AIR WAR COLLEGE

AIR UNIVERSITY

Net-Centric Warfare 2.0:

Cloud Computing and the New Age of War

by

Robert S. Spalding III, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the United States government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

List of Figures

Abstract

The rapid evolution of cyber technologies demands a new concept of Network-Centric Warfare – a new construct built on the foundation of the new interactive web. The rapid advancement of information technologies and the development of cloud computing by large commercial information technology trendsetter organizations like Google, should lead the Department of Defense to ask: does cloud computing represent the future of network-centric operations and warfare for the United States military? For the Department of Defense to embrace cloud computing requires it to adopt the internet, rather than a fixed IT infrastructure, as its network backplane. The Department will be required to rapidly embrace and employ new Network-Centric concepts (referred to in this paper as Network-Centric Warfare 2.0) and address issues such as cost; military operations in a collaborative environment; empowering individuals; granting greater access to Department and Service-specific information; developing processes and procedures for new parallel and serial operations; and rapidly developing and employing new technologies to provide enhanced data fusion capabilities.

I. Introduction

On 1 May, 2003 President George W. Bush stood on the deck of the USS Lincoln and proclaimed "major combat operations in Iraq have ended."[1] According to General Tommy Franks, the President was honoring the Coalition Forces Commander's request to signify the end of Phase III combat operations.[2] Pundits have pointed to this act and missteps as the reason that the United States is still at war in Iraq. A failure of Network-Centric Warfare in post-combat and stabilization operations has been cited as one reason initial efforts at stabilizing Iraq did not go well.[3] The main critique is that while today's Network-Centric force well suited for traditional maneuver, it is ill prepared for the irregular war that followed termination of major combat operations in Iraq. This paper addresses issues related to that debate.

During the same period the insurgency was raging in Iraq, Don Tapscott and Anthony Williams published their book, *Wikinomics*. The authors describe a new economic model based on "mass" collaboration enabled by Web 2.0, or the interactive internet - (think blogs, wikis, social networks, etc.)[4] *Wikinomics* presents an economic model based on Web 2.0 which is different from the economic model based on internal networks described in the book *Network Centric Warfare* written by Alberts et al in 1999. This earlier book is viewed as the foundation for Network-Centric Warfare.[5]

The rapid evolution of cyber technologies demands a new concept of Network-Centric Warfare – a new construct built on the foundation of the new interactive web. The rapid advancement of information technologies and the development of cloud computing by large commercial information technology trendsetter organizations like Google, leads the Department of Defense to ask: does cloud computing represent the future of network-centric operations and warfare for the United States military?

For the Department of Defense to embrace cloud computing requires it to adopt the internet, rather than a fixed IT infrastructure, as its network backplane. The Department will be required to rapidly embrace and employ new Network-Centric concepts (referred to in this paper as Network-Centric Warfare 2.0) and address issues such as cost, military operations in a collaborative environment, empowering individuals, granting greater access to Department and Service-specific information, developing processes and procedures for new parallel and serial operations, and rapidly developing and employing new technologies to provide enhanced data fusion capabilities.

The book *Network Centric Warfare* was broad in scope. It described the change in society brought on by the information revolution.[6] The book proposed a theory of Network-Centric Warfare based on this foundation.[7] A review of a book which develops Network-Centric Warfare 2.0 to an equivalent degree is beyond the scope of this paper; thus this paper will limit the analysis narrowly to the concepts of Web 2.0 and cloud computing and how it can be used to develop a new model for Network-Centric Warfare.

Wikinomics argues Web 2.0 and cloud computing are impacting companies in ways that challenge traditional corporate organizational structures.[8] Additionally, the rapid development of cloud computing technologies portends new challenges for institutional and structural protections for individual privacy and other civil liberties.[9] These issues are best addressed by legal scholars and will not be specifically explored in this paper. Organizational theory and new management practices are also outside the scope of this paper. The focus of this paper is to introduce key concepts related to Web 2.0 and cloud computing and briefly explore their impact on the future military concept of Network-Centric Warfare.

Chapter two will discuss a proposed model and describe the six Web 2.0 concepts and their impact on Network-Centric Warfare. This paper will explore these concepts within the construct of Network-Centric 2.0 and place them within the context of the nation's instruments of power – diplomacy, information, military, and economics – and how they are used in times of war and conflict.

Chapter three describes the most critical challenges associated with cloud computing. These will be juxtaposed against the key benefits explored in chapter four. Finally, chapter five will summarize findings and provide some pointed recommendations for senior leaders to consider.

Key Terms

For the purposes of this examination, we must define a number of key terms of reference. These definitions are designed to provide the appropriate context for systems and activities as they exist today while also incorporating their anticipated, yet logical, evolution as necessitated by the rapid development of Cyberspace and nanotechnologies. Thus some definitions may differ with those presented in current publications.

- **Web 2.0** – "the business revolution in the computer industry caused by the move to the Internet as a platform, and an attempt to understand the rules for success on that new platform."[10]

- **Cloud computing** – (noun) the technology, infrastructure, processes, and procedures that underlies the Web 2.0 concept.[11]
- **Cyberspace** – “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”[12]
- **Internet** – For the purpose of this examination the Internet is synonymous with Cyberspace.
- **Software as a Service (SaaS), Internet as a platform** – users accessing software and data through an online domain for a small fee rather than purchasing an individual license and maintaining expensive software on individual computers. In other words, computing services are delivered in much the same manner as electrical power.[13]
- **Application –** software delivered through the Internet to the user’s web browser enabled device.
- **Net-centri**c – an operating model of a diversified organization united around a central purpose, coordinated and synchronized via social networks, and augmented by a sensor grid available to all through the cloud.[14]
- **Power to the edge** – “involves the empowerment of individuals at the edge of an organization (where the organization interacts with its operating environment to have an impact or effect on that environment) or, in the case of systems, edge devices.”[15]

Summary

Cloud computing and Web 2.0 arguably represent a fundamental transformation of how software and information is accessed, stored, translated, and used since the dawn of the information age. This transformation has the potential to impact almost all aspects of society including the military concept known as Network-Centric Warfare.

The Internet is poised to become the network backplane of the United States military. Computing power could be delivered to military personnel through the Internet from a virtual massive commercial cloud – the same cloud providing similar services to non-military individuals and organizations. Once widely implemented, traditional IT organizations, personnel, equipment, procedures and management that are the core of today's military network backplane will begin to disappear. Like any traditional institution, these IT departments will likely resist this change.

[1] CNN.com, *Bush Makes Historic Speech Aboard Warship,* (2003), http://www.cnn.com/2003/US /05/01/bush.transcript/.

[2] Lorie Byrd, *Mission Accomplished,* (PoliPundit.com 2004), http://polipundit.com/index.php?p=3604.

[3] Lawrence Sellin, *Net Centric War Doesn't Have All the Answers,* (2008), http://www.upi.com /Security_Industry/2008/11/10/Net_centric_war_doesnt_have_all_the_answers/UPI-88761226362604/.

[4] Don Tapscott and Anthony D. Williams, *Wikinomics*, (New York: Penguin Group, 2006), 2.

[5] David S. Alberts, John J. Garstka and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, (Washington, D.C.: DoD C4ISR Cooperative Research Program, 1999), http://www.dodccrp.org/files/Alberts_NCW.pdf, 15.

[6] David S. Alberts, John J. Garstka and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 56.

[7] David S. Alberts, *Network Centric Warfare,* 87.

[8] Don Tapscott, *Wikinomics.*

[9] Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud,* (SSRN, 2008), http://ssrn.com /paper=1151985.

[10] Tim O'Reilly, *Web 2.0 Compact Definition: Trying Again,* (2006), http://radar.oreilly.com/archives/2006 /12/web-20-compact.html.

[11] There are several definitions for cloud computing. For instance Wikipedia defines cloud computing four different ways:

a. "Cloud computing is Internet-based ("cloud") development and use of computer technology ("computing")."

b. “It is a style of computing in which IT-related capabilities are provided “as a service,” allowing users to access technology-enabled services from the Internet ("in the cloud") without knowledge of, expertise with, or control over the technology infrastructure that supports them.”

c. “Cloud Computing is a paradigm in which information is permanently stored in servers on the Internet and cached temporarily on clients that include desktops, entertainment centers, tablet computers, notebooks, wall computers, handhelds, sensors, monitors, etc.”

d. “Cloud computing is a general concept that incorporates software as a service (SaaS), Web 2.0 and other recent, well-known technology trends, in which the common theme is reliance on the Internet for satisfying the computing needs of the users. For example, Google Apps provides common business applications online that are accessed from a web browser, while the software and data are stored on the servers.”

Cloud computing is all of these and more. The difficulty in defining the concept is one example of why it is so transformational. The difficulty stems from cloud computing’s altering value based on the viewpoint of the user. To the manager it impends the diminution of authority. To the scientist it is the power of collaboration. To the information security manager it is the loss of control. To the user it is empowerment.

Regardless of which definition you choose, there are similarities that make the term cloud computing applicable. They are: 1) Software and data is hosted by a group of servers which can be accessed through the Internet. 2) The cloud can be scaled on the fly, and servers are load-leveled to optimize performance. 3) Files can be manipulated by more than one user at a time, which requires collaboration to synchronize efforts. 4.) Data is separated virtually.

The implications are: 1) Work can be done from anywhere (including outer space), if you have a browser capable device connected to the Internet. 2) Collaboration. 3) Openness. 4) Parallel processes.

[12] OSD definition found in: Noah Shachtman, *26 Years after Gibson, Pentagon Defines 'Cyberspace',* (Wired, 2008), http://blog.wired.com/defense/2008/05/pentagon-define.html.

[13] Electrical power is paid for when the switch is turned on, and billing stops when the switch is turned off. With SaaS, you pay for only that time you are using the software. When you logout, billing stops. This makes computing incredibly affordable for organizations. There is no longer a requirement to retain a large infrastructure.

[14] The original definition was a model that implies “a high-performance information grid that provides a backplane for computing and communications.” This is the model envisioned before the invention of mass production of information. (From Vice Admiral Arthur K. Cebrowski and John J. Garstka, “Network-Centric Warfare: Its Origin and Future,” (1998), *Naval Institute Proceedings*.)

[15] David S. Alberts and Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age*, (Washington, D.C.: DoD Command and Control Research Program, 2005), 5.

II. Net-Centric Warfare 2.0: Rebooting the Cyberspace Domain

The future operating environment of Net-Centric Warfare could be cloud computing, Web 2.0, and the Internet as military's network backplane. Of these, Web 2.0 is transformational and will arguably alter society and in turn, the military. The Cyberspace domain (the Internet) is emerging as the pre-eminent domain for synchronizing all elements of national power – the United States military, a critical instrument of national power, must operate within this domain. Just how this new Network-Centric 2.0 will work and how it compares to the current way the Department of Defense does business is the subject of this chapter.

The Six Concepts of Web 2.0 and Cloud Computing

There are six concepts implicit within the transformation from Web 1.0 to Web 2.0; these apply to Net-Centric Warfare – cost, collaboration, empowerment, transparency/digital divide, data fusion, and parallel vs. serial operations. These concepts could, if fully implemented, fundamentally alter humanity as they will likely transform culture, education, government, and commerce. Any fundamental change to society will eventually spread to and be incorporated by the United States military. This will ultimately transform how the United States wages war.

Cost

Cloud computing offers reduced costs by allowing organizations to divest IT infrastructure. Google and other cloud computing providers are constantly improving the delivery of computing services over the Internet. These improvements include more advanced software and processes for running large banks of integrated servers.[16] More importantly, the scale of the cloud requires rapid and constant infusions of new hardware that is easily assimilated. New hardware often means newer and more capable technology is frequently being added in great numbers – this scale in turn drives down the costs associated with adding the new hardware.[17] Such speed and flexibility means, in most cases, new hardware can be added without harming or diminishing the overall capability of the cloud.

One significant advantage of cloud computing is it centralizes computing resources, allowing organizations to achieve economies of scale. For example, Google offers email with 25 Gigabytes of storage to individual customers and Google apps to companies for $50 each year per person.[18] As a result, employees in participating companies can work and access their files from virtually anywhere allowing them greater flexibility and mobility, something their largely fixed enterprise infrastructures cannot provide.

The flexibility and potential infrastructure and personnel savings afforded by a future Department of Defense system will arguably become more important if defense budgets decline in the future.[19] Finally, one sure way to measure the effectiveness of a new concept is to examine how quickly the business community is adopting it. Jim Young of Google said they are adding approximately 3,000 new business customers a month.[20] Cloud computing appears poised to improve military efficiency and effectiveness.

Collaboration

Network Centric Warfare lists collaboration as one of the benefits of a Network-Centric force.[21] This collaboration enables the joint force to synergize operations. Web 2.0 and cloud computing, however, provide the opportunity for "mass" collaboration.[22] Cloud based "mass" collaboration extends well past the United States military's current joint integration effort to include the interagency, international partners, and the public. *Wikinomics* offers several excellent examples of the kind of collaboration made possible by Web 2.0.

If irregular war, insurgency, or as Colonel Hammes author of *The Sling and the Stone* describes it, fourth generation warfare represents the majority of future conflict, the idea of "mass" collaboration fits well. Whether the strategy is enemy- or population-based, cooperation from the indigenous population is necessary.[23] The current network-centric 1.0 communication systems separate the force from the population electronically – in other words, the people have limited or no access to information of value to both communities on an unclassified military network. One alternative method would be to create a common on-line environment to work together with the population.

Network-Centric Warfare 2.0, more aptly described as Social Network-Centric Warfare, would enable soldiers and citizens to develop virtual relationships. Furthermore this connectivity would extend to include State Department, CIA, FBI and other agency's personnel.

Some examples of government agency uses of social networks are:

- “EPA's Facebook network, for example, has over 750 members—anyone with an EPA email address can become a member of the group. There are similar examples for most agencies.
- USA.gov started a Facebook USAgov page in March 2008, for RSS feeds, videos, photos, and other news. The public is invited to become a "fan" of this page.
- The CIA has used Facebook as a recruiting tool to invite students to apply for employment.
- The Library of Congress' Photostream in Flickr is a good example of posting the government's public domain photos on a social networking site where the public can comment on the photos.” [24]

More than any other concept, the “mass” collaboration opportunities afforded by Web 2.0 will challenge American institutional cultures, including the United States military, to adapt to this rapidly emerging and popular online social construct. Students are taught to cherish individual effort from an early age. Businesses are often dissuaded from collaboration by anti-trust laws. Government offices compete over turf. To realize the benefits of Web 2.0, people and institutions must literally and figuratively be “rewired.” In an information society, individuals with big egos will eventually be replaced by those who cooperate and work well with others, but the change required will not be easy.

Empowerment

One example of the potential impact of cloud computing is called a mashup (Figure 1). A mashup is the combination of two or more cloud services creating a new way to use data. One example of a mashup is “iGuide,”[25] an interactive travel map. Using Google Map’s open application programming interface (API), the website creators combine a mapping function with information about each travel location. Users merely click on the map to get detailed information about a particular travel destination. “DC Crime Finder” is a mashup created by a private citizen using Washington D.C. government crime data, which works similarly to provide an interactive map view of where crime occurs in the city.[26]

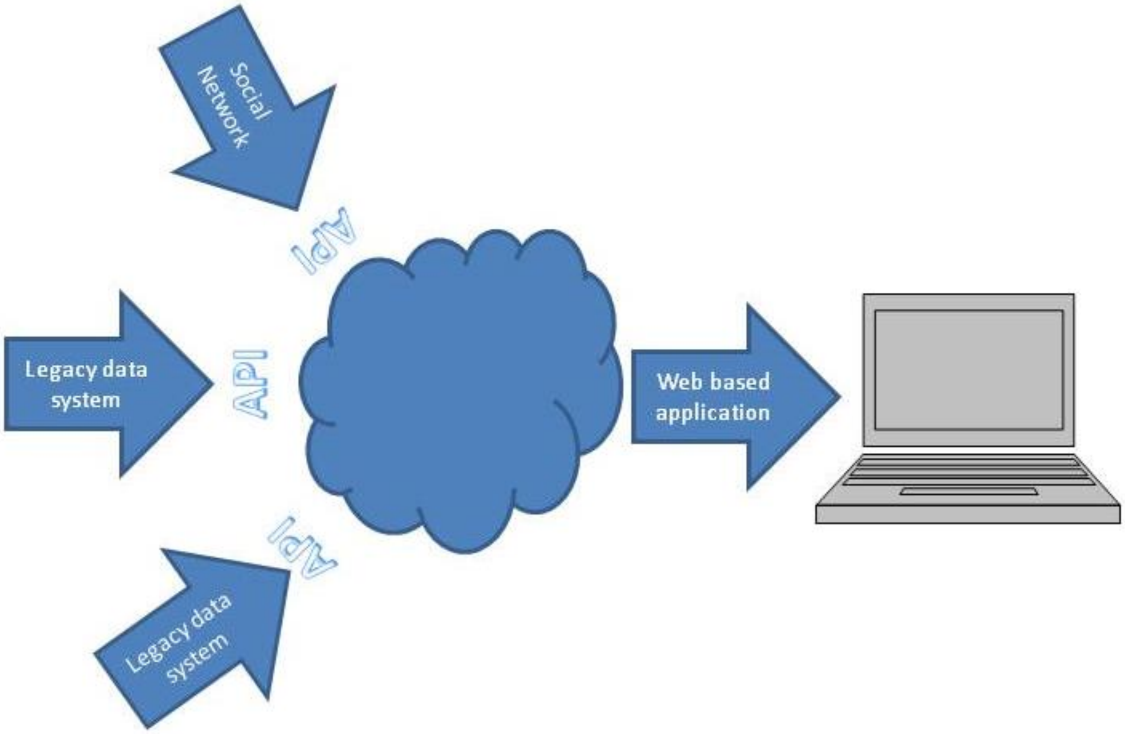

Figure 1. Visual Depiction of a Mashup.

Mashups empower users with the ability to create new ways to interact with data. Anyone can use open APIs to create new mashups. For example, Google allows anyone to create mashups with Google Maps as long as you accept the terms of service which are fairly broad (Google gets credit for its part, the mashup must be provided free of charge, etc.).[27] Google even provides documentation showing the user how to build a mashup.[28] This has the effect of bringing the power of a large IT department to the average "person on the street" who has some free time and a good idea. This person on the street does not need the expertise to build the infrastructure to connect two disparate data systems; the power of cloud computing merely asks how the user would like to display the information.

Mashups are just one example of how cloud computing empowers users. The ability for project managers to bring many people together without assistance from an IT department is another. Google's website explains collaboration with Google Docs:

> "Google Docs enables multiple users in different locations to collaborate simultaneously on the same project. This is what is meant by "collaboration."
>
> For example, when Alice in New York enters something into her document, spreadsheet or presentation, Meredith in Los Angeles can see the changes in real time and respond to them immediately. Instead of having to compare and consolidate their individual files, both women edit a single document. Plus, editing is possible from any computer with Internet access."[29]

One officer interviewed for this paper noted his struggle to conduct exercise planning over the internet. Under the current system where each service or organization maintains their own network environment, there is no option to conduct virtual collaboration. As a result planning has to be done in-person. This costs the government more money in airfare and time lost for travel.[30]

The capability to build social networks is another method of empowerment. Currently users must rely on their IT department to create email lists. These lists cannot be easily shared with other organizations or individuals nor are they frequently updated. Social networks provide a venue to help an address list grow and evolve.[31] As users change jobs they are free to join certain groups and leave others. Since social networks evolve in real time, there is normally no need for the user to wait for, or rely on, an IT department struggling to keep their system current.

Transparency/Digital Divide

Wikinomics describes several examples where companies have increased earnings by publicly releasing previously confidential information. By agreeing to be transparent, these companies were able to collaborate in new ways that were valuable to the firm. Companies are not the only ones pursuing the path of transparency. The city of Washington D.C. has begun to open its databases to the public. Citizens are now free to create their own mashups. Vivek Kundra said, "One innovative DC resident took it upon herself to aggregate government data on service requests, crimes, and building and public space permit applications to create an online information clearinghouse for her own neighborhood. Her neighbors use her site to track economic and real estate developments in their own backyard. Commenting on her success [she] said, "I wanted to leverage the talents and interests of our technologically-savvy citizens to create some real public value, at a fraction of the cost."[32] This does not imply the United States military must abandon its requirements for secrecy. Rather it requires the Department of Defense to critically review security requirements in light of the transparency required to fully utilize the Web 2.0 environment.

Transparency is a difficult concept for an organization like the United States military because of real fears about compromising security. Stove-piped communities carefully restrict access to data to keep it from appearing in the public domain.[33] They are supported by recent security incidents in Department of Defense that reaffirm no digital data is safe from prying eyes. Electronic compromise of information, some of which is classified, has caused Department of Defense to increase efforts to lock down the networks and further restrict access to national security data and information.[34] As a result their information capabilities are not always well utilized, because the people who might find their data useful are often unable to access it in the same way they might access data in the Washington D.C. mashup example.[35] This particular issue is addressed by strategic keystone two[36] in the *United States Intelligence Community Information Sharing Strategy*.[37]

Thus, Network-Centric Warfare 2.0 may create a digital divide. Some Department of Defense organizations will become more transparent while others will continue to restrict access to national security information. Transparent organizations will see the demand for their data increase. Over time, the demand for special access and new information capabilities will decrease as mashups get better at combining commercial and government data to provide new services and highly specialized information.

Parallel vs. Serial Operations

The collaboration capabilities inherent in Web 2.0 allow some operations to proceed in parallel. Since transparency normally extends to all levels of an organization, all levels can act on new information as it is acquired – there is no delay in incorporating and using the new information at any level or retooling the cloud. For example blogs, wikis and social networks allow the leader to communicate directly in real-time with all levels of the organization. Personnel at all levels are then able to act simultaneously on the new guidance. General James Cartwright, the Vice Chairman of the Joint Chiefs of Staff, has used blogs to better communicate with his organizations.[38] The General writes: “The Napoleonic Code and Network-Centric Collaboration cannot exist in the same space and time.”[39]

Data Fusion

Like cost, data fusion is another direct benefit of cloud computing. In order to be truly effective, this capability relies on transparency and collaboration. When operating in the cloud, data about where you connect, how you connect, and who you interact with can be captured and analyzed.[40] This data is not useful until you have it; until you have it, you do not know how useful the information gleaned from having access and being able to analyze the data can be.

For example, Google saves information about searches for flu symptoms. Since Google can save information about the geographical location where the search was initiated, patterns of pandemic may emerge when the data is aggregated.[41] Google writes:

> "we compared our query counts with data from a surveillance system managed by the U.S. Centers for Disease Control and Prevention (CDC) and found that some search queries tend to be popular exactly when flu season is happening. By counting how often we see these search queries, we can estimate how much flu is circulating in various regions of the United States."[42]

Tagging is another Web 2.0 phenomenon that increases the value of data. Jenn Riley writes: "tagging is the process of assigning personal keywords ("tags") to resources by users."[43] Geo-tagging, another valuable cataloguing tool refers to assigning geographic coordinates to a resource. The resource can be a photo, a blog, or a wiki; basically any type of electronic data. Ellyssa Kroski, author of *The Hive Mind: Folksonomies and User-based Tagging,* writes:

> "With the advent of social software and Web 2.0, we usher in a new era of Internet order…The wisdom of crowds, the hive mind, and the collective intelligence are doing what heretofore only expert catalogers, information architects and website authors have done. They are categorizing and organizing the Internet and determining the user experience, and [it is] working. No longer do the experts have the monopoly

> on this domain; in this new age users have been empowered to determine their own cataloging needs. Metadata is now in the realm of the Everyman."[44]

What this means is that everyone with access to the internet, not just the intelligence community, is able to organize and catalogue data to yield new information.

Network-Centric Warfare 2.0

> *Network-Centric Warfare (NCW) is about human behavior within a networked environment.*
> --A. K. Cebrowski, Director, Office of Force Transformation, Office of the Secretary of Defense

> *Oscar Morales created a Facebook group called "Un Millon de Voces Contra las FARC ("One Million Voices against the FARC")… In less than 12 hours the group had more than 900 members, tripling the number of users every day after that… On February 4, [2008] the world watched as people around the globe took to the streets to show the FARC that enough was enough. Spain's EFE news service put the number of marchers worldwide at more than 10 million.*
> --Jennifer Woodard Maderazo, reporter for Media Shift

The Model

The Network-Centric Warfare concept envisioned by Admiral Arthur Cebrowski and John Garstka proved prescient during Kosovo and again during the initial phases of the wars in Iraq and Afghanistan. Yet critics claim the United States military still struggles to realize the opportunities inherent in Network-Centric Warfare in the irregular warfare environment of present day Iraq and Afghanistan.[45] John Garstka (one of the authors of *Network-Centric Warfare*), blames lack of communications standards for diluting Network-Centric Warfare's benefits.[46]

While the current wars in Iraq and Afghanistan have done much to promote "jointness," the last tactical communications mile continues to be a challenge. Even some new major weapon system communication systems (F-22, F-35) are not compatible with each other.[47] The Joint Tactical Radio System (JTRS) Program was "beset by spiraling costs and a lack of clear oversight in some areas, key parts of the multibillion-dollar effort teetered on the brink of cancellation."[48]

Network Centric Warfare as currently envisioned by the Department of Defense also does not allow for the ability to interact with the population in an irregular environment. The communications infrastructure providing the foundation for Network-Centric Warfare is designed to be used solely by the military.[49] With this architecture in place, how can the United States military interact with the population in the Cyberspace domain? Currently, the answer is the military's ability to interface with the public is extremely limited. This is a key impediment when engaged in an irregular fight where the population still has not decided to support the United States' effort.[50]

Network-Centric Warfare 2.0 instead utilizes a nation's existing communications infrastructure to enable what might be termed a Social Network-Centric force. Air Force doctrine calls for seizing control of the enemy's airspace to be one of the joint force's first priorities.[51] Similarly, Network-Centric Warfare 2.0 makes seizing control of an enemy's commercial communications infrastructure one of the United States military's first priorities.

When gaining control of a nation's commercial communications infrastructure is deemed too difficult, or in cases where no infrastructure exists, the United States military would then rapidly establish a communications infrastructure utilizing satellite, airborne, ground and vehicle-borne gateways.[52] Commercial 4G wireless technologies such as Long Term Evolution and WiMax could represent the first iteration of the architecture. [53] These networks allow live streaming video to be sent and received by a handheld device. [54] Communication devices and simplified pictorial instructions could be included in airdrops of

Humanitarian Daily Rations (HDR) to the local population in a remote area where no infrastructure exists. These devices would allow the United States military, interagency, and coalition partners to deliver information services directly to the affected population. This concept could work equally well for humanitarian and disaster relief operations.

There are some forces like stealth aircraft and Special Operations Forces (SOF) who may not want the telltale electronic signature that comes with being connected to such a network. These, however, represent only a small portion of the joint force. These assets and their associated personnel would also have the ability to connect to low probability of intercept (LPI) networks.[55] Therefore when these forces desire stealth, they could switch off the commercial network connection equipment. This dual mode architecture (a combination of commercial and military networks) answers the two main critiques of Network-Centric Warfare -- lack of communication standards and the inability to coordinate DIME actions. It also offers the added benefit of bringing the power of Web 2.0, cloud computing, and social networks to the Network-Centric force. The following figures graphically portray the Network-Centric 2.0 concept.

Social Network Warfare

People use social networking websites to socialize, find a future spouse, or to even find a job. With Network-Centric Warfare 2.0, the United States military could use them to fight wars.[56] Using the Net-Centric 2.0 model, multiple government agencies would be connected through social networks. Collaboration would then occur via cloud computing. Mashups could be created by users to rapidly exploit information and present it in ways valuable to the users. Information and services could be delivered directly to the population utilizing the same networks.

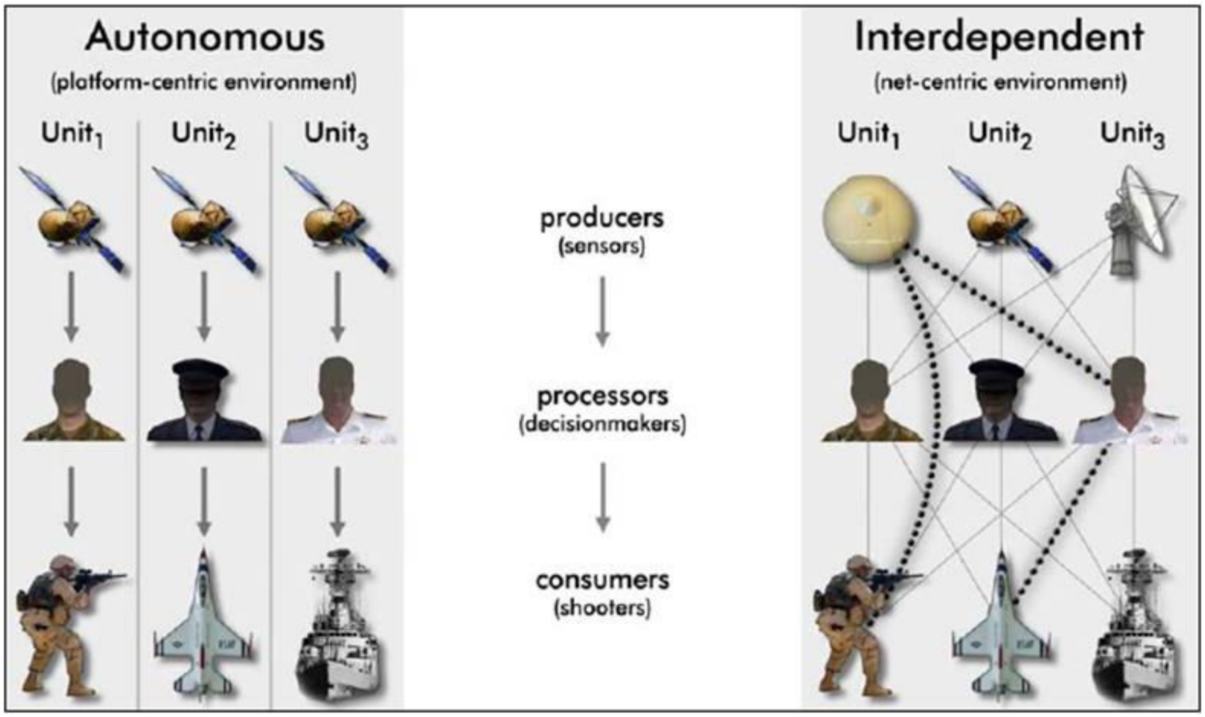

Figure 2. Net-Centric Warfare 1.0

Note: Excerpted from Net-Centric Environment Joint Functional Concept version 1.0, 7 April 2005

Since all users work through the cloud, trends could be analyzed globally. For instance, a Joint Force Commander seeking to understand the latest environment could examine what information was being searched for in the last 2 hours. A spike in requests about specific subjects or technologies might indicate a new evolution in enemy tactics. Since this search can be regionalized, tactical commanders can narrow searches down to an individual unit and then relate the unit's operations to other information from the same region. These are merely a few of the capabilities available to a Network-Centric 2.0 force.

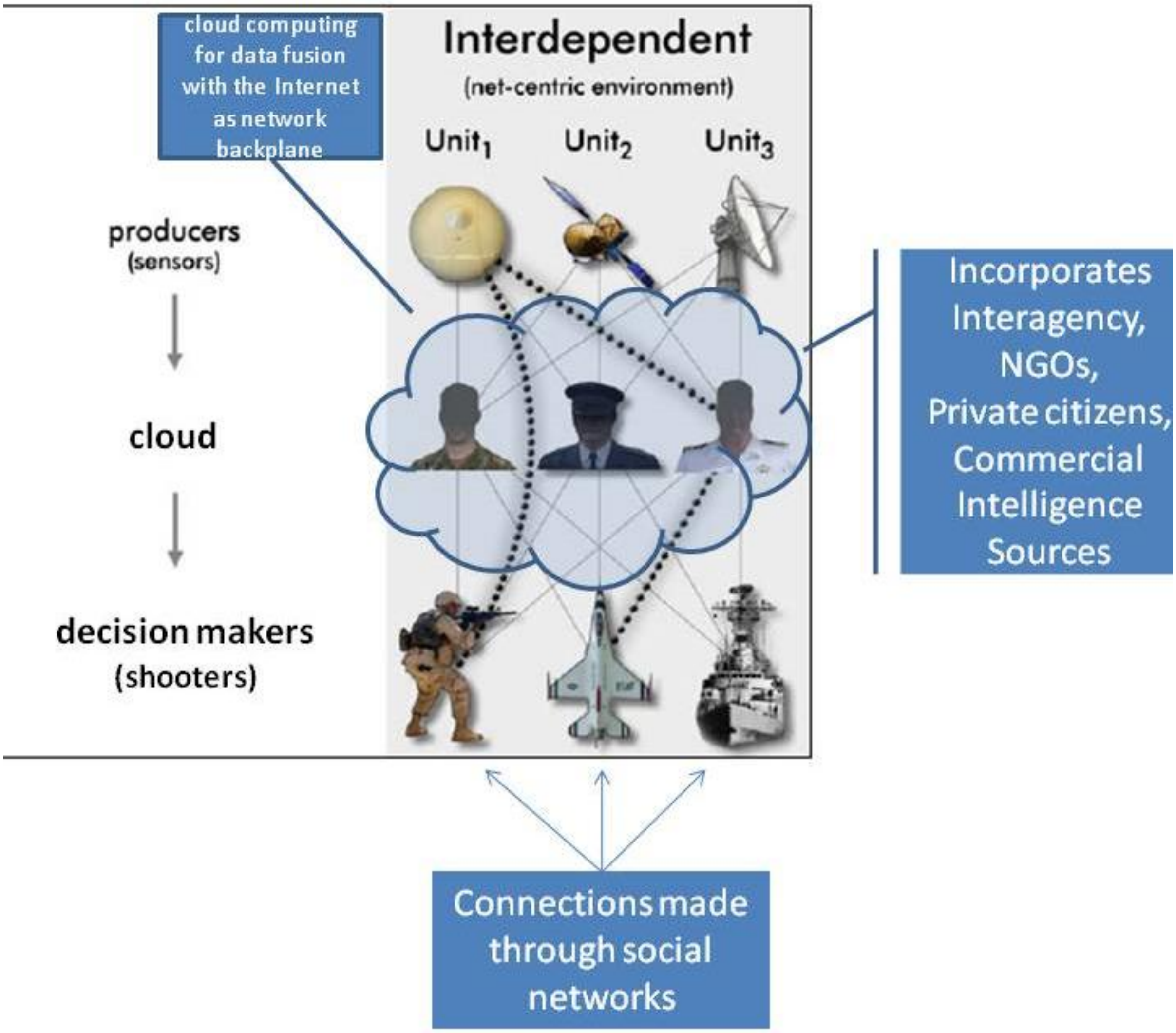
cloud computing for data fusion with the Internet as network backplane
Interdependent
(net-centric environment)
Unit$_1$
Unit$_2$
Unit$_3$
producers
(sensors)
cloud
decision makers
(shooters)
Incorporates Interagency, NGOs, Private citizens, Commercial Intelligence Sources
Connections made through social networks

Figure 3. Net-Centric Warfare 2.0

Summary

This Chapter examined why Web 2.0 and cloud computing represent the future of Net-Centric warfare. It further explored six Web 2.0 concepts and demonstrated how future Network-Centric Warfare can benefit. Finally, a model for a social network and cloud computing based Net-Centric Warfare 2.0 was presented. The next chapter will introduce many of the challenges associated with Web 2.0 and cloud computing.

[16] Varun Aggarwal, *Computing in the Clouds,* (2001), http://www.expresscomputeronline.com/20080218/ technology01.shtml.
[17] "Google and the Wisdom of Clouds," *Scholarly Communications Report* 12 (1) (2008).
[18] Michael Arrington, *Google Puts the Squeeze on Free Apps (Updated),* (TechCrunch, 2009), http:// www.techcrunch.com/2009/01/23/google-puts-the-squeeze-on-free-apps/.
[19] James Staten, *Is Cloud Computing Ready for the Enterprise?,* (2008), http://www.forrester.com /Research/Document/Excerpt/0,7211,44229,00.html. 1.
[20] Interview with Jim Young on November 7, 2008.
[21] David S. Alberts, *Network Centric Warfare,* 11.
[22] Don Tapscott, *Wikinomics*, 11.
[23] Michael J. Artelli and Richard F. Deckro, *Fourth Generation Operations: Principles for the 'Long War'.* (2008), http://pdfserve.informaworld.com/876168__793319714.pdf.
[24] Bev Godwin, *Social Networks and Government,* (Webcontent.gov, 2008), http://www.usa.gov/webcontent /technology/social_networks.shtml.
[25] iGuide, *Iguide Interactive Travel Guide,* (2009), http://iguide.travel/.
[26] Mark Headd, *DC Crime Finder,* (Vox Populi 2008), http://www.voiceingov.org/blog/?p=150.
[27] Google. *Google Maps/Google Earth APIs Terms of Service*, (2008), http://code.google.com/apis/maps /terms.html.
[28] Jason Cooper, *Deploying a Mashup as a Google Gadget,* (Google.com , 2007), http://code.google.com /support/bin/answer.py?answer=82481&topic=12044.
[29]Google, *Collaborating: About Collaboration,* (2008), http://www.google.com/support/writely/bin/ answer.py?hl=en&answer=44677.
[30] Interview with Lt Col David Avila, USAF, on 20 November 2009.
[31] Stephen Lewis, *Friendship and Borders: Facebook, Turkish Etymology, a Virtual Kurdistan, and a Moment of Remembrance,* (Hak Pak Sak, 2008), http://hakpaksak.wordpress.com/2008/05/28/friendship-and-borders-facebook-turkish-etymology-a-virtual-kurdistan-and-a-moment-of-rememberance/.
[32] J. D. Kathuria, *Meet Vivek Kundra: Bringing the "Digital Public Square" to You* (2008), http://blog. executivebiz.com/vivek-kundra-bringing-the-digital-public-square-to-you/991. 1.
[33] Ian Lesser, Bruce Hoffman, John Arquilla, David Ronfeldt and Michele Zanini, *Old Madness, New Methods,* (Rand, 2008), http://www.rand.org/publications/randreview/issues/rr.winter98.9/madness.html.
[34] Fox News, *Pentagon Hit by Unprecedented Cyber Attack,* (2008), http://www.foxnews.com/politics /2008/11/20/pentagon-cyber-siege-unprecedented-attack/.
[35] Richard Solomon and Sheryl J. Brown, *Creating a Common Communications Culture: Interoperability in Crisis Management,* (2005), http://www.usip.org/virtualdiplomacy/publications/reports/17.html.
[36] "The strategic keystones describe the principles around which we have designed our strategy and are those that will be adhered to as the information sharing model evolves in the Intelligence Community."
[37] Director of National Intelligence, *United States Intelligence Community Information Sharing Strategy,* (2008), http://www.fas.org/irp/dni/iss.pdf. 10.
[38] Joe Katzman, *Special Analysis: Stratcom's 4-Star Blogger,* (Windsofchange.net, 2005), http://www. windsofchange.net/archives/006576.html.
[39] Ibid.
[40] Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud,* (SSRN, 2008), http://ssrn.com/paper=1151985
[41] Google. *Flu trends*, (2008), http://www.google.org/flutrends/.
[42] Google, *Flu Trends: How Does This Work?,* (2009), http://www.google.org/about/flutrends/how.html.
[43] Jenn Riley, *Tagging,* (2006), http://techessence.info/tagging.
[44] Ellyssa Kroski, *The Hive Mind: Folksonomies and User-Based Tagging,* (2007), http://infotangle.blogsome. com/2005/12/07/the-hive-mind-folksonomies-and-user-based-tagging/.
[45] Noah Shachtman, *How Technology Almost Lost the War: In Iraq, the Critical Networks Are Social — Not Electronic,* (2007), http://www.wired.com/politics/security/magazine/15-12/ff_futurewar.
[46] Interview with John Garstka on 7 November 2009.
[47] Stephen Trimble, *USAF Delays Communications Link for F-22, Other Fighters,* (2008), http://www.

flightglobal.com/articles/2008/08/18/314759/usaf-delays-communications-link-for-f-22-other-fighters.html.

[48] Henry S. Kenyon, *Tactical Radio Program Takes New Course,* (2006), http://www.imakenews.com/signal /e_article000581121.cfm?x=b11,0,w.

[49] Oracle, *Building a Network-Centric Warfare Architecture,* (2004), http://www.oracle.com/industries /government/ncwwhitepaperr1.pdf. 3.

[50] SWJ Editors, *Air Force Doctrine for Irregular Warfare,* (Small Wars Journal, 2007), http://smallwarsjournal .com/blog/2007/08/air-force-doctrine-for-irregul/.

[51] USAF, *Counterair Operations: Air Force Doctrine Document 2-1.1,* (2008), http://www.dtic.mil /doctrine/jel/service_pubs/afdd2_1_1.pdf. v.

[52] Stephen Trimble, *Seamless Airborne Networks Are Becoming a Reality Thanks to Bridging Technology,* (2007), http://integrator.hanscom.af.mil/2007/January/01252007/01252007-15.htm.

[53] Matt Hamblen, *Wimax Vs. Long Term Evolution: Let the Battle Begin,* (2008), http://www.computerworld. com/action/article.do?command=viewArticleBasic&articleId=9085202.

[54] Nortel, *Long Term Evolution,* (2009), http://www2.nortel.com/go/solution_content.jsp?segId=0&catId=0 &parId=0&prod_id=61700.

[55] Joe D'Andrea, *Are Next-Generation Fighter Aircraft Being Asked to Support Intelligence at the Expense...* (2007), http://www.reuters.com/article/pressRelease/idUS184215+04-Dec-2007+PRN20071204.

[56] The Army released a study detailing how terrorists could use twitter to synchronize actions. See Fox News, *U.S. Army Says Blogging Site 'Twitter' Could Become Terrorist Tool,* (2008), http://www.foxnews.com /story/0,2933,444089,00.html.

III. The Challenge of Cloud Computing

There are numerous identified challenges to cloud computing that must be overcome prior to any wholesale adoption by the Department of Defense. As the concept of cloud computing is relatively new, most IT experts believe its hype is greater than its current operational utility. Today’s cloud computing applications are very rudimentary while the technologies supporting them are still developing. Security is also a real and serious concern. There are also issues stemming from a lack of standardization and data portability.[57]

The Microsoft Effect

Productivity today benefits from the standardization created by Microsoft's enormous PC market share. Currently the cloud computing environment has not settled on a standard operating platform[58] (e.g., VHS versus Beta, MAC versus PC, etc.). Therefore it may be difficult for users to initially move from one cloud provider to another.[59] Currently, there is no such thing as a cloud word processor or spreadsheet program that is as pervasive as the Microsoft equivalents for the PC.[60]

As of 2009, there is no way to know who will win the cloud computing standardization battle. Currently Google, a giant in internet technology, is one of the leaders in terms of the big three applications: word processing, spreadsheet, and presentations.[61] Google’s applications however, are generic and relatively unknown to most users.[62]

Tools such as Wikipedia, Google docs and Facebook allow people to collaborate and socialize within their respective domain. The current lack of standardization across applications from different cloud computing providers makes cross-platform collaboration sporadic or non-existent.[63] Until the standardization issue is resolved, it will be difficult to collaborate effectively in a cloud-based environment.

Businesses and government organizations like Department of Defense have not yet determined how to incorporate social networking sites into their respective enterprise. Although some applicability has been demonstrated, social networking sites are mostly viewed as detrimental to the work environment since, as currently constructed, they are not designed as work-related applications and thus serve to distract employees from their work [64]

If standards are not developed for connecting what is arguably a plethora of cloud computing solutions available, then it will be difficult to evolve these applications beyond their personal social construct into something value-added to work, much less provide capabilities for Social Network Warfare. For instance, if Department of Defense personnel use Google Talk and State Department personnel use Yahoo instant messenger, they cannot communicate with each other via instant messaging. In addition, email global address lists are separate. The result is depicted in Figure 4.

Security

Securing information in the cloud is arguably the biggest problem and a definite source of concern for IT and security professionals.[65] It is one thing to have one PC connected to the Internet and potentially exposed to outside exploitation by unauthorized users while the primary authorized user is at work. It is quite another to place the entire work enterprise on the cloud. Although there are methods for securing files so they cannot be viewed by unauthorized users, it is still possible for unauthorized users to gain access to those files.[66]

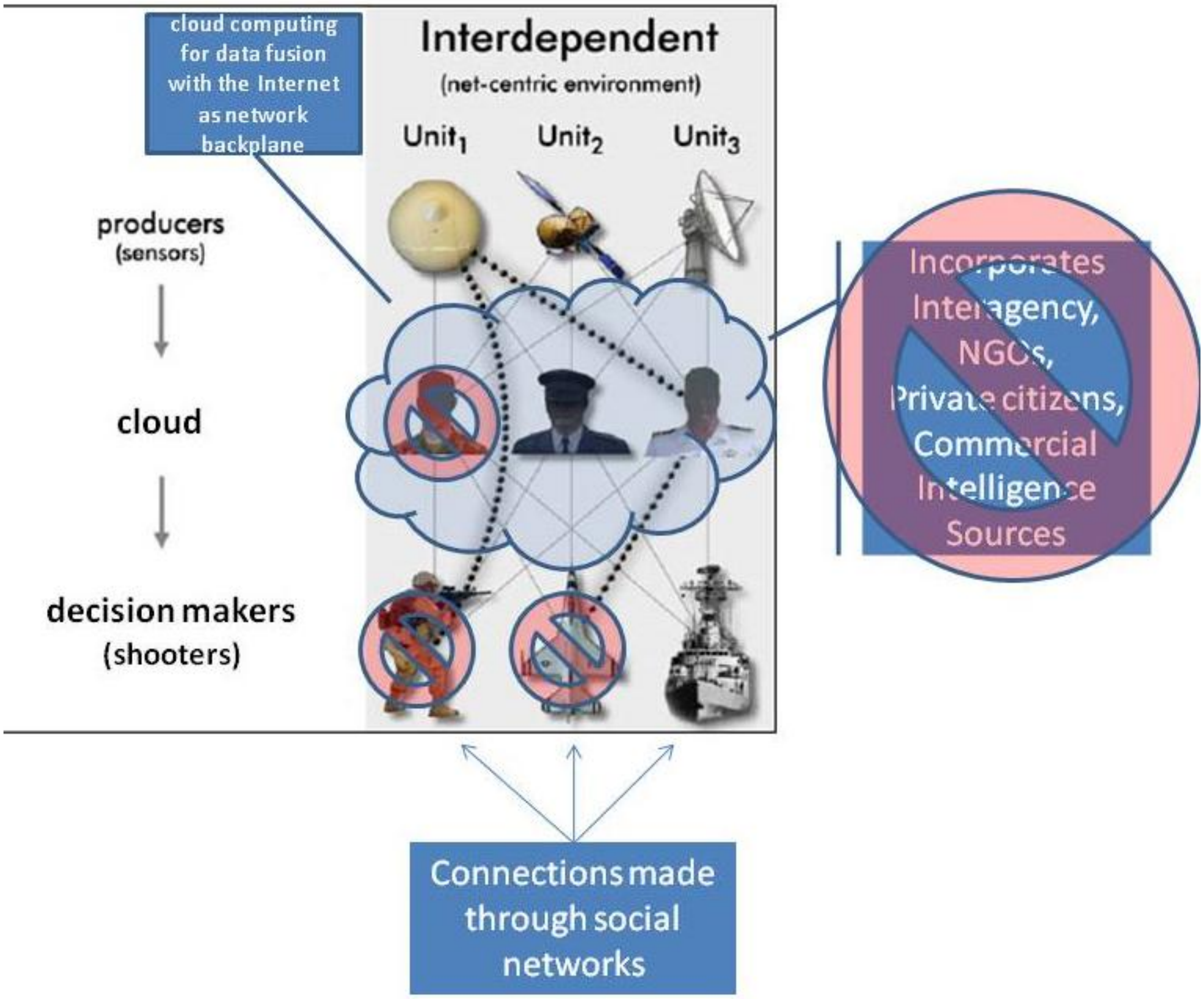
cloud computing for data fusion with the Internet as network backplane
Interdependent
(net-centric environment)
Unit$_1$
Unit$_2$
Unit$_3$
producers
(sensors)
cloud
decision makers
(shooters)
Incorporates Interagency, NGOs, Private citizens, Commercial Intelligence Sources
Connections made through social networks

Figure 4. Net-Centric Warfare 2.0 with Numerous Federal clouds

Placing the entire federal government enterprise in the cloud could make it vulnerable to compromise. Already Department of Defense networks face attacks on a daily basis.[67] There have been some highly publicized break-ins that have led to data compromise. In 2007, Chinese People's Liberation Army hackers broke into Department of Defense networks and downloaded files.[68]

An intelligence officer and a Defense Information Services Agency senior manager familiar with the threat of espionage were interviewed for this paper and both expressed grave concerns about the security aspects related to cloud computing.[69] Chief among their concerns was who has access to the data and how to protect sensitive data. Data stored in the cloud is accessible 24/7, making it vulnerable to anybody with the time and resources to exploit the system.

If a future cloud-based data storage system is compromised, almost any benefit could actually become a liability. A breach could easily erode and undermine all the best capabilities cloud computing could provide.

One potentially effective counter to this vulnerability is through pooling of data since it may provide systemic protection against widespread disruption of service across the federal enterprise. In other words, unaffected pools are still available for the respective organization to access while those pools suspected of being breached can be quickly isolated and cleared. When viewed from this perspective the inability to collaborate quickly across different departments may actually prevent widespread IT system failure.

In essence, security casts a pall over any presumed benefits of cloud computing. If the enemy has the capability to compromise the cloud, then any benefit can presumably be taken away. Even worse, it can become a liability – it can be used against you. Also, because of cloud computing's promise of increased collaboration, the effects could spread throughout the federal enterprise more rapidly than if organizational systems were kept separate.

Bandwidth

To live and function within the cloud you must have a broadband connection; dial-up will not work.[70] Therefore any organization contemplating joining and operating in the cloud must increase user bandwidth to compensate for the distributed nature of the cloud construct.

Bandwidth is currently a problem in Department of Defense. Mike Gipson, Associate Director of Combat Support at the U.S. Strategic Command at Offutt Air Force Base, Nebraska said he is constantly juggling bandwidth. Even with 35 satellites flying in military satellite (MilSat) constellations, ‘we have to direct the best birds to the highest-priority needs,’ Gipson said.[71] Predator Unmanned Aerial Vehicle (UAV) orbits are also limited by available bandwidth. “While the military has a lot more satellite capacity now (the exact amount is a secret), demand has increased even faster. UAV reconnaissance aircraft use enormous amounts of satellite capacity. The Global Hawk needed 500 megabits and Predators about half as much. The major consumer of bandwidth is the live video.”[72] Bandwidth also affects satellite communication availability as well as internet connections in the theater.[73] Placing additional requirements on existing infrastructure would further stress the system.

Summary

Cloud computing is still in its infancy and it is too early to tell whether it will prove useful to businesses, much less the military. The overarching challenge is security. Even if those are solved, issues relating to bandwidth and delivery of software as a service present infrastructure problems. Finally, merging social networks with the business enterprise pose problems of differentiating legitimate work from leisure activity.

Yet, all is not lost. Most critics of cloud computing are members of the IT community, so their arguments may reflect a desire to resist change and protect their interests. Human institutions fear change. A move to cloud computing would be transformational as it transfers significant power from a limited IT community to a great mass of users.

In addition, there are numerous ways to offset risks. It should be noted there are risks to operating in the land, sea, air, and space domains. This does not mean, however, that Department of Defense can refuse to operate there. Instead the risks are mitigated with technology as well as new tactics, techniques and procedures. The same must be developed for operating in the Internet. The next chapter counters the critics who say the United States military cannot operate in the Internet domain.

[57] Scot Finnie, "Peering Behind the Cloud." *Computerworld*, (2008), 22.

[58] Michael Miller, *Cloud Computing*, (Indianapolis, IN: Que Publishing, 2008), 34.

[59] B. Hayes, "Cloud Computing," *Communications of the ACM* 51, no. 7: (2008), 9-11.

[60] Erik Arnold, "Get Your Head out of the Clouds," *Searcher* 16, no. 10: (2008), 51.

[61] E. Arnold, "Leveraging Clouds to Make You More Efficient: How SaaS-y Are You?," *Online* 32, no. 3:, (2008), 31-35.

[62] Michael Miller, *Cloud Computing*, 28.

[63] Richard Adhikari, *IBM Sheds Light on Cloud Certification, Consulting Plans*, (2008), http://www.serverwatch.com/news/article.php/3787276.

[64] Bernhard Warner, *Is Social Networking a Waste of Time?*, (2008), http://technology.timesonline.co.uk/tol/news/tech_and_web/article3536749.ece.

[65] B. Hayes, *Cloud Computing.*

[66] Andy Greenberg, *Cloud Computing's Stormy Side*, (2008), http://www.forbes.com/2008/02/17/web-application-cloud-tech-intel-cx_ag_0219cloud.html.

[67] Shane Harris, *China's Cyber-Militia*, (2008), http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php.

[68] Demetri Sevastopulo, *Chinese Hacked into Pentagon*, (2007), http://www.ft.com/cms/s/0/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac.html?nclick_check=1.

[69] Interview with Lt Col Amy Tweed 12 November 2008, and Robert Vietmeyer on 6 November 2008.

[70] Michael Miller, *Cloud Computing*, 29.

[71] Susan M. Menke, *DoD Sings Satellite Bandwidth Blues*, (Government Computer News, 2004), http://gcn.com/Articles/2004/03/05/DOD-sings-satellite-bandwidth-blues.aspx?Page=1.

[72]StrategyWorld.com, *Bandwidth Blues*, (2007), http://www.strategypage.com/htmw/htspace/articles/20070430.aspx.

[73] John H. Cushman Jr., *Pentagon's Urgent Search for Speed* , New York Times, 1 December 2002.

IV. Rebutting the Critics

Facing the Challenges: Operating in the Internet Domain

Security

Although security is a concern, there are no specifically enumerated examples in the literature as to what those challenges are. Furthermore, it appears data in the cloud can be made more secure than data residing in stovepiped networks. Backing-up files, encrypting data, and monitoring usage globally are strengths that can overcome the vulnerabilities due to data loss or compromise.[74]

In addition, Department of Defense personnel conducting operations via the cloud may be harder to track, because they would blend in with the rest of the world using cloud services. Instead of attacking known military (.mil) networks, enemies would have to sort out Department of Defense personnel from everybody else. With billions of users in the cloud, this would presumably make their job more difficult.

Consider the spread of computer viruses or Trojan horse programs on a network. An infection in one person’s computer on the network can, over time, cause connectivity problems for the entire network.[75] Instead, cloud-based networks are social. Documents no longer need to be copied wholesale onto thumb drives or other memory media to the next network, but rather are shared from their current location. Thus the use of thumb drives or similar media devices would not be required.[76]

The current client-side model used by the United States military ensures that information assurance will continue to be a vexing problem for Department of Defense. Users frequently do not back up their data, and are usually horrified to find they may have no options to retrieve their important data from a failed system.[77] While network drives are usually periodically backed-up, this data represents only a portion of what people use on a regular basis.[78]

Cloud-based data on the other hand is always backed up.[79] Furthermore, since the data resides in the cloud, users have the ability to seek solutions to their problems in the archives. Users can search over all of the data, and the cloud can provide search summaries enabling the users to filter the information to find what may be most useful to them.[80] If they do not have access, they can request access through the owner.[81] Either way the data is always there and is relatively easy to access. It is also more secure from accidental deletion or equipment failure.

Break-ins which have occurred in systems in the past have resulted in data compromises.[82] While data encryption may not necessarily ensure the security of the data, it does make it more difficult for hackers to exploit the files they retrieve.[83] Any exploitation could only occur only after the files were decrypted.

Google claims that its proprietary Google File System (GFS) is inherently more secure than the current method of storage.[84] The GFS splits data into pieces and then spreads the pieces among many machines. These pieces are brought together when requested. Someone gaining access to any of Google's machines would find an environment equivalent to the inside of a shredder basket; each piece contains only a portion of the total contents.

Putting the pieces together would be difficult because all of the applicable shredder baskets would have to be found and the contents combined and then sorted.[85]

One other benefit of a cloud computing is anonymity. [86] When a user logs into a Department of Defense network it is easy to identify them as a Department of Defense user. A user on a local ISP, however, is almost indistinguishable from all of the other users. Cyberspace warriors can use this ability to hide amongst the information clutter. This would complicate the enemy's efforts to locate Department of Defense personnel.

Finally, it is time for the United States military to balance agility with security in the Cyberspace domain. What is meant by agility? In the context of this paper it means the speed at which personnel can leverage the Cyberspace domain to accomplish a task. For example, say a military member is required to give a briefing in a certain location. In order to give the briefing which has been prepared using Microsoft PowerPoint, the military member has five minutes to configure the audiovisual equipment to deliver the presentation. Suppose also that security requirements require a process that ensures it takes a minimum of 10 minutes to stage the appropriate electronic files and equipment. Who makes the determination to circumvent the security procedures when benefits exceed the risk of delivering the presentation in a timely manner? In today's Network-Centric environment the answer is no one.

In nearly all other areas of military endeavor, the commander is responsible for assessing the benefits and risk of action or inaction. In the Cyberspace domain, however, this power has been taken away from commanders. Centralized Network Operations Centers (NOC) exert control to ensure the integrity of the system.[87] This is because the institutions created to build, manage, and control the Cyberspace domain remain focused on security.[88] The commander has little to no ability to influence these actions.

Network Centric Warfare 2.0 returns this power to the commander by distributing the risk among many users. There is virtually no danger of destabilizing an institutional network, because each military member maintains their own connection to the cloud. Sometimes everyone in a unit will have a connection from the same commercial provider. Often, however, they will not. This both enhances unit Cyberspace security and allows the commander to make tradeoffs between risk and security in the Cyberspace domain.

The Microsoft Effect

Microsoft products dominate the computing market -- this is a significant problem and given the still emerging nature of cloud computing, there is no foreseeable solution on the horizon. Currently the major players in cloud computing are trying to dominate the market so that they become the defacto standard.[89] While this would be the best for businesses in terms of standardization, it may not provide the reliability needed. If the Department of Defense relied only on one provider, and the service fails or is compromised, then Department of Defense is at the mercy of their capability to restore service.

A better model is for many cloud providers to exist with slightly different architectures. This would allow Department of Defense to move users to other providers when a service disruption exists. This requires a community of providers who could provide Department of Defense capability to surge similar to the wartime capacity provided by the Civil Reserve Air Fleet.

One possible solution for the Department of Defense would be to create its own cloud, one operating independently from all others. This would be a less than optimal solution, however, because DISA's emphasis of security over agility.[90] To be successful, DISA must be as open as other systems to enable users to obtain the maximum benefit of cloud computing. Authorized users should be able to access the system from any device or platform at any time, whether it is their own system, an Internet café, or an Afghani goat herder's laptop.

Bandwidth

There is no calculus available to determine bandwidth requirements in the future. What is known is bandwidth growth is rapidly expanding to meet demand. Similar in some respects to Moore's law, Gilder's law refers to George Gilder who explained that bandwidth availability triples every 12 months. This is predicted to be reliable for the foreseeable future.[91]

One example of a project that seeks to expand worldwide bandwidth capacity is O3B (stands for "other three billion"). Department of Defense would be one of the beneficiaries. O3B is a company attempting to build a broadband wireless Internet solution that will reach those areas of the world with little or no broadband penetration. If O3B is successful, Africa, Asia and other underdeveloped regions would have access to ubiquitous broadband.[92] The Department of Defense could use this network as well to provide broadband and cloud access to its personnel. A worldwide wireless Internet network would enable Department of Defense personnel to have unfettered access to the Internet wherever they are.

In addition, Department of Defense is planning to eliminate "communications bandwidth as a constraint."

The Naval Studies Board writes:

> The Global Information Grid (GIG) is the vision of the Office of the Secretary of Defense (Networks and Information Integration) (OSD(NII)) for a single, secure-packet-based communications infrastructure providing seamless, end-to-end connectivity for all DOD platforms and facilities …. The GIG is based on commercial technology (i.e., the commercial Internet Protocol (IP) is the fundamental transport mechanism)."[93]

The GIG has recently been dealt a setback because the USAF has decided to scale back or cancel Transformational Satellite (TSAT) – key to providing worldwide bandwidth capability.[94] This will likely delay deployment of the GIG until a suitable alternative can be fielded.

Summary

Like other operating environments – land, sea, air, and space – the Internet is a contested environment. For land, sea, air, and space, the commander's job is to assess risk and then develop procedures to mitigate these risks. The United States military has decided to change this military paradigm when it comes to the Internet.

The Department of Defense does not require commanders understand Internet risks sufficiently to operate without the virtual equivalent of a fortress wall. Instead, the Department of Defense has traded agility in the cyber domain for what might be argued is the illusion of security. Time and again this strategy has failed to protect Department of Defense information or networks. The Department of Defense should rely on Commanders to make their own decisions regarding how and when they venture "outside the virtual wire."

If not, the Department of Defense will likely succumb to many of the same problems created for it by the insurgency in Iraq. By leaving garrison, military personnel can meet the population virtually. Through the Internet, soldiers, bureaucrats, educators and doctors can engage the public and contribute to the development of society. Meanwhile, the military can garner valuable information enabling them to quickly separate insurgents from the population. By operating in the Internet the military will learn more about the environment and thus develop more effective ways to mitigate risk than by relying on another institution to do it for them.

[74] In an email, Jim Young of Google responded thusly to questions about security: “Google runs its operations on the very same cloud. We have 3000 companies a day signing up and using Google Apps. What do you hear in the news and from the hacker community? What do you see in the news regarding IT security challenges and breaches? Where is it occurring? Is it in the Cloud or with traditional systems? With all the money the Department of Defense is spending now on IT defenses, how can there are some many well-documented and known incidents?
That is not to say any system is impervious, but I tend to side with quantifiable statistics. Every time you hear someone say Cloud Computing is insecure, ask them where there money is. Not only that, but the data regarding their financial transactions. Is it at home on their PC or in a bank IT system that uses a shared cloud storage infrastructure. Why does the "under the mattress mentality" so prevalent when it comes to data as well?”

[75] Noah Shachtman, *Under Worm Assault, Military Bans Disks, Usb Drives*, (Wired, 2008), http://blog.wired.com/defense/2008/11/army-bans-usb-d.html.

[76] Fox News, *Pentagon Hit by Unprecedented Cyber Attack*, (2008), http://www.foxnews.com/politics/ 2008/11/20/pentagon-cyber-siege-unprecedented-attack/.

[77] D. F. Tweney, *Your Company's Biggest Data Risk? It Might Just Be the Employees*, (2002), http://dylan.tweney.com/writing.php?display=323.

[78] Andrew Wenger, "Data Protection with SaaS," *Communications News* 45, no. 9: 30-30, (2008).

[79] Michael Miller, *Cloud Computing*, 26.

[80] Google, *Searching for Your Docs: Advanced Search Options*, (2009), http://docs.google.com /support/bin/answer.py?answer=93297&hl=en.

[81] Google, *Discussions > Something Is Broken - Documents > Sorry, the Page (or Document) You Have Requested Does Not Exist*, (2008), http://groups.google.com/group/Something-in-Writely-is-Broken/browse_thread/thread/588181a6887549e/c8b99e54ee94b012?lnk=gst&q&pli=1.

[82] Jill R. Aitoro, *Defense Officials Still Concerned About Data Lost in 2007 Network Attack*, (2008), http://www.govexec.com/story_page.cfm?articleid=39456.

[83] C. Hewitt, "Orgs for Scalable, Robust, Privacy-Friendly Client Cloud Computing," *IEEE Internet Computing* 12, no. 5 (2008), 96-99.

[84] Google, *Discussions > Something Is Broken - Documents > Sorry, the Page (or Document) You Have Requested Does Not Exist*, (2008), http://groups.google.com/group/Something-in-Writely-is-Broken/browse_thread/thread/588181a6887549e/c8b99e54ee94b012?lnk=gst&q&pli=1.

[85] Sanjay Ghemawat, Howard Gobioff, and Shun-Tak Leung, "The Google file system," *SIGOPS Oper. Syst. Rev.* 37, no. 5, (2003), 29-43.

[86] This author argues that Department of Defense networks actually create the requirement for point defense making them more vulnerable to attack. See Col. Stephen W. Korns, *Botnets Outmaneuvered,* (2009), http://www.armedforcesjournal.com/2009/01/3801084.

[87] Glenn Derene, *The Coming Cyberwar: Inside the Pentagon's Plan to Fight Back,* (Popular Mechanics, 2008), http://www.popularmechanics.com/technology/military_law/4277463.html?page=1.

[88] Interview with Robert Vietmeyer of DISA, 6 November 2009.

[89] Allan Leinwand, *It's 2018: Who Owns the Cloud?,* (2008), http://gigaom.com/2008/07/31/its-2018-who-owns-the-cloud/.

[90] Derrick Harris, *DISA CIO: Cloud Computing 'Something We Absolutely Have to Do'* (2008), http://www.on-demandenterprise.com/topic/datacenter/DISA_CIO_Cloud_Computing_Something_We_Absolutely_Have_to_Do_31270309.html?viewAll=y.

[91] Joseph S. Nye and John D. Donahue, *Governance in a Globalizing World*, (Brookings Institution Press, 2000), 138

[92] O3B CEO, "Constellation Will Benefit Emerging Economies," (2008), *Satellite News*, 31:2-2: Access Intelligence LLC d/b/a PBI Media, LLC.

[93] Naval Studies Board, *Autonomous Vehicles in Support of Naval Operations*, (2005), http://books.nap.edu/openbook.php?record_id=11379&page=158. 167.

[94] Gayle S. Putrich, *USAF Delays CSAR-X to '09; TSAT to '10*, (2008), http://www.defensenews.com /story.php?i=3788679.

V. Recommendations and Summary

The benefits of Web 2.0 will extend to all areas of human society. War as a social phenomenon is no different. The spread of the Internet will allow the synchronization of all elements of national power through the tools enabled by Web 2.0. This will in turn allow the military to simultaneously pursue parallel operations along all four key instruments of national power – diplomatic, informational, military, and economic -- at the strategic, operational, and tactical levels.

Because of the enormous changes inherent in Web 2.0, America must completely rethink how it uses data and information to protect national security. This must be done in a collaborative environment where all stake holders are allowed to bring their perspectives to the table. To help the process, some recommendations are provided as food for thought.

Recommendations

1. Create a Cyberspace Corps of Engineers

In the beginning the Internet was perhaps “nice to have” but not essential for modern combat. This has changed. In the future information society, the loss of the Internet could prove catastrophic to the modern way of life. One of the greatest threats to this way of life is a high-altitude nuclear burst. If terrorists were able to seize and launch a nuclear-tipped ballistic missile into space and detonate it, the consequences could prove catastrophic. Navigation, communication, finance, entertainment, government, and the military would all be affected.

When confronted with this devastation, the United States military must determine how to continue effective ongoing military operations. This is because the United States military has looked at network operations as an enabler for its method of waging war. Little thought has been given about how this effect would impact the rest of society.

At some point, however, a threshold was crossed. Like the levies preventing water from flowing into the city of New Orleans, the nation's Internet Service Providers stand between a thriving cyberspace and nothing. Despite this there are no plans for the military to defend this fragile and vulnerable commercial network. This is considered the responsibility of the commercial providers.[95] "The U.S. Army Corps of Engineers has approximately 34,000 dedicated Civilians and Soldiers delivering engineering services to customers in more than 90 countries worldwide" in support of infrastructure requirements.[96] Extending this type of defense capability to cyberspace may be prudent.

In addition, since cyberspace extends worldwide, the United States must encourage the development of similar organizations among the world's Internet enabled nations. The United States Cyberspace Corps of Engineers would work with the international partners to first protect and defend cyberspace. Then they would seek to extend cyberspace, making it accessible by all. Not only would this extend the benefits of globalization to all societies, it would enable the United States to extend and synchronize all elements of national power.

Once we can be assured of a stable cyberspace for society, the United States military will feel more comfortable operating in this domain. This frees the United States military to develop methods for attack and defense within the cyberspace, without having first to deploy the network wherever the fighting will occur. Deploying the network would be the responsibility of the Cyberspace Corps of Engineers. These experts would best understand how to deploy the Internet in a contested environment and how to bring this capacity to the population as well as the United States military, Interagency and allied partners.

2. Make the Internet the military's network backplane

War is a social phenomenon, one fought by people. By sanitizing its cyberspace, the military is constraining itself from defending society in every domain. By moving the United States military and the rest of the Interagency to the cloud, we can leverage the search tool of Web 1.0, and the social networks and SaaS of Web 2.0 to create a truly collaborative community dedicated to national security.

New technologies will help the cloud evolve to extend these capabilities to create a physical world that is interactive. The introduction of robotics and the increasing connectedness of everything will make it possible to manipulate the environment in ways that benefit us all. While this will still be a contested domain, those with good intentions will outweigh malevolent forces. By extending this capability to everyone, the United States military can collaborate with the public to enhance national security.

One method that could be used to move the military to commercial networks would be to provide a "Cyberspace allowance" to military personnel. Using this allowance, personnel would acquire commercial equipment and services to access the Internet. The military would establish required standards to ensure all personnel's equipment is geo-locatable, Internet Protocol (IP) addressable, capable of sending and receiving text, video, and audio as well as compatible with any networks deployed by the Cyberspace Corps of

Engineers. Military personnel would provide their contact information to a cloud-based database, and periodic unit recalls would verify the data accuracy.

3. Continue to study how the cloud is affecting society

This paper has suggested that privacy is one casualty of Web 2.0. There are likely others. Legal, scientific, and other experts need to consider these impacts on the future. Possible solutions to deleterious effects could be worked out in virtual worlds and implemented.

Summary

This paper has argued that cloud computing and Web 2.0 portend transformational changes for human society. These technologies and processes will affect industry, education and government in ways similar to the changes brought about by the industrial and information revolutions. The United States military will be affected as well.

With any technological innovation that introduces social disruption it is to necessary recognize the salient features in order to better organize and cope with the challenges. Therefore six concepts were introduced - cost, collaboration, empowerment, transparency/digital divide, data fusion, and parallel vs. serial operations. In addition, new challenges were identified that create risk for organizations as they attempt to integrate these technologies into their institutional matrices. Finally, the risks were compared and contrasted with the rewards to provide an overall assessment.

Thus while fraught with challenges, Web 2.0 and cloud computing most likely represent the future for industry, education, government, and thus the United States military.

As a result, the Department of Defense must determine the best way to integrate them into future operations.

[95] Otto Kreisher, *Panelists Cite Threats to U.S. Computer Networks*, (2007), http://www.govexec.com/dailyfed/1007/101007cdam1.htm.

[96] US Army Corps of US Army Corps of Engineers, *About Us*, (2009), http://www.usace.army.mil/about/Pages/Home.aspx.

References

304th MI Bn, *Supplemental to the 304th Mi Bn Periodic Newsletter*, (2008), http://www.fas.org/irp/eprint/mobile.pdf.

Adhikari, Richard. "IBM Sheds Light on Cloud Certification, Consulting Plans." 2008. http://www.serverwatch.com/news/article.php/3787276.

Age.com. "Several Countries Trying to Hack into Us Military System: Pentagon." September 5, 2007. http://www.theage.com.au/news/Technology/China-hacked-into-Pentagon-computer-network/2007/09/04/1188783222981.html.

Aggarwal, Varun. "Computing in the Clouds." 2001. http://www.expresscomputeronline.com/20080218/technology01.shtml.

Aitoro, Jill R. "Defense Officials Still Concerned About Data Lost in 2007 Network Attack." 2008. http://www.govexec.com/story_page.cfm?articleid=39456.

Alberts, David S., Garstka, John J., and Stein, Frederick P. *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington, D.C.: DoD C4ISR Cooperative Research Program, 1999.

Alberts, David S., and Hayes, Richard E. *Power to the Edge: Command and Control in the Information Age, Information Age Transformation Series*. Washington, D.C.: DoD Command and Control Research Program, 2005.

Allbritton, Christopher. "Control Your Appliances over the Internet." 2004. http://www.popularmechanics.com/technology/upgrade/1279916.html.

Amazon. "Amazon Elastic Compute Cloud (Amazon Ec2)." 2008. http://aws.amazon.com/ec2/.

Arnold, Erik. 2008. Get Your Head out of the Clouds. *Searcher* 16 (10):50-53.

Arnold, E. 2008. Leveraging Clouds to Make You More Efficient: How SaaS-Y Are You? *Online* 32 (3):31-35.

Arrington, Michael. "Google Puts the Squeeze on Free Apps (Updated)." *TechCrunch* 2009. http://www.techcrunch.com/2009/01/23/google-puts-the-squeeze-on-free-apps/ .

Artelli, Michael J., and Deckro, Richard F. "Fourth Generation Operations: Principles for the 'Long War'." 2008. http://pdfserve.informaworld.com/876168__793319714.pdf .

BBC. "Us Blocks Soldiers from Websites." 2007. http://news.bbc.co.uk/2/hi/americas/6655153.stm .

Bender, Bryan. "New Leadership Planned to Fight WWD Terrorism." 2008. http://www.boston.com/news/nation/articles/2008/12/03/new_leadership_planned_to_fight_wmd_terrorism/.

Brett, C. CPI-C - SaaS Hidden Interface. *Computer Decisions* 20 (7)1988:58-59.

Brewin, Bob, and Verton, Daniel. "Cyberattacks Spur Talk of Third Dod Network " *CNN* 1999. http://www.cnn.com/TECH/computing/9906/22/dodattack.idg/

Briscoe, Robert. "Egocentric Spatial Representation in Action and Perception." 2008. http://cogprints.org/5780/1/ECSRAP.F07.pdf .

Brodzinsky, Sibylla. "Facebook Used to Target Colombia's FARC with Global Rally." The Christian Science Monitor. 2008. http://www.csmonitor.com/2008/0204/p04s02-woam.html .

Butler, Chris. "The Flow of History." 2007. http://www.flowofhistory.com/units/eme/17/FC111.

Byrd, Lorie. "Mission Accomplished." PoliPundit.com. 2004. http://polipundit.com/index.php?p=3604.

Campen, Alan D. *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War*. AFCEA International Press, 1992.

Cebrowski, Vice Admiral Arthur K., and Garstka, John J. Network-Centric Warfare: Its Origin and Future. *Naval Institute Proceedings*. 1998.

Choudhary, V. Comparison of Software Quality under Perpetual Licensing and Software as a Service. *Journal of Management Information Systems* 24 2007 (2):141-165.

CNN.com. "Bush Makes Historic Speech Aboard Warship." 2003. http://www.cnn.com/2003/US/05/01/bush.transcript/.

Coffin, Jill. Analysis of Open Source Principles in Diverse Collaborative Communities. *First Monday* 11 (6). 2006.

Coleman, Kevin. "The Cyber Attack Danger." Defensetech.org 2008. http://www.defensetech.org/archives/004478.html.

Cook, Malcolm, Noyes, Janet M., and Masakowski, Yvonne. *Decision Making in Complex Environments*. London: Ashgate Publishing, 2007.

Cooper, Jason. "Deploying a Mashup as a Google Gadget " Google.com. 2007. http://code.google.com/support/bin/answer.py?answer=82481&topic=12044.

Curry, Roger, Kiddle, Cameron, Markatchev, Nayden, Simmonds, Rob, Tan, Tingxi, Arlitt, Martin, and Walker, Bruce. Facebook Meets the Virtualized Enterprise. *HP Labs*. 2008.

Cushman, John H. Jr. 2002. Pentagon's Urgent Search for Speed *New York Times*, 1 December 2002.

D'Andrea, Joe. "Are Next-Generation Fighter Aircraft Being Asked to Support Intelligence at the Expense..." 2007. http://www.reuters.com/article/pressRelease/idUS184215+04-Dec-2007+PRN20071204.

Defense Information Systems Agency, *Fiscal Year (FY) 2007 Budget Estimates,* (2007), http://www.defenselink.mil/comptroller/defbudget/fy2007/budget_justification/pdfs/0

1_Operation_and_Maintenanace/O_M_VOL_1_PARTS/DISA.pdf.

Delic, Kemal A., and Walker, Martin Anthony. Emergence of the Academic Computing Cloud. *Ubiquity* 9 (31). 2008.

Derene, Glenn. "The Coming Cyberwar: Inside the Pentagon's Plan to Fight Back." Popular Mechanics 2008. http://www.popularmechanics.com/technology/military_law/4277463.html?page=1.

Director of National Intelligence, *United States Intelligence Community Information Sharing Strategy,* (2008), http://www.fas.org/irp/dni/iss.pdf.

The Economist, *After Bill: Microsoft after Gates,* (2008), http://proquest.umi.com/pqdweb?index=0&did=1501651281&SrchMode=1&sid=9&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1223919112&clientId=417.

Feith, Douglas J. "Why We Went to War in Iraq " 2008. http://online.wsj.com/article/SB121504452359324921.html?mod=opinion_main_commentaries.

Finnie, Scot. Peering Behind the Cloud. *Computerworld*, 22-22. 2008.

Forrester Consulting, *Leveraging Legacy: The Fast Track to SOA*, (2007), http://www.unisys.com/eprise/main/admin/corporate/doc/Leveraging_Legacy-Fast_Track_to_SOA_-_revised_FINAL.PDF.

Fox News, *U.S. Army Says Blogging Site 'Twitter' Could Become Terrorist Tool,* (2008), http://www.foxnews.com/story/0,2933,444089,00.html.

______. "Pentagon Hit by Unprecedented Cyber Attack." 2008. http://www.foxnews.com/politics/2008/11/20/pentagon-cyber-siege-unprecedented-attack/ .

Friedman, Thomas L. *The World Is Flat*. New York: Farrar, Straus and Giroux, 2005.

Garreau, Joel. *Radical Evolution: The Promise and Peril of Enhancing Our Minds, Our Bodies -- and What It Means to Be Human*. New York: Random House, 2006.

Ghemawat, Sanjay, Gobioff, Howard, and Leung, Shun-Tak. 2003. The Google File System. *SIGOPS Oper. Syst. Rev.* 37 (5):29-43.

Glassman, James K. . "Briefing on U.S. Public Diplomacy and the War of Ideas." 2008. http://www.state.gov/r/us/2008/111372.htm.

Godwin, Bev "Social Networks and Government." Webcontent.gov. 2008. http://www.usa.gov/webcontent/technology/social_networks.shtml.

Google and the Wisdom of Clouds. *Scholarly Communications Report* 12 (1). 2008.

Google. "Collaborating: About Collaboration." 2008. http://www.google.com/support/writely/bin/answer.py?hl=en&answer=44677 .

———. "Discussions > Something Is Broken - Documents > Sorry, the Page (or Document)

You Have Requested Does Not Exist. ." 2008. http://groups.google.com/group/Something-in-Writely-is-Broken/browse_thread/thread/588181a6887549e/c8b99e54ee94b012?lnk=gst&q&pli=1.

———. "Flu Trends." 2008. http://www.google.org/flutrends/.

———. "Google Maps/Google Earth Apis Terms of Service." 2008. http://code.google.com/apis/maps/terms.html.

———. "Flu Trends: How Does This Work?" 2009. http://www.google.org/about/flutrends/how.html .

———. "Searching for Your Docs: Advanced Search Options." 2009. http://docs.google.com/support/bin/answer.py?answer=93297&hl=en.

Greenberg, Andy. "Cloud Computing's Stormy Side." 2008. http://www.forbes.com/2008/02/17/web-application-cloud-tech-intel-cx_ag_0219cloud.html.

Gross, Grant. "Google, IBM Promote Cloud Computing." PC World 2007. http://www.pcworld.com/businesscenter/article/138195/google_ibm_promote_cloud_computing.html.

Grossman, Robert L., Gu, Yunhong, Sabala, Michael, and Zhang, Wanzhi. Compute and Storage Clouds Using Wide Area High Performance Networks. *Future Generation Computer Systems* 25 (2) 2009.179-183.

Hamblen, Matt. "Wimax Vs. Long Term Evolution: Let the Battle Begin." 2008. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9085202.

Hammes, Thomas X. *The Sling and the Stone*. St Paul: Zenith Press, 2006.

Harris, Derrick. "DISA CIO: Cloud Computing 'Something We Absolutely Have to Do' " 2008. http://www.on-demandenterprise.com/topic/datacenter/DISA_CIO_Cloud_Computing_Something_We_Absolutely_Have_to_Do_31270309.html?viewAll=y.

Harris, Shane. "China’s Cyber-Militia." 2008. http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php.

Hawick, K. A., James, H. A., Patten, C. J., and Vaughan, F. A. "Discworld: A Distributed High Performance Computing Environment." 1998. Springer-Verlag Berlin.

Hayes, B. 2008. Cloud Computing. *Communications of the ACM* 51 (7):9-11.

Headd, Mark. "DC Crime Finder." Vox Populi 2008. http://www.voiceingov.org/blog/?p=150.

Herring, Terry W. "Network-Centric Warfare – Effective or Information Overload." Air University 2006. http://www.google.com/url?sa=U&start=4&q=https://www.afresearch.org/skins/rims/

q_mod_be0e99f3-fc56-4ccb-8dfe-670c0822a153/q_act_downloadpaper/q_obj_5f43ed5e-b9ec-4cac-9374-9059ea5d646b/display.aspx%3Frs%3Denginespage&ei=mcuIScnyNdW5twf2r9igBw&sig2=iW272F-VoB9nJXPYEDKruA&usg=AFQjCNFPL9GvilkRG_xBNIqT7Gf43zLlXQ.

Hewitt, C. Orgs for Scalable, Robust, Privacy-Friendly Client Cloud Computing. IEEE *Internet Computing* 12 (5) 2008.96-99.

Honan, Mathew. "Review: Loopt for Iphone Location-Aware Social Network Finds Your Friends " 2008. http://www.macworld.com/article/136738/2008/11/loopt.html .

iGuide. "Iguide Interactive Travel Guide." 2009. http://iguide.travel/ .

InetDaemon. "History of the Internet." 1996. http://www.inetdaemon.com/about/index.shtml

Jaegar, Paul T., Lin, Jimmy, and Grimes, Justin M. Cloud Computing and Information Policy: Computing in a Policy Cloud? *Journal of Information Technology and Politics* 5 (3) 008. :34.

Joint Staff, *Net-Centric Environment Joint Functional Concept Version 1.0,* http://www.dtic.mil/futurejointwarfare/concepts/netcentric_jfc.pdf.

Kathuria, J. D. "Meet Vivek Kundra: Bringing the “Digital Public Square” to You " 2008. http://blog.executivebiz.com/vivek-kundra-bringing-the-digital-public-square-to-you/991.

Katzman, Joe. "Special Analysis: Stratcom's 4-Star Blogger." Windsofchange.net 2005. http://www.windsofchange.net/archives/006576.html.

Kenyon, Henry S. "Tactical Radio Program Takes New Course." 2006. http://www.imakenews.com/signal/e_article000581121.cfm?x=b11,0,w.

Korns, Col. Stephen W. "Botnets Outmaneuvered." 2009. http://www.armedforcesjournal.com/2009/01/3801084.

Kreisher, Otto. "Panelists Cite Threats to U.S. Computer Networks." 2007. http://www.govexec.com/dailyfed/1007/101007cdam1.htm.

Kroski, Ellyssa. "The Hive Mind: Folksonomies and User-Based Tagging." 2007. http://infotangle.blogsome.com/2005/12/07/the-hive-mind-folksonomies-and-user-based-tagging/.

Krulak, Gen Charles C. Strategic Corporal. *Marines* 28 (1) 1999. 26.

Lawlor, Maryann. Information Systems Agency Services the Services. *Signal Online*. 2005.

Lawrence, Calvin. "Adapting Legacy Systems for SOA." 2007. http://www.ibm.com/developerworks/webservices/library/ws-soa-adaptleg/.

Leinwand, Allan. "It’s 2018: Who Owns the Cloud?" 2008. http://gigaom.com/2008/07/31/its-2018-who-owns-the-cloud/.

Lesser, Ian, Hoffman, Bruce, Arquilla, John, Ronfeldt, David, and Zanini, Michele. "Old

Madness, New Methods." Rand. 2008. http://www.rand.org/publications/randreview/issues/rr.winter98.9/madness.html .

Lewis, Stephen. "Friendship and Borders: Facebook, Turkish Etymology, a Virtual Kurdistan, and a Moment of Remembrance." Hak Pak Sak. 2008. http://hakpaksak.wordpress.com/2008/05/28/friendship-and-borders-facebook-turkish-etymology-a-virtual-kurdistan-and-a-moment-of-rememberance/.

Liepman, James M. Jr. Cyberspace: The Third Domain. *Air University*. 2005.

Lin, Jimmy. Exploring Large-Data Issues in the Curriculum: A Case Study with Mapreduce. *Proceedings of the Third Workshop on Issues in Teaching Computational Linguistics*. 2008:5.

Logothetis, Dionysios, and Yocum, Kenneth. "Ad-Hoc Data Processing in the Cloud." 2008. http://www.cs.ucsd.edu/~kyocum/pubs/mortar_vldb08.pdf.

Lynch, Marc. "Al-Qaeda's Media Strategies." 2006. http://www.nationalinterest.org/Article.aspx?id=11524.

Lyon, Martin P. Fose: The Grass Is Greener... *Public Manager* 37 (2) 2008. 5.

M2PressWIRE. "Mitsubishi, Nec, Tokyo University Realize Successful Interconnection of Quantum Encryption Networks for First Time in Japan." M2PressWIRE. 2006. http://search.ebscohost.com/login.aspx?direct=true&db=nfh&AN=16PU1327681452&site=ehost-live.

Maderazo, Jennifer Woodard. "Facebook Becomes Catalyst for Causes, Colombian Farc Protest." MediaShift.com. 2008. http://www.pbs.org/mediashift/2008/02/facebook-becomes-catalyst-for-causes-colombian-farc-protest053.html.

Marquand, Robert, and Arnoldy, Ben. China Emerges as Leader in Cyberwarfare. (Cover Story). *Christian Science Monitor* 99 (203) 2007. 1-4.

Menke, Susan M. "Dod Sings Satellite Bandwidth Blues." Government Computer News. 2004. http://gcn.com/Articles/2004/03/05/DOD-sings-satellite-bandwidth-blues.aspx?Page=1.

Miller, Claire Cain. 2008. How Obama’s Internet Campaign Changed Politics. *New York Times*, 7 November 2008.

Miller, Michael. *Cloud Computing*. Indianapolis, IN: Que Publishing, 2008.

Milojicic, D. Cloud Computing - Interview with Russ Daniels and Franco Travostino. *IEEE Internet Computing* 12 (5) 2008:7-9.

Morehouse, Jim. "Time Critical Targeting." 2008. http://www.au.af.mil/au/awc/awcgate/af/morehouse.pdf.

Naval Studies Board. "Autonomous Vehicles in Support of Naval Operations." 2005. http://books.nap.edu/openbook.php?record_id=11379&page=158.

Nortel. "Long Term Evolution." 2009.

http://www2.nortel.com/go/solution_content.jsp?segId=0&catId=0&parId=0&prod_id=61700.

Numerous. "Cloud Computing." http://en.wikipedia.org/wiki/Cloud_computing.

———. "Proprioception." Wikipedia. http://en.wikipedia.org/wiki/Proprioception.

Nye, Joseph S., and Donahue, John D. *Governance in a Globalizing World*: Brookings Institution Press, 2000.

O3B CEO. "Constellation Will Benefit Emerging Economies." Access Intelligence LLC d/b/a PBI Media, LLC. 2008. http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=34599452&site=ehost-live.

Oracle. "Building a Network-Centric Warfare Architecture." 2004. http://www.oracle.com/industries/government/ncwwhitepaperr1.pdf.

O'Reilly, Tim. "Web 2.0 Compact Definition: Trying Again." 2006. http://radar.oreilly.com/archives/2006/12/web-20-compact.html.

Peck, Morgen E. Standardizing the Brain-Machine Interface. *IEEE Spectrum* 45 (4) 2008.

Perelman, Deb. "Demand for Business-Tech Integrators Causing SOA Job Surge." eWeek.com 2008. http://www.eweek.com/c/a/Enterprise-Applications/Demand-for-BusinessTech-Integrators-Causing-SOA-Job-Surge/.

Piccerillo, Major Robert A., and Brumbaugh, David A. 2004. Predictive Battlespace Awareness: Linking Intelligence, Surveillance and Reconnaissance Operations to Effects Based Operations. *2004 Command and Control Research and Technology Symposium*.

Picker, Randal C. "Competition and Privacy in Web 2.0 and the Cloud." SSRN, January 6, 2009 2008. http://ssrn.com/paper=1151985.

Putrich, Gayle S. "USAF Delays CSAR-X to '09; TSAT to '10?" 2008. http://www.defensenews.com/story.php?i=3788679.

Ramaswamy, L., Liu, L., and Iyengar, A. Scalable Delivery of Dynamic Content Using a Cooperative Edge Cache Grid. *IEEE Transactions on Knowledge and Data Engineering* 19 (5) 2007. 614-630.

Riley, Jenn. "Tagging." 2006. http://techessence.info/tagging.

ScienceDaily. "New Sensor Being Designed to Detect, Identify Invisible Agents Faster." Science Daily. 2002. http://www.sciencedaily.com/releases/2002/02/020225084319.htm.

Sellin, Lawrence. "Net Centric War Doesn't Have All the Answers." 2008. http://www.upi.com/Security_Industry/2008/11/10/Net_centric_war_doesnt_have_all_the_answers/UPI-88761226362604/.

Senate Commission on the Prevention of Weapons of Mass Destruction Proliferation and

Terrorism, *World at Risk*, (2008), http://documents.scribd.com/docs/2avb51ejt0uadzxm2wpt.pdf.

Sevastopulo, Demetri. "Chinese Hacked into Pentagon." 2007. http://www.ft.com/cms/s/0/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac.html?nclick_check=1.

Shachtman, Noah. "How Technology Almost Lost the War: In Iraq, the Critical Networks Are Social — Not Electronic." 2007. http://www.wired.com/politics/security/magazine/15-12/ff_futurewar

———. "26 Years after Gibson, Pentagon Defines 'Cyberspace'." Wired 2008. http://blog.wired.com/defense/2008/05/pentagon-define.html.

———. "Under Worm Assault, Military Bans Disks, USB Drives." Wired 2008. http://blog.wired.com/defense/2008/11/army-bans-usb-d.html.

Shozu. "What Is Shozu?" 2008. http://www.shozu.com/portal/tour.do?operation=whyuse .

Solomon, Richard, and Brown, Sheryl J. "Creating a Common Communications Culture: Interoperability in Crisis Management." 2005. http://www.usip.org/virtualdiplomacy/publications/reports/17.html.

Spencer, Jack. "The Electromagnetic Pulse Commission Warns of an Old Threat with a New Face." The Heritage Foundation 2004. http://www.heritage.org/research/nationalsecurity/bg1784.cfm.

Staten, James. "Is Cloud Computing Ready for the Enterprise?" 2008. http://www.forrester.com/Research/Document/Excerpt/0,7211,44229,00.html.

StrategyWorld.com. "Bandwidth Blues." 2007. http://www.strategypage.com/htmw/htspace/articles/20070430.aspx.

Sullivan, Francis. I Wandered Lonely as a Cloud. *Computing in Science and Engineering* 10 (3) 2008. 1.

Sun, Xiuhong. "A Wimax Networked Uav Telemetry System for Net-Centric Remote Sensing and Range Surveillance." 2006. http://sbir.nasa.gov/SBIR/abstracts/06/sbir/phase1/SBIR-06-1-O2.03-9072.html?solicitationId=SBIR_06_P1.

SWJ Editors. "Air Force Doctrine for Irregular Warfare." Small Wars Journal. 2007. http://smallwarsjournal.com/blog/2007/08/air-force-doctrine-for-irregul/.

Taipei Times. "Beware Lurking PRC Cyber Army." World News Connection. 2007. http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=CPP20070912968074&site=ehost-live.

Tapscott, Don, and Williams, Anthony D. *Wikinomics*. New York: Penguin Group, 2006.

Thomas, Dave. 2008. Enabling Application Agility - Software as a Service, Cloud Computing and Dynamic Languages. *Journal of Object Technology* 7 (4):4.

Transformation, Office of Force. "The Implementation of Network-Centric Warfare." 2005. http://www.oft.osd.mil/library/library_files/document_387_NCW_Book_LowRes.pdf.

Trimble, Stephen. "Seamless Airborne Networks Are Becoming a Reality Thanks to Bridging Technology." 2007. http://integrator.hanscom.af.mil/2007/January/01252007/01252007-15.htm.

———. "USAF Delays Communications Link for F-22, Other Fighters." 18/08/08 2008. http://www.flightglobal.com/articles/2008/08/18/314759/usaf-delays-communications-link-for-f-22-other-fighters.html.

Turner, M., Budgen, D., and Brereton, P. 2003. Turning Software into a Service. *Computer* 36 (10) 2003. 38-+.

Tweney, D. F. "Your Company's Biggest Data Risk? It Might Just Be the Employees." 2002. http://dylan.tweney.com/writing.php?display=323.

USAF. "Counterair Operations: Air Force Doctrine Document 2-1.1." 2008. http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_1_1.pdf .

US Army Corps of Engineers. "About Us." 2009. http://www.usace.army.mil/about/Pages/Home.aspx.

Waldrop, M. M. Data Center in a Box - a Shipping Container Stuffed with Servers Could Usher in the Era of Cloud Computing. *Scientific American* 297 (2) 2007. 90-93.

Warner, Bernhard. "Is Social Networking a Waste of Time?" 2008. http://technology.timesonline.co.uk/tol/news/tech_and_web/article3536749.ece.

Wenger, Andrew. 2008. Data Protection with Saas. *Communications News* 45 (9):30-30.

Wilson, Greg. "EC2: Commoditized Computing." 5 January 2006. http://pyre.third-bit.com/blog/archives/626.html.

Yahoo! Inc. "Yahoo! And Computational Research Laboratories to Collaborate on Cloud Computing Research." 2008. http://proquest.umi.com/pqdweb?index=8&did=1540149941&SrchMode=1&sid=4&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1223918776&clientId=417.