National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CLICKS-KRIEG! THE OFFENSIVE-DEFENSIVE NEXUS IN CLAUSEWITZIAN CYBERSPACE

LCdr R.K. Dolan

JCSP 40

Exercise *Solo Flight*

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 40

Exercice *Solo Flight*

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 40 – PCEMI 40

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

CLICKS-KRIEG! THE OFFENSIVE-DEFENSIVE NEXUS IN CLAUSEWITZIAN CYBERSPACE

LCdr R.K. Dolan

Word Count: 3053

Compte de mots: 3053

CLICKS-KRIEG! THE OFFENSIVE-DEFENSIVE NEXUS IN CLAUSEWITZIAN CYBERSPACE

INTRODUCTION AND THESIS

The last twenty years have seen a colossal change in terms of the influence that computer networks have had in both contemporary society and on the battlefield. In 2014, more than two billion people around the globe accessed the Internet on a daily basis, and modern militaries have fully embraced the concept of "Network Centric Warfare." Computers networks have emerged as both the major driver of social change and as the premier military force-multiplier of the 21st century.

At first glance, cyber operations in the 21st century seem far removed from a book published in 1832 which made only passing reference to the role of technology in war.[1] Clausewitz did, however, openly acknowledge that the means and modes of warfare change over time – his own era was far too revolutionary to believe anything else. "Wars in every period have independent forms and independent conditions."[2] The underlying principles of war that Clausewitz highlighted remain constant, regardless of how much the tools that implement those principles have changed. Clausewitz "intended to provide a thinking man with a frame of reference . . . rather than to serve as a guide, which at the moment of action lays down precisely the path he must take."[3]

The digitization of modern warfare has not only revolutionized the traditional warfare domains of land, sea, and air, but has also created its own warfare domain – cyberspace. This paper will illustrate that while the technologies behind cyberspace are

[1] Antulio J. Echevarria, "War And Politics: The Revolution In Military Affairs And The Continued Relevance Of Clausewitz" Joint Forces Quarterly, Winter 1995-96. Available online at http://www.clausewitz.com/readings/Echevarria/ECHJFQ.htm Internet: Accessed 05 May 2015.

[2] David Aucsmith, "War in Cyberspace." Available online at http://cyberbelli.com. Internet: accessed 02 May 2015. Pg.2.

[3] Michael Howard, Clausewitz On War. Washington: Library of Congress, 1998. Pg. 12.

entirely new, the strategic objectives of cyberwar are not. In their search to understand cyberspace and write guiding doctrine for cyberwar, policy makers and military leaders can utilize classical strategy to better understand the new cyber environment. After a brief introduction of key concepts in both Clausewitz's classic *On War* and in cyberspace, this paper will highlight Clausewitzian theories on the nature of the offence and defence in war. The continued relevance of these theories in relation to cyberwar will be clearly shown, and Clausewitz's arguments regarding the primacy of the defence and the revolutionary nature of an armed, mobilized populace will be proven to retain their validity, even in cyberspace.

CYBERSPACE: THE FIFTH DOMAIN OF WAR

In 2005, the U.S. National Defense Strategy stated, "Cyberspace is a new theater of operations… the Pentagon has formally recognized cyberspace as a new domain of warfare."[4] Later that same year, the *Economist* proclaimed, "Warfare has entered the fifth domain: cyberspace."[5] In the last decade, the term "cyberspace" and the activities that occur within it have been poorly defined and have assumed what one author called "the shape of an elephant assessed by a group of blind people."[6] While many definitions exist, for the purposes of this paper cyberspace is defined as, "a global domain within the information environment consisting of the interdependent network of information

[4] Diego Rafael Canabarro, "Reflections on The Fog of (Cyber)War." *National Center for Digital Government.* Available online at http://www.umass.edu/digitalcenter/research/working_papers/13_001_Canabarro-Borne_FogofCyberWar.pdf Internet: Accessed 04 May 2015. Pg. 8.

[5] Ibid, 12.

[6] Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends." *Institute for System Studies and Analysis.* Available online at https://ccdcoe.org/publications/virtualbattlefield/01_SHARMA_Cyber_Wars.pdf Internet: Accessed 05 May 2105. Pg. 3.

technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[7]

To define cyberspace as a warfare domain, similar to air, land, and maritime, is a recent phenomenon and a significant acknowledgement of the importance of cyberspace to modern warfare. Governments around the world have recognized that much as maritime operations rely on safe harbours and navigable water, cyber operations depend on an interdependent network of IT infrastructure that includes computers, mobile devices, and the data that flows through them. In this context, cyberspace can be understood as a domain of war created by man, facilitated by technology and dependant upon communications. With key physical components potentially residing in multiple countries, and with networks spanning geopolitical boundaries, cyberspace is a unique domain of warfare.[8] For example, a cyber specialist working for the Canadian government in Ottawa may routinely utilize network servers physically located in a land-based data complex in Europe or Asia, in order to retrieve data that can be transmitted via wireless networks that pass though land, air, and space. In the 21st century, cyberspace forms a global common that empowers military forces, economic trade and all aspects of cultural interaction. It is a new and pervasive environment, and both state and non-state actors actively contest its freedom of use.[9]

---

[7] United States Department of Defense, *Joint Publication 3-12 (R), Cyberspace Operations*. 05 February 2013. Available online at http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf Internet: Accessed 26 May 2015. Pg.v.

[8] Ibid.

[9] Aucsmith, 3.

CYBER OFFENSE: THE MEANS OF ATTACK

The term "cyberwar" should be understood to mean the use of cyberspace by a state or non-state actor to disrupt, deny, degrade, manipulate, or destroy information resident in computer networks, or to destroy or damage the computers or networks themselves.[10] Offensive attacks in cyberwar are initiated and conducted by either state or non-state actors. Due to their access to resources and manpower, cyber-attacks conducted by nation states are potentially the most dangerous.[11] China, Russia, and the United States, for example, all have robust and well-funded cyberwar programs. Non-state actors can either be individuals attempting to gain illegal access to networks for criminal or ideological purposes, or transnational groups such as Anonymous, ISIS or Hezbollah who use cyberspace to fundraise, indoctrinate potential recruits, and to plan and conduct operations.[12]

While state and non-state actors may utilize a wide variety of cyber weapons to launch an offensive, they typically seek to either deny, degrade, disrupt or destroy a targeted network or piece of infrastructure. Like their more conventional brethren, these attacks may serve a strategic purpose, such as compromising civil security by targeting national information systems, or have strictly tactical objectives, such as disrupting military communications in a certain district or disabling a specific weapon system.[13]

Cyber-attacks can also span the entire spectrum of conflict, ranging from relatively passive surveillance and espionage, to more obtrusive attacks that deny access to

---

[10] Craig B. Greathouse, "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?" *Cyberspace and International Relations: Theory, Prospects and Challenges.* Springer Link Publishers, 2014. Pg. 22.

[11] US DOD *Joint Publication 3-12, pg. I-6.*

[12] Ibid, I-6.

[13] Greathouse, 24.

information and even damage or destroy actual physical infrastructure. Espionage is commonplace in cyberspace, with nations such as China using cyberspace to conduct extensive espionage operations against political, industrial, and military targets throughout the West.[14] One American government official claimed that "Chinese intelligence services have essentially stolen enough classified and proprietary information to fill the Library of Congress."[15]

Denial of Service (DoS) attacks are a more aggressive form of cyber-attack which overwhelm a particular website or network by overloading it with data and crashing the network. In April 2007, Russian entities utilized DoS attacks to target strategic and operational objectives in Estonia, which disrupted government websites, shut down bank services and crippled the Estonian media, all in response to a political disagreement between the two nations.[16] Later that same year, Russia conducted similar DoS attacks in Georgia, where they were meant to assist Russian troops as they moved into disputed territory.[17] "Georgian elites were unable to communicate with each other and the outside world during the military campaign, thus retarding their ability to react to events in a timely manner."[18]

The most advanced form of cyber-attack is one that affects physical infrastructure via digital means. In this scenario, the software which controls an important piece of enemy infrastructure is destroyed or damaged by a cyber-attack. This might include a

---

[14] John B. Sheldon, "Deciphering Cyberpower - Strategic Purpose in Peace and War." *Strategic Studies Quarterly*, Summer 2011. Available online at http://www.au.af.mil/au/ssq/2011/summer/sheldon.pdf Internet: accessed 11 May 2015. Pg. 96.

[15] Ibid, 99.

[16] Samuel Liles, "Applying Traditional Military Principles to Cyber Warfare." 4th International Conference on Cyber Conflict, 2012. Available online at https://ccdcoe.org/publications/2012proceedings/3_2_Liles&Dietz&Rogers&Larson_ApplyingTraditionalMilitaryPrinciplesToCyberWarfare.pdf Internet: Accessed 03 May 2015. Pg. 171.

[17] Greathouse, 27.

[18] Sheldon, 97.

computer system operating an adversary's electrical grid, water distribution system, banking network, etc. Until recently, this type of attack had been theorized but not implemented; however, that changed in 2010 with the discovery of the Stuxnet virus. Developed by the American government, Stuxnet managed to attack and disable vital components of the Iranian nuclear program by targeting the specific computerized control systems used at the underground nuclear facility.[19] For the first time, Stuxnet proved that physically damaging a target via cyberspace *is* possible.

CYBER OFFENCE: THE METHOD OF MASS MOBILIZATION

The evolution of cyber-attack tools has been significant, but the real revolution lies in how these weapons have spread to an increasingly cyber-connected populace. This cyber-mobilization, similar to the French Revolution's *levée en masse*, has made cyberwar the business of an entire population, rather than just the military. As Clausewitz commented on the Napoleonic wars, "Instead of governments and armies, the full weight of the nation was thrown into the balance… War, untrammeled by any conventional restraints, had broken loose in its elemental fury."[20] In the 19th century, the *levée en masse* was truly a turning point in modern warfare, as a combination of conscription, education and ideology swelled the ranks of the Army and brought broad popular support to the war effort: "The French populace was reached, radicalized, educated, and organized to save the revolution and fight its wars."[21]

---

[19] (Farwell and Rohozinski 2011)

[20] Howard, 110.

[21] Audrey Kurth Cronin, "Cyber-Mobilization: The New Levée en Masse." *Parameters*, Summer 2006. Available online at http://spgia.gmu.edu/wp-content/uploads/PDFs/Audrey_Kurth_Cronin/cybermobilization.pdf Internet: Accessed 02 May 2015. Pg.79.

The parallels between the 21st century and the revolutionary years that influenced Clausewitz's *On War* are numerous. Modern communication via the Internet has never been more deregulated or democratic, similar to conditions in France at the end of the 18th century.[22] Technology and education caused print media of the revolutionary era to expand dramatically, without any form of regulation or oversight regarding the veracity of the information being printed.[23] Similarly, cyberspace has democratized global communications with increasingly cheap and ubiquitous access to the Internet, prompting a remarkable increase in public access to information and virtual venues to exchange ideas. As in 19th century France, this creates opportunities for radicalization and mass mobilization.

Cyberspace enables the recruitment and radicalization of citizens who may be physically located thousands of miles from the actual battlespace. In March of 2015, three teenage British girls were detained in Heathrow Airport, enroute to Syria, after having been recruited by ISIS via social media. Following their arrest, the director of the US National Counterterrorism Center commented, "You have the Islamic State using all forms of media and outreach… youth are being drawn like the Pied Piper to this movement in the Middle East."[24] Much like the Stuxnet virus described earlier, this is another example where activities in cyberspace are having a tangible and damaging impact on the physical battlefield.

---

[22] Cronin, 84.

[23] Adam Elkus, "Rise of Cyber Mobilization." Feb 2009. Available online at https://www.oodaloop.com/uncategorized/2009/02/13/the-rise-of-cyber-mobilization/ Internet: Accessed 04 May 2015. Pg. 2.

[24] Rebecca Kaplan, "ISIS Recruiting Teenagers." *CBS News*, March 10 2015. Available online at http://www.cbsnews.com/news/isis-recruiting-teenagers-why-the-government-is-sounding-the-alarm/ Internet: Accessed 20 May 2015.

As historian Audrey Cronin wrote, "It is no accident that the rise of mass warfare coincided with a huge explosion in the means of communication."[25] Just as Napoleon used revolutionary fervor to form a popular army, today's combatants are increasingly creating a cyber levée en masse that mobilizes the power of the people.[26] The cyber-attacks against Georgia in 2008, for example, were reportedly conducted by groups of patriotic Russian hackers, distributed throughout the country, rather than being centrally orchestrated by the Kremlin itself.[27] This ability to rally and direct a mob of physically disparate yet closely networked bodies in cyberspace represents the new *levée en masse*, and its impact on the cyber offensive is just as revolutionary now as it was in the 19th century.[28]

> From the global spread of Islamist-inspired terrorist attacks, to the rapid evolution of insurgent tactics in Iraq, to the riots in France, and well beyond, the global, non-territorial nature of the information age is having a transformative effect on the broad evolution of conflict.[29]

CYBER DEFENCE: THE DIGITAL FORTRESS

Book VI of *On War*, titled "The Defence," is by far the longest chapter; it arguably speaks to the importance Clausewitz placed on the ideas therein. Clausewitz argues that although the offense may initially have the advantage, "the defensive form of warfare is intrinsically stronger than the offensive."[30] Given enough time, the defence will gain the "home soil" advantage due to its familiarity with the local terrain, the benefit of a well-established fortress, and the support of the public in the surrounding countryside.[31] He

---

[25] Cronin, 78.
[26] Liles, 173.
[27] Greathouse, 28.
[28] Liles, 173.
[29] Elkus, 4.
[30] Howard, 357.
[31] Ibid, 393.

advocated a theory of defensive attrition; the defender holds out until the attacker's will and/or resources are depleted and can no longer hold the territory he has gained or maintain his lines of communication.[32] Modern cyber defence utilizes the same strategy.

With both state and non-state actors armed with cheap and readily available tools for infiltration and destruction, cyber defence seems daunting. Information technology specialists generally agree that there are three fundamental principles of security in the cyber domain: confidentiality, integrity, and availability. If you can prevent the unauthorized disclosure of information (espionage), keep it from being maliciously modified (distort/destroy) and ensure that the information is available when required (delay/deny), you will have thwarted the fundamental forms of cyber-attack and maintained cyber security.[33]

Cyber defence currently depends on the concept of "defence in layers" in much the same way as armies in both the modern era and in Clausewitz's time relied on "defence in depth." By limiting physical access to information systems and by erecting digital firewalls, multiple layers of defence are installed in order to make penetration of the network impossible.[34] Like a fortress under siege relying on a deep moat and high walls, these defences only slow the attacker – given enough time and enough resources, any cyber defence can be breached. Vulnerabilities in the hardware or software that shapes the cyber terrain can lead to defensive failure, as can mistakes by those who use it. Effective cyber defence relies on an attack being slowed enough that either the attacker is

---

[32] Mary Kaldor, "Inconclusive Wars: Is Clausewitz Still Relevant in these Global Times?" *Global Policy* Volume 1, Issue 3. October 2010. Available online at http://www.globalpolicyjournal.com/articles/conflict-and-security/inconclusive-wars-clausewitz-still-relevant-these-global-times Internet: Accessed 09 May 2015.

[33] Aucsmith, 4.

[34] Sharma, 5.

deterred and gives up, or that the attack takes long enough that the origin can be detected and dealt with, either in the physical domain or via a cyber counterattack.

THE MASSES VS THE FORTRESS: WHO WINS?

As described above, the cyber offensive is characterized by its lightning speed, limitless range, low cost and relative anonymity.[35] The ability of cyber-attacks to seem both instantaneous and ubiquitous can put a computer network under tremendous pressure.[36] For these reasons, several academics have argued that contrary to Clausewitz's theories, in cyberwar the offense holds and maintains the advantage. In 2010, Harvard professor Jack Goldsmith wrote that "cyberspace is an arena where the offense already has a natural advantage."[37] In a 2011 article, Rafal Rohozinski from the University of Toronto wrote an article in which he was strident in depicting offensive cyberattacks as intrinsically stronger than defensive cyber-security.[38] The arguments of these authors and others are based on the fact that cyber-attacks utilize relatively inexpensive and readily accessible weapons, while cyber defence can be expensive to establish and highly complex to properly maintain. Malware and the other tools of cyber-attack are typically less complex, cheaper and faster to create, quickly arming the titular "masses," while the fortress of cyber defence relies on a complex architecture of firewalls and technical procedures. As Joseph Nye wrote, "When the average malware contains

---

[35] Jeppe Jacobsen, "The cyberwar Mirage and the Utility of Cyberattacks in War." *DIIS Working Paper*, 2014. Available online at http://www.diis.dk/files/media/publications/import/extra/diis-wp_2014-06_teglskov_web_1.pdf Internet: Accessed 16 May 2015. Pg.14.

[36] Sheldon,98.

[37] Jack Goldsmith, "The Cyberthreat, Government Network Operations, and the Fourth Amendment." Brookings Institute, December 2010. Available online at http://www.brookings.edu/~/media/research/files/papers/2010/12/08-4th-amendment-goldsmith/1208_4th_amendment_goldsmith.pdf Internet: Accessed 06 May 2015.

[38] Rafal Rohozinski, "Stuznet and the Future of CyberWar." *Survival: Global Politics and Strategy*, February-March 2011. Available online at https://www.iiss.org/en/publications/survival/sections/2011-2760/survival--global-politics-and-strategy-february-march-2011-f7f0/53-1-05-farwell-and-rohozinski-f587 Internet: Accessed 15 May 2015. Pg. 4.

only 125 lines of code, while defensive systems have millions, offensive cyberattacks appear a cheap and attractive capability."[39]

The cost-benefit analysis of cyber offence vs defence does initially seem to favour the latter. Not only is cyber-attack relatively cheap to execute, due to the advantages of anonymity and difficulties with attribution, there is also little penalty for failure. Reconnaissance of an enemy computer network can be conducted with little fear of retaliation.[40] Cyber-attacks offer immediate return on investment, as once an adversary system is compromised, it can be rapidly exploited for immediate rewards.[41] In comparison, cyber defence is expensive, challenging, and with little immediate return on investment.

Despite these arguments to the contrary, it must be realized that the low cost, low risk advantages of the cyber offense are short-lived, and that Clausewitz's assertion of the primacy of the defence is still valid. The great equalizer is the sheer size, scale and diversity of cyber defences, particularly when considered alongside the highly limited endurance of cyber-attacks. The vast number of different IT systems operating around the globe, each with unique firewall configurations and security protocols, drastically limits the effectiveness of cyber weapons. Each cyber weapon must be tailored to defeat a specific vulnerability within a specific defensive network in order to be successful.[42] "The infinite engineering options available for those who develop information systems

---

[39] Joseph Nye, "Cyber Power." Harvard Kennedy School, May 2010. Available online at http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf Internet: Accessed 04 May, 2015. Pg. 12.

[40] Kenneth Geers, "Sun Tzu and Cyber War." Available online at http://korben.info/wp-content/uploads/defcon/SpeakerPresentations/Geers/DEFCON-20-Kenneth-Geers-Sun-Tzu-and-Cyber-War.pdf Internet: Accessed 07 May 2015. Pg. 6.

[41] Ibid.

[42] Canabarro, 10.

imply that the development of cyber offense capabilities might be too ineffective to be translated into a strategic advantage."[43]

Furthermore, cyber defence retains the advantage because it retains its utility, despite how many attacks are thrown at it. Once a cyber-attack is detected, the vulnerability in the targeted system can be fixed, making it immune to that particular method of attack and stronger than it had been previously. The attacking software, on the other hand, quickly becomes ineffective as knowledge of it spreads amongst the cyber defence community, thereby rendering the mode of attack ineffective in the future. Thus when cyberattacks are used, the attacker is likely to lose the ability to use the same type of attack again. This renders cyberattacks "use and lose capabilities."[44]

Finally, cyber-attacks require extensive reconnaissance in order to be effective. If the offence targets a specific military facility within enemy territory, the attacker needs extensive knowledge of the targeted facility's IT-systems, needs to discover and exploit known and unknown vulnerabilities, and then successfully plan, test and execute the cyberattack. These limitations make meticulous pre-operational cyber-attack planning timing critical.[45] "In light of cyberattacks' inferior ability to cause direct damage, it is understandable that the United States and NATO decided to use conventional military air-bombings in Libya during the Arab Spring in 2011, and not cyberattacks."[46]

In the sixth book of *On War*, Clausewitz acknowledged that the offence had the initiative and the element of surprise, but stated that "the defensive form of warfare is in-

[43] Ibid.
[44] Jacobsen, 16.
[45] Geers, 8.
[46] Jacobsen, 16.

trinsically stronger than the offensive."[47] In cyberspace, the advantage shifts to the defence and remains there once the opening salvos of the cyber offensive have been dealt with. Any perceived offensive advantages are likely due to the fact that cyber conflict has, to date, been limited to "first strike, sneak attack" scenarios. In the long-term game of cyber attrition, the defence wins.

CONCLUSION

The small wars of today and the next major war of the future will most certainly involve attacks in the cyber domain. State and non-state adversaries are already utilizing cyberspace to strengthen their positions and weaken our own. We must, therefore, understand the nature of the cyber threat and how we can defend against it.

Throughout history, political and military leaders have adapted the strategic teachings of the past to the technological realities of the present. Lessons learned from contemporary conflicts in which cyber operations have played a role can be better understood when using *On War* and other classics of strategy as an interpretive guide. Cyberspace is such a new arena of conflict that basic defence and attack strategies are still unclear. There have been no major wars (yet) between modern, cyber-capable adversaries. With this lack of practical experience, the importance of theoretical guidance becomes paramount, particularly when discussing the offensive and defensive aspects of cyberwar. Clausewitz's arguments regarding the offensive-defensive nexus, the strength of the defence and the power of the mobilized populace, are just a few of the many ideas that continue to resonate strongly in cyberspace.

[47] Howard, 361.

BIBLIOGRAPHY

Aucsmith, David. "War in Cyberspace." Available online at http://cyberbelli.com. Internet: Accessed 02 May 2015.

Canabarro, Diego Rafael. "Reflections on The Fog of (Cyber)War." *National Center for Digital Government.* Available online at http://www.umass.edu/digitalcenter/research/working_papers/13_001_Canabarro-Borne_FogofCyberWar.pdf Internet: Accessed 04 May 2015.

Cronin, Audrey Kurth. "Cyber-Mobilization: The New Levée en Masse." *Parameters*, Summer 2006. Available online at http://spgia.gmu.edu/wp-content/uploads/PDFs/Audrey_Kurth_Cronin/cybermobilization.pdf Internet: Accessed 02 May 2015.

Echevarria, Antulio J. "War And Politics: The Revolution In Military Affairs And The Continued Relevance Of Clausewitz" Joint Forces Quarterly, Winter 1995-96. Available online at http://www.clausewitz.com/readings/Echevarria/ECHJFQ.htm Internet: Accessed 05 May 2015

Elkus, Adam. "Rise of Cyber Mobilization." February 2009. Available online at https://www.oodaloop.com/uncategorized/2009/02/13/the-rise-of-cyber-mobilization/
Internet: Accessed 04 May 2015.

Geers, Kenneth. "Sun Tzu and Cyber War." Available online at http://korben.info/wp content/uploads/defcon/SpeakerPresentations/Geers/DEFCON-20-Kenneth-Geers-Sun-Tzu-and-Cyber-War.pdf Internet: Accessed 07 May 2015.

Goldsmith, Jack. "The Cyberthreat, Government Network Operations, and the Fourth Amendment." Brookings Institute, December 2010. Available online at http://www.brookings.edu/~/media/research/files/papers/2010/12/08-4th-amendment-goldsmith/1208_4th_amendment_goldsmith.pdf Internet: Accessed 06 May 2015.

Greathouse, Craig B. "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?" *Cyberspace and International Relations: Theory, Prospects and Challenges.* Springer Link Publishers, 2014. Pg. 21 – 40.

Howard, Michael. Clausewitz On War. Washington: Library of Congress, 1998.

Jacobsen, Jeppe. "The cyberwar Mirage and the Utility of Cyberattacks in War." *DIIS Working Paper*, 2014. Available online at http://www.diis.dk/files/media/publications/import/extra/diis-wp_2014-06_teglskov_web_1.pdf Internet: Accessed 16 May 2015.

Kaldor, Mary. "Inconclusive Wars: Is Clausewitz Still Relevant in these Global Times?" *Global Policy* Volume 1, Issue 3. October 2010. Available online at http://www.globalpolicyjournal.com/articles/conflict-and-security/inconclusive-wars-clausewitz-still-relevant-these-global-times Internet: Accessed 09 May 2015.

Kaplan, Rebecca. "ISIS Recruiting Teenagers." *CBS News*, March 10 2015. Available online at http://www.cbsnews.com/news/isis-recruiting-teenagers-why-the-government-is-sounding-the-alarm/ Internet: Accessed 20 May 2015.

Liles, Samuel. "Applying Traditional Military Principles to Cyber Warfare." 4th International Conference on Cyber Conflict, 2012. Available online at https://ccdcoe.org/publications/2012proceedings/3_2_Liles&Dietz&Rogers&Larson_ApplyingTraditionalMilitaryPrinciplesToCyberWarfare.pdf Internet: Accessed 03 May 2015.

Nye, Joseph. "Cyber Power." Harvard Kennedy School, May 2010. Available online at http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf Internet: Accessed 04 May, 2015.

Rohozinski, Rafal. "Stuznet and the Future of CyberWar." *Survival: Global Politics and Strategy*, February-March 2011. Available online at https://www.iiss.org/en/publications/survival/sections/2011-2760/survival--global-politics-and-strategy-february-march-2011-f7f0/53-1-05-farwell-and-rohozinski-f587 Internet: Accessed 15 May 2015.

Sharma, Amit. "Cyber Wars: A Paradigm Shift from Means to Ends." *Institute for System Studies and Analysis.* Available online at https://ccdcoe.org/publications/virtualbattlefield/01_SHARMA_Cyber_Wars.pdf Internet: Accessed 05 May 2015.

Sheldon, John B. "Deciphering Cyberpower - Strategic Purpose in Peace and War." *Strategic Studies Quarterly*, Summer 2011. Available online at http://www.au.af.mil/au/ssq/2011/summer/sheldon.pdf Internet: Accessed 11 May 2015.

United States Department of Defense, *Joint Publication 3-12 (R), Cyberspace Operations*. 05February 2013. Available online at http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf Internet: Accessed 26 May 2015.