

**Cyber War's Final Frontier: Network
Centric Warfare Framework**

Amit Grover

Cyber War's Final Frontier: Network Centric Warfare Framework

"If the nation went to war today in a cyberwar, we would lose..."

John Michael McConnell, former Director of National Intelligence and former Director of the National Security Agency [1].

Abstract

This paper explores various concepts related to Cyberwarfare and the Network Centric Warfare framework, and based on the ever-increasing frequency and sophistication of cyber attacks as well as the inherent similarity in the backbone structure of the Internet and the Network Centric Warfare framework concludes that NCW Framework will prove to be Cyber War's Final Frontier. This paper is divided into 7 sections. Section 1 gives a brief introduction of the key terms involved whereas section 2 covers the background literature review. While section 3 discusses threats and vulnerabilities relevant to a Network Centric Warfare framework, section 4 focuses on well known network attacks. Section 5 covers major cyber warfare incidents and related terminology. Section 6 covers the potential of cyber attacks on the Network-Centric Warfare framework and countermeasures and section 7 formulates the conclusion.

1. Introduction

This section deals with definition and background information of key terms such as Cyber warfare, Information warfare, C⁴ISR, and Network Centric Warfare.

1.1 Cyber warfare

The US Department of Defense defines ‘cyberspace’ as the “*the notional environment in which digitized information is communicated over computer networks*”. Cyber Warfare is the use of existing and emerging internet – based technologies to conduct warfare in cyberspace with the aim of attacking and disrupting information systems and communication networks.

1.2 Information warfare

The term ‘Information Warfare’ or IW is similar in meaning to Cyber warfare though with a more streamlined goal of achieving competitive advantage. As per The Institute for the Advanced Study of Information Warfare (IASIW) [5], “*Information warfare is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military, political or business adversaries.*”

Information Warfare is generally subdivided into Information Assurance and Information Denial:

- (a) **Information Assurance:** IA focuses on assuring the flow of mission critical information in the event of any attack on the information infrastructure. IA is not limited to assuring the availability of information but deals with all the information security goals of not only preserving the CIA (confidentiality, integrity, and availability) of information systems but also ensuring proper authentication and non-repudiation of critical information.

(b) **Information Denial:** Information denial is the offensive part of Information Warfare wherein the focus is to disrupt the adversary's mission critical operations to get a competitive advantage.

Based on the target audience, Information Warfare can be classified into 3 classes [10, 11]:

- (a) **Personal Information Warfare:** This is known as Class I Information Warfare and is aimed against individual privacy involving attacks on personal and confidential data.
- (b) **Commercial Information Warfare:** This is known as Class II Information Warfare and involves industrial espionage and broadcasting of false information against business rivals using the internet.
- (c) **Global Information Warfare:** This is known as Class III Information Warfare and is aimed at countries, political alliances / spheres of influence, global economic forces, sensitive national information systems and infrastructure.

1.3 C⁴ISR concept of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

C⁴ISR is a term used for effective interfacing of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance technologies and procedures to deliver a decisive war fighting advantage [6]. The C⁴ISR framework is now known as the Department of Defense Architecture Framework (DoDAF). This comprehensive framework facilitates effective decision making at all levels (tactical, strategic and operational) through organized information sharing. The time-line of evolution of the C⁴ISR framework to the present day DoD Architecture Framework is depicted in figure 1[7].

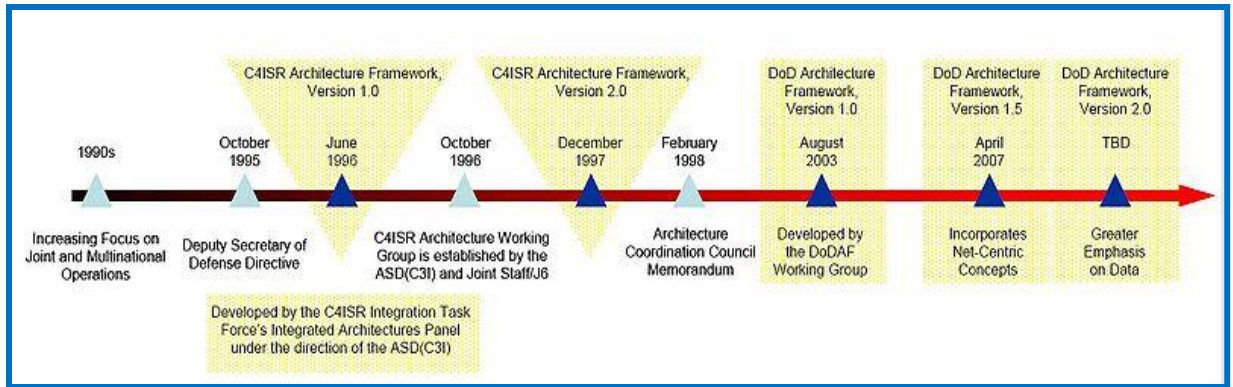


Figure 1: Evolution of the C⁴ISR framework

1.4 Network Centric Warfare

As per a DoD publication [2], *“the term “network-centric warfare” broadly describes the combination of emerging tactics, techniques, and procedures that a fully or even partially networked force can employ to create a decisive war fighting advantage.”*

It is also referred to as ‘Network Centric Operations’ or NCO. Network Centric Warfare focuses on the effective war fighting efficiency that can be generated by interfacing the various aspects of a combat operation in geographically dispersed locations [4]. The C⁴ISR framework or the DoDAF refers specifically the US military’s implementation of a Network Centric Warfare framework. The objectives of Network Centric Warfare include [3, 8]:

- a. Better synchronization of geographically dispersed combat units
- b. More effective combat power by networking sensors, weapons and decision makers
- c. Increased speed of executing command and control procedures
- d. Seamless interoperability between coalition forces
- e. Access to real time information at every echelon of the military hierarchy
- f. Increased survivability and greater lethality in combat operations

The integration of various weapons and sensors and other combat systems in the three dimensions of land, sea and air warfare (including support by space-based satellite

communication and surveillance) is depicted schematically in the figure 2 below [9]. This NCW integration not only includes conventional military systems but also specialized systems such as the JSTARS (Joint Surveillance Targeting Attack Radar System) and the Global HAWK Unmanned Aerial Vehicles (UAVs). A schematic of the Global Hawk Unmanned Aerial Vehicle Sensor Systems is shown in figure 3.

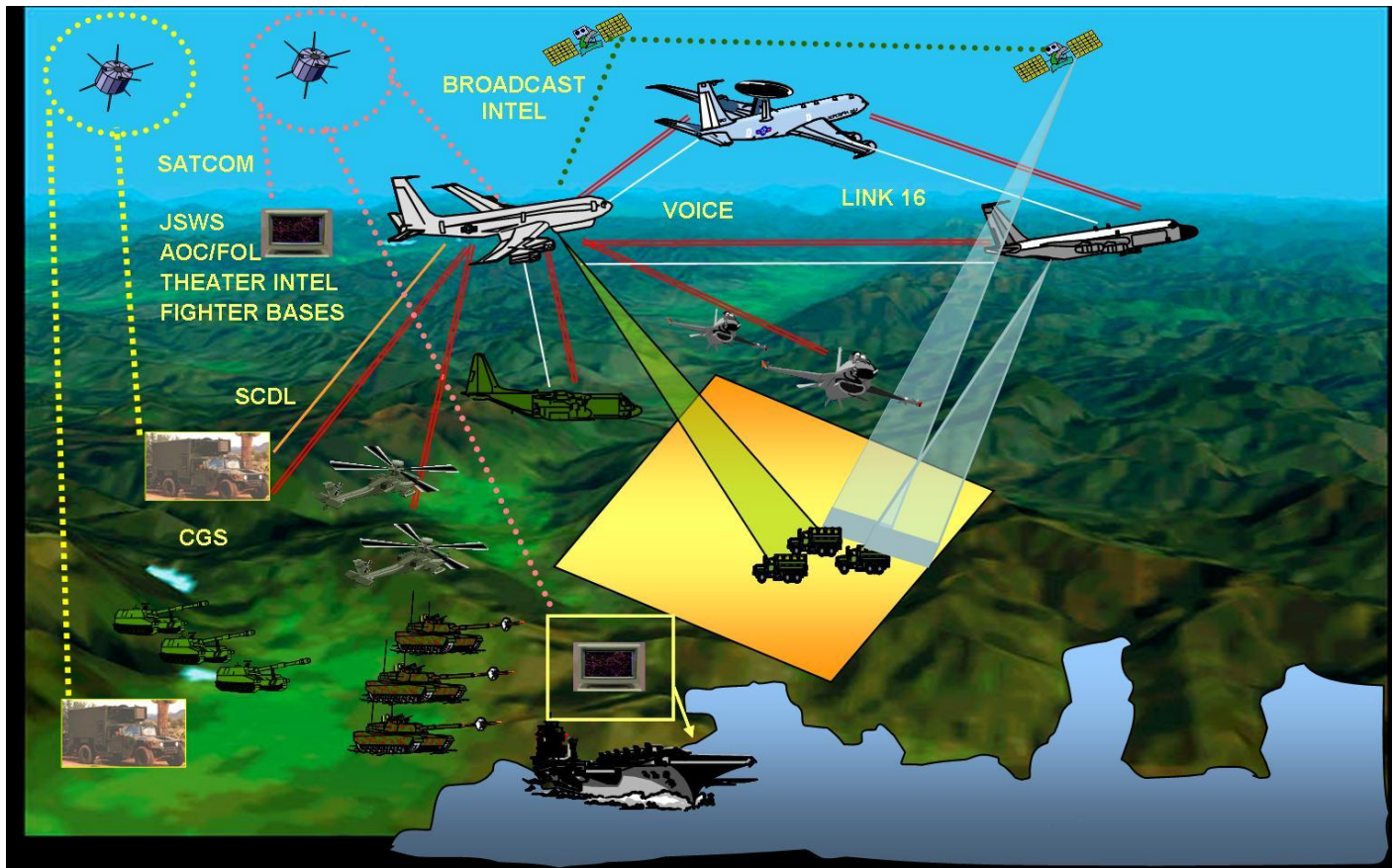


Figure 2: NCW Implementation

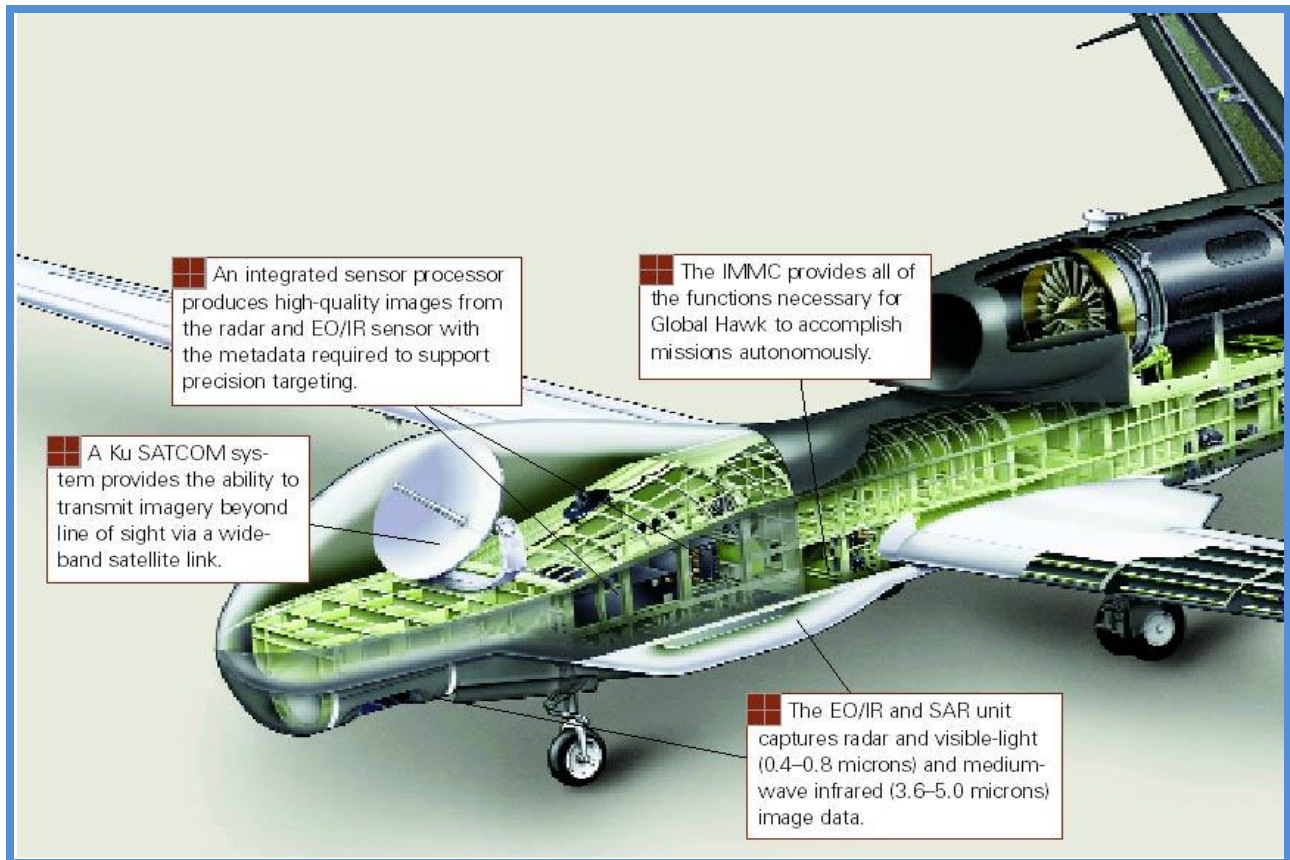


Figure 3: Global Hawk Unmanned Aerial Vehicle Sensor Systems

The recent deployment a state-of-the-art video-crunching NCW system to the AfPak theatre is expected to be significant force multiplier, as reported by officials at Joint Forces Command [27]. The \$29 million Valiant Angel system developed by Lockheed Martin was named to honor the memory of a Navy intelligence official, Angela “Angie” Houtz, who died in the Sept. 11 attack on the Pentagon. Valiant Angel has now been rechristened as the National System for Geo-Intelligence Video Services (NVS) and will allow troops and intelligence operatives better real-time as well as offline access to the humungous amount of video and wide-area imagery gathered by American and allied aircraft as well as other ISR systems [39].

The key elements of a Network Centric Warfare framework include:

- i) Integration of Intelligence, Surveillance and Reconnaissance (ISR) sensors with Command, Control and Communication infrastructure involving manned as well as unmanned airborne, ground or seagoing platforms.
- ii) Capability to operate in the visible, infrared or radar spectra in real-time in a reliable and coordinated manner.

Apart from achieving the stated objectives, a network centric approach to warfare which allows real time data transfer between attack aircrafts, surveillance systems and geostationary satellites dramatically decrease the incidents of collateral damage as shown in the photograph (Figure 4). The Pre and Post strike images show how targets were taken out with surgical precision while minimizing any collateral damage.



Figure 4: Minimizing any collateral damage

2. Literature review

My literature review revealed that while there is a lot of mainstream media coverage regarding incidents of cyber crime that inflict financial damage to the corporate world or even cyber attacks linked to terrorist organizations, the coverage of network system vulnerabilities that might affect the nation's war fighting capability is limited to defense – related journals and publications. This is primarily because not only is network security a complicated topic but the fact that a very small percentage of the people appreciate the technicalities of a Network-Centric Warfare framework, thereby limiting the potential target audience. While a cyber attack on financial or social networking websites, even if it affects millions of users worldwide, would only involve financial or social consequences; a devastating cyber attack on the nation's Network-Centric Warfare framework has the potential to endanger precious lives and a nation's honor in addition to unprecedented financial loss. References [33 – 38] were particularly useful in understanding the technicalities involved in a Network Centric Warfare framework.

3. Threats and vulnerabilities relevant to a Network Centric Warfare framework

Like the public Internet, a typical Network Centric Warfare framework uses the TCP/ IP suite of protocols as its backbone and therefore is automatically susceptible to most of the threats and vulnerabilities relevant to the Internet. In addition to common threats, the NCW framework is also susceptible to attacks aimed at destroying the operational capability of critical infrastructure and espionage. Major threats and vulnerabilities include:

- i) **Malicious code / malware:** Malicious software designed to compromise a target machine without the user's consent is one of the biggest and most potent threats to cyber security. Malware can include viruses, worms, Trojan, rootkits, spyware, crimeware, browser hijackers, keyloggers, backdoors, botnets, logic bombs etc.
- ii) **Denial of Service:** This kind of attack involves overwhelming of the target system's resources resulting in unavailability of services when required. When the target is attacked simultaneously by many nodes, it is known as a Distributed Denial of

Service. Generally these are perpetuated by first compromising vulnerable systems and then controlling those compromised systems (zombies) to launch a coordinated attack.

iii) **Targeted attacks by hackers:** More sophisticated attacks where the attacker either wants to steal some specific data or carry out a denial of service on a specific target.



Figure 5: Threats and vulnerabilities relevant to a Network Centric Warfare framework

- iv) **Application security flaws:** Vulnerabilities like Cross –Site Scripting (XSS) or SQL Injection flaws can be exploited by attackers to cause severe damage to the victim
- v) **Timing Vulnerabilities:** TOCTTOU or TOC/TOU (Time-of-check-to-time-of-use) attacks exploit timing vulnerabilities in systems when the authentication is done too far in advance of granting access to resources.
- vi) **Lack of centralized data processing control for diverse systems :** Since NCW seeks to integrate diverse systems and each system has its own data processing control standards and procedures, vulnerabilities are bound to creep in that can be exploited by sophisticated users.
- vii) **Vulnerabilities brought about by interfacing inherently different technologies to facilitate interoperability:** Most weapon systems and sensors that are interfaced for achieving NCW advantages are created by different vendors each using its own proprietary data handling systems. Achieving seamless interoperability between inherently different technologies often compromises the security of the systems.
- viii) **Communication channel jamming attacks:** These form a central part as communication between the different units is the key requirement for the effectiveness of a NCW framework.
- ix) **Internal threats:** Threats from insiders are often the most difficult to detect and prevent as humans can't be monitored and controlled as easily as machines.
- x) **Swarming:** This refers to a simultaneous coordinated attack by several small units called 'swarm' units against a single target while remaining in constant communication and using real-time information to streamline the attacks. This is similar to a Distributed Denial of Service attack carried out by a botnet except that it is not directed against a website but against critical infrastructure and each of the swarm units is a voluntary participant as opposed to involuntary zombie machines in a botnet.

4. Well known Network attacks

Commercial network based attack incidents get regular media coverage. Though these incidents were not aimed specifically at the NCW framework they still provide lessons that can be learned to protect any national critical infrastructure. Some major incidents include:

a. Network attack in 2006-2007 that resulted in theft of around 170 million credit card numbers

Albert Gonzales, a 28 year-old Florida resident who used the code name the 'soup nazi' has been indicted for the largest ever data breach involving theft of around 170 million credit card numbers [12]. He was the mastermind who was helped by Stephen Watt, a Morgan Stanley investment banker who wrote the sniffing programs and two Russian co-conspirators, known as "Hacker 1" and "Hacker 2." The card information was stolen from Heartland Payment Systems, Inc, a credit card processor and retailers including TJX Companies (TJMaxx and Marshall's), BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, 7-Eleven, Inc., grocery chain Hannaford Brothers Co., and Dave & Buster's. The techniques used involved war driving to locate vulnerable networks and then using a combination of packet sniffers, SQL injection techniques and other malware to create backdoors into the corporate networks and then steal the data.

b. Trojan attack that stole around 1.6 million records from Monster.com

In 2007, a Trojan horse called Infostealer.Monstres was used to steal more than 1.6 million records from the job search company Monster.com belonging to several hundred thousand people [13]. The compromised data included names, e-mail addresses, home address, phone numbers, and other information. This stolen data was then used to target the victims with precision phishing mails that were used to install dangerous and sophisticated malware such as Banker.c and Gpcoder.e on their machines. Banker.c by is an information-stealing Trojan equipped with a key logger that monitors the infected computers for log-on

attempts to online banking and other financial accounts and records the username and password. This data is then transmitted the back to the attacker in a surreptitious manner. The other Trojan, Gpcoder.e belongs to the category of “ransomware”, that is, malware which encrypts files on the hacked computer and then holds those files hostage until the user pays a ransom to decrypt the data.

c. **Conficker worm**

In November 2008, experts detected a highly sophisticated worm called Conficker or Downadup [14, 15]. It used numerous advanced malware techniques and exploited weak administrator passwords and other flaws in the Microsoft Windows operating system to compromise machines and turn them into zombies that could be controlled remotely by the attacker as part of a bot-net. It is now believed to be the largest computer worm infection since the 2003 SQL Slammer, with more than 15 million government, business and home computers in over 200 countries compromised. This attack was a wake – up call in the context of a Network Centric Warfare framework as the following news reports indicate the extent of damage:

- i. **French fighter planes grounded by computer virus** [16]: French fighter jets were unable to take off after military computers were compromised by Conficker and were unable to download flight plans from the database. In fact for some time, the French Navy was instructed not to switch on their computers as Conficker had infected the internal naval network.
- ii. **The British MoD networks were severely affected** for more than two weeks by Conficker [17] resulting in reduced operational availability. As per the military review ‘Defense Tech’, “the British Defence Ministry had been attacked by a hybrid of the virus that had substantially and seriously infected the computer

systems of more than 24 RAF bases and 75 per cent of the Royal Navy fleet including the aircraft carrier Ark Royal.”

- iii. Other victims included the **Greater Manchester Police which could not access a national criminal database for 3 days** [18] and prevented the police from issuing traffic tickets and other penalty notices [19].
- iv. What was perhaps more serious was that Conficker disrupted the **functioning of the British Parliament or the House of Commons** [20].
- v. Conficker also disrupted the functioning of a **hospital network across Sheffield** [21].

The Microsoft Malware Protection Center (MMPC) has identified the following variants of Win32/Conficker [22]:

- a) Worm:Win32/Conficker.A: identified on November 21, 2008
- b) Worm:Win32/Conficker.B: identified on December 29, 2008
- c) Worm:Win32/Conficker.C: identified on February 20, 2009
- d) Worm:Win32/Conficker.D: identified on March 4, 2009
- e) Worm:Win32/Conficker.E: identified on April 8, 2009

Figure 6 is an illustration describing the working of the Conficker worm [23]:

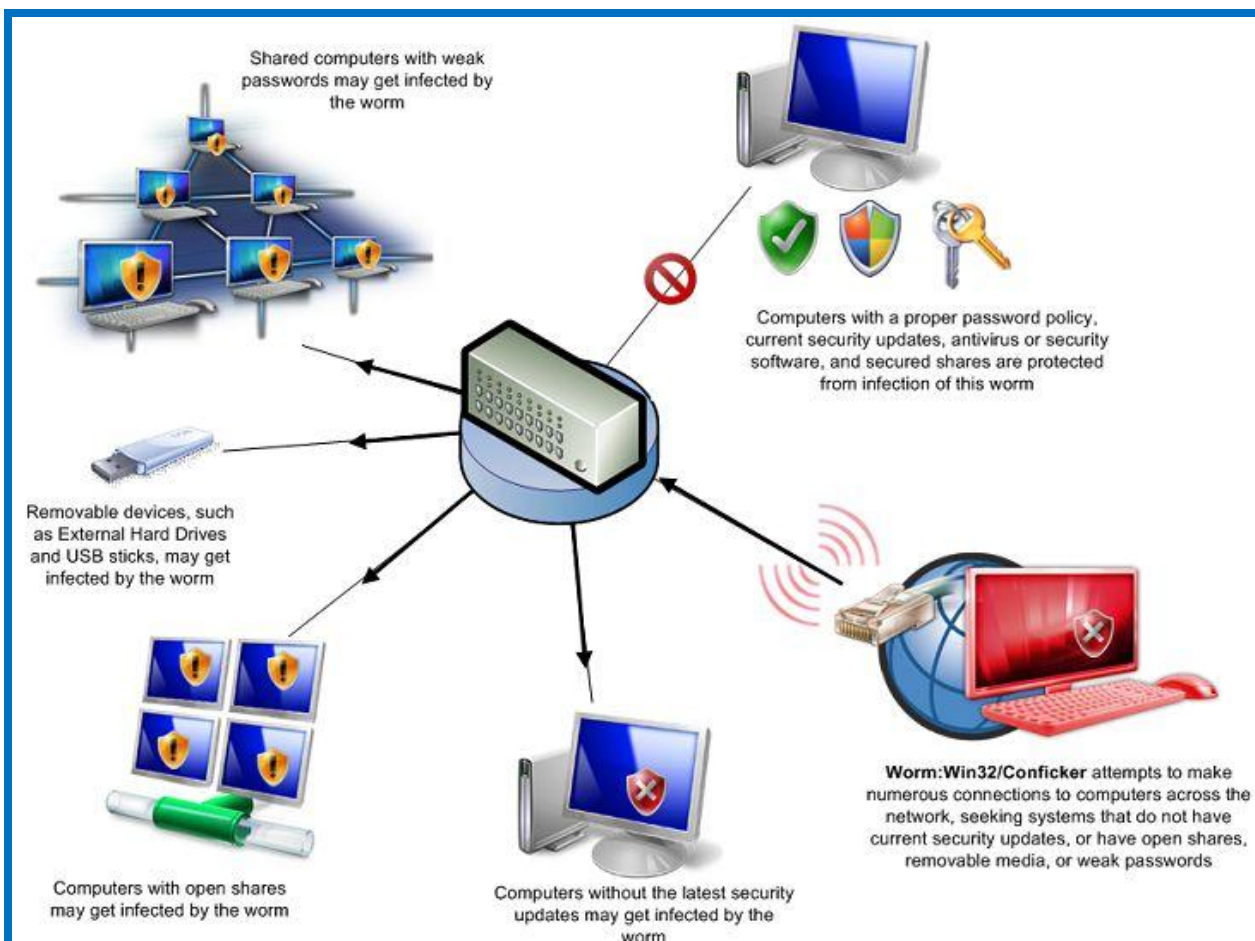


Figure 6: Working of the Conficker worm

As per Microsoft, “the mechanism to command and control Conficker.D-infected machines is a two-step process as shown in figure 7:

- (a) By registering just a single domain name out of the 50,000 generated per day, roughly 1% of the total number of Conficker.D-infected machines will be able to receive commands from the malware author.
- (b) Using its P2P mechanism, these machines will be able to distribute the original commands to other Conficker.D-infected peers.”

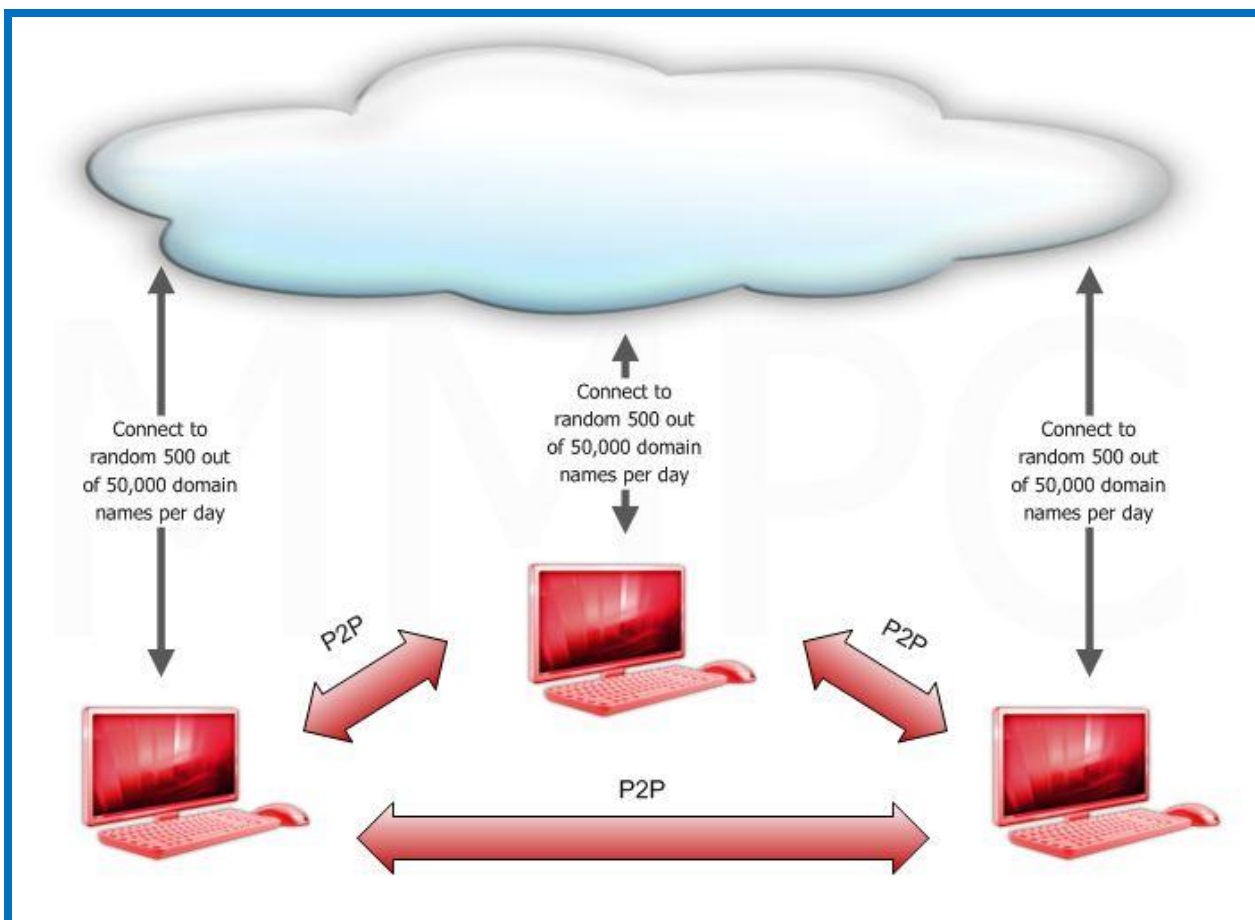


Figure 7: Conficker.D mechanism

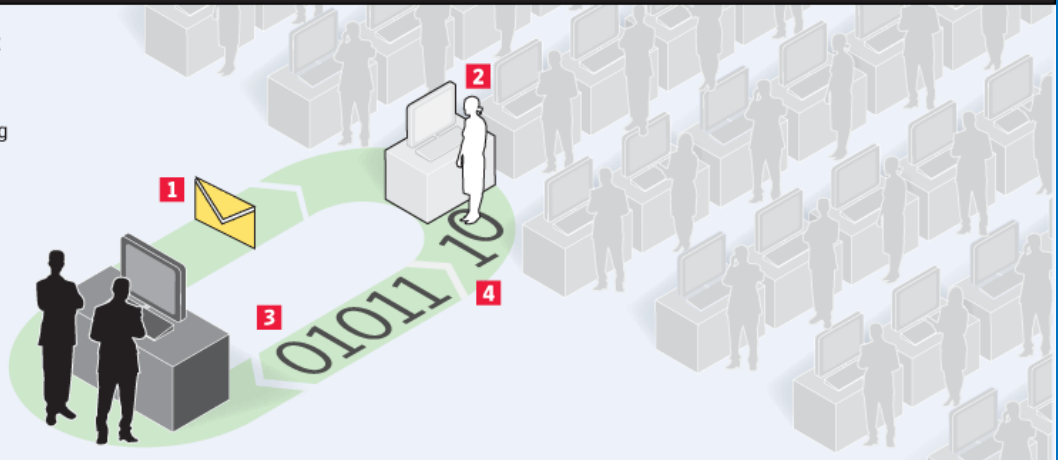
d. Kneber botnet / Zeus

The Kneber botnet / Zeus is a Trojan that steals banking and social networking information by using a key logger [24]. It has compromised more than 74,000 accounts on nearly 2,411 companies including the Bank of America, Facebook, NASA, Monster, ABC, Oracle, Cisco, Amazon, and Business Week. The number of compromised computers is in millions with approximately 3.6 million in the US

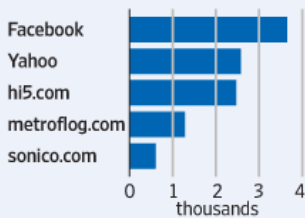
The Zeus botnet targets computers running Windows XP specifically though older versions of Windows are also susceptible. The United States Department of Transportation is among the victims of data theft of the Zeus botnet. The mechanism of spread is depicted in figure 8 below [25]:

Recruiting a Botnet Army | How the attack spread

- 1** Hackers entice users to click on contaminated Web sites or open email attachments.
- 2** Users open the file, installing the malicious software.
- 3** The malware is used to capture data typed into Web forms or find login credentials stored on the user's system and then send it back.
- 4** The software checks in periodically for updates, allowing the hacker to revise or update the malware.



Number of credentials stolen via the ZeuS spyware virus, by site



Source: NetWitness
Erik Brynildsen and Randy Yeip/
The Wall Street Journal

Countries affected by the ZeuS virus

At least one computer affected

Number of compromised machines

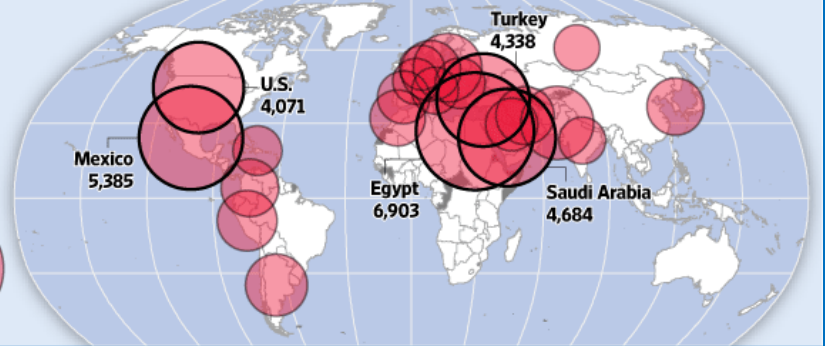
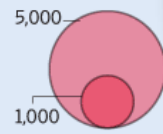


Figure 8: The Kneber botnet

e. Torpig

Torpig, also known as Sinowal or Mebroot is a type of botnet spread by a variety of Trojan horses that has compromised more than 2000 domains by circumventing anti-virus applications. RSA security labs claim that this botnet has compromised more than 270,000 banking accounts and 240,000 credit and debit cards throughout the world.

f. Hacking of US drones

In 2009, the Wall Street Journal reported that militants in Iraq as well as Afghanistan had used COTS software worth \$26.00 to hack into the live video feeds from US Predator drones [26]. The report mentioned that militants used software programs

such as SkyGrabber -- available for as little as \$25.95 on the Internet -- to regularly capture drone video feeds, thereby removing the battlefield advantage that is gained by the element of surprise. The vulnerability lies in an unencrypted downlink between the unmanned Predator drone (shown in figure 9) built by General Atomics Aeronautical Systems Inc. of San Diego and the ground control station.



Figure 9: Hacked US Predator drone

5. Cyber warfare incidents and related terminology

a. Stuxnet

The Stuxnet worm discovered in 2010 is touted as a new generation of cyber warfare and is unique for being the first malware that subverts industrial systems and includes a root-kit for targeting Programmable Logic Controllers (PLCs). PLCs are digital computers used for automation of electro-mechanical processes in various industries. Stuxnet was designed with great care to hit only certain industrial targets. Its multi-

layer attack focuses on systems that use the Siemens Supervisory Control And Data Acquisition (SCADA) systems, Windows family of Operating Systems, Siemens PCS 7, WinCC and STEP7 industrial software applications that run on Windows, and one or more Siemens S7 PLCs. Different variants of the Stuxnet worm have affected five Iranian institutions and are credited with severely restricting the functioning of Iran's uranium enrichment infrastructure. Based on the sophistication of the attack as well as the fact that almost 60% of all known attacks have been in Iran, experts believe that it may have been deliberately targeting Iranian "high-value infrastructure" including either the Bushehr Nuclear Power Plant or the Natanz nuclear facility [40]. News reports also attribute the successful targeting of the Iranian nuclear plant to thorough testing of the effectiveness of the worm in Dimona, Israel which houses nuclear centrifuges virtually identical to those at Natanz [41]. Based on various news reports and views of experts it is believed that Stuxnet was a joint American-Israeli cyber warfare project designed to sabotage the Iranian nuclear program.

b. Starz

In April 2011, Iran claimed that it had been hit by a second wave of cyber warfare in the form of an "espionage virus" called "Stars". The head of an Iranian military unit that deals with countering sabotage stated that the virus is being investigated and initial reports indicated that Stars is "harmonious" with computer systems and *"inflicts minor damage in the initial stage and might be mistaken for executive files of governmental organizations."*

c. Operation Aurora

This refers to a series of cyberattacks in 2009 that Google claims originated in China. The targets included big US businesses such as Google, Adobe Systems, Juniper Networks, Yahoo, Symantec, Northrop Grumman, Rackspace and Dow Chemicals [29]. It is believed that the aim of Operation Aurora was to access and possibly alter source code repositories at these high tech, security and defense contractor companies.

d. Titan Rain

This refers to a series of attacks on US computer systems initiated in 2003 and directed at NASA, Lockheed Martin, Sandia National Labs, and Redstone Arsenal and described by the SANS institute as "most likely the result of Chinese military hackers attempting to gather information on U.S. systems"

e. Moonlight Maze

This refers to a series of coordinated attacks on US computer systems initiated in 1999 believed to have originated from Moscow and aimed at obtaining classified information relating to missile guidance systems and naval codes.

f. GhostNet

This refers to a large scale cyber spying operation controlled by China that has compromised "high-value political, economic and media locations in 103 countries" [31] as reported by Information Warfare Monitor (IWM) investigators. As per reports, Around 1,295 computer systems belonging to embassies, foreign ministries, banks, news offices and other government offices, and the Dalai Lama's Tibetan exile centers in India, London and New York City were compromised.

g. Honker Union

This refers to a group of Chinese hackers known for hacktivism or cyber-political activism.

h. The Dark Visitor

This refers to a blog run by a former US Army officer that emphasizes Chinese hacking attacks and among other things exposed the 2008 Chinese DDoS attack on CNN.com

6. Potential of cyber attacks on the Network-Centric Warfare framework and countermeasures

Given the almost identical nature of the backbone structure (hardware, software and communication technologies) of the public internet and the private Network Centric Warfare framework, there is a clear and present danger of a crippling attack on specific parts of the NCW framework. Experts believe that the absence of any major attack till date may be attributed to the lack of political will rather than a lack of technical capability. While cyber attacks against websites can be treated as proxy war or cold war tactics primarily causing nuisance or only business losses, any specific attack against a Network Centric Warfare framework is bound to be treated by the target country as an act of war and is bound to generate a response against the perpetrator that would include conventional warfare strategies. This has been the primary deterrent that has prevented the occurrence of any high-profile incident targeting the Network Centric Warfare framework.

During a hearing of the Senate Committee on Commerce, Science and Transportation as part of the deliberations for Cyber Security Act of 2009, Michael McConnell, a former director of national security and national intelligence, testified that US being the most connected nation and the one that relies most heavily on a Network Centric Warfare framework, is the most vulnerable and stands to lose the most. He stated, *“If the nation went to war today in a cyberwar, we would lose”*. James Lewis, a senior fellow at the nonprofit Center for Strategic and International Studies (CSIS) added that the US is *“under attack every day, losing every day vital secrets”* and that *“There are people who could attack us now: Russia, China, some others, our potential military opponents. And we know they've done reconnaissance on the electrical grid.”* Experts agreed that certain countries have the capability to shut down and disrupt basic utilities like power and water supply in various parts of the US.

A recent report by security company M86 Security, indicated that Malware-carrying spam and attacks via social networking sites such as Twitter and Facebook grew dramatically in the second half of 2009, indicating that cyberattacks in general are bound

to grow at a very high rate unless proper precautions are taken [30]. The report says, “the vast majority of spam is now sent through botnets hiding on infected computers--the second half of 2009 alone saw 78 percent of all spam triggered by the top five botnets, such as Rustock and Pushdo”. The distribution of spam by botnet for the period June to Dec 2009 is shown in figure 10 below:

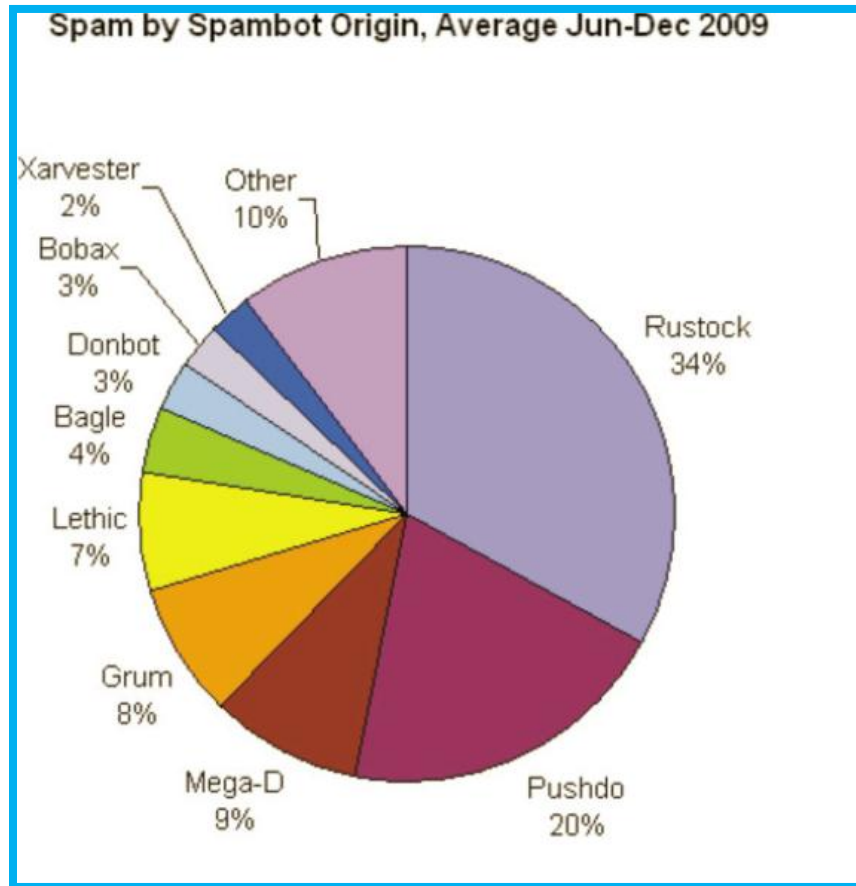


Figure 10: Distribution of spam by botnet

7. Conclusion

The relevance of information systems security can hardly be overemphasized. While cyber-warfare losses are already in millions of dollars, the real catastrophe would be when cyber attacks cross the realm of the inherently insecure public networks and cause damage to secure networks that form the infrastructure of Network-Centric Warfare. It is logical to infer that the Network Centric Warfare Framework will prove to

be Cyber War's Final Frontier. Much more than financial loss alone, such a scenario holds the potential for loss of precious innocent lives as well as compromising national honor especially when the country is engaged in two wars. While more needs to be done to secure the NCW framework, the Cybersecurity Act of 2009 is a step in the right direction. It allows the President to "declare a cybersecurity emergency" and shut down or limit Internet traffic in any "critical" information network "in the interest of national security." [28]. Further, it also grants the Secretary of Commerce "access to all relevant data concerning [critical] networks without regard to any provision of law, regulation, rule, or policy restricting such access."

References

1. Experts warn of catastrophe from cyberattacks By Elinor Mills, CNET News.com on February 25, 2010 <http://www.zdnetasia.com/experts-warn-of-catastrophe-from-cyberattacks-62061413.htm>
2. "Network-Centric Warfare - Creating a Decisive Warfighting Advantage" , Director, Force Transformation, Office of the Secretary of Defense
3. Network Centric Warfare: Background and Oversight Issues for Congress, Clay Wilson, Congressional Research Service, The Library of Congress
4. *Network centric warfare* : Developing And Leveraging Information Superiority; David S Alberts, John J Garstka, Frederick P Stein
5. <http://www.psycom.net/iwar.1.html>
6. C4ISR For Future Naval Strike Groups, National Research Council (U.S.), Committee on C4ISR for Future Naval Strike Groups Staff, Washington, DC, USA: National Academies Press, 2006.
7. DoD Architecture Framework Version 1.5
8. http://www.aeronautics-sys.com/ncw_network_centric_warfare
9. Remote Sensing And Military Transformation - Lifting The Fog Of War, Brian D. Graves - ES 771, <http://www.emporia.edu/earthsci/student/graves1/project.html>
10. Information warfare, Winn Schwartz
11. Information Warfare, Daniel Ventre, ISTE Ltd and John Wiley and sons

12. http://www.afterdawn.com/news/article.cfm/2009/09/13/albert_gonzalez_plads_guilty_to_stealing_170_million_credit_card_numbers
13. <http://www.networkworld.com/news/2007/082007-monster-trojan.html>
14. http://www.upi.com/Top_News/2009/01/26/Virus-strikes-15-million-PCs/UPI-19421232924206/
15. <http://edition.cnn.com/2009/TECH/ptech/01/16/virus.downadup/?iref=mpstoryview>
16. <http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html>
17. http://www.theregister.co.uk/2009/01/20/mod_malware_still_going_strong/
18. http://news.bbc.co.uk/2/hi/uk_news/england/manchester/8492669.stm
19. http://www.theregister.co.uk/2009/07/01/conficker_council_infection/
20. http://www.theregister.co.uk/2009/03/27/conficker_parliament_infection/
21. http://www.theregister.co.uk/2009/01/20/sheffield_conficker/
22. <http://technet.microsoft.com/en-us/security/dd452420.aspx>
23. <http://www.microsoft.com/security/worms/conficker.aspx>
24. Massive Hack Attack Shows Major Flaws in Today's Cybersecurity, <http://www.foxnews.com/scitech/2010/02/18/massive-hack-attack-shows-major-flaws-todays-cybersecurity/>
25. <http://online.wsj.com/article/SB10001424052748704398804575071103834150536.html?mod=yhoofront>
26. Insurgents Hack U.S. Drones, <http://online.wsj.com/article/SB126102247889095011.html>
27. <http://www.c4isrjournal.com/story.php?F=4543953>
28. <http://motherjones.com/politics/2009/04/should-obama-control-internet>
29. Wikipedia.org
30. Malware and social network attacks surge in '09, http://news.cnet.com/8301-1009_3-10454870-83.html
31. Chinese hackers 'using ghost network to control embassy computers' <http://www.timesonline.co.uk/tol/news/uk/crime/article5996253.ece>
32. <http://news.bbc.co.uk/2/hi/technology/7701227.stm>
33. The Implementation of Network-Centric Warfare, Department of Defense, Office of Force Transformation, [2005]
34. Measures of effectiveness for the Information Age Navy, Walter Perry et al., National Defense Research Institute
35. Network-Centric Warfare and Wireless Communications http://www.meshdynamics.com/documents/MD_MILITARY_MESH.pdf
36. Network-Centric Warfare: Its Origin and Future By Vice Admiral Arthur K. Cebrowski, U.S. Navy, and John J. Garstka http://www.kinexion.com/ncoic/ncw_origin_future.pdf

37. Network-Centric Warfare And Its Function In The Realm Of Interoperability, Joseph M. Ladymon, Acquisition Review Quarterly — Summer 2001
38. The *C4ISR* Architecture Framework, Integrated Architectures Panel of the C4ISR Integration Task Force
39. Intell video moves to a Netflix model, Paul Richfield,
<http://gcn.com/articles/2011/03/29/c4isr-1-battlefield-full-motion-video.aspx>
40. Was Stuxnet Built to Attack Iran's Nuclear Program?, Robert McMillan, IDG News,
http://www.pcworld.com/businesscenter/article/205827/was_stuxnet_built_to_attack_iran_s_nuclear_program.html
41. Israeli Test on Worm Called Crucial in Iran Nuclear Delay,
<http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>
42. Iran says it has uncovered second cyber attack,
http://news.yahoo.com/s/ap/20110425/ap_on_re_mi_ea/ml_iran_cyber_attack