National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CYBER WARFARE

Maj D.G. Wood

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*

CYBER WARFARE

Maj D.G. Wood

Word Count: 3227

Compte de mots: 3227

CYBER WARFARE

Introduction

Cyber warfare has emerged as a new environmental domain. Recently, we have seen successes in cyber warfare yield significant strategic results, economically, militarily and politically. In 2000, Nortel shares were worth 30 percent of the total value of the Toronto Stock Exchange's TSE 300, and it was one of the largest corporations in Canada.[1] In 2009, Nortel filed for bankruptcy. Noting persistent cyber espionage conducted by China, Brian Shields, the former senior systems security advisor at Nortel stated that Chinese cyber espionage was a "…considerable factor…"[2] in Nortel's demise. Using cyber espionage, Chinese competitors were able to copy Nortel's technology, and compete against them. The impact was the collapse of a major Canadian corporation, and financial losses to thousands of Canadians.

Prior to 2008, Iran was using centrifuges to enrich uranium, with the stated intent of developing a nuclear weapon. Knowing full well that they were to be the target, Israel began requesting assistance from the Americans in order to plan a kinetic strike against Iran's nuclear enrichment plant.[3] Washington instead allegedly collaborated with Israel to develop the Stuxnet worm, which targeted the computer control systems of the uranium centrifuges. Damage reports for this cyber-attack have varied; however, there is

[1] MarketWatch, "There's more up north than Nortel," last accessed 8 May 2015, http://www.marketwatch.com/story/theres-more-than-nortel-north-of-the-border

[2] Canadian Broadcasting Corporation, "Nortel collapse linked to Chinese hackers," last accessed 8 May 2015, http://www.cbc.ca/news/business/nortel-collapse-linked-to-chinese-hackers-1.1260591

[3] The New York Times, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," last accessed 8 May 2015, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0

agreement that the Iranians were set back several years in their plans.[4] The result has been that Iranian weapon production has been delayed, Israel did not launch a kinetic attack, and uneasy peace has continued. A tactical cyber-attack resulted in a strategic effect. Cyber has emerged both as a new environmental domain and as a new way of war-fighting. Given that this is a relatively new area of war-fighting expertise, the question must be asked, how will cyber wars be fought as stand-alone engagements, how will wars be fought integrating cyber into a joint campaign, and can a war be won based solely on fighting in the cyber domain? The argument will be made that while Cyber can strongly contribute to the winning conditions necessary for victory, you cannot achieve decisive victory using cyber techniques alone.

Cyber Warfare Operational Design: General Overview

Cyber warfare is defined as the conduct of military operations "…according to information-related principles."[5] This includes the destroying or disrupting of an enemy's communications and information systems, while protecting friendly information and communications systems.[6] This allows the friendly force to have full situational awareness of itself, its environment and the enemy, while denying the same to an opponent.[7] Bonner notes that cyber warfare has evolved similarly to how airpower developed a century ago.[8] Just as the Germans used attaining air superiority to initiate the start of their Blitzkrieg campaigns, attaining cyber superiority has been noted as being

[4] The New York Times, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," last accessed 8 May 2015, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0

[5] John Arquilla, and David Ronfeldt, "Cyberwar is Coming!," in *Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica: RAND Corporation, 1997), 30.

[6] *Ibid*.

[7] *Ibid*.

[8] E. Lincoln Bonner III, "Cyber Power in 21st-Century Joint Warfare," *Joint Force Quarterly* 74, (3rd Quarter 2014): 103.

"…critically important in joint warfare."[9] Further, with respect to operational design, Bonner advocates that once cyber superiority has been attained, cyber war fighters should initially focus their efforts on supporting the air campaign.[10] Arquilla notes this synergy between cyber and air superiority as well, noting numerous battles where commanders who possessed information superiority went on to win air superiority (and later, the war). In his most striking example, he notes in 2001 how 200 American Special Forces personnel in Afghanistan, with at most 40,000 Northern Alliance forces, defeated 70,000 Taliban and Al Qaeda fighters using networked communications and overwhelming air power.[11] They used a shared web page to coordinate airstrikes.[12] The networked communication between dispersed forces in conjunction with airpower gave them an exponentially greater level of effect due to the "…faster, unfiltered flow of data."[13]

In order to achieve cyber superiority, Bonner recommends first eliminating an opponent's ability to conduct cyber attack and cyber reconnaissance, and then eliminate the opponent's cyber defences.[14] Concurrently, friendly forces should have in place cyber defences of their own, to prevent an enemy from attacking them. He argues that in the operational design, once cyber superiority is attained, focusing initial cyber effects on support for the air war first is critical, due to the fact that surface combatants on the land or at sea move slowly.[15] Aircraft can move hundreds of nautical miles per hour. The

---

[9] *Ibid*., 109.
[10] *Ibid*.
[11] John Arquilla, "From Blitzkrieg to Blitzkrieg: The Military Encounter with Computers," *Communications of the ACM* 54, no. 10 (2011): 59.
[12] *Ibid.*
[13] *Ibid.*
[14] E. Lincoln Bonner III, "Cyber Power in 21st-Century Joint Warfare," *Joint Force Quarterly* 74, (3rd Quarter 2014): 109.
[15] E. Lincoln Bonner III, "Cyber Power in 21st-Century Joint Warfare," *Joint Force Quarterly* 74, (3rd Quarter 2014): 109.

greater speed of the air war can result in air operations unfolding "…more rapidly than land or sea operations."[16]

While there are more backdoors and mechanisms for exploiting weaknesses in the cyber domain than can be elaborated in these pages, general categories are beginning to emerge under which many of these attack modes can be classified. These categories, in turn, can then be applied to each of the phases of cyber warfare. These categories are (from Libicki, 2007 and 2009):

a. Asymmetrically dependant cyber relationships. A nation, either through government or industry, develops an information system that is so useful that other nations become dependent on its use, eventually resulting in a technological and information dependency.[17] Using elements inserted into the software, the controlling nation could conduct espionage, or launch cyber-attacks (i.e. Windows backdoors exploited by the National Security Agency).

b. Surprise cyber attack. This would be launched against an opponent's information systems prior to or in conjunction with a surprise military attack.[18] This attack would exploit flaws in the software, open portals or computers that are insecure (i.e. distributed denial of service attacks –

[16] *Ibid*.

[17] Martin C. Libicki, "Hostile Conquest as Information Warfare," in *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), 3.

[18] Martin C. Libicki, *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND Corporation, 2009, 144.

DDOS - launched by Russia against Georgia (2008).[19] These attacks involve directing multiple packets of data from large numbers of compromised computers at targets, overwhelming them).[20]

c. Eruption. This attack is used to illuminate and identify targets that have command operated signal systems (such as identify, friend, and foe – IFF systems). An attacking force would transmit a surreptitious signal, and immediately electronically illuminate all of an opposing forces fielded units,[21] allowing an attacker to fix the position of enemy targets.

d. Disruption. This attack incapacitates information systems for a time, providing an attacker an opportunity to exploit the weakness. This category of attack can result in enemy communications being squelched (due to their unexpected transmission), paralyzed command and control systems, and weapons that become electronically locked up.[22]

e. Corruption. With this attack, an attacking force inserts corrupted software into an opponent's information system. This results in weapons systems pointing in the wrong direction, sensors misinterpreting data, command and control systems that misroute or delete data packets, or

---

[19] Paulo Shakarian, "The 2008 Russian Cyber Campaign Against Georgia," *Military Review* 91, no. 6 (2011): 63.

[20] Jelena Mirkovic and Peter Reiher. "A taxonomy of DDoS attack and DDoS defense mechanisms." *ACM SIGCOMM Computer Communication Review* 34, no. 2 (2004): 40.

[21] Martin C. Libicki, *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND Corporation, 2009, 145

[22] *Ibid.,* 146.

intermittent data failures[23] (i.e. the Stuxnet cyber-attack against Iran's uranium plant).

f. Simultaneous cyber attacks. Libicki refers to this also as "…parallel warfare in cyberspace…"[24] This would involve attacks on multiple opponent systems at once, such as the communications network, electrical network and transportation system simultaneously.[25]

Cyber Warfare as a Standalone Capability

Just as the West deployed air power against Libya, and now against ISIS in both Iraq and Syria as a standalone capability, so too can cyber warfare be deployed. Libicki notes that cyber warfare is now classified as an official response that can be undertaken by a government. He lists, in increasing order of belligerence, the following potential responses by a nation:

a. Diplomatic and economic;

b. Cyber;

c. Physical;

d. Nuclear.[26]

In response to Russian aggression in Ukraine, the West applied a steady progression of diplomatic, then economic measures. Cyber warfare has now been added

---

[23] Martin C. Libicki, *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND Corporation, 2009, 147.

[24] *Ibid.*

[25] *Ibid.* 148.

[26] Martin C. Libicki, *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND Corporation, 2009, 29.

to this list of potential responses by a nation. A good example could be retaliation against North Korea in December 2014. After President Obama vowed that the United States would retaliate for the damaging Sony cyber-attack, North Korea immediately began to experience disruptions to their internet connectivity. At times, they were completely severed from the internet.[27] Due to the clandestine nature of cyber warfare, the Americans neither acknowledged responsibility, nor did they indicate the means used. While this form of warfare is fought at times in the shadows, there is evidence of cyber warfare being employed as a stand alone capability. A number of recent examples are noted in the literature.

a. Cyber espionage.

i. 2009 – Nortel Networks collapses. Following less than a decade of Chinese cyber espionage against it that allegedly aided its competitors, Nortel Networks filed for bankruptcy.[28]

ii. April 2015 - the American cyber security firm FireEye detected a Russian cyber espionage campaign against an American ally involved in enforcing economic sanctions against Russia.[29] The Russian attackers were exploiting zero day flaws in Windows and Adobe Flash software in an attempt to spy on the West's sanctions policy. Zero day flaws are software holes or errors

[27] The New York Times, "North Korea Accuses U.S. of Staging Internet Failure," last accessed 10 May 15, http://www.nytimes.com/2014/12/28/world/asia/north-korea-sony-hacking-the-interview.html?_r=0

[28] Canadian Broadcasting Corporation, "Nortel collapse linked to Chinese hackers," last accessed 8 May 2015, http://www.cbc.ca/news/business/nortel-collapse-linked-to-chinese-hackers-1.1260591

[29] Bloomberg, "Russian Hackers Use Zero-Days to Try to Get Sanctions Data," last accessed 10 May 15, http://www.bloomberg.com/news/articles/2015-04-18/russian-hackers-use-zero-days-in-attempt-to-get-sanctions-data

that have not been previously detected, and that are exploited by an attacker to enter a system.[30]

b. Cyber attack. While attacks of this type are clandestine by nature, a review of the literature has revealed a number of cyber attacks over the years, demonstrating that cyber warfare is already being used as a standalone capability.

i. 1982 – Siberian pipeline explosion. Russia purchased "Supervisory Control and Data Acquisition software"[31] (SCADA). The CIA allegedly inserted malicious code that allowed the SCADA to operate normally for a time, and then caused pipeline pressures to increase to the point where an explosion occurred.[32]

ii. 2007 – Suspected Russian cyber attacks against Estonia in response to Estonia's moving of a Russian World War II memorial. The cyber attacks began as "…ping floods and simple denial of service attacks."[33]These attacks then escalated as botnets (zombie computers controlled via malware) launched coordinated distributed denial of service attacks, disabling many Estonian government websites.[34]

---

[30] *Ibid.*

[31] Thomas Rid, "Cyberwar Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (Feb 2012): 10.

[32] Thomas Rid, "Cyberwar Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (Feb 2012): 10.

[33] *Ibid*., 11.

[34] *Ibid.*, 12.

iii. 2010 - Suspected American/Israeli Stuxnet worm attack. Discovered in July 2010.[35] Chen notes that Stuxnet intrigued researchers due to its target, its complexity, and the implications for future cyber attacks.[36] Stuxnet was a zero day exploit attacker (i.e. attacking a software flaw in Windows not previously known), that specifically targeted a logic controller made by Siemens and was aimed at computers that controlled machinery (namely centrifuges at Iran's Natanz uranium enrichment facility).[37]

iv. 2015 – Cyber reconnaissance Trojan deployed against the Middle Eastern energy sector. In January of 2015, Symantec detected a Trojan attack directed against Middle Eastern energy companies.[38] The source was not identified, however given that targets were companies in the helium, gas and petroleum industries, Symantec surmised that the attacker would have an interest in these industries.[39]

v. TBD - Chinese logic bomb attack. Rid notes that this type of attack is often cited in describing possible cyber attack scenarios against the United States. Concurrent with Chinese aggression against an American ally (i.e. Taiwan), the fear is

---

[35] Thomas M. Chen, "Stuxnet, the real start of cyber warfare," *IEEE Network* 24, no. 6 (2010): 2.
[36] *Ibid.*
[37] *Ibid*., 3.
[38] Symantec, "New reconnaissance threat Trojan.Laziok targets the energy sector," last accessed 10 May 15, http://www.symantec.com/connect/app#!/blogs/new-reconnaissance-threat-trojanlaziok-targets-energy-sector
[39] *Ibid.*

> that China would turn on logic bombs previously inserted into utility control software and launch simultaneous cyber attacks against the American power grid.[40] This simultaneous cyber attack would affect the American financial system, transportation system, and other industries dependent on electricity.[41]

Cyber Warfare as a Component in Joint Operational Design

Just as air superiority preceded the Blitzkrieg, recently the world has witnessed cyber attacks occur at the beginning of a Russian operation against Georgia. Rid notes that this conflict was "…the first time an independent cyber attack happened in synchronization with a conventional military operation."[42] Hollis concurs, noting that this "…appears to be the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in the other warfighting domains…"[43] The Russians placed the decisive points for the cyber line of operation at the beginning of their plan, and attacked Georgian hackers first.[44] Hollis himself noted the significance that by first eliminating the Georgian hackers, Russia was trying to "…forestall or mitigate a counter-attack (or returning fire) from Georgian hackers."[45] The cyber attack

---

[40] Thomas Rid, "Cyberwar Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (Feb 2012): 9.

[41] *Ibid.*

[42] Thomas Rid, "Cyberwar Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (Feb 2012): 13.

[43] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, no. 11 (January 6, 2011): 2.

[44] *Ibid.*, 3.

[45] *Ibid.*

began slowly at first, three weeks before the start of the ground war.[46] In total, 54 key government, communications and financial websites were attacked, preventing Georgian citizens from accessing "…web sites for information and instructions."[47]

By 2014, Bonner had refined cyber operational design even further, proposing that upon attaining cyber superiority, the next step is for the cyber campaign to focus on support to the air war.[48] In terms of decisive points within the cyber line of operation, Bonner suggests a logical sequence. These include achieving cyber superiority, conducting cyber interdiction, and launching cyber attacks.[49]

Achieve Cyber Superiority

To achieve cyber superiority, an attacking force must eliminate an opponents cyber attack and cyber reconnaissance capabilities. The Russian example against Georgian hackers is a good example.[50] Concurrently, the attacker must suppress an opponents cyber defence capabilities.[51] The attacker could exploit asymmetric dependencies in software shared between nations, or it could launch a surprise cyber attack.

Conduct Cyber Defence

---

[46] *Ibid*., 2.
[47] *Ibid.*, 2.
[48] E. Lincoln Bonner III, "Cyber Power in 21st-Century Joint Warfare," *Joint Force Quarterly* 74, (3rd Quarter 2014): 109.
[49] E. Lincoln Bonner III, "Cyber Power in 21st-Century Joint Warfare," *Joint Force Quarterly* 74, (3rd Quarter 2014): 109.
[50] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, no. 11 (January 6, 2011): 3.
[51] E. Lincoln Bonner III, "Cyber Power in 21st-Century Joint Warfare," *Joint Force Quarterly* 74, (3rd Quarter 2014): 109.

While attacking an opponent's cyber capabilities, the attacker must protect its own cyber capabilities. The simplest cyber defence is an air gap, basically, physically separating your system from any non-trusted system. Secondly, the best cyber defence is a strong cyber offence, eliminating the opponent's cyber attack capability (i.e. the Georgian hackers). The larger and more networked your own system, however, the more difficult your own cyber defence can be. To aid in cyber defence, one must ensure the most up to date software patches have been installed; map out networks in order to discover unsecured portals, and maintain rigorous system access control.[52]

Conduct Cyber Interdiction

Similar to the Allied air attacks against Germany prior to the Normandy invasion, which focused on rail marshalling yards and later bridges,[53] Bonner recommends that an attacking force focus on the cyber equivalent of these capabilities. In particular, an attacking force should direct its cyber interdiction efforts against "data fusion centres"[54] (cyber rail marshalling yards), and against "tactical data links"[55] (cyber bridges). Physical interdiction can also be conducted against bridges, which allow fibre optic cables to traverse waterways. This must be used judiciously, however, as an attacker may wish to use these same physical cyber connections later to launch further cyber attacks.

Cyber Attack OPFOR Critical Infrastructure

---

[52] Martin C. Libicki, *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND Corporation, 2009, 144.

[53] Philip Meilinger, "A History of Effects-Based Air Operations," *The Journal of Military History* 71, no. 1 (January 2007): 152.

[54] E. Lincoln Bonner III, "Cyber Power in 21st-Century Joint Warfare," *Joint Force Quarterly* 74, (3rd Quarter 2014): 109.

[55] *Ibid.*

Once an attacker has achieved cyber superiority, they can then launch attacks against an opponent's energy industry, transportation system, power grid, air traffic control system and water systems.[56] There is evidence that cyber reconnaissance in support of this is going on to this day. Admiral Michael Rogers, National Security Agency Director, informed a Senate Panel that potential cyber attackers have been leaving "…cyber fingerprints on our critical infrastructure…"[57] as they probe American utilities. Computer systems controlling the United States power grid are subject to a cyber or physical attack "…once every four days…"[58]

Once cyber superiority is attained, support should then be directed towards the air war. Prior to a 2007 Israeli air attack against a Syrian nuclear facility, Syria's modern, Russian built air defence system showed blank screens as a large Israeli air attack approached.[59] It is suspected the Israeli's somehow sent signals telling the Syrian systems to display blank radar screens[60]. While blinding an opponent during a simultaneous cyber attack against numerous key utilities, an attacker, in support of the air war, could then simultaneously conduct an eruption cyber attack. This would result in the transponders of the opposing force to unexpectedly illuminate. This would betray the positions and identities of an opponent's air assets, and potentially those of its naval and land forces as

---

[56] Security Week, "Cyber Attackers Leaving Warning "Messages": NSA Chief", last accessed 9 May 15, http://www.securityweek.com/cyber-attackers-leaving-warning-messages-nsa-chief

[57] Security Week, "Cyber Attackers Leaving Warning "Messages": NSA Chief", last accessed 9 May 15, http://www.securityweek.com/cyber-attackers-leaving-warning-messages-nsa-chief

[58] USA Today, "Bracing for a big power grid attack: 'One is too many', " last accessed 10 May 15, http://www.usatoday.com/story/news/2015/03/24/power-grid-physical-and-cyber-attacks-concern-security-experts/24892471/

[59] Richard A. Clarke and Robert K. Knake, *Cyber War, The Next Threat to National Security and What to do about it*, (HarperCollins e-books, 2010), chapter 1.

[60] *Ibid*.

well. The blinding simultaneous cyber attack, in conjunction with a simultaneous eruption and air attack could be used to next achieve air superiority.

Build and Maintain Informational Situational Awareness

The aim of cyber warfare is to allow the friendly force to have full situational awareness of itself, its environment and the enemy, while denying the same to an opponent.[61] Due to improved situational awareness, Arquilla notes that it is the "…super-empowerment of those who actually conduct the fighting that most distinguishes our era of informational advances from earlier ones."[62] The eruption attack should illuminate many targets for insertion into the tactical plot. Once cyber and air superiority are attained, the recognized operating picture can be more easily maintained. Enemy aircraft, and later ships and land vehicles could be targeted while the enemy is still blinded. The air, land and sea lines of operation could then proceed according to plan.

Analysis: Can Wars be won with Cyber Alone?

Clausewitz argued that the destruction of an opponent's fighting capability is the aim of warfare.[63] Further, "…gaining and controlling territory is considered success."[64] Given the paradigms above, the question must now be asked, can you win a war using cyber alone? Applying Clausewitz's argument, cyber warfare is an enabler for the other capabilities to destroy an opponent's fighting capability. Cyber warfare suppresses an

---

[61] John Arquilla, and David Ronfeldt, "Cyberwar is Coming!" in *Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica: RAND Corporation, 1997), 30.

[62] John Arquilla, "From Blitzkrieg to Blitzkrieg: The Military Encounter with Computers," *Communications of the ACM* 54, no. 10 (2011): 59.

[63] Antulio J. Echevarria, *Clausewitz and Contemporary* War (Oxford: Oxford University Press, 2007), 133.

[64] James Clancy, and Chuck Crossett, "Measuring Effectiveness in Irregular Warfare," *Parameters* XXXVII, no. 3 (Summer 2007): 90.

opponent's ability to launch a cyber-attack, enables an attacker to blind an opponent by knocking his utilities offline, and it illuminates hostile targets. It may achieve some destroy effects as was seen with the Stuxnet worm. It does not, however, destroy the opponent's fighting capability, as demanded by Clausewitz, nor does it gain and control territory. According to this current line of thinking, it cannot win wars alone.

Warden challenges Clausewitz's notion that the "…clash of men on the front…"[65] to the point of destruction is best way to win a war. He notes that even Japan and Germany conceded "…long before the total destruction of their fielded military forces."[66] He argues that a state can realize "…its political objectives…"[67] by simply forcing its opponent "…to make concessions."[68] In lieu of massive force on force conflict, he argues that one should instead attack the centres of gravity as per his concentric ring model, and that if either a sufficient number of rings or a single critical ring can be struck; one can force an opponent to concede.[69] He applied this model to air power, when arguing air power alone could win wars. Using this same paradigm, however, one could argue that eventually the chaos resulting from a massive cyber attack alone could force an opponent to make concessions (and thus win the war).

The dominant theory in military studies remains that of Clausewitz. Applying that model, the conclusion is that one cannot win wars with cyber alone. If one looks beyond

---

[65] Col John A. Warden "Employing Air Power in the Twenty-first Century." In *The Future of Air Power in the Aftermath of the Gulf War*, edited by Richard H. Schultz, Jr. and Robert L. Pfaltzgraff, Jr. Maxwell AFG, AL: Air University Press, 1992, 62.

[66] *Ibid*., 63.

[67] *Ibid.*

[68] *Ibid.*

[69] *Ibid*., 65.

Clausewitz, however, and considers Warden's paradigm, one could consider different answers to the question "can you win wars with cyber alone?"

Conclusion

Cyber warfare has evolved similarly to airpower, and has emerged to be a warfare domain all on its own. In recent years, the West has employed airpower alone against both the Libyan regime and now ISIS in Iraq and Syria. So too can cyber warfare be deployed. Cyber warfare has now been added to the list of strategic options that a nation can employ against another.

Cyber warfare has also been recently integrated into the overall operational design of recent international military operations. The Russian/Georgian conflict provided great insight as to how this integrated operational design might work. The Russians placed the cyber decisive points at the start of their operational design, and attacked the Georgian cyber hacking community first, before any other target. This disabled Georgia's ability to launch a counter attack (resulting in Russian cyber superiority). They then attacked government and economic sites, depriving Georgians of information while their military forces were moving.

Work by Bonner in 2014 refined cyber operational design even further, proposing that once an attacker gains cyber superiority, the next step is for the cyber campaign to support the air war.[70] In terms of decisive points within the cyber line of operation,

[70] E. Lincoln Bonner III, "Cyber Power in 21st-Century Joint Warfare," *Joint Force Quarterly* 74, (3rd Quarter 2014): 109.

Bonner suggests a logical sequence. These include achieving cyber superiority, conducting cyber interdiction, and launching cyber attacks.

Cyber would then assist the air war, as demonstrated by the Israelis in 2007.[71] While being a powerful enabler for the other operational domains (air, land, sea, SOF), when applying Clausewitz's paradigm, it is assessed that while Cyber can strongly contribute to the winning conditions necessary for victory, you cannot achieve decisive victory using cyber techniques alone.

[71] Richard A. Clarke and Robert K. Knake, *Cyber War, The Next Threat to National Security and What to do about it*, (HarperCollins e-books, 2010), chapter 1.

BIBLIOGRAPHY

Arquilla, John. “From Blitzkrieg to Blitzkrieg: The Military Encounter with Computers.” *Communications of the ACM* 54, no. 10 (2011): 58 – 65.

Arquilla, John, and David Ronfeldt. “Cyberwar is Coming!” In *Athena's Camp: Preparing for Conflict in the Information Age.* Santa Monica: RAND Corporation, 1997.

Bloomberg. “Russian Hackers Use Zero-Days to Try to Get Sanctions Data.” Last accessed 10 May 15. http://www.bloomberg.com/news/articles/2015-04-18/russian-hackers-use-zero-days-in-attempt-to-get-sanctions-data

Bonner, E. Lincoln III. “Cyber Power in 21st-Century Joint Warfare.” *Joint Force Quarterly* 74, (3rd Quarter 2014): 102 - 109.

Canadian Broadcasting Corporation. “Nortel collapse linked to Chinese hackers.” Last accessed 8 May 2015. http://www.cbc.ca/news/business/nortel-collapse-linked-to-chinese-hackers-1.1260591

Chen, Thomas M. “Stuxnet, the Real Start of Cyber Warfare?” *IEEE Network* 24, no. 6 (2010): 2 – 3.

Clancy, James, and Chuck Crossett. "Measuring Effectiveness in Irregular Warfare." *Parameters* XXXVII, no. 3 (Summer 2007): 88-99.

Clark, Richard A. and Robert K. Knake. *Cyber War, The Next Threat to National Security and What to do about it*. HarperCollins e-books, 2010.

Echevarria, Antulio J. *Clausewitz and Contemporary War*. Oxford: Oxford University Press, 2007.

Hollis, David. “Cyberwar Case Study: Georgia 2008.” *Small Wars Journal*, no. 11 (January 6, 2011): 1 - 10.

Libicki, Martin C. *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND Corporation, 2009.

Libicki, Martin C. “Hostile Conquest as Information Warfare.” In *Conquest in Cyberspace: National Security and Information Warfare*. New York: Cambridge University Press, 2007.

MarketWatch. “There’s more up north than Nortel.” Last accessed 8 May 2015, http://www.marketwatch.com/story/theres-more-than-nortel-north-of-the-border

Meilinger, Philip. "A History of Effects-Based Air Operations." *The Journal of Military History* 71, no. 1 (January 2007): 139 - 167.

Mirkovic, Jelena and Peter Reiher. "A taxonomy of DDoS attack and DDoS defense mechanisms." *ACM SIGCOMM Computer Communication Review* 34, no. 2 (2004): 39-53.

Rid, Thomas. "Cyberwar Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (Feb 2012): 5 - 32.

Security Week, "Cyber Attackers Leaving Warning "Messages": NSA Chief", last accessed 9 May 15, http://www.securityweek.com/cyber-attackers-leaving-warning-messages-nsa-chief

Shakarian, Paulo."The 2008 Russian Cyber Campaign Against Georgia." *Military Review* 91, no. 6 (2011): 63 - 68.

Symantec. "New reconnaissance threat Trojan.Laziok targets the energy sector." Last accessed 10 May 15. http://www.symantec.com/connect/app#!/blogs/new-reconnaissance-threat-trojanlaziok-targets-energy-sector

The New York Times. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." Last accessed 8 May 2015. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0

The New York Times. "North Korea Accuses U.S. of Staging Internet Failure." Last accessed 10 May 15. http://www.nytimes.com/2014/12/28/world/asia/north-korea-sony-hacking-the-interview.html?_r=0

USA Today. "Bracing for a big power grid attack: 'One is too many'." Last accessed 10 May 15. http://www.usatoday.com/story/news/2015/03/24/power-grid-physical-and-cyber-attacks-concern-security-experts/24892471/

Warden, Colonel John A. "Employing Air Power in the Twenty-first Century." In *The Future of Air Power in the Aftermath of the Gulf War*, edited by Richard H. Schultz, Jr. and Robert L. Pfaltzgraff, Jr. Maxwell AFG, AL: Air University Press, 1992. Pages 57-82.