed and coordinated within the main battlespace to achieve synergistic effects in the physical *and* psychological dimensions of conflict. The effects can be gained at all levels of war. [58]

The summer 2006 war between Israel and Hizballah is an example of hybrid warfare. Hizballah proved successful in mixing an organized political movement with decentralized cells that were able to create dilemmas for the Israeli Defense Force (IDF). The IDF thought it was facing the same old guerilla force, but soon found out it was fighting a hybrid force in the air, land, maritime, space, and cyberspace domains. Hizballah fought Israeli tanks with Russian made anti-tank weapons; fired C-802 anti-ship cruise missiles at Israeli ships; fired surface to air missiles (SAM) at Israeli Air Force (IAF) aircraft; kidnapped IDF soldiers; conducted armed reconnaissance with unmanned aerial systems (UASs); intercepted IDF cell phones; there were even reports that U. S. – made single channel ground and airborne radio system (SINCGARS) frequency hopping combat radio transmissions were intercepted and decrypted.[59]

Hizballah hacked into several websites to communicate the message of Al-Manar (Arabic for the beacon) television to a global audience. Specifically, they broke into a Texas cable company's network in order to use their Internet protocol address as a base to run web sites that broadcast Al-Manar television.[60] Hizballah simply added an extension on a network telephone line allowing their traffic to flow and then spread the word via e-mail and blogs that it can be found at that IP address, thus completing the hijack that created a dilemma for the IDF.[61] How do you stop a website in an ally's country from broadcasting?

Hybrid warfare is often described as the blurring and blending of war forms in combinations of increasing frequency and lethality.[62] The seemingly amorphous Hizballah achieved success by utilizing disciplined highly trained and distributed cells to conduct Omni-directional, synchronous, and asymmetric operations. A significant portion of their success can be linked to cyberspace operations. Hacking computer systems, communicating via the Internet, flying computer controlled UASs, and intercepting cell phone and radio communications clearly

demonstrate the employment of cyberspace operations where the primary purpose is to achieve military objectives in or through cyberspace. Less conspicuous, but still extremely successful, uses of cyberspace in Hizballah's hybrid warfare are the extensive communication, recruiting, training, fundraising and propagandizing. In addressing irregular methods, General Mattis provides sound guidance: "They seek to accumulate a series of small tactical effects, magnify them through the media and by information warfare…This is our most likely opponent in the future."[63]

General Alexander states, "The ultimate strategic objective of these [cyberspace] operations is to ensure freedom of action within cyberspace and to deny the enemy the same."[64] Similarly, "Autonomous communication is the paramount objective for Hizbollah [sic]."[65] Hizballah hybrid warfare employs various modes of modern communication to link actions to human decision makers in order to terrorize, thereby influencing human decision making. Josef Goebbels, Hitler's Minister of Propaganda, once said: 'We do not talk to say something, but to obtain a certain effect'.[66]

Goebbel's statement demonstrates that human activity – decision and the intent behind those decisions – is as fundamental to IO and CO as the technology. Our society is bewitched with technology, often seeing it as the decisive, sanitary answer to whatever problem is on the table. Many modern decision makers, both civilian and military, view cyberspace operations as interconnected, globalized, clean and precise. Indeed in his 1996 essay *The Emerging Primacy of Information*, Martin Libicki put forth the argument that "cyberspace will tend to eliminate geopolitics through its influence on military security, rather than (or at least in addition to) its influence on international politics."[67] This belief in the 'magic bullet' is as dangerous today as it was during all previous conflict. As Clausewitz so eloquently stated,

> Kind-hearted people might of course think there was some ingenious way to disarm or defeat an enemy without too much bloodshed, and might imagine this is the true goal of the art of war. Pleasant as it sounds, it is a fallacy that must be exposed: war is such dangerous business that the mistakes which come from kindness are the very worst. The maximum use of force is in no way incompatible with the simultaneous use of the intellect.[68]

Cyberspace is an evolving domain of warfare, but the reality is that no matter how much technology is used to conduct kinetic or non-kinetic operations in any or all of the domains; war is still as Clausewitz states "an act of force to compel our enemy to do our will."[69] Cyberspace operations are just as capable of violent, dirty, and deadly facets of the Battle of Thermopylae, Nelson's Battle of Trafalgar, and Strategic Bombing of World War II. Further, cyberspace operations do not occur in a vacuum. Enemies are not a machine or a piece of technology. Clausewitz states, "In war, the will is directed at an animate object that *reacts*."[70]

Examples of Early 21st Century Information Warfare and Cyberspace Operations

Information warfare (IW) is not new. Militrary theorists from Sun Tsu and Machiavelli to Lefebvre, Rostorguyev, Shen Weiguang, Vego, Thomas, et al. have written on the power of information in warfare. Whether it is classical deception that originated in antiquity or the use of electronics to influence the masses IW and cyber warfare have proven themselves valuable in conflict. Our military must understand the possibilities – offensive and defensive with these capabilities.

Cyberspace is used for communication, navigation, research, banking, shopping, entertainment, record keeping, recruiting, planning, and just about any activity that can be done in the other domains. Therefore, any of these activities can be adversely affected by cyberspace. It is important to understand how our adversaries can and will use operations in cyberspace for their advantage. Many are aware of familiar cyberspace dangers, like malware, phishing, whereby personal information is illegally, and sometimes unknowingly, accessed, resulting in identity theft. Other common cyberspace dangers are detailed by Melissa Hathaway, then Cyber Coordination Executive for the Office of the Director of National Intelligence, in an October 8, 2008 Op-Ed piece, describing cyber 'attacks' on information:

- **Information theft.** Stealing data from a target personal device, system or network is the most common threat. For example, a disgruntled Boeing employee was charged last year with lifting more than 320,000 sensitive company files by using a thumb drive to tap the corporate system. Boeing estimated that the stolen documents would have cost it between $5 billion and $15 billion in lost revenue had they been given to competitors.

- **Information disruption.** Hackers who sneak into government systems and alter crucial operating data are a growing concern. In 2006, a disgruntled Navy contractor inserted malicious code into five computers at the Navy's European Planning and Operations Command in Naples, Italy. Two computers were rendered inoperable when the program was executed. Had the other three computers been knocked offline, the network that tracks U. S. and NATO ships in the Mediterranean Sea and helps prevent military and commercial vessels from colliding would have been shut down.

- **Information denial.** Cases in which private or government computer systems are shut down by floods of automated hits are also on the rise. In April 2007, Russian nationalists used such a "distributed denial of service" attack to block access to the networks of the Estonian parliament, the president's office and many of that country's banks, news organizations and Internet service providers.[71]

Attacks of this nature are serious on a small scale, but could be catastrophic on a large scale. What role will IO and CO have in future conflict? Will they be combined in hybrid ways to create dilemmas for the adversary? The following examples of cyberspace and information operations to date should not be considered an all-inclusive list; rather they should be considered a springboard to new possibilities.

Lashkar-e-Taiba (LeT) – Mumbai, India

In November 2008 a little known terrorist group named Lashkar-e-Taiba (LeT) conducted three days of terror in the Indian metropolis of Mumbai, killing 179 and wounding over 325 people. Their operation was extremely well planned and executed, utilizing both IO and CO to achieve their objectives. The extreme violence of the attacks sent a message and CO were used extensively to get the terrorists in the places necessary to inflict the maximum amount of carnage. Global Positioning Systems (GPS) were used to navigate from the home base, and Google Earth™ maps were used to survey the operations area.[72] Voice over Internet Protocol

(VoIP) was used to direct forces and create dilemmas for the opposition.[73] To highlight the global and near instantaneous aspects of cyberspace, the Pakistani based handlers and foot soldiers in Mumbai used a VOIP call dealer based in the U. S. to obtain the connectivity necessary to orchestrate events.[74] The terrorists were provided with 15 PC-to-phone accounts, 10 common–client accounts and five Direct Inward Dialing Austrian phone numbers.[75] The fact that Internet connectivity likely transited far outside a direct path between India and Pakistan had little or no adverse effect on the terrorist's operations. In fact it aided them in that when the Indian security forces attempted to locate those directing and conducting the attacks, they could not.[76]

Russian Information Warfare – Informatsionnoe Protivoborstvo (Information Confrontation) Informatsionnaya Voyna (Information War)

Numerous Russian authors to include general and flag officers have written on the topic of information warfare (IW) for more than a century. Russian theory and practice of IW spans the Cold War to contemporary operations in the Caucuses and Ukraine. The path of Russian thinking and use parallels the growth of electronic communication throughout the twentieth century and into the twenty–first. As more people gained access to radios, television, computers, and smart phones the electronics have been used and adapted to move selected content, as a force, to target audiences with the goal of getting people to act in favor of the Russian aims.

Russian IW is commonly divided into how information-technical (electronics) and information-psychological (humans) actions are used to influence automated and human decision–making. The information–technical aspects of IW largely deal with how electronics are used in support of political and military objectives. This may include design and adaptation of electronics and systems to use malware to get the electronics to act independent of the owners intent. Understanding of the information–technical aspects of warfare will clearly be vital to future conflict, but are beyond the scope of this paper.

Information–psychological warfare is largely about presenting an individual or group selected information that influences them to decide in your favor. A significant part of Russian theory on this form of warfare centers on the concept of Reflexive Control (RC). RC is about interfering with the decision–making of the adversary leadership. "Reflexive control is defined as the means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action."[77] In his 2004 article, *Russia's Reflexive Control Theory and the Military*, for the Journal of Slavic Military Studies, Timothy Thomas, conveys the use of RC in events of the 1995 bombing of the Sarajevo market square:

> Within minutes of the bombing, CNN and other news outlets were reporting that a Serbian mortar attack had killed many innocent people in the square. Later, crater analysis of the shells that impacted in the square, along with other supporting evidence, indicated that the incident did not happen as originally reported. This evidence also threw into doubt the identities of the perpetrators of the attack. One individual close to the investigation, Russian Colonel Andrei Demurenko, Chief of Staff of Sector Sarejevo at the time stated, "I am not saying the Serbs didn't commit this atrocity. I am saying that it did not happen as originally reported." A US and Canadian officer soon backed his position. Demurenko believed that the incident was an excellent example of reflexive control, in that the incident was made to look like

> it happened in a certain way to confuse decision–makers. [Sic][78]

RC has been used effectively in Russia's 'cold, warm, and hot' conflicts of the twenty–first century. The value of RC as a weapon in contemporary conflict is described by Major General N. I. Turko, "The most dangerous manifestation in the tendency to rely on military power relates more to the possible impact of the use of reflexive control by the opposing side through developments in the theory and practice of information war rather than to the direct use of the means of armed combat."[79]

In RC much of the content that is presented is deception, propaganda, mis–information, disinformation, or outright lies. These are valuable tools that have been used to influence human decision–making since mankind began communicating. They have been used across the spectrum of influence from religion, political, military, and corporate sectors of society to achieve objectives. In peace and war the manipulation of the truth sows the seeds of doubt so that the manipulator may say the 'truth' is a matter of opinion. This in turn opens the door for the decision–maker to more easily decide in favor of the manipulator.

Russia – Georgia 2008

There was a dedicated attack on Georgian government web sites in the summer of 2008. The cyber attacks pre-dated the actual movement of forces and kinetic operations in what became known as the Russia-Georgia War of 2008. While it has not been proved that the Russian government conducted or condoned the cyber attacks, it has been generally accepted that many of the computers orchestrating the attacks were controlled by Russian hackers. A Los Angeles Times editorial reported,

> Analysts say the online attacks, which appear to have begun well before Russian tanks rolled in, resembled the work of garden-variety cyber pranksters. Georgian government websites were overwhelmed with swarms of data, and some were defaced by hackers. There was no clear proof of Russian military involvement (investigators have reportedly traced some of the data to Russian servers tied to organized-crime groups), so the perpetrators may have been nationalists. Still, the timing suggests that even if the responsible parties weren't in uniform, they coordinated their moves with the Russian military.[80]

Most of the media reports centered on the use of BotNets to conduct distributed denial of service (DDoS) attacks against Georgian government and civilian web sites.

In the Russia–Georgia incidents, the individuals conducting the DDoS had both physical and cognitive objectives. A primary physical objective was disabling the communications network of the Georgian leadership prior to the movement of Russian Forces into South Ossetia. This can be seen as synchronizing command and control and cyberspace operations as operational fires.[§§]

[§§] Cyber fires may be depicted as Operational Fires – the application of one's lethal and/or nonlethal firepower for generating a decisive impact on the course and outcome of a campaign or major operation. They represent today an inherently multi-service or joint function. They are not simply fire support; hence, the success of an operational maneuver is not necessarily dependent on these fires. However, they can facilitate one's operational maneuver. They are conducted in the operational and/or strategic depths of the enemy's defenses. Milan N. Vego. *Joint Operational Warfare Theory and Practice.* Newport RI: (Naval War College, 2009), VIII-59-60

The DDoS shut down much of the Georgian government's communication inside Georgia and to the outside world.

Another objective was to create fear and discontent within the Georgian population. The attackers inserted pictures of Adolf Hitler into government web sites.[81] These pictures were linked to existing and modified pictures of Georgian President Mikheil Saakashvili to make him appear *Hitleresque*. This had a great psychological impact on the citizens of Georgia due to their history with Nazi Germany. Additionally, the Russian government broadcast into Georgia television and radio programming that supported Russian interests. The people in control of the computers, television, and radio were able to manipulate the connectivity and content dimensions of the information environment.

At the Cyber Defence and Network Security 2012 conference in London Andro Barnovi, the Deputy Defence Minister of Georgia described the operational goals of the Russian cyberspace operations conducted against Georgia:

> Sense of insecurity within the society; Mistrust to government; Panic caused by misinformation; Hindering government information policy; Direct economic damage; Disorder of communication systems; Weakened coordination within governmental agencies; Dysfunction of Command and Control systems and subsequent direct physical damage [Sic]; Decrease of legitimacy of the government activities inside the country and abroad; Acquire reliable information about the actions and dislocations of Georgian army units and leadership.[82]

This list of goals is illustrative in that it includes both physical and cognitive objectives, and affected both human and automated decision–making. While the DDoS (cyber) attacks, often attributed to the Russian Business Network (RBN), were an important aspects of the early stages of the war, an in-depth look reveals that attacking forces employed a mixture of conventional weapons, irregular tactics, terrorism, and criminal behavior, networks, coercion / co-option, and IRCs to create dilemmas for Georgia while attempting to achieve Russian objectives.

In March 2009, the Project Grey Goose, Phase II Report: *The Evolving State of Cyber Warfare* reported on a 2007 article titled *Russian Federation Military Policy in the Area of International Information Security: Regional Aspect.* The article provides insight into just how holistic the Russian thinking is with respect to the intertwining of cyberspace and the bad aspects of human activity,

> In our view, isolating cyberterrorism and cybercrime from the general context Of international information security is, in a sense, artificial and unsupported by Any real objective necessity. This is because the effect of a "cybernetic" weapon does not depend on the motivation of a source of destructive impact, whereas it is primarily motivation that distinguishes acts of cyberterrorism, cybercrime, and military cyberattacks. The rest of their attributes may be absolutely similar. The practical part of the problem is that the target of a cyberattack, while in the process of repelling it, will not be informed about the motives guiding its source, and, accordingly, will be unable to qualify what is going on as a criminal, terrorist or military-political act. **The more so that sources of cyberattacks can be easily given a legend as criminal or terrorist actions** (Emphasis added by Greylogic).[83]

Project Grey Goose developed the links and legends between the Russian government and the Russian Business Network,

> The StopGeorgia.ru forum was part of a bulletproofed network that relied on shell companies and false WHOIS[***] data to (a) prevent its closure through Terms of Service violations, and (b) to mask the involvement of the Russian FSB/GRU.[†††] By mimicking the structure of the Russian Business Network, a cyber criminal enterprise, it creates plausible deniability that it is a Kremlin funded Information Operation (IO).[84]

The use of cyberspace operations to control selected aspects of the connectivity and content dimensions of the information environment created great problems for the Georgian government. President Saakashvili could not communicate with his leadership or his people and he could not allow the attackers (cyber, television, and radio) to continue. Ultimately, the Georgian government took down the television and radio broadcasts from Russia to prevent further manipulation of the Georgian people.[85] In this case, Georgia's adversary used both cyberspace operations as operational fires and information operations to control the narrative. The CO achieved cyber control in degrees necessary to allow Russian Federation forces freedom of action, first in the cyber domain and subsequently, in the physical domains. This control of content across multiple forms of connectivity to Georgian, regional, and global target audiences had strategic implications. The Georgian's were forced to attempt filtering their communications with regional and global allied nation's connectivity. When this failed, they sued for peace.[86]

Russia – Ukraine 2014

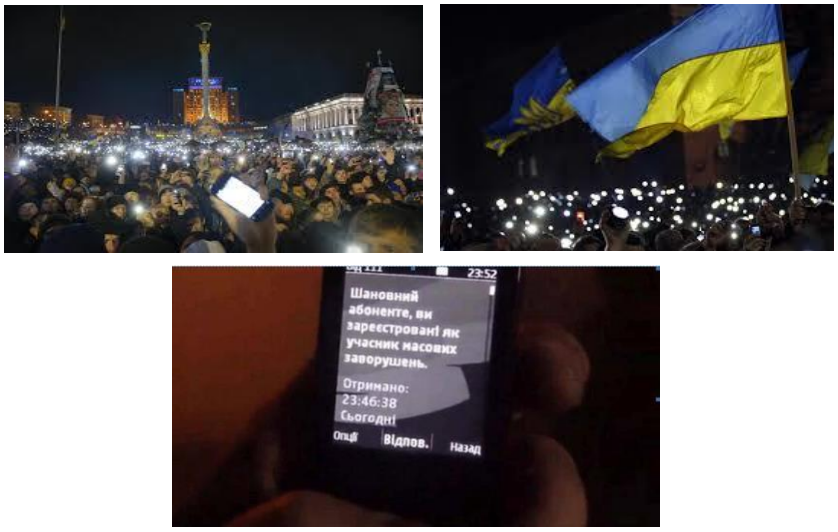
Throughout early 2014 fighting in the Crimea and Eastern Ukraine saw numerous foot soldiers in civilian clothes acting like infantry and special forces. The fact that they were not in uniforms enabled Russia to successfully use the information environment with their familiar tools – propaganda, mis-information, disinformation, or outright lies to inform, persuade, and influence decision makers in support of their larger objectives. A careful analysis of Figure 3 by N. R. Jenzen-Jones on the Armaments Research Services web page notes that the people on the streets with covered faces had military boots and GM-94 grenade launchers, weapons and clothing consistent with trained soldiers or Russian Special Forces (Spetsnaz).[87] Additionally, they appear to move and position themselves like a well-trained tactical military unit. Were these hybrid forces in Ukraine?

[***] WHOIS is a way of questioning computer data bases in order to identify registered users, domain names, and Internet Protocol (IP) addresses among other information.

[†††] FSB is the Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii, Federal Security Service, of the Russian Federation and the main successor of the KGB. The GRU is Glavnoye Razvedyvatel'noye Upravleniye, the foreign military intelligence directorate of the General Staff of Russian Federation Armed Forces.

Figure 3. Russian Forces in Crimea[88]

Figure 4 shows images from the Ukranian protests against Russian involvement in the Crimea and Ukraine in early 2014. They represent the vast use of mobile telephones by both the protestors and the pro–Russian government who was able to use them to target the owners with information operations. The phones had a variety of roles in the protests. Initially they were lit (similarly to candles, lighters, or flashlights) to show support of the masses. Secondarily they were used to document events with still and video images; to influence local, regional, and global actors to support the protestors. And finally the phones were used by pro–Russian supporters to tell the protestors that, "Dear subscriber, you are registered as a participant in a mass disturbance."



"You are registered as a participant in a mass disturbance."

Figure 4. Images of mobile phone use in Ukranian protests in early 2014[89]

What might the psychological impact be of getting such a text message? If an adversary can target someone's mobile phone in a city square, what other information do they know about the user and how might that be further used in messaging or targeting?

In July 2014 in Eastern Ukraine, Russia skillfully presented local, regional, and global decision–makers with just the right content to get them to decide and act in Russia's favor. RC was used in the aftermath of the shoot down of Malaysian Air flight MH 17 by a Russian made Buk SAM system; reportedly controlled by pro–Russian separatists. Russian media outlets provided numerous theories as to the cause. These ranged from Russia Today (the first Russian English–language television news channel broadcasting Russian views on global news 24/7) reporting and using social media to spread that MH 17 was shot down by Ukrainian military SAMs while targeting Putin's plane, two Ukrainian SU-25 fighter aircraft, or the U. S. Central Intelligence Agency (CIA).[90]

Figure 5. Snapshot of Russia Today Twitter[91]

Similar to the 1995 Sarejevo incident, reported analysis of events, along with other supporting evidence, indicated that the incident did not happen as originally reported; this evidence also threw into doubt the identities of the perpetrators of the attack.

In these cases Russia's means of conveying specially prepared information to their opponent (locals, NATO, Europe, and the world) inclined them to voluntarily make the predetermined decision desired by Russia – to have second thoughts about protesting or that there is no Russian military involvement in the Crimea or Eastern Ukraine. Russia's desired action for NATO and Europe was for them to take little or no action. By not acting, they provided Russia freedom of action to pursue their objectives on the ground. How might IO and CO, with the vastly increased speed of movement and penetration into societies, be combined with RC to create dilemmas in future conflicts?

Al-Qaeda and Associated Movements

Following Operation ENDURING FREEDOM in 2001, Al-Qaeda and its Associated Movements (AQAM) moved from planning and training in their strongholds in Afghanistan to a distributed form of distance learning on the World Wide Web. Muaskar al Battar and numerous

other web sites provide support, education, and training that leads to kinetic actions. The Muaskar al Battar web site opens with:

> Oh Mujahid [holy warrior] brother, in order to join the great training camps you don't have to travel to other lands. Alone, in your home or with a group of your brothers, you too can begin to execute the training program. You can all join the Al Battar Training Camp.[92]

The name of this organization is significant in that Al Battar is the sword of the prophets. Swords in general represent prominent themes in Islamic thought. "Swords are seen as noble weapons that embody the purity, nobility, and overall righteousness that is associated with early Islamic heroes and their jihadi campaigns."[93]

> The al-Battar sword was taken by the prophet Muhammad as booty from the Banu Qaynaqa. It is called the "sword of the prophets" and is inscribed in Arabic with the names of David, Solomon, Moses, Aaron, Joshua, Zechariah, John, Jesus, and Muhammad. It also has a drawing of King David when he cut off the head of Goliath to whom this sword had belonged originally. The sword also features an inscription which has been identified as Nabataean writing.[94]

Since its inception Al-Qaeda's on-line training has evolved "to include small unit infantry tactics and intelligence operations such as collecting data, recruiting members of state security services, and setting up phone taps."[95] In May of 2012, news media reported on AQAM's call for cyber attacks against Western nations,

> "Internet piracy is an important field of jihad," the narrator of the video says, according to a translation. He advises followers with expertise to "target the websites and information systems of big companies and government agencies of the countries that attack Muslims." The video calls for cyberattacks against networks such as the electric grid and compares vulnerabilities in the United States' critical cyber networks to the vulnerabilities in the country's aviation system before 9/11, according to a statement Tuesday from the Senate Committee on Homeland Security and Governmental Affairs.[96]

Web sites such as Al Battar, Al-Manar and the manipulation of the Georgian government sites are examples of how cyberspace operations are used to achieve objectives. In the words of Dr. Kuehl, these web sites are using cyberspace in shaping and changing the three dimensions of the information environment. They create information content itself (a Web page), share that content through new forms of connectivity (the Internet links make that Web page accessible to a billion plus people), and affect human interaction and communication. Web sites are a key to the intertwining of cyberspace and human activity in that they represent some of the most prolific ways to influence people to decide and act in ones favor.

The Islamic State in Iraq, Syria, and the Levant – [also known as IS, ISIS and ISIL]

AQAM's use of information warfare can be seen as version 1.0 use of IRCs and IS has created version 2.0. By taking advantage of the increased connectivity and tools to move information to decision makers they are quickly influencing greater numbers of people to decide and act in their favor. A September 2014 Central Intelligence Agency (CIA) report stated that IS, "can muster between 20,000 and 31,500 fighters across Iraq and Syria."[97] This number is between two and three times the estimated strength that was reported just weeks earlier. The foreign fighters come from as many as 80 countries including approximately 2,000 Westerners.[98] Many of these Westerners were pre-teenagers or teenagers on September 11th 2001. Resulting in numerous members having grown up with personal computers, smart phones, and tablets and who are skilled at using social media in achieving personal and group objectives.

The significance of the Westerners is that some bring computer and other science degrees to the fight along with an understanding of Western culture. These are important aspects in appreciating how to use the IE in support of objectives and ends; how to link the right content to the connectivity in order to deliver it to the right human decision–maker. Their content is spread via the connectivity of numerous social media platforms like Twitter, Facebook, and YouTube enabling their propaganda to reach desired target audiences.[99] In addition to the fielded forces there are reports that as of September 2014 there were over 27,000 "pro-ISIS accounts" on Twitter propagating their message.[100]

IS's sophisticated media network combines technology and information content, most often in the form of video images to produce highly effective propaganda. IS uses everything from what appears to be commercially available drones to high quality production facilities to produce and edit specific content. The use of videos is significant in that they are highly emotive and those who view them do not need to know how to read or write in order to decide to act in IS's favor. IS uses organized Twitter hashtag campaigns that are linked to its "one billion campaign" – a calling by radical fundamentalists for support from Muslims around the world to support their cause.[101]

The Caliph of IS is Abu Bakr al-Baghdadi (a nom de guerre).‡‡‡ al-Baghdadi is reported to have a BA, MA, and PhD in Islamic Studies from the Univiersity of Baghdad.[102] His knowledge of the history of Islam is an important part of the content that he presents to the masses. IS's knowledge of the IE allows them to enjoy freedom of action and this presents significant challenges to Western nations attempting to counter IS's message.

In the summer of 2014 the U. S. State Department launched, "a tough and graphic propaganda counteroffensive against the Islamic State, using some of the group's own images of barbaric acts against fellow Muslims to undercut its message."[103] Interestingly IS responded with a form of information jujitsu by calling on YouTube, Facebook, Twitter and others to take down the State Department content as it violated the terms of use agreements not to show graphic violence.[104] Even if the State Department is somewhat successful with these tactics against IS they are still outmaneuvered by the sheer number of IS supporters with social media savvy. The intelligence firm Recorded Future and Sky News found [IS] supporters are creating new accounts almost as soon as their old ones are suspended.[105]

One of the State Department YouTube videos was designed as a fake recruiting ad for the Islamic State.

‡‡‡ Caliph, also spelled calif, Arabic - khalīfah "successor" ruler of the Muslim community. (Encyclopaedia Britannica. http://www.britannica.com/EBchecked/topic/89726/caliph (Accessed December 11, 2014)

> "Run – do not walk to ISIS Land," the video implores viewers. The video tells recruits they can learn "useful new skills" -- like "blowing up mosques" and "crucifying and executing Muslims." Illustrating the sarcastic appeal is an array of bloody images and videos, including of people being crucified, decapitated heads arranged next to each other, and mosques being blown up. The "ad" ends with the line: "Travel is inexpensive, because you won't need a return ticket!"[106]

The main issue with this type of counter messaging is that the people producing it (the U. S. State Department and its contractors) seem to be viewing the problem and solution through Western eyes. Westerners understand and appreciate the sarcasm, but does the intended target audience?

An example of understanding how to use the information environment of the day to inform, persuade, and influence both local and mass audiences in the middle-East comes from T. E. Lawrence's *Seven Pillar of Wisdom*. Lawrence of Arabia[§§§] states,

> The master key of opinion lay in the common language: where also, lay the key of imagination. Moslems whose mother tongue was Arabic looked upon themselves for that reason as a chosen people. Their heritage of the Koran and classical literature held the Arabic speaking peoples together. Patriotism, ordinarily of soil or race, was warped to a language. A second buttress of a polity of Arab motive was the dim glory of the early Khalifate, whose memory endured among the people through centuries of Turkish misgovernment. The accident that these traditions savoured rather of the Arabian Nights than of sheer history maintained the Arab rank and file in their conviction that their past was more splendid than the present of the Ottoman Turk.[107] (Note: *It is interesting that this quote comes from Lawrence's chapter on the towns of Syria*.)

A significant part of Lawrence's success was his ability to use content to propagate the notion of World War I in the middle-East as a peoples war. Lawrence was after all an insurgent, helping the Arabs revolt against the repressive governance of the Ottoman Turks. His understanding of the content and connectivity links, language and printing press (an IRC of the day), were keys to influencing people to decide in his favor. Lawrence cleary understood the value of the moral aspects of war to achieve an emotional response. He also knew the value of the technology of the day to influence a wider audience stating, "The printing press is the greatest weapon in the armoury of the modern commander."[108]

Taking a twenty-first century perspective, David DeWalt the head of Fire Eye Cyber Security warned the West of IS's growing cyber and information warfare capabilities. "Isis has already had success in utilizing technology, using the web for recruiting, distribution of terrorist information and scare tacticts."[109] Their recruitment goals include cyber warriors that have both advanced degrees in computer science and individuals that are skilled in delivering the right content to the right audience. IS's offensive cyber force is led by,

---

[§§§] It is often asked, how did a five and a half foot tall, blonde hair, blue eyed Englishman become Lawrence of Arabia. Part of what gave Lawrence his deep understanding of the people of the Arabian Peninsula was that while studying history at Jesus College, Oxford he undertook a three month walking expedition to learn about Crusader castles in Ottoman Syria. Lawrence traveled over a thousand miles on foot and by horse and donkey living among the people, learning their language and *culture*.

> [A] British hacker known as Abu Hussain Al Britani, whose real name is Junaid Hussein. He fled his hometown of Birmingham for Syria a year ago to join the group and U.S. intelligence sources say he is one of several key recruiters. Al Britani once led a group of teenage British hackers called Team Poison, and now actively calls for computer-literate jihadists to come to Syria and Iraq.[110]

Included in the list of IS members skilled in cyberspace operations is Ahmad Abousamra. Born in France, Abousamra was educated at Northeastern University and the University of Massachusetts, Boston; receiving a degree in Computer Science.[111] Steve Salinksy of the Middle East Media Research Institute reports on their defensive cyberspace operations, "The jihadists are investing a lot in encryption technologies and they have developed their own software to protect their communications and when western agencies work out how to crack them they adapt quickly."[112]

IS's successes on the battlefield and their ability to stand up to and communicate 'directly' with President Obama, Prime Minister Cameron of the United Kingdom, and the people of the world are nearly all high quality video productions. Like Lawrence IS understands their various target audiences and the importance of using IRCs in support of their military objectives and political ends. Al Britani tweeted in September 2014, "You can sit at home and play call of duty (a video game) or you can come here and respond to the real call of duty... the choice is yours."[113] David Carr of the New York Times contends that the video of everything from the events on the battlefield, the brutal beatings and murder of locals, to the beheading of U. S. and British journalists is clearly meant to provoke a reaction from those who see it.[114]

IS's use of the IE and cyberspace operations is refined enough to develop its own Twitter app for Android devices.[115] The app is named *The Dawn of Glad Tidings* (Figure 6), which is in itself an information operation designed to influence people to use it.

Figure 6. The Dawn of Glad Tidings app, developed by ISIS, originally available through the Google Play store, but later removed.[116]

Analysis of the app done by the Citizen Lab at the University of Toronto notes that it is a relatively unsophisticated application; one that simply aggregates pre-existing data streams.[117] While there is no indication of links of the users Twitter account to automatic tweets, the app has

a built in web-based tool that displays information from websites and RSS/Atom feeds. **** [118] At a minimum this improved connectivity enables the users to increase the speed of movement and depth of penetration of their message content into society.

Just as Lawrence understood the importance of Islamic history, represseive governments, and the images of a splendid past, Abu Bakr al-Baghdadi skillfully uses history and morality to stir the emotions of the people who have been repressed by recent masters. When combined with the connectivity and content that social media apps provide their actions can have significant impact on events. IS's actions are highly emotive; they breed everything from successful recruitment and training to action and inaction; many who see the events simply decide not to act against IS out of fear. So how then can the cyber and information savvy forces of IS be countered? Is the best course of action to combat this type of foe with hard power, soft power, or hybrid means?

People's Republic of China (PRC) – Three Warfares

The PRC realized the power of information warfare by watching Operation DESERT STORM play out in the global media.[119] The precise application of U. S. information–based firepower jump started the PRC's move from a mechanized to an informationized force.[120] Since then numerous Chinese authors have written on the importance of utilizing the 'information superhighway' in future conflict. In their influential 2005 document *Warfare Strategy Theory*, Major Generals Peng Guangqian and Yao Youzhi assert that:

> It is necessary to be proficient at utilizing the information superhighway, creating misleading information, spreading the fog of war, and jamming and destroying the enemy's strategic awareness, thereby using strategy to control the adversary. It is necessary to be proficient at using electronic feints, electronic camouflage, electronic jamming, virus attacks, and space satellite jamming and deception leading the enemy to draw the wrong conclusion and attaining the goal of strategic deception. [121]

Chinese IW theory and definitions have evolved rapidly over the last few decades; often feeding off U. S. and Western IW concepts.[122] In nourishing itself off of the West, China has developed a view of IW that sees a credible IW force allowing China to become a threat to more powerful nations.[123] It too looks at how information is used to affect human and automated decision–making. Current PRC thinking describes IW as having six forms: Operational Security, Deception, Computer Network Attack, Electronic Warfare, Intelligence, and Physical Destruction.[124] These are brought together in the construct of Integrated Network Electronic Warfare (INEW) to bridge the gaps between the human and the electronics in IW. In INEW, electronic warfare (EW) disrupts acquiring and forwarding of information and computer network warfare (CNW) disrupts processing and use of information.[125]

Strategically the PRC has adopted a three dimensional concept for fighting information age wars that is not unlike the approach used by Hamas and others unable to compete symmetrically. The Chinese construct is entitled Three Warfares and uses Psychological Warfare, Public Opinion / Media Warfare, and Legal Warfare (or Lawfare) in support of their military objectives and political ends. It is closely linked to Beyond Limits Warfare and relies heavily on presenting

**** RSS/Atom Feeds are web feeds that allow software to check for updates. RSS stands for rich site summary. Atom feeds from Atom Publishing Protocol is a simple HTTP-based protocol for creating and updating web resources. This type of ICT increases the connectivity of the user from one to many.

adversaries or potential adversaries information content so that they may decide in China's favor. The three warfares are broken into the following subsets that rely heavily on IW:

- **Psychological Warfare.** Seeks to influence and/or disrupt an opponent's decision-making capability, to create doubts, foment anti-leadership sentiments, to deceive opponents and to attempt to diminish the will to fight among opponents. It employs diplomatic pressure, rumor, false narratives and harassment to express displeasure, assert hegemony and convey threats. (China's economy is used to particular effect)

- **Public Opinion / Media Warfare.** Is a constant, on-going activity aimed at long-term influence of perceptions and attitudes. It leverages all instruments that inform and influence public opinion including films, television programs, books, the Internet, and the global media network (particularly Xinhua and CCTV)…Media Warfare aims to: preserve friendly morale; generate public support at home and abroad; weaken an enemy's will to fight and alter an enemy's situational assessment.

- **Legal Warfare (or Lawfare).** Exploits the legal system to achieve political or commercial objectives. It has a prominent role in the warfare trilogy. Lawfare has a range of applications. They range from conjuring laws to inform claims to territory and resources, to employing bogus maps to 'justify' claims. In a distorted application of domestic law, for example, Beijing designated the village of Sansha on the Paracel Islands, as a Hainan Prefecture to extend China's administrative writ into the South China Sea.[126]

With a likely goal of denying the U. S. and allied navies access to selected areas of the Western Pacific and the South China Sea China is combining legal warfare with public opinion / psychological warfare to create doubt as to who has the 'legal' ownership of several disputed islands and ilets in the region. By inserting research teams on small land masses or even building light houses on them China stakes claim to them as soverign territory.[127] These claims in turn open the doors for redrawing the international boundaries in the region that impact access to natural resources and the national defense of States in the region. The state–run China News Service is justifying the need to build five lighthouses with safety of navigation; citing the lack of navigational aids and charts in the region.[128] While the current international boundaries remain intact we must ask what impact any new boundaries would have on freedom of navigation of merchant fleets or the freedom of action of navies. If an islet is big enough for a lighthouse could it also house an anti–ship cruise missile battery?

Additionally, China's use of cyberspace centers on computer network exploitation to achieve its national strategic objectives. Their strong reliance on the electromagnetic spectrum defines the essence of Chinese IW. However, the human element of warfare remains equally important. Shen Weiguang, China's "father of information warfare" lists the main tasks of IW as disrupting the enemy's cognitive system and its trust system.[129] In the early 21st century, China has used cyberspace to data mine terabytes of information from U. S. science, technology and military computers. One of the most well known of these cyber incidents is Titan Rain, an attack independently corroborated by other nations. The joint program, Information Warfare Monitor Project, between Canada's University of Toronto and the United Kingdom's Cambridge University, expands on Chinese cyberspace operations:

> The cyber attacks against the U. S. stand out because security researchers have traced them back to the Chinese government. "Normally it is not possible to attribute the source of an attack, because source addresses can be spoofed," says Alan Paller, director of research at the SANS (SysAdmin, Audit, Network, Security) Institute in Bethesda, Md., which trains and certifies technology workers in cyber security. In China's case, though, analysts tracked a series of 2005 cyber assaults against U. S. computers—dubbed "Titan Rain"—to 20 computer workstations in China's Guangdong province, Paller says.[130]

TIME Magazine reported in 2005 that the hackers were "…eager to access American know-how…"[131] The article continued,

> Beyond worries about the sheer quantity of stolen data, a Department of Defense (DOD) alert obtained by TIME raises the concern that Titan Rain could be a point patrol for more serious assaults that could shut down or even take over a number of U. S. military networks.[132]

In April 2009 the Wall Street Journal reported that the U. S. electric grid had been penetrated by cyber spies. "The Chinese have attempted to map our infrastructure, such as the electric grid."[133] The article continued, "Authorities investigating the intrusions have found software tools left behind that could be used to destroy infrastructure components, the senior intelligence official said. He added, "If we go to war with them, they will try to turn them on.""[134]

There are now many organizations at work attempting to understand China's objectives. The Foreign Military Studies Office (FMSO) at Fort Leavenworth, Kansas has been studying China for a while.[135] In *Dragon Bytes–Chinese Information Warfare Theory and Practice*, Thomas quotes from one of the primary Chinese publications - *Information Warfare*.

> There will be point-to-point confrontation between computers as well as theater-to-theater confrontation. There will be wireless confrontation as well as via cables… there will be wartime confrontation as well as confrontation in peacetime. There will be confrontation between military computers as well as between civilian computers.[136]

China's use of cyberspace and information operations has become increasingly pervasive – so much so that it is easy to see the threads in modern Chinese writings of Sun Tzu's strategies of "Know the enemy and know yourself; in a hundred battles you will never be in peril and … those skilled in war subdue the enemy's army without battle."[137] Dr. Rafal Rohozinski, the Principal Investigator, Information Warfare Monitor and the SecDev Group speaking at the April 2009 Information Warfare Conference – InfowarCon stated that 51% of all malware reports back to computers located in China.[138] In his article *China's Electronic Long-Range Reconnaissance*, Thomas discusses China's People's Liberation Army's (PLA) use of electronic stratagems for their computer network operations:

> Computer network operations have become part of the peacetime strategic activities of the PLA. More worrisome is the purpose of these incursions. Is it reconnaissance? Or is the purpose of these incursions to place Trojan horses or some other device into U. S. and other partner systems to disable or destroy them in case of war?[139]

In February 2013 the U. S. based information security company Mandiant published a report "APT1 Exposing One of China's Cyber Espionage Units." (APT is an acronym for the term advanced persistent threat.) Mandiant has been investigating computer security incidents at hundereds of organizations globally since 2004. Their investigations convince Mandiant that the groups conducting these activities are based primarily in China and that the Chinese government is aware of them.[140††††]

The report clealy draws the linkages between what APT1 is doing in and through cyberspace and the other domains and how the actions tie back to specific buildings in China and recognized units of the Peoples Liberation Army (PLA). It states,

> Our analysis has led us to conclude that APT1 is likely government – sponsored and one of the most persistent of China's cyber threat actors. We believe that APT1 is able to wage such a long-running and extensive cyber espionage campaign in large part because it receives direct government support. In seeking to identify the organization behind this activity, our research found that People's Liberation Army (PLA's) Unit 61398 is similar to APT1 in its mission, capabilities, and resources. PLA Unit 61398 is also located in precisely the same area from which APT1 activity appears to originate.[141]

Table 1 is Mandiant's matching of the characteristics between APT1 and Unit 61398.

Characteristic	APT1 (as directly observed)	Unit 61398 (as reported)
Mission area	» Steals intellectual property from English-speaking organizations » Targets strategic emerging industries identified in China's 12th Five Year Plan	» Conducts computer network operations against English-speaking targets
Tools, Tactics, and Procedures (TTPs)	» Organized, funded, disciplined operators with specific targeting objectives and a code of ethics (e.g., we have not witnessed APT1 destroy property or steal money which contrasts most "hackers" and even the most sophisticated organize crime syndicates)	» Conducts military-grade computer network operations
Scale of operations	» Continuously stealing hundreds of terabytes from 141 organizations since at least 2006; simultaneously targeting victims across at least 20 major industries » Size of "hop" infrastructure and continuous malware updates suggest at least dozens (but probably hundreds) of operators with hundreds of support personnel	» As part of the PLA, has the resources (people, money, influence) necessary to orchestrate operation at APT1's scale » Has hundreds, perhaps thousands of people, as suggested by the size for their facilities and position within the PLA
Expertise of Personnel	» English language proficiency » Malware authoring » Computer hacking » Ability to identify data worth stealing in 20 industries	» English language requirements » Operating system internals, digital signal processing, steganography » Recruiting from Chinese technology universities
Location	» APT1 actor used a Shanghai phone number to register email accounts » Two of four "home" Shanghai net blocks are assigned to the Pudong New Area » Systems used by APT1 intruders have Simplified Chinese language settings » An APT1 persona's self-identified location is the Pudong New Area	» Headquarters and other facilities spread throughout the Pudong New Area of Shanghai, China
Infrastructure	» Ready access to four main net blocks in Shanghai, hosted by China Unicom (one of two Tier 1 ISPs in China) » Some use of China Telecom IP addresses (the other Tier 1 ISP)	» Co-building network infrastructure with China Telecom in the name of national Defense

Table 1: Matching Characteristics[142‡‡‡‡]

†††† Their conclusions are based exclusively on unclassified, open source information derived from Mandiant observations. None of the information in this report involves access to or confirmation by classified intelligence.

‡‡‡‡ Readers of this paper are encouraged to read the entire Mandiant report. It may be found at http://intelreport.mandiant.com/. Readers should be aware there have been reports of malware embedded in fraudulent .pdf copies of the report being sent via email and downloaded from other than the Mandiant web site.

Figure 7 below is a representation of Unit 61398's position within the PLA. It provides insight into how the PLA views command and control (C2) of their cyber forces. The image shows the linkages to the signals intelligence (SIGINT), computer network operations (CNO), including various bureaus and research institutes for cyberspace operations. It also highlights traditional military elements of operations and intelligence, along with relationships to their Services. C2 will be discussed later as a joint function.

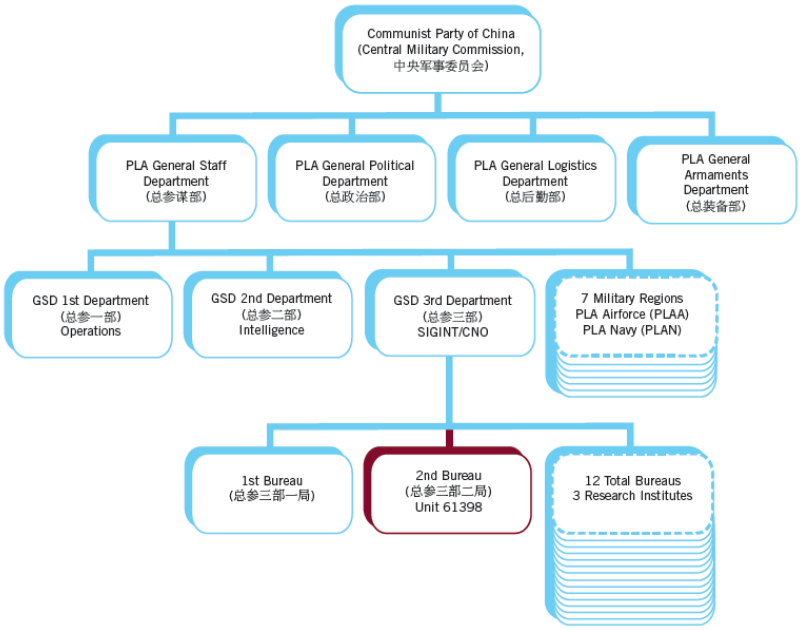


Figure 7. Unit 61398's Position within the PLA[143]

While the U. S. and other nations face many and varied APTs, Mandiant's report clearly lays out how a potential future adversay has been stealing terabytes of science, technology, engineering, and math (STEM) information and intellectual property for years. The prudent military leader and planner has to think how the theft of this vast amount of information will affect future conflict with the nation that stole the information from them *and* their allies.

Privateers and Information Currency

The issue of attribution for cyberspace operations presents challenges for governments and militaries. Direct linkages to nation states and non-state actors believed to be conducting espionage and more are often difficult to prove due to the ubiquitous nature of human activities in cyberspace. Many cyber analysts feel that nation states are now making attacks even more difficult to track by the practice of issuing 'letters of marque' to individuals and groups, who then act on behalf of the nation state.[144] These cyberspace privateers use their personal computers to navigate the domain and are 'authorized' by the nation states to perform functions necessary to those nations' interests.

Information is a currency. Information resident in the electronics, computers, and smart phones of the twenty–first century is just as important today as the information needed by the Soviet Union to run its industrial control systems was in the early 1980s. While privateers of old were allowed to keep a percentage of the booty taken from enemy ships captured at sea, the

twenty–first century prize and booty consist of access to computers and their resident information. Nation states are often looking to obtain military and STEM information. The privateers utilize computer network operations (exploitation and attack) to access that information. Information not deemed valuable enough for a nation state to process and utilize for its own gain can easily be left as booty for the cyberspace privateers. Examples of privateer booty are identity or financial information such as social security or credit card numbers. This type of information has value; it can be sold to organized criminals who can use it to create fraudulent identities or fake credit cards.

What are the relationships between privateers, criminal networks, and nations? Whether it is a non-state adversary like Al-Qaeda, groups that provide state-like functions such as Hizballah, ones with the desire to become states as in ISIS, or nation states as China and Russia, the future is bright for those who can successfully use the IE and cyberspace operations in support of achieving objectives in the physical domains.

The Information Environment and Cyberspace Operations to Radicalize and Terrorize

The IE and cyberspace allows groups and individuals to reach out and influence global audiences. As discussed earlier, much of the connectivity, content, and cognition for the attacks are focused on propagating ideology, recruiting, training, and terrorizing. We have seen content in the form of on-line magazines like *Inspire* (the English language magazine produced by Al Qaeda) and social media networks like Twitter, Facebook, Instagram, and Tumblr all used in support of objectives and political ends.

When acts of terror are committed by individuals or small groups upon a state the perpetrators are often said to be lone wolves or self radicalized. In the interconnected world of the early twenty-first century is it realistic to believe that individuals or small groups are sitting around developing their ideology from books? Or is it more likely they are viewing content produced by a larger group with specific goals; with content moved globally through the dimensions of the IE to electronics and humans? In the first decade plus of this century many of the perpetrators of individual and small group acts of terror had connections to authority figures, access to emotional content, or received on–line training that either enabled or enhanced their horrific acts.

Major Nidal Hasan, a U. S. Army psychiatrist was convicted of the murdering 13 and injuring more than 30 soldiers and Department of Defense Policemen on November 5th 2009 at Fort Hood, Texas. Hasan is on record with a series of e–mails to the now dead radical cleric, Anwar al–Awlaki seeking approval for his future actions.[145] On April 15, 2013 the Tsarnaev Brothers murdered 3 and injured more than 250 while terrorizing spectators and participants at the Boston Marathon finish line. Their weapons of choice were pressure cooker bombs that they learned to build in part by reading Al–Qaeda's on–line magazine *Inspire*.[146] On September 29, 2014 Alton Nolen murdered and beheaded a 54 year old woman at Vaughan Foods in Moore, Oklahoma. The Washington Post reported, "His [Nolen's] Facebook page — which a federal law enforcement official described to The Washington Post as "provocative" — featured, among other things, a photo of Osama bin Laden."[147]

How might terror attacks be combined with other means and modes in future conflict? An IS trained and funded offensive cyberspace operation to take down a SCADA grid on critical infrastructure? What dilemmas would this combination of means and modes create for those being attacked? The 9/11 Commission Report found that one of the biggest failures prior to the attacks on September 11th 2001 was the U. S. government's failure to imagine the possibility of such attacks.[148]

Operational Art

Operational Art (Op Art) is about achieving efficiencies – sound application saves blood and treasure. The challenge of understanding this global domain and what it means to military leaders and planners can be aided by embedding the events that happen in cyberspace in the context of Op Art. The study of the operational art of war can and should take time. Volumes have been written on the art of warfare. Sun Tzu's *Art of War*, Clausewitz's magnum opus *On War,* and Vego's tome *Joint Operational Warfare–Theory and Practice* are but a few of the great works that investigate and analyze operational art. Op Art is "…the field of study that orchestrates all available sources of military and nonmilitary power in order to accomplish the ultimate strategic or operational objective."[149]

Op Art begins with basic questions: What are the objectives of the person or people conducting operations? What effects are they trying to achieve? Op Art can be broken into smaller parts in order to build an 'operational' picture. For the purposes of this paper, the discussion of Op Art will be confined to the elements of operational factors and joint functions. These elements include the factors of space, time, and force and the joint functions: command and control, intelligence, fires, movement and maneuver, protection, and sustainment.[150] Vego states, "For maximum effectiveness in the employment of one's combat forces, a number of supporting structures and activities, arbitrarily called "functions," should be fully organized and developed."[151] It should be noted that U. S. Joint doctrine and Vego differ slightly on what elements should be included as operational functions.[152] However, Vego goes on to say, "The list of what constitutes an operational function should not be considered something unchangeable."[153]

In his 1989 article *The Loose Marble–and the Origins of Operational Art*, James Schneider states, "The Hallmark of operational art is the integration of the temporally and the spatially distributed operations into one coherent whole."[154] He goes on to say that the two characteristics at the heart of operational art are simultaneous and successive operations.[155] The ubiquitous nature of cyberspace and its nearly limitless movement it gives to information means that operational art can aid in understanding both information operations and cyberspace operations.

Cyberspace is unique in that it provides the avenue for huge amounts of data and information to cross all levels of war from the tactical to the strategic and to move from one domain to another – nearly instantaneously. Additionally, many militaries and governments are so reliant on cyberspace to move military information that they will be challenged to employ joint functions without freedom of action in the domain. Movement in cyberspace is not constrained by the traditional physical actions normally considered by humans. This speed and unrestricted movement requires the military commander to seriously consider the relationship between the operational factors of time, space and force, and how the factors affect the joint functions.

Nimitz and Nelson

Admirals Nimitz and Nelson displayed an intuitive understanding of operational art. Each achieved great success only after he had studied his profession of arms and planned for multiple contingencies. The following examples show why our military should study the cyberspace domain in the context of operational art.

Much has been written about Operation GRANITE, Admiral Nimitz's island hopping campaign through the Central Pacific. Operation GRANITE, a series of opposed amphibious landings and battles, was a component of the U. S. efforts that led to the unconditional surrender

of Japan. An understanding of the manner in which U. S. and allied forces successfully defeated the Japanese serves as an in depth study of operational art.

Nimitz displayed his knowledge of operational factors and functions in many ways: bypassing certain islands to offset a temporal disadvantage, having the right forces to attack, conducting operational fires in the bombing of the Japanese long range aircraft on Formosa, organizing the logistics necessary to support mobile forces, and combining the command organization of 3rd and 5th Fleets-one conducting planning and one conducting operations (the key to maintaining tempo and keeping the Japanese off balance) were all part of the successful employment of operational art.

Suffice it to say Admiral Nimitz understood the factors of space, time, and force and balanced the use of functions to achieve success. He did not have to think differently about operations because his ships were steam vice sail powered, or because he had carrier based aviation and amphibian tractors to project force instead of cannon and Royal Marines in longboats. Nimitz's ability to achieve victory through the balancing of operational factors and functions came in part from his year at the Naval War College. In a letter written to the President of the War College forty years after his attendance, he said:

> The enemy of our games was always–Japan–and the courses were so thorough that after the start of WWII – nothing that happened in the Pacific was strange or unexpected. Each student was required to plan logistic support for an advance across the Pacific – and we were well prepared for the fantastic logistic efforts required to support the operations of war…I credit the Naval War College for success [as] I achieved in strategy & tactics both in peace & war.[156]

When speaking of Nelson's great victories, his ability to lead and achieve decisive victories is most often mentioned. Both leadership and experience are major parts of what make up the ability to "think operationally." Geoffrey Till discussing an operational approach to securing command of the seas, states, "Although we tend to focus on Nelson's tactical conduct *at* the Battles of the Nile or Trafalgar, his ultimate operational skill lay less in that than in the successful campaigns he had conducted *beforehand* to ensure that those battles were indeed fought and conducted under favourable conditions."[157]

The Royal Navy's *Fighting Instructions* of the day were focused on fighting an enemy at long range utilizing their superior cannon and strict operational command. This often led to indecisive battles. Geoffrey Till's *beforehand* refers to Nelson's many victories and in part to the winter and spring of 1805 Nelson spent chasing his opponent across the Atlantic and back. During this time Nelson refined both his skills and operational thinking.

In May 1805, Nelson published his own *Instructions,* which led ultimately to the document that became known as his "Trafalgar Memorandum." The Trafalgar Memorandum lays out Nelson's understanding of the operational factors at hand and how he envisioned operational command. The most significant change to *Fighting Instructions* comes from what has been labeled as the 'Nelson's Touch'. "Captains are to look to their particular line as their rallying point. But in case signals can neither be seen nor perfectly understood, no Captain can do very wrong if he places his ship alongside that of an enemy."[158] When Nelson's instructions were disseminated to his Captains, he wrote: "When I came to explain to them the *Nelson touch,* it was like an electric shock. Some shed tears, all approved –'It was new – it was singular – it was

simple! And from admiral downward, it was repeated – It must succeed, if ever they will allow us to get at them.'"[159]

Like Nimitz, Nelson displayed his understanding of operational factors and functions in various ways. Upon arrival off the Spanish coast on 14 September 1805, he found the opposing fleet in the port of Cadiz. Knowing that winter and foul weather would soon approach, Nelson instructed his larger ships of the line to remain out of sight and his smaller faster frigates to move in close. The purpose was to collect intelligence and to entice the combined French and Spanish fleets to come out and fight. Nelson's operational movement and maneuver and deception worked and the combined fleets sailed 20 October. As the battle approached, Nelson knew that command and control would be nearly nonexistent once the enemy was engaged. He instructed the now famous signal to be hoisted, "England expects every man to do his duty." The Battle of Trafalgar took place the 21st of October. The combination of the Trafalgar Memorandum and the signal flags became Nelson's command and control of the fleet. In an official dispatch following the battle, Admiral Collingwood, who took command of the battle when Nelson was mortally wounded stated, "as the mode of attack had been previously determined on and communicated to flag-officers and captains, few signals were necessary."[160] Clearly Nelson's ultimate operational skill off Cape Trafalgar in October 1805 was in part due to his understanding and employment of what would become known as operational art.

Thoughts on Operational Art Cyberspace Operations and Information Operations

The DoD Strategy for Operating in Cyberspace states that, "DoD will treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential."[161] Some of the challenges that the DoD face begin with how operational commanders will need to think about cyberspace operations; knowing where and how the cyberspace operations are being used. For example, when a bomb falls on a target, did it come from a manned aircraft or a UAS – did the attacker employ cyber capabilities to achieve the objective? If a UAS was used could it have been interdicted by using CO to attack the links between the vehicle and the controller? What are the objectives of the cyberspace operation? Are they physical or cognitive objectives? Are the objectives nested and do they support the commander's objectives and mission? Is the right tactical force in place to attack the EMS and does the commander have the authority to exercise control of it? If the adversary has disrupted the EMS – can you still use it? Operational Art is the bridge between strategy and tactics. It gives the commander a framework to begin understanding the complexities of war. By understanding these complexities the U. S. Service chiefs and the operational commanders will better understand how to organize, train, and equip the force and employ it. Operational Art begins with understanding the relationship between factors and functions. The importance is emphasized by Vego, "A commander's need to fully understand the factors of space, time, and force and then to balance them against the objective is as old as warfare itself."[162]

Operational commanders – combatant commanders and their subordinate joint force commanders do not fight with tactical units, they fight with operational factors and joint functions. Commanders must balance operational factors and joint functions to get the tactical forces in place so they can fight and win. The relationship between factors and functions is important in that if a commander has a disadvantage in one, strengths from the others must be utilized to overcome that disadvantage; equally, if the commander has an advantage in one, that advantage must be utilized to achieve victory.[163]

Operational Factors

Given the examples of Admiral Nimitz and Admiral Nelson, a review of cyberspace in the context of operational art is relevant. A comparison of the fastest ship (approximately 35 knots) and the fastest plane (flies mach 3+ (~2200 mph at sea level)) with digital information (moving via electromagnetic radiation at nearly 670 million miles per hour (or 186,000 miles per second)) shows the true global nature of cyberspace. The military commander must understand the relationships of time, space, and force when conducting operations in his area of responsibility. A brief discussion of cyberspace as seen through the lens of the operational factors follows.

Time –There is no set time, as we know it, for cyberspace. Content and code moving through cyberspace travels at approximately the speed of light. A digital message, images, or malware can move around the world nearly instantaneously.

Space – Cyberspace is all around us – it is truly a global domain. The nodes made up by electronics exist in the four traditional domains. Representative examples include: servers, computers, cellphone towers, and power plants on land; planes, radars, UASs in the air; ships, radars, missile defense ships at sea; and satellites in space. Traditional lines of operation are blurred when messages covertly hosted on a server in Texas are read in the Middle East. These messages then influence people to act. VoIP companies in the U. S. unwittingly provide C2 networks for non-state actors and nation states wanting to harm U. S. forces.

The concept of Cyber–Key Terrain (C–KT) was brought up in the CYBER FLAG 15-1 War Game conducted by the U. S. military.[164] Key Terrain is defined in U.S. joint doctrine as, "Any locality, or area, the seizure or retention of which affords a marked advantage to either combatant."[165] While there is no current joint definition of C–KT, the concept was used in CYBER FLAG 15-1 to shape discussions concerning both offensive and defensive cyberspace activities. As would be natural for practitioners of operational art the discussions on the operational factor space during the game were directly related to the joint functions that will be addressed below.[166]

Force – Force can be tangible and intangible and vary from lethal to psychological; it can affect both human and automated decision making. Information (content and code) are forces that affect human and automated decision–making in nearly all aspects of modern warfare. Information content – often in the form of video is sent around the world with the objective of getting individuals to act in specific ways. The commander must balance information force within the operational factors space (physical and cyber), other forms of force (lethal), and time to get tactical forces in place to fight and win. Information must be balanced with the joint functions in that functional and component commanders all require information to move across the operating environment in order to successfully achieve their objectives.

David defeated Goliath with an asymmetric attack. A single hacker or Bot Herder can coordinate thousands of computers to accomplish millions of actions in a cyber–attack. A belligerent or privateer with a personal computer can obtain corporate or military information or worse shut down a SCADA power grid, which could result in death. And an adversary can send an emotive video from anywhere in the world that drives prople to act.

Content and code projected through cyberspace to the physical spaces affects human and automated decision making. As discussed earlier code can get electronics to act independent of

the owner's intent and destroy machines. Content can get humans to act; "Join the great patriotic hackers to attack the Republic of Georgia, download the code and your PC can become a Bot," was the battle cry of Russian 'cyber minute men' in 2008. They proved a single Bot Herder can control thousands of computers that execute billions of actions. And ISIS tripled their forces in a few weeks by delivering the right content to decision–makers.

Stuxnet is the name of the much publicized malware that attacked Iranian nuclear processing facilities beginning in 2010. By targeting the program logic controllers (PLC) of the nuclear centrifuges it was designed to overspeed the units and cause the fast spinning machines to tear themselves apart.[167] In reality it had realitively minor effects on production with estimates damage estimates ranging from 15 to 20 percent of its target. The most significant factor is that the malware affected both human and automated decision making in that it made the equipment produce substandard material and destroy machinery while giving signals (content) to the human operators that all was working well. How will Stuxnet type force be adapted to operational warfare? How will the forces of content and code be delivered to the tactical force? Will it be delivered via the Internet or some form of removable media? What is the relationship between the weapon and the human? Is there a need for humans to be part of the tactical force in place or will it all be done remotely?

How does the operational commander utilize cyberspace and the IE to get his message out in countering an insurgency or Humanitarian Assistance / Disaster Relief Operations? In an early 19th century example of commander understanding the IE, when he felt his story was not being told 'correctly', Napoleon formed or took control of various newspapers that then presented his side of the story.[§§§§] In recognizing the links between connectivity, content and congnition, Napoleon was reputed to have said, "Four hostile newspapers are to be feared more than a thousand bayonets."

Joint Functions - (Joint Publication 3-0)

Cyberspace and its ability to empower information to reach billions of people and electronics will increasingly add to the complexity of modern warfare. The increased complexity can be mitigated by understanding how CO and IO impact the joint functions when temporally and spatially integrating distributed operations. Vego provides keen insight into the importance of operational functions. "The operational commander is responsible for properly sequencing and synchronizing not only joint forces but also operational functions, prior to and in the course of a campaign or major operation."[168] In early 21st century warfare the manner in which the commander thinks about, sequences, and synchronizes the operational functions with respect to cyberspace and the traditional domains of war will be crucial to success. This should begin with determining what is the right structure for establishing the chain of command and its supporting and supported relationships within a command or force – this is known as command organization and is a key prerequisite for effective command and control (C2).[169]

[§§§§] Napoleon accomplished this by establishing (or achieving control of) six newspapers: the *Journal de général Bonaparte et des hommes vertueux*, the *Courrier de l'Armée d'Italie*, and *La France vue de l'Armée d'Italie*, in 1797, and the *Journal de Malte*, the *Courier de l'Égypte*, and *La Décade Égyptienne* in 1798. http://www.gutenberg-e.org/haw01/frames/fhaw03.html (Accessed 20 Nov 2008)

> The term *command organization refers to both the physical and human elements of the* military organization established to ensure the most effective employment of one's forces for accomplishing the assigned military objective(s). Sound command organization should allow the individual commander to continuously monitor the situation within his area of responsibility plus his area of interest. It should provide a high degree of flexibility in meeting unexpected changes in the situation. It should also provide for the rapid communication of directives in a clear and concise manner. A sound command organization should be flexible, cohesive, and resilient.[170] [Emphasis added]

The DoD is currently attempting to determine the right command organization for the C2 of its cyber forces. While much of the physical and human elements of the relationships between USSTRATCOM and USCYBERCOM are delineated in U. S. law the command relationships between USCYBERCOM the combatant commanders and their ability to C2 cyber forces are not as clear.

Command and Control – The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.[171]

The foundation for all command and control (C2) is the authority to command the force; it comes from both law and position.[172] Law provides the official power to act, yet history shows us that this is not always sufficient to achieve results. Responsibility (also known as accountability) is the natural partner of authority to achieve sound C2.[173] The ability to actually arrange personnel, equipment, communications, and facilities in a complex multi-domain battlefield is challenging at best. Effective C2 is about getting the right information to the right decision–maker at the right time in order to make sound decisions.[174] Today that information moves almost exclusively through cyberspace and the electronics necessary to both communicate and operate many weapons systems.

There are several challenges to effective C2 of both cyber and other forces in conducting cyberspace operations (DODIN, DCO, and OCO). The first is that there is a near total reliance on cyberspace to communicate; move information to decision makers across all levels of war. This challenge to C2 is underpinned by the fact that many of the networks and nodes that are used to communicate and move data are not solely government / DoD owned or operated. Physical control of these is often leased to the government or there is some form of public / private partnership (PPP). The PPP constructs are cost effective for the DoD, but with the cost savings comes risks that the communication networks are accessed by potential adversaries and are not as resilient as traditional weapons systems. Additionally within a JFCs theater of operations, area of operations (AOR), or joint operations area (JOA) there may be multiple DoD networks with multiple "owners," many with confusing operational interdependencies.[*****]

[*****] This is where the combat support agency, Defense Information Systems Agency (DISA) and the joint information environment (JIE) come into play. The JIE is the planned communication architecture that will optimize DoD's ICT assets by converging communications, computing, and enterprise services into a single joint

In these cases no one military commander may have command authority over the network; yet it may be required to control the forces. While the DoD has developed processes and agreements to work with sister services and corporations that move information (i.e. Inmarsat™ and commercial carriers that use Super High Frequency (SHF) communications) these connectivity points generally have a limited number of controlled users when compared to the billions of users of the Internet.

Another challenge is that currently the authority to conduct many cyberspace operations are often held at the highest levels of command. Largely due to the sensitivities associated with OCO and their potential to have unintended effects, many of the release authorities for OCO are not available to tactical and operational commanders. This policy begs the questions: Will joint force commanders (JFCs) in future conflicts need to employ cyber forces differently from the ways they employ land, maritime, air, and space forces? If indeed operational warfare is about the JFC balancing operational factors and joint functions to get the tactical forces in place so they can fight and win, should JFCs have operational control of cyber forces or should they be supported by some sort of element out of USCYBERCOM with different authorities?

With the myriad of actors and their interests in cyberspace should commanders expect to have unity of command of cyber forces?[†††††] What are the challenges to employing the concept of unity of effort[‡‡‡‡‡] for the C2 of cyber assets and forces? Unity of effort may work in coordinating the non-DOD owned and operated networks and nodes of the telecommunication companies and the defense industrial base, but how can coordination and cooperation be achieve when the connectivity exists in nations outside of the United States – with friends, allies, neutrals, and potential enemies?

The 2013 Joint Doctrine for Cyberspace Operations describes the cyberspace command and control organization for each combatant command (CCMD) as having Joint Cyberspace Center (JCC), see Figure 8 below. The CCMD will have combatant command (COCOM) of the JCC.[§§§§§] It is planned that the JCC will be supported by a Cyber Support Element (CSE) from USCYBERCOM. The JCC will have administrative control (ADCON) over the CSE and operational control (OPCON) of the Joint Task Force [Cyber].[******] The CCDR will have

---

platform to be used by all Departments. While DISA purports that the JIE will solve these problems, a working secure JIE is not yet operational.

[†††††] The operation of all forces under a single responsible commander who has the requisite authority to direct and employ those forces in pursuit of a common purpose. (Joint Pub 3-0, *Operations*). It is one of the chief tenets of C2 of forces in the physical domains.

[‡‡‡‡‡] Coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization, which is the product of successful unified action. (Joint Pub 1, *Doctrine for the Armed Forces of the United States*, 25 March 2013)

[§§§§§] *Combatant Command* (COCOM) is the nontransferable command authority established by Title 10, United States Code (USC), Section 164, exercised only by commanders of unified or specified CCMDs unless otherwise directed by the President or SecDef. COCOM, which cannot be delegated, is the authority of a CCDR to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. (Joint Publication 3-0 *Operations*, III-4).

[******] *Administrative Control* (ADCON) is defined as direction or exercise of authority over subordinate or other organizations in respect to administration and support (Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 3). *Operational Control* (OPCON) is command authority that may be exercised by commanders at any echelon at or below the level of CCMD to perform those functions of command

COCOM of the JCC, JTF [Cyber] for contingency operations, the theater network coordination center (TNCC) and the component commands. There will be supporting relationships with the combat support agencies (CSA) National Security Agency (NSA), Defense Information Systems Agency (DISA), Defense Intelligence Agency, National Geospatial–Intelligence Agency (NGA), etc. CSE personnel support and expertise will come from the Service Cyber Commands—Commander Tenth Fleet, Fleet Cyber Command (FLTCY); Second Army, Army Cyber Command (ARCY); Twenty-Fourth Air Force, Air Force Cyber Command (AFCY); and Marine Forces Cyber Command (MAR4CY). Additional cyberspace support will come from the Defense Information Systems Agency (DISA) and its DISA Network Centers (DNC) and Theater Net Ops Control Centers (TNCC) via the new directive authority for cyberspace operations (DACO). DACO provides DISA the authority over all of DODIN for operations guidance and defense as well as the ability to issue orders to anyone in the DODIN, including elements such as the services.[175] The joint doctrine cyberspace command and control construct has a JTF as the primary OCO element.[††††††] It is heavily weighted towards steady-state operations that are focused on the various forms of DCO discussed earlier (see Figure 2).

over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. OPCON includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. This authority should be exercised through the commanders of subordinate organizations, normally through subordinate JFCs and Service and/or functional component commanders. OPCON normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions; it does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training (Joint Publication 3-0 *Operations*, III-4).

[††††††] A JTF is a joint force that is constituted and so designated by SecDef, a CCDR, a subordinate unified command commander, or an existing commander, joint task force (CJTF) to accomplish missions with specific, limited objectives and which do not require centralized control of logistics." (Joint Publication (JP) 3-0, IV-7) In future conflict certain CO may be missions with specific, limited objectives, however, the many and varied uses of cyberspace operations to achieve objectives and ends by both state and non – state actors described in this primer mean that all forces and components will likely need to employ full spectrum DCO and OCO in support of their objectives.

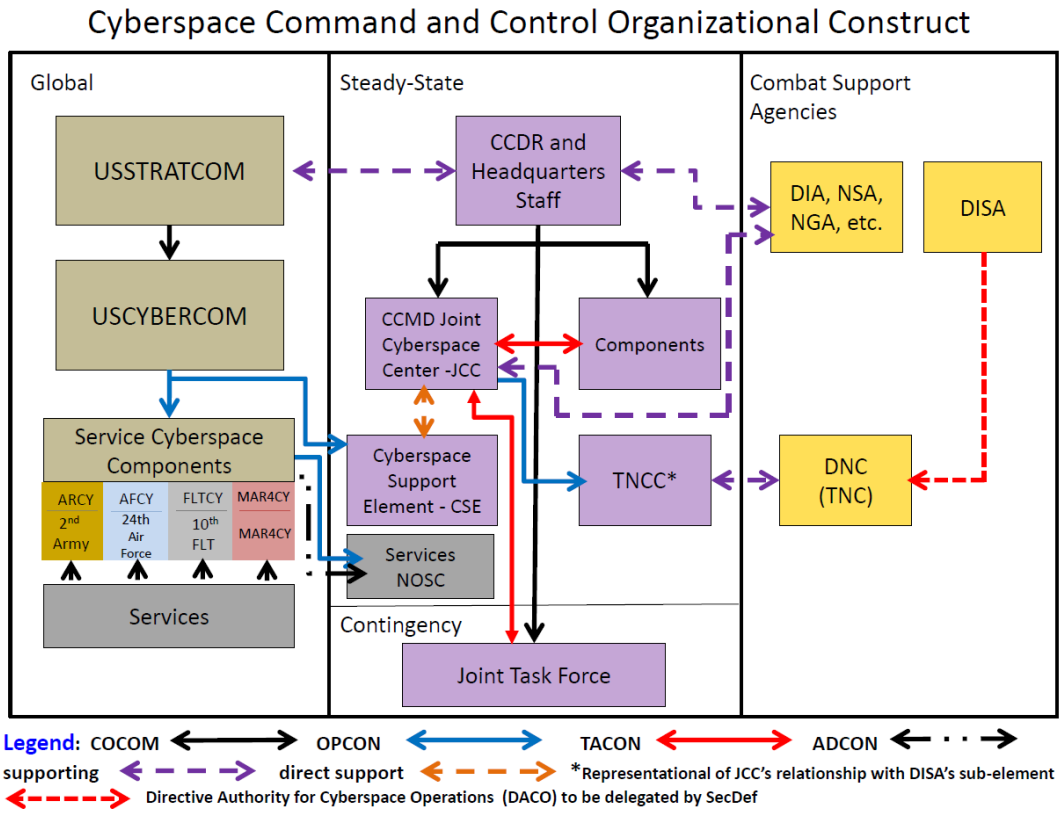


Figure 8. Cyberspace Command and Control Organizational Construct - Joint Publication 3-12R *Cyberspace Operations*, 5 February 2013[176]

An alternative Cyberspace C2 model was put forth by USCYBERCOM that presents a more balanced use of both DCO and OCO giving CCDRs and JFCs and their components more access to cyber forces; see Figure 9. This C2 construct has each CCMD forming a Joint Force Cyber Component Commander (JFCCC) as the primary OCO element.[‡‡‡‡‡‡] The CCMD will have combatant command (COCOM) of the JFCCC. The JFCCC will be on par with the other component commanders. The CSE from USCYBERCOM will support the JFCCC similarly to the way they support the JCC. This model has a more robust CSE which is planned to make up a cyber combat mission force (CCMF). The mission of the CCMF is to develop and employ, on order, offensive cyber capabilities to achieve – or directly support the achievement of – CCMD objectives during OPLAN execution; integrated synchronized and /or deconflicted with fires in other domains (Air, Land, Maritime).[177]

[‡‡‡‡‡‡] The JFC can establish functional component commands to conduct operations when forces from two or more Services must operate in the same physical domain or accomplish a distinct aspect of the assigned mission. These conditions apply when the scope of operations requires that the similar capabilities and functions of forces from more than one Service be directed toward closely related objectives and unity of command is a primary consideration. For example, functionally oriented components are useful when the scope of operations is large and the JFC's attention must be divided between major operations or phases of operations that are functionally dominated. (Joint Publication (JP) 3-0, IV-8)

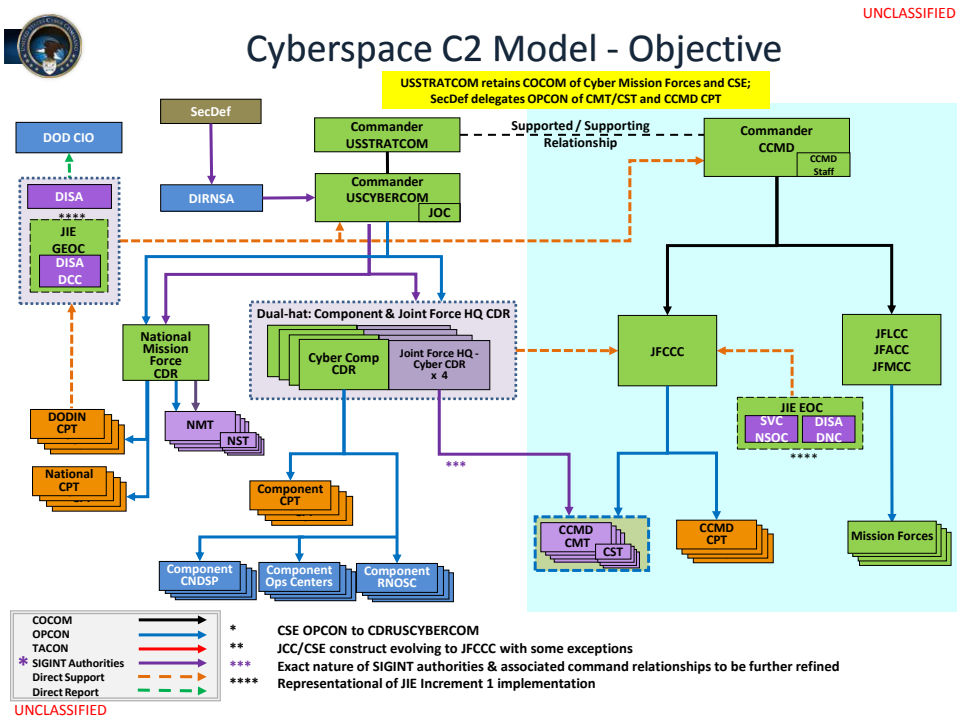


Figure 9. Cyberspace Command and Control (C2) Model – Objective – Deputy Commander US Cyber Command brief 12 November 2013[178]

This objective model has various cyber forces delineated to perform both defensive and offensive cyberspace operations. The cyber protection teams (CPTs) perform DCO and the cyber mission teams (CMTs) and cyber support teams (CSTs) perform OCO. The Secretary of Defense will delegate OPCON of the CCMD CPTs, CMTs, and CSTs as necessary.

Both of these C2 models are positive signs that the DoD is struggling with Vego's concept of the right physical and human elements of the military organization established to ensure the most effective employment of one's forces for accomplishing the assigned military objective(s).[179] So what then is the best command organization and way to C2 cyber forces for combatant commanders and joint force commanders to successfully fight and win future wars? Some issues that need to be addresses relate to the authority and accountability of cyber forces with respect to the integration of the CMTs, CSTs, and CPTs with other component forces. Will they be OPCON to the JFC's component commander the way Radio Battalions and Electronic Warfare (EW) assets were OPCON to tactical units providing the SIGINT that enabled freedom of action in past wars? Or will OPCON be exercised by a contingency JTF from the CCDR Headquarters or even USCYBERCOM at Fort Meade, Maryland?

Intelligence (Intel) – Is defined as, "The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations."[180] What does a commander do when his Special Forces team is conducting strategic reconnaissance and he cannot communicate with them via cyberspace? How much 'secure' information is stored on a computer or moved through cyberspace? How much knowledge about

you has your adversary gained by observation, investigation, analysis, and understanding via cyberspace? What role will cyberspace ISR play in operations? Cyberspace ISR are intelligence actions conducted by the JFC authorized by an execute order (EXORD) or conducted by attached SIGINT units under temporary delegated SIGINT operational tasking authority.[181] Traditionally these activities are conducted in cyberspace to gain intelligence required to support future operations, including OCO or DCO.[182] In today's interconnected world these activities are often required to synchronize and integrate the planning and operations across the all levels of war. Because of the various combat support agencies and interagency actors operating in cyberspace, cyberspace ISR requires both detailed deconfliction, and cyberspace forces that are trained and certified to a common standard with the intelligence community (IC).[183]

Fires – U. S. Joint doctrine defines fires as, "The use of weapon systems to create specific lethal or nonlethal effects on a target."[184] Cyberspace operations are fires. Fires can be employed at all three levels of war strategic, operational, and tactical. Operational fires are designed to get an adversary to react operationally. The concept of strategic fires has not been discussed much outside of the employment of nuclear weapons. Strategic fires are traditionally executed by the highest levels of command. Stuxnet can be seen as strategic fires; fires that are designed to get an adversary to react strategically. It is one of the first acknowledgements that code as force can be used to destroy national assets and impact a nations strategic goals. Cyberspace allows for OCO to create specific lethal and non-lethal effects across all levels of war. Military Information Support Operations (MISO), Military Deception (MILDEC), and Strategic Communication (SC) are traditional IRCs that can be greatly enhanced when cyber enabled.[§§§§§§] The speed of movement and depth of penetration provided by cyberspace empower these IRCs to reach more audiences and specific decision makers – creating nonlethal effects. How will these types of fires play out in future operational and tactical environments from both an offensive and defensive perspective? How will cyberspace operations be used to get an adversary to react operationally?

Movement and Maneuver – "Encompasses the disposition of joint forces to conduct operations by securing positional advantages before and during combat operations and by exploiting tactical success to achieve operational and strategic objectives. This function includes moving or deploying forces into an operational area and maneuvering them to operational depths for offensive and defensive purposes. It also includes assuring the mobility of friendly forces."[185] What is the C–KT that will be moved to and maneuvered through in support of the commander's objectives? In a disturbed or disrupted electromagnetic environment, how do you navigate at sea or in the desert if GPS does not work? How does the fact that the U. S. military uses unclassified, commercial off-the-shelf software, similar to FEDEX and UPS, in tracking global

[§§§§§§] MISO – Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives. MILDEC – Actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. SC – Focused United States Government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of United States Government interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power. (JP 1-02)

shipments of military cargo affect the Time Phased Force Deployment Data (TPFDD) and receipt of cargo at a Seaport of Debarkation (SPOD) or Airport of Debarkation (APOD)? What decisions must the commander make if he is told by his U. S. Transportation Command (TRANSCOM) Liaison Officer (LNO) that significant parts of his combat power has been sent to the wrong SPOD by a hacker accessing USTRANSCOM computers? [*******]

Sustainment – The provision of logistics and personnel services required to maintain and prolong operations until successful mission accomplishment.[186] USTRANSCOM relies almost exclusively on cyberspace to know where its cargo is and when it will arrive. USTRANSCOM's Automated Identification Technology & In-Transit Visibility (AIT & ITV) branch is the Distribution Process Owner (DPO) tasked with ensuring these technologies are synchronized throughout the DoD supply chain to enhance asset visibility and maximize deployment and distribution operational efficiencies.[187] AIT and ITV are linked in various ways to the communication networks of commercial shipping companies. Can the Combatant Commander's Deployment and Distribution Operations Center (DDOC) track beans, bullets and black oil if it's or the commercial shippers networks are infected with malware? Additionally, if an operational commander is responsible for the resupply of beans, bullets, and fuel of his tactical forces, what does the resupply of tactical cyber forces look like? Will electricity in some form be the fuel and code be the bullets that needs to be provided so the tactical forces can fight and win? How do you resupply and repair your cyber forces in the middle of a war? Can new content and code be moved forward when cyberspace is disputed or denied?

Protection – Is the preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area.[188] How does a commander need to think about protecting his military and non-military sources of power? How do you protect your force when the enemy is using a C2 node halfway around the world and the combat power (the information) moving through it moves 25,000 miles in nanoseconds? How do you neutralize the communication or C2 node in New Jersey or Texas? One of the strengths of the U. S. military is its ability to utilize cyberspace to integrate information (via technology) and move it to our decision makers faster and more securely than our adversary. Can the data resident in our computer systems be manipulated by outside sources? What happens when our decisions are delayed or we can no longer use the technological advantage we rely on? What happens when a previously low tech adversary gets UASs and precision guided munitions (PGMs) and uses them to collect intelligence or attack? What about hackers gaining access to .mil web sites? Would it be useful to know what types of training manuals (i.e. explosives or biological warfare) people are reading about in the region to which you are deploying? How are Radio Controlled Improvised Explosive Devices (RCIED) being set off?

[*******] USTRANSCOM is a functional combatant commander whose mission is: Develop and direct the Joint Deployment and Distribution Enterprise to globally project strategic national security capabilities; accurately sense the operating environment; provide end-to-end distribution process visibility; and responsive support of joint, U. S. government and Secretary of Defense-approved multinational and non-governmental logistical requirements. Federal Express (FEDEX) and United Parcel Service (UPS) are commercial cargo and package shippers that pioneered the use of the internet to track the global movement of their cargo. They rely heavily on digital signals sent from their trucks and planes in order to have near real time knowledge of where every piece of cargo is while in transit. USTRANSCOM has adopted a version of these commercial tracking systems.

With the significant reliance on cyberspace to move information to and from decision makers and its supporting role in achieving freedom of action in all domains commanders must be able to use both cyberspace and information operations in balancing factors and functions to get tactical forces in place so they can fight and win.

Conclusion

In discussing cyberspace operations at the National Defense University, Kuehl raised the question, "Has warfare as we understand it, featuring "blast, heat, and fragmentation," become obsolete?"[189] The effects created by the reported 1981 trans-Siberian pipeline explosions and the 2009 accidental SCADA inputs at the Sayano–Shushenskaya hydroelectric dam were clearly kinetic and resulted in blast, heat, and fragmentation. The difference between the reported 1981 events in the Soviet Union and now is that the insertion of the malware does not have to be done through a person installing a hard drive or inserting removable media into a computer. Stuxnet has shown us that malicious code can be used as a weapon.

The examples provided in this primer of how IO and CO were used in contemporary conflict unmistakably show how those who planned and executed the actions imaginatively combined means and modes to create dilemmas for their adversary. How will means and modes be combined in future conflict? An adversary can use video, print media, social media, the Internet, malware or a good hacker to attack both physical and moral targets. Which will have a greater impact on the outcome – physical destruction or an emotional response?

The role of content in contemporary conflict must also be understood to effectively use the information environment in support of military objectives and political ends. The ability for more than forty percent of the world's populations to access information content via cyberspace means that the use of information as force will only grow.

The intertwining of cyberspace and human activity has created a reliance on the information that moves through the domain in nearly all aspects of daily life. That reliance for both human and automated decision–making whether is is civilian, military, friend, or foe will only continue to grow. Referring back to Hoffman's analysis of 'Beyond Limits Warfare', cyberspace is the medium in which actions can become omni-directional, synchronous, and asymmetric. If the operational functions are properly balanced with operational factors in using IO and CO, cyberspace and hybrid warfare can be natural partners.

Remembering that hybrid warfare is about combining means and modes to create dilemmas for one's adversaries; cyberspace allows for them to be combined across the domains of warfare. What opportunities and dilemmas might be created by the next great social media tool after Facebook™? Because cyberspace is intertwining human activity with electronics, how will that social media platform be used in future warfare in and among the people? What new electronics will be used to move information to decision makers?

Sun Tzu's thoughts on communicating ground, where all parties have equal access, is as appropriate today as it was in the 4th century BCE. Sun Tzu stated, "In communicating ground, I would pay strict attention to my defences."[190] This thought can be updated for twenty–first century warfare; commanders should think defensively about what can and cannot be done in and through cyberspace and with cyberspace operations. If commanders plan to use 'technology' to win, they will need to think first, What do I need to defend in order to have freedom of action? Commanders should also think about how connectivity can be degraded and denied. Are my computers 100% secure? How can I get secure information that is needed to make decsions? The effects created by cyberspace operations can be both lethal and nonlethal.

But what are the objectives of cyberspace operations? Attempting to achieve ones objectives through cyberspace operations is directly related to compelling humans to act in your favor. Nonlethal effects can be obtained by manipulating the physical, information and cognitive dimensions of the IE to achieve objectives. As Shen Weiguang said, these could be simply 'disrupting the enemy's cognitive system and its trust system'. If a JTF commander loses trust in the force's systems or capabilities and/or fails to properly employ them–our adversaries have won. Additionally, if a population loses faith in its government or military–the adversary has won. This type of psychological victory fits squarely into the definition of WME. Our enemies and competitors have the capabilities to use cyberspace operations to achieve military objectives and to compel their enemy to do their will.

War in cyberspace is no different than the other four domains; there are time, space, and force challenges that must be understood. This centers on how code and content are used as force to affect automated and human decision–making. We need to understand the new technology and the human activity behind it. As Clausewitz said, "The invention of gunpowder and the constant improvements of firearms are enough in themselves to show the advance of civilization has done nothing practical to alter or deflect the impulse to destroy the enemy, which is central to the very idea of war."[191] The importance of learning to fight in cyberspace with both code and content as force cannot be overstated. The 2011 Department of Defense Strategy for Operating in Cyberspace states:

> The Department and the nation have vulnerabilities in cyberspace. Our reliance on cyberspace stands in stark contrast to the inadequacy of our cybersecurity – the security of the technologies that we use each day. Moreover, the continuing growth of networked systems, devices, and platforms means that cyberspace is embedded into an increasing number of capabilities upon which DoD relies to complete its mission. Today, many foreign nations are working to exploit DoD unclassified and classified networks, and some foreign intelligence organizations have already acquired the capacity to disrupt elements of DoD's information infrastructure. Moreover, non-state actors increasingly threaten to penetrate and disrupt DoD networks and systems. We recognize that there may be malicious activities on DoD networks and systems that we have not yet detected.[192]

Clausewitz's and Goebbels thoughts on the psychological impact (the use of content as force) in war are perhaps more relevant today than when they were written when content can be sent to so many nearly instantaneously to obtain a certain effect. This type of force can obtain outcomes and exert a decisive influence on the elements involved in war. The challenge for information age commanders and planners remains the same as it has been for war throughout the last two centuries; how can they balance the operational factors of time, space, and force with required functions to degrade the enemy in order to allow the tactical forces to defeat them.

Way Ahead – Information Operations and Cyberspace Operations

In his futuristic book, *7 Deadly Scenarios, A Military Futurist Explores War in the 21st Century,* Andrew Krepinevich, describes a set of military capabilities that support Chinese military philosophy. Krepinevich is President of the Center for Budgetary Assessments and consultant to numerous U. S. government agencies. His job has been described as thinking the unthinkable–and to prepare a response in the event our worst nightmare becomes a reality.[193] The

Chinese philosophy is called *Shashou jian* or Assassin's Mace. Shashou jian was a club with which the "assassin" incapacitated his enemy, suddenly and totally, instead of fighting him according to traditional rules of combat.[194] Krepinevich states,

> As the U. S. Military increasingly relies on Information as a critical component of its military effectiveness, and the use of networks to gather, organize, and move information, PLA theorists have, for years, argued that the Americans' heavy reliance on cyberspace may be their Achilles heel.[195]

Compounding this idea, at the September 2014 NATO summit in Wales, General Philip Breedlove, USAF, and Commander USEUCOM stated that, "Russia is waging the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."[196] Additionally, in November 2014 Admiral Michael Rogers, USN the Director National Security Agency (NSA) and Commander U. S. Cyber Command, speaking to the House Intelligence Committee stated that, "China along with one or two other countries had the capability to successfully launch a cyber-attack that could shut down the electric grid in parts of the United States."[197]

Whether wars are termed asymmetric or hybrid, 21st century information and cyberspace operations will continue to take advantage of the intertwining of domains and human activity. In discussing hybrid warfare, David Kilcullen states, "today's conflicts clearly combine new actors with new technology and new or transfigured ways of war, but the old threats also remain and have to be dealt with at the same time and in the same space, stressing the resources and overloading the systems of western militaries."[198]

IO and CO can and will be used by current and future adversaries to achieve their objectives. The ability to think 'operationally' is one of the most important attributes for military leaders. The study of operational art creates a foundation for this thinking. Current and future commanders must understand the relationship between factors and functions to know if they have advantages or disadvantage. If a disadvantage is determined, the commander needs to utilize strengths from the others to overcome that disadvantage. Equally, when the commander has an advantage in one or more, they must utilize them to achieve victory.

Commanders should expect our adversaries to utilize IO and CO in attempting to influence human and automated decision–making. Here again, Clausewitz has some wisdom for the commanders,

> War is the realm of uncertainty; three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty[199] …The general unreliability of all information presents a special problem in war: all action takes place, so to speak, in a kind of twilight, which like fog or moonlight tends to make things seem grotesque and larger than they really are[200]…But a commander must submit his work to a partner, space, which he can never completely reconnoiter, and which because of the constant movement and change to which he is subject he can never really come to know.[201]

Clausewitz suggests the importance of knowing how to fight a war without the benefits of modern technology and communication systems. How then should an operational commander prepare for war in the 21st century? Certainly, the ability to 'think operationally' begins with a firm understanding of operational art. Secondly, a commander should be prepared to fight with

little or no reliable connectivity, as our adversaries have the ability to degrade or deny access to cyberspace. Future operational commanders would do well to heed the words of Colonels Liang and Xiangsui, "In warfare and non-military warfare, which is primarily national and supra-national, there is no territory which cannot be surpassed; there is no means which cannot be used in the war; and there is no territory and method which cannot be used in combination."[202]

Ultimately commanders and planners must become skilled at using information operations and cyberspace operations in support of military objectives and political ends in order to compete with current and future adversaries.

End Notes

[1] Pictures that represent domain relationships obtained from www.defense.gov
[2] Oxford English Dictionary, 11th ed. Domain is defined as an area owned or controlled by a ruler or a government> a sphere of activity or knowledge.
[3] The author is indebted to Captain Stephanie A. Helm, USN (Ret'd) for suggesting the operational art framework for this part of the paper.
[4] http://www.af.mil/information/bios/bio.asp?bioid=6865 (Accessed April 30, 2012)
[5] http://www.nro.gov/history/csnr/leaders/directors/dir7.html (Accessed May 6, 2012)
[6] Thomas C. Reed. *At the Abyss, an Insider's History of the Cold War*. New York, NY. Ballantine Books. 2004, 268
[7] Michael Warner (2012): *Cybersecurity: A Pre-history*, Intelligence and National Security, 27:5, 790.
[8] Ibid.
[9] Bill Gertz, *Computer-based attacks emerge as threat of future, general says.* The Washington Times, Tuesday, September 13, 2011, http://p.washingtontimes.com/news/2011/sep/13/computer-based-attacks-emerge-as-threat-of-future-/?page=all (Accessed December 8, 2011)
[10] http://www.sans.org/security-resources/glossary-of-terms/ (Accessed April 30, 2012)
[11] Weapon of Mass Destruction (WMD) defined in U. S. Office of the Chairman of the Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*. Joint Publication (JP) 1-02, (Washington, DC: CJCS, 12 April 2001 as amended through 19 August 2009). Weapon of Mass Effect defined in Homeland Security Advisory Council Weapons of Mass Effect Task Force on Preventing Entry of Weapons of Mass Effect. January 10, 2006.
[12] Winn Schwartau, Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age, 2nd edition (New York, Thunder's Mouth Press, 1996), Ch.2, pp. 71-86
[13] Oxford English Dictionary, 11th ed. Wetware is defined as human brain cells viewed as counterparts of computer systems.
[14] U. S. Office of the Chairman of the Joint Chiefs of Staff, *Information Operations*. Joint Publication (JP) 3-13, Washington DC: CJCS 27 November 2012, I-1. The concept of renaming the dimensions of the IE to the three C's of connectivity, content, and cognition comes from a brief presented by Dr. Daniel T. Kuehl from the National Defense University and fits well with understanding content and code as a force that moves through cyberspace.
[15] U. S. Office of the Chairman of the Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms.* Joint Publication (JP) 1-02, Washington DC: CJCS 08 November 2010, (As amended through 15 March 2013), 138
[16] Center for International Media Assistance. Special Report. National Endowment for Democracy. 4. http://cima.ned.org/648/cell-phone-report-2.html (accessed March 16, 2009)
[17] Oxford English Dictionary, 11th ed.
[18] Winn Schwartau. *Information Warfare – Chaos on the Electronic Superhighway*, New York: Thunder's Mouth Press, 1994. 49
[19] U. S. Office of the Chairman of the Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms.* Joint Publication (JP) 1-02, Washington DC: CJCS 08 November 2010, (As amended through 15 February 2014), 64
[20] Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, Eds., Cyberpower & National Security (Potomac Books, 2009), 28
[21] Keith B. Alexander, "Warfighting in Cyberspace." *Joint Force Quarterly*, (Washington D.C.: National Defense University Press, Issue 46, 61
[22] Robert M. Gates, U. S. Secretary of Defense, Memorandum for the Secretaries of the Military Departments, et al. *Establishment of a Subordinate Unified U. S. Cyber Command Under U. S. Strategic Command for Military Cyberspace Operations*, June 23, 2009.
[23] Ibid.
[24] U. S. Office of the Chairman of the Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms.* Joint Publication (JP) 1-02, Washington DC: CJCS 08 November 2010, (As amended through 15 February 2014), 64
[25] Ibid, 192
[26] Ibid, 69

[27] Slide from LtGen Jon Davis, USMC, Deputy Commander US Cyber Command brief to US Naval War College student body 12 November 2013
[28] An SQL injection inserts malware into a software entry field for execution. An example would be, "send the data base to the attacker."
[29] Phishing is a scam where Internet fraudsters send messages to lure personal, financial, corporate, or government information from unsuspecting victims. For more information on phishing see http://www.onguardonline.gov/topics/phishing.aspx (accessed March 16, 2009)
[30] See David T. Fahrenkrug (Lt Col, USAF), "Cyberspace Defined", in *The Wright Stuff* (Air University, 17 may 2007), at http://www.au.af.mil/au/aunews/archive/0209/Articles/CyberspaceDefined.html . The Air University has a number of sources on cyberspace; see http://www.au.af.mil/info-ops/cyberspace.htm for a list.
[31] Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, Eds., *Cyberpower & National Security* (Potomac Books, 2009), 32.
[32] Clausewitz, 127
[33] Benjamin Weinthal. *Media are Hamas's main strategic weapons, says visiting US historian.* http://www.jpost.com/Operation-Protective-Edge/Media-are-Hamass-main-strategic-weapons-says-visiting-US-historian-372579 (Accessed October 14, 2014)
[34] Ibid.
[35] Ibid.
[36] The DHS/USCG goes on to state, Each ship "mark" could reflect the actual size of the ship, with position to GPS or differential GPS accuracy. By "clicking" on a ship mark, you could learn the ship name, course and speed, classification, call sign, registration number, MMSI, and other information. Maneuvering information, closest point of approach (CPA), time to closest point of approach (TCPA) and other navigation information, more accurate and more timely than information available from an automatic radar plotting aid, could also be available. Display information previously available only to modern Vessel Traffic Service operations centers could now be available to every AIS-equipped ship. http://www.navcen.uscg.gov/enav/ais/ (Accessed May 4, 2009)
[37] Raymond Gilpin, U. S. Institute for Peace, April 10, 2009. http://www.usip.org/on_the_issues/somalia_piracy.html (accessed May 4, 2009)
[38] Blog - a contraction of the word weblog. Weblog – a personal website on which an individual record opinions, links to other sites, etc. on a regular basis. Oxford English Dictionary 11th Ed. New media is broadly defined as those consumer level digital devices and the forms of instantaneous, interactive communication they make possible because of their integration with global communication networks. Center for Strategic Leadership, US Army War College and the SecDev Group, Bullets and Blogs New Media and the Warfighter. Carlisle, PA: Center for Strategic Leadership, 2009
[39] Center for International Media Assistance. Special Report. 4
[40] Ibid.
[41] http://www.internetworldstats.com/stats4.htm#european (Accessed December 9, 2014)
[42] International Communications Technologies Facts and Figures – The World in 2014, e.pdf
[43] http://www.internetworldstats.com/stats4.htm (Accessed December 9, 2014)
[44] International Communications Technologies Facts and Figures – The World in 2014, e.pdf
[45] http://adelinapeltea.com/2014-the-state-of-worldwide-internet-social-media-and-mobile-penetration/ (Accessed August 8, 2014)
[46] Conversation with Mr. Mark Clancy Citigroup, Inc. November 5, 2009. Mr. Clancy stated that in November 2008, nearly US$3Trillion were moved electronically per day by electronic funds transfers (EFT).
[47] Qiao Liang and Wang Xiangsui. *Unrestricted Warfare*. (Beijing: PLA Literature and Arts Publishing House) February 1999. 188
[48] Ibid. 189
[49] Ibid.
[50] The New York Times. November 9, 1858.
[51] Ibid.
[52] http://www.historic-uk.com/HistoryUK/England-History/ssGreatBritain.htm (accessed February 3, 2009)
[53] Milan Vego, *Joint Operational Warfare Theory and Practice*, Newport, RI, Naval War College Press, 2007. I-3
[54] General James T. Conway, USMC, Admiral Gary Roughead, USN and Admiral Thad W. Allen, USCG, *A Cooperative Strategy for 21st Century Seapower*, Washington, D.C., October 2007, 4

[55] James N. Mattis and Frank Hoffman, "Future Warfare: The Rise of Hybrid Wars" *U. S. Naval Institute Proceedings* (Annapolis, MD: U. S. Naval Institute, Issue November 2005, Vol. 132/11/1,233
[56] Frank Hoffman, "Hybrid Warfare and Challenges." *Joint Force Quarterly*, (Washington D.C.: National Defense University Press), Issue 52, 35
[57] Frank Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars, Arlington, VA: Potomac Institute for Policy Studies, December 2007, 35
[58] Hoffman, "Hybrid Warfare and Challenges" 36
[59] Mohamad Bazzi, "Hizballah cracked the code," Newsday.com, September 18, 2006. http://www.newsday.com/news/printedition/stories/ny-wocode184896831sep18,0,2368668.story (Accessed February 11, 2009)
[60] Hilary Hilton. TIME. August 8, 2006. http://www.time.com/time/world/printout/0.8816.1224273.00.html (accessed February 12, 2009)
[61] Ibid.
[62] Frank Hoffman, "Hybrid Warfare and Challenges." *Joint Force Quarterly*, (Washington D.C.: National Defense University Press, Issue 52, 35
[63] Mattis and Hoffman. "Future Warfare: The Rise of Hybrid Wars."
[64] Alexander, 59
[65] Maura Conway. *Cybercortical Warfare: The Case for Hizbollah.org.* 11
[66] Ibid. 13
[67] Martin Libicki, *The Emerging Primacy of Information.* Orbis, 00304387, Spring 96, Vol. 40, Issue 2, 1.
[68] Clausewitz. 75
[69] Ibid.
[70] Ibid. 149
[71] Melissa Hathaway. October 8, 2008. McClatchy-Tribune News Service. Op-Ed.
[72] Jeremy Kahn. *Mumbai Terrorists Relied on New Technology for Attacks*, http://www.nytimes.com/2008/12/09/world/asia/09mumbai.html?_r=1 (Accessed February 27, 2009)
Google Earth is a registered trademark of Google. Google Earth lets you fly anywhere on Earth to view satellite imagery, maps, terrain, 3D buildings, from galaxies in outer space to the canyons of the ocean. You can explore rich geographical content, save your toured places, and share with others. http://earth.google.com/#utm_campaign=en&utm_medium=ha&utm_source=en-ha-na-us-sk-eargen&utm_term=earth%20download (accessed November 9, 2009)
[73] Voice over Internet Protocol (VoIP) is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line. Some VoIP services may only allow you to call other people using the same service, but others may allow you to call anyone who has a telephone number - including local, long distance, mobile, and international numbers. Also, while some VoIP services only work over your computer or a special VoIP phone, other services allow you to use a traditional phone connected to a VoIP adapter. http://www.fcc.gov/voip/, (accessed February 27, 2009)
[74] *Terrorism-related Incidents in Maharashtra since 2006*, http://www.satp.org/satporgtp/countries/india/database/maharashtra_Incidents.htm (Accessed December 29, 2014)
[75] Ibid.
[76] Jeremy Kahn. *Mumbai Terrorists Relied on New Technology for Attacks*, http://www.nytimes.com/2008/12/09/world/asia/09mumbai.html?_r=1 (Accessed February 27, 2009)
[77] Timothy L. Thomas. *Recasting the Red Star Russia Forges tradition and Technology Through Toughness*. Fort Leavenworth, KS, Foreign Military Studies Office, 2011, 118
[78] Timothy L. Thomas. *Russia's Reflexive Control Theory and the Military*. The Journal of Slavic Military Studies, 2004, 238
[79] Ibid. 121
[80] http://www.latimes.com/news/opinion/la-ed-cyberwar17-2008aug17,0,5922456.story (accessed March 9, 2009)
[81] Russian Invasion of Georgia. Report of Russian Cyberwar on Georgia 10 November 2008. http://georgiaupdate.gov.ge/doc/10006922/CYBERWAR-%20fd_2_.pdf, (accessed November 9, 2009)
[82] Andro Barnovi. Deputy Defence Minister of Georgia. Brief to Cyber Defence & Network Security Conference, London January 2012

[83] Moscow Military Thought (English), "Russian Federation Military Policy in the Area of International Information Security: Regional Aspect" 31 Mar 07, Cited in Greylogic. Project Grey Goose Phase II Report: The Evolving State of Cyber Warfare. March 20, 2009.
[84] Greylogic. Project Grey Goose Phase II Report: The Evolving State of Cyber Warfare. March 20, 2009.
[85] *Cyberwarfare: 2008 Russian Invasion of Georgia*. Presentation to InfowarCon 2009 by Mr. Jeffrey Carr, Principal of GreyLogic LLC and Principal Investigator for Grey Goose, Dr. Rafal Rohozinski, Principal Investigator, Information Warfare Monitor and the SecDev Group, Ms. Eneken Tikk, Head of Legal Team, NATO Cooperative Cyber Defence Centre of Excellence.
[86] Rafal Rohozinski, CEO of The SecDev Group. Brief to the "Gaps in Thinking About Cybered Conflict and Governance Workshop" Brown University and U.S. Naval War College, Providence, RI., June 7, 2013
[87] N. R. Jenzen-Jones. Armaments Research Services web page. http://www.armamentresearch.com/gm-94-grenade-launchers-in-use-with-russian-forces-in-crimea/ (Accessed July 31, 2014)
[88] Armaments Research Services web page. http://www.armamentresearch.com/gm-94-grenade-launchers-in-use-with-russian-forces-in-crimea/ (Accessed July 31, 2014)
[89] www.scmp.com – Thousands of fans display their mobile phones as lights of support at a pro-EU rally in Kiev; www.thewire.com – Anti-government protestors light torches and mobile devices during a rally in central Independence Square, Kiev February 21, 2014; The text message received by Ukrainian protesters reads, "Dear subscriber, you are registered as a participant in a mass disturbance." (Image credit: RFE/RL) http://endthelie.com/2014/01/22/protesters-in-vicinity-of-clashes-in-kiev-receive-ominous-unsigned-text-message/
[90] Taylor Wofford. *Russia State Media Says CIA Shot Down Malaysia Airlines Flight MH 17*. http://www.newsweek.com/russian-state-media-says-cia-shot-down-malaysian-airlines-flight-mh-17-260381 (Accessed July 31, 2014)
[91] RT "Covers" the Shooting Down of MH17. Stop Fake.org – Struggle against fake information about events in Ukraine. http://www.stopfake.org/en/rt-covers-the-shooting-down-of-mh17/ (Accessed July 31, 2014)
[92] Steve Coll and Susan B. Glasser, e-QAEDA - From Afghanistan to the Internet - Terrorists Turn to the Web as Base of Operations, Washington Post, August 7, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR2005080501138.html (Accessed August 11, 2009)
[93] The Combating Terrorism Center. *The Islamic Imagery Project, Visual Motifs in Jihadi Internet Propaganda*. (Department of Social Sciences, West Point, March 2006), 96
[94] http://www.usna.edu/Users/humss/bwheeler/swords/batar.html (Accessed August 11, 2009)
[95] Philip Seib. *The Al-Qaeda Media Machine*. (Ft Leavenworth KS: Military Review May-June 2008), 76
[96] http://www.cnn.com/2012/05/23/politics/al-qaeda-electronic-jihad/ (Accessed May 23, 2012)
[97] ISIS can 'muster' between 20,000 and 31,500 fighters, CIA says. Jim Sciutto, Jamie Crawford and Chelsea J. Carter. http://www.cnn.com/2014/09/11/world/meast/isis-syria-iraq/index.html (Accessed September 12, 2014)
[98] Ibid.
[99] David Carr. *With Videos of Killings, ISIS Sends Medieval Message by Modern Method* http://www.nytimes.com/2014/09/08/business/media/with-videos-of-killings-isis-hones-social-media-as-a-weapon.html?ref=todayspaper (Accessed September 8, 2014)
[100] Judson Berger. *State Department Enters Propaganda War with ISIL*. www.military.com/.../state-department-enters-propaganda-with-isis.html?comp=7000023317843&rank=1 (Accessed September 14, 2014)
[101] Anthony Cuthbertson. *Iraq Crisis: Isis Launch Twitter App to Recruit, Radicalise and Raise Funds. International Business Times.* http://www.ibtimes.co.uk/iraq-crisis-isis-launch-twitter-app-recruit-radicalise-raise-funds-1453154 (Accessed October 22, 2014)
[102] "Abu Bakr al-Baghdadi: Islamic State's driving force" BBC News. 31 July 2014. (Accessed July 31, 2014)
[103] Berger. *State Department Enters Propaganda War with ISIL.*
[104] Michael Isikoff. *In high-tech battle, Washington and Islamic State compete over hearts and minds Radical group's Internet warriors use savvy tactics to take down US videos and tweets* http://news.yahoo.com/in-high-tech-battle--us--islamic-state-compete-over-hearts-and-minds-143054814.html (Accessed September 11, 2014)
[105] Berger. *State Department Enters Propaganda War with ISIL.*
[106] Ibid.
[107] T. E. Lawrence. "The Seven Pillars of Wisdom a Triumph." Garden City, NY, Doubleday, Doran & Company, Inc., 1935, 336

[108] T. E. Lawrence. "The Evolution of A Revolt" *The Army Quarterly and Defence Journal* (October 1920)
[109] Hannah Kuchler. "Warning of Isis Cyber Threat." Financial Times September 18, 2014. http://www.ft.com/cms/s/0/92fb509c-3ee7-11e4-adef-00144feabdc0.html#axzz3DtUu29VX (Accessed September 20, 2014)
[110] Jamie Dettmer. "Digital jihad: ISIS, Al Qaeda seek a cyber caliphate to launch attacks on US." http://www.foxnews.com/world/2014/09/14/digital-jihad-isis-al-qaeda-seek-cyber-caliphate-to-launch-attacks-on-us/ (Accessed September 20, 2014)
[111] Lauren Landry. *A UMass Boston Grad Is Allegedly Behind ISIS' 'Sophisticated' Social Media Strategy – Ahmad Abousamra also attended Northeastern University, according to reports*. http://bostinno.streetwise.co/2014/09/05/who-is-ahmad-abousamra-northeastern-graduate-allegedly-behind-isis-social-media/ (Accessed September 21, 2014)
[112] Ibid.
[113] Ibid.
[114] Carr. *With Videos of Killings, ISIS Sends Medieval Message by Modern Method*
[115] Citizen Lab Research Brief No. 40, June 2014. https://citizenlab.org/2014/06/monitoring-information-controls-in-iraq/ (Accessed October 22, 2014)
[116] Citizen Lab Research Brief No. 45, July 2014. https://citizenlab.org/2014/07/iraq-information-controls-update-analyzing-internet-filtering-mobile-apps/ (Accessed October 22, 2014)
[117] Ibid.
[118] Ibid.
[119] Timothy L. Thomas. *Dragon Bytes Chinese Information-War Theory and Practice*. Fort Leavenworth, KS, Foreign Military Studies Office, 2004. 5
[120] Ibid. 5-6
[121] Peng Guangqian and Yao Youzhi, ed. *The Science of Military Strategy* (Beijing: People's Republic of China: Military Science Publishing House, 2005), 475-476
[122] Timothy L. Thomas. Dragon Bytes Chinese Information-War Theory and Practice. Fort Leavenworth, KS, Foreign Military Studies Office, 2004. 5-6
[123] Ibid.
[124] Ibid. 55
[125] Ibid. 57
[126] Stefan Halper, et al. "China: Three Warfares." A paper prepared for Andrew Marshall, Director, Office of Net Assessment, Office of the Secretary of Defense, Washington , D.C., May 2013
[127] China to Build Lighthouses on Five Isles in Defiance of U. S. Calls http://www.reuters.com/article/2014/08/07/us-china-southchinasea-idUSKBN0G70VI20140807 (Accessed August 8, 2014)
[128] Ibid.
[129] Timothy L. Thomas. Dragon Bytes Chinese Information-War Theory and Practice. Fort Leavenworth, KS, Foreign Military Studies Office, 2004. 32
[130] http://www.infowar-monitor.net/modules.php?op=modload&name= News&file=article&sid= 1472&mode= thread&order=0&thold=0 (accessed February 19, 2009)
[131] Time Magazine. http://www.time.com/time/magazine/article/0,9171,1098961,00.html (accessed March 4, 2009)
[132] Ibid.
[133] Siobhan Gorman, *Electric Grid in U. S. Penetrated by Spies*, Wall Street Journal, April 8, 2009, http://online.wsj.com/article/SB123914805204099085.html (accessed April 29, 2009)
[134] Ibid.
[135] FMSO conducts analytical programs focused on emerging and asymmetric threats, regional military and security developments, and other issues that define evolving operational environments around the world. http://fmso.leavenworth.army.mil/ (accessed March 26, 2009)
[136] Timothy L. Thomas. *Dragon Bytes Chinese Information-War Theory and Practice*. Fort Leavenworth, KS, Foreign Military Studies Office, 2004. 18
[137] Sun Tzu. 84 and 79
[138] InfowarCon is a recurring conference of IO professionals sponsored by the Association of Old Crows. Mr. Rohozinski spoke on both Russian and Chinese cyber and information warfare activities.

[139] Thomas. *China's Electronic Long Range Reconnaissance*. 47
[140] Mandiant. APT1 Exposing One of China's Cyber Espionage Units. February 2013, 2
[141] Ibid.
[142] Ibid. 59-60
[143] James C. Mulvenon and Andrew N. D. Yang, editors, *The People's Liberation Army as Organization: Reference Volume v1.0*, (Santa Monica, CA: RAND Corporation, 2002), 96, http://www.rand.org/pubs/conf_proceedings/CF182.html, accessed February 6, 2013.
[144] The theory of cyber privateers was put forth by Mr. Rohozinski at InfowarCon 2009 and supported by other cyber analysts at the conference.
[145] Larry Shaughnessy. *Hasan's e-mail exchange with al-Awlaki; Islam, money and matchmaking*. http://security.blogs.cnn.com/2012/07/20/hasans-e-mail-exchange-with-al-awlaki-islam-money-and-matchmaking/ (Accessed October 6, 2014)
[146] Thomas Durante. *Investigators discover Boston bombs were detonated by a remote control as suspect admits he learned to build the devices from al Qaeda propaganda magazine*. http://www.dailymail.co.uk/news/article-2313782/Dzhokhar-Tsarnaev-Boston-Marathon-bomber-admits-learned-build-bomb-Inspire-magazine.html (Accessed October 6, 2014)
[147] Abby Ohlheiser. *What we know about Alton Nolen, who has been charged with murder in the Oklahoma beheading case*. http://www.washingtonpost.com/news/post-nation/wp/2014/09/30/what-we-know-about-alton-nolen-who-has-been-charged-with-murder-in-the-oklahoma-beheading-case/ (Accessed October 6, 2014)
[148] National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*. New York: W.W. Norton & Company, 2004. 339
[149] Vego. I-3
[150] Joint Publication 3-0, III-1
[151] Vego. VIII-3
[152] Vego identifies key operational functions as command organization, intelligence, command and control warfare, fires, logistics, and protection. Ibid.
[153] Ibid. VIII-4
[154] James J. Schneider. "*The Loose Marble- and the Origins of Operational Art"*, Parameters. (Carlisle, PA, Journal of the U. S. Army War College, Vol XIX, No. 1, March 1989. 87
[155] Ibid.
[156] E.B. Potter. Nimitz. (Annapolis, MD: Naval Institute Press, 1976), 136
[157] Geoffrey Till. *Seapower A Guide for the Twenty-First Century*. (Oxford, UK: Frank Cass, 2006), 162
[158] Geoffrey Bennett. *The Battle of Trafalgar*. (London: B.T. Batsford Ltd, 1977), 140
[159] Ibid. 138
[160] Julian S. Corbett, *The Campaign at Trafalgar* (London: Longmans, Green and Co, 1910), 342
[161] Ibid. 4
[162] Vego. III-3
[163] Conversation with COL William Hartig, USMC (Ret'd) February 20, 2009
[164] Helm, Stephanie A., CYBER FLAG 15-1 Trip Report (Unclassified) U.S. Naval War College. 26 November 2104.
[165] Joint Publication (JP) 1-02. 153
[166] Helm CYBER FLAG 15-1 Trip Report (Unclassified).
[167] Kushner, David. "The Real Story of Stuxnet". *ieee.org*. IEEE Spectrum. (Accessed August 8, 2014)
[168] Vego. VIII-3
[169] Vego. VIII-7
[170] Ibid.
[171] U. S. Office of the Chairman of the Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms.* Joint Publication (JP) 1-02, Washington DC: CJCS 08 November 2010, (As amended through 15 November 2011), 61
[172] U. S. Marine Corps Doctrine Publication (MCDP) 6. (Washington DC, 1996), 39
[173] Ibid.
[174] Ibid. 96

[175] Robert K. Ackerman. *U.S. Cyber Command Grants DISA Head Directive Authority*. http://www.afcea.org/content/?q=node/13874 (Accessed January 5, 2015)
[176] Diagram reproduced from U. S. Office of the Chairman of the Joint Chiefs of Staff, *Cyberspace Operations*. Joint Publication (JP) 3-12R, Washington DC: CJCS 5 February 2013, IV-8. C2 lines of authority are changed to color to better display the exercise of authority, control, and coordination. The original JP diagram had the relationship between DISA and the DNC as a solid black line denoting COCOM which does not exist between a combat support agency and its subordinates. This diagram modifies the C2 relationship to show the emerging construct of directive authority for cyberspace operations (DACO) relationship between DISA and DISA's network centers.
[177] LtGen Jon Davis, USMC, Deputy Commander US Cyber Command brief to US Naval War College student body 12 November 2013.
[178] Slide from Davis brief to USNWC 12 November 2013.
[179] Vego. VIII-7
[180] Joint Publication (JP) 1-02. 130
[181] U. S. Office of the Chairman of the Joint Chiefs of Staff, *Cyberspace Operations*. Joint Publication (JP) 3-12R, Washington DC: CJCS 5 February 2013, II-4-5
[182] Ibid.
[183] Ibid.
[184] Joint Publication (JP) 1-02. 127
[185] Joint Publication 3-0 Operations. III-27
[186] Joint Publication (JP) 1-02. 255
[187] USTRANSCOM AIT & ITV website http://www.transcom.mil/ait/ (accessed May 28, 2014)
[188] Joint Publication (JP) 1-02. 213
[189] Dan Kuehl referencing a discussion with then Lt Gen Alexander, USA at Cyber Education Workshop December 2, 2008.
[190] Sun Tzu, *The Art of War* Translated by Samuel B. Griffith. New York: (Oxford University Press, 1971), 130
[191] Clausewitz.76
[192] U. S. Department of Defense. *Strategy for Operating in Cyberspace*. (Washington D.C., July 2011), 1
[193] Commentary on dust jacket of *7 Deadly Scenarios A Military Futurist Explores War in the 21st Century*. (New York, Bantam Dell 2009)
[194] Lev Navrozov, Chinese Geostrategy: 'Assassin's Mace' http://archive.newsmax.com/archives/articles/2005/10/20/172811.shtml (accessed September 17, 2009)
[195] Andrew F. Krepinevich. *7 Deadly Scenarios A Military Futurist Explores War in the 21st Century*. (New York, Bantam Dell 2009), 194.
[196] Peter Pomerantsev, Russia and the Menace of Unreality How Vladimir Putin is revolutionizing information warfare. http://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/ (Accessed September 15, 2014)
[197] http://www.foxnews.com/politics/2014/11/20/nsa-director-china-can-damage-us-power-grid/ (Accessed November 21, 2014)
[198] David Kilcullen. *The Accidental Guerrilla*. (Oxford, UK: Oxford University Press 2009), 5-6
[199] Clausewitz. 101
[200] Ibid. 140
[201] Ibid. 109
[202] Liang and Xiangsui. 199

Selected Bibliography

Bennett, Geoffrey. *The Battle of Trafalgar*. London: B.T. Batsford Ltd, 1977

Combating Terrorism Center, *The Islamic Imagery Project, Visual Motifs in Jihadi Internet Propaganda*. Department of Social Sciences, United States Military Academy. West Point, NY, 2006

Corbett, Julian S., The Campaign of Trafalgar. London, Longmans, Green and Co, 1910

Clausewitz, Carl von. *On War*. Princeton, NJ. Princeton University Press, 1976

Hoffman, Frank. *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies Arlington, VA, 2007

Kilcullen, David, *The Accidental Guerrilla*. Oxford, UK: Oxford University Press, 2009

Kimmage and Ridolfo, *Iraqi Insurgent Media: The War of Ideas and Images* An RFE/RL Special Report. RFE/RL, Inc., Washington, DC, 2007

Kramer, Franklin D., Starr, Stuart H., Wentz, Larry K. Eds., *Cyberpower and National Security*. Washington, DC, Potomac Books, 2009

Krepinevich, Andrew F., *7 Deadly Scenarios*. New York, NY: Bantam Books, 2009

Potter, E.B., *Nimitz*. Annapolis, MD: Naval Institute Press, 1976

Qiao Liang and Wang Xiangsui. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, 1999

Reed, Thomas C., *At the Abyss: An Insiders History of the Cold War*. New York, NY. Ballantine Books, 2004

Schwartau, Winn. *Information Warfare – Chaos on the Electronic Superhighway*. New York. Thunder's Mouth Press, 1994

_____. *Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age, 2nd edition.* New York, Thunder's Mouth Press, 1996

Thomas, Timothy. *Cyber Silhouettes – Shadows Over Information Operations*. Fort Leavenworth, KS, Foreign Military Studies Office, 2005

_____. *Dragon Bytes Chinese Information-War Theory and Practice*. Fort Leavenworth, KS, Foreign Military Studies Office, 2004

_____. *Recasting the Red Star, Russia Forges Tradition and Technology Through Toughness.* Fort Leavenworth, KS, Foreign Military Studies Office, 2011

Till, Geoffrey. *Seapower A Guide for the Twenty-First Century*. London. Frank Cass, 2004

Tzu, Sun. *The Art of War*. Translated by Samuel B. Griffith. New York: Oxford University Press, 1971

U. S. Department of Defense, *Strategy for Operating in Cyberspace*, Washington, DC: July 2011

U. S. Office of the Chairman of the Joint Chiefs of Staff, *Joint Operations*. Joint Publication (JP) 3-0, Washington, DC: CJCS, 17 September 2006, Change 1 13 February 2008

_____. *Cyberspace Operations*. Joint Publication (JP) 3-12R, Washington, DC: CJCS, 5 February 2013

_____. *Information Operations*. Joint Publication (JP) 3-13, Washington, DC: CJCS, 27 November 2012

Vego , Milan. *Joint Operational Warfare*. Newport, RI. U. S. Naval War College, 20 September 2007