National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CYBERWARFARE WILL NOT REPLACE CONVENTIONAL WARFARE

Maj R.T. Stimpson

JCSP 41

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 41

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 41 – PCEMI 41
2014 – 2015

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

CYBERWARFARE WILL NOT REPLACE CONVENTIONAL WARFARE

Maj R.T. Stimpson

Word Count: 6342

Compte de mots : 6342

Every age has its own kind of war, its own limiting conditions, and its own peculiar preconceptions

-Carl von Clausewitz, *On War*

INTRODUCTION

Maintaining a capable military force is an expensive endeavor for countries. In order to stay militarily competitive and relevant, countries need to be constantly upgrading technology, replacing obsolete capability with new. Participating in actual war, even on a limited scale can skyrocket national debt and put countries on the brink of economic collapse. Economic and resource costs are not the only costs of war, non-tangible costs such as political, human and emotional costs to the country can endure for generations.

Enter the notion of Cyberwarfare. There is no denying that cyberweapons are effective. They can be used offensively and defensively and are capable of delivering military effects that can at times be similar to what can be delivered in physical space. Cyberweapons can target not only an adversary's military capability but also strategic state targets such as economic and government infrastructure. The most minor of attacks can temporarily cripple an entire state psychologically, economically and physically when the entire cyber spectrum is considered.[1]

An article in *Fortune* magazine purported that many small countries have given up trying to compete with larger nations in the purchase and development of conventional weapons. For these small nations, "enabled by Internet connectivity, cyberwar provides more bang for the buck than investment in conventional weapons."[2] The idea that a country could *virtually* participate in war using cyberweapons instead of engaging in physical war with conventional weapons and achieve similar national goals is intriguing. If a cyberwar fought with cyberweapons achieved

[1] Matthew Devost and Neal Pollard, "Taking Cyber-Terrorism Seriously," *Terrorism Research Centre* (2002).
[2] Peter Suciu, "Why Cyberwarfare is so Attractive to Small Nations," *Fortune Magazine*, 2014, .

the same ends as war, but resulted in less cost, why would one not equip their forces and fight the ‘cyberwar’?

This essay will deconstruct some of the current arguments for cyberwarfare as an alternative to conventional warfare. It will argue that cyberwarfare can effectively complement conventional warfare but is not an alternative to conventional warfare.

It is organized in three parts. The first part will review the various arguments made for why countries should pursue cyberwarfare. Claims that cyber is more affordable, accessible and less risky will be examined. Part two will review cyber as a replacement for objectives commonly achieved with conventional weapons, such as deterrence, a new version of airpower and the decisiveness of war itself. The third part will take a pragmatic view of the utility of cyberwarfare and demonstrate how it can support and enhance other forms of warfare and tactics. Throughout the discussion various cyber terms that have no universally accepted definition will be used. The glossary on page 26 will provide definitions of key words for the purposes of this paper.

PART I

Cost

Cyberweapons have been hyped as an attractive alternative to conventional weapons due to their affordability. Amy Chang a research associate in the technology and national security program at the Center for a New American Security states, “cyber warfare is a great alternative to conventional weapons, it is cheaper for and far more accessible to these small nation-

states."[3]Ross Rustici argues that "Cyberweapons are a *cheap* way to build a global strike capability against networked states."[4] He argues that poor states, who were incapable of challenging larger more technologically advanced states with conventional weapons can now take can now them on in cyber.

They are both partially correct. A cyberwarfare capability can be purchased on the internet for a couple hundred dollars; one can purchase malware and botnets or hire the services of a self-trained hacker.[5] Gabriel Weimann identifies that "all terrorists need is an online connection and personal computer."[6] What could be purchased at this price can be crude but very effective. The ILOVEYOU virus was able to shut down businesses for hours and caused around 6 billion dollars in damages.[7] Why would one waste money on expensive conventional weapon that need upgrades and become obsolete when they can drop $200 on *Craigslist* for a virus or the services of a 'weekend cyberwarrior'?

Not all cyberweapons are created equally. As effective (causing damage to unprotected computers) as it was, ILOVEYOU was not a militarized cyberweapon; it could not be directed against a specific target, could not be controlled and was not sophisticated enough to penetrate sensitive military networks. It proved to be more of an annoyance by indiscriminately attacking hundreds of countries and millions of random emails.[8] Thomas Rid points out that exceptional cyber weapons require a lot of technical expertise and funding, hence they would not be the preferred weapons of poor countries or non-state actors.[9] A true cyberwarfare capability is

[3] Ibid.
[4] Ross Rustici, "Cyberweapons: Leveling the International Playing Field," *Strategic Studies Institute* (2011).37.
[5] M. Lee and L. Hornby, "Google Attack Puts Spotlight on China's "Red" Hackers." *Reuters* (2010).
[6] Gabriel Weimann, "Cyberterrorism: How Real is the Threat?" *USA Institute of Peace* (2004).
[7] S. Kirschner, "I Love You...Not." *Popular Science.*, 2000, .48-49.
[8] Ibid.
[9] Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst and Company, 2013a).45.

expensive. The technologically advanced Stuxnet was able to discern targets and could be controlled by the user after launch. It is estimated that Stuxnet cost around US$3 million dollars to create.[10] Additionally it is believed that the virus was tested by experts for many months before it was actually launched.[11] As malware and viruses become more and more complex so do the defenses that prevent them from infecting computers. Advanced defenses will only raise the costs and the entry requirements into militarized cyberspace.

Accessibility

Launching a real cyberattack is harder to achieve than media and movies portray it. An obvious disadvantage to the state that wishes to replace physical weapons with cyber weapons is that all future opponents 1) need to be present in cyberspace and 2) they need to be vulnerable to cyberattack.

The first element is self-evident. You can't attack someone in cyberspace if they don't have a presence in cyberspace. There are many countries, mostly poor and not technically advanced, whose government, military and citizens are minimally connected. An attempted cyberattack against such an unconnected country would have little to no effect and might even go unnoticed. An advantage of physical weapons is that they can be employed against anyone within range. Declaring cyberwar on a group that is not networked or dependent on IT systems will not be all that productive.

Cyberattack, the critical component of cyberwarfare is reliant on, *vulnerability.* "One distinction between cyberwarfare and warfare in all other media must be made: cyber warfare requires that the targets have made mistakes in their implementation and use of digital

[10] A. Hesseldahl, "Computer Worm may be Targeting Iranian Nuclear Sites," *Bloomberg* (2010).
[11] Ibid.

equipment"[12] If the adversary has a tight cybersecurity perimeter that is not penetrable, then there is no cyberattack that can occur. A country that is in cyberspace can at any time reduce or remove their presence. Making cyberattack difficult is not impossible. One way to protect oneself against cyberattack is electronic isolation. By "air-gapping" a network from the rest of the world a state makes it very difficult for outsiders to penetrate a system.[13] The majority of classified US Defense and other Western defense networks are air-gapped making if very difficult to conduct a cyberattack.[14] "Air-gapping" can reduce one's vulnerability, however human error plays a role in even the most perceptively secure systems, as was the case with Buckshot Yankee. Buckshot Yankee, "the most significant breach of U.S. military computers was caused by a flash drive inserted into a U.S. military laptop on a post in the Middle East in 2008."[15] The virus compromised a large amount of defense related sensitive material. Whether a network is connected to the internet or not, cyberwarfare in all cases requires a window of opportunity that is not necessarily going to be open when and where you need it to be.

Even when the opportunity exits to penetrate a system, an advanced country reliant on cyberspace is going to employ advanced cyber defenses. Vulnerabilities will be hard to exploit. It is not difficult to immunize one's networks from cyberattack. Advanced cyberdefenses are layered with other security measures to include "computing instructions that can only be manipulated by hands on access to the hardware, preventing malware or malicious software with

[12] Martin Libicki, "Why Cyber War Will Not and should Not have its Grand Strategy," *Strategic Studies Quarterly* (2014).31.
[13] Bruce Schneier, "Want to Evade NSA Spying? Don'T Connect to the Internet," *Wired* (2013).
[14] Ibid.
[15] Ellen Nakashima, "Defense Officials Discloses Cyberattacks," *The Washington Post*2010.

rogue instructions being placed on the machines."[16] This makes cyberattack against an advanced state target very challenging.

Vulnerability is requisite but so is preparation time. It is true a cyberattack could be launched at the click of a keyboard and the cyber projectile can arrive at target destination instantaneously. There is however a substantial amount of preparation that needs to occur prior to an attack whether retaliatory or pre-emptively. The Stuxnet attack would have needed extensive knowledge of the nuclear facilities in Iran but also people with nuclear reactor expertise.[17]

The need for so many pre-conditions to exist makes cyber not a particularly responsive means to retaliate. When attacked by a physical weapon it is relatively easy to respond with another physical weapon. If you are in range, your adversary is probably in range. For a cyberattack to be effective as a pre-emptive strike option, the target needs to be known well in advance, time is needed to probe the opponent's system for vulnerabilities before attack. This is one of the reasons cyberattack was not used during the NATO attack on Libya in 2011. The attack was not foreseen in time to employ cyber means.[18] One is not necessarily vulnerable to your cyberweapon by virtue of their cyberspace presence.

Network vulnerabilities when found, are fleeting, especially with technologically advanced states. When they are exploited and attacked they will be sensed by the defender and repaired quickly. "Even if a potent cyber-weapon could be launched successfully once, it would

---

[16] Libicki, *Why Cyber War Will Not and should Not have its Grand Strategy*30.
[17] R. Langner, *Cracking Stuxnet: A 21st Century Cyberweapon, Cracking Stuxnet: A 21st Century Cyberweapon.* Ted.com, 2011 .
[18] Ellen Nakashima, "US Cyberweapons had been Considered to Disrupt Gaddafi's Air Defenses," *The Washington Post*2011.

be highly questionable if an attack, or even a salvo, could be repeated in order to achieve a political goal."[19]

There are many things that can be done to reduce cyber and network weakness. If an attack was impending there are substantially even more measures that can be taken. Just because one has a cyberweapon does not mean one can use it at a time and place of choosing. It needs to be enabled by the opponent's carelessness and ignorance. For this reason alone cyberweapons will never be a replacement for conventional weapons.

Risk and Cyberwarfare

Patrick Lin in his *Atlantic* article sees cyberwarfare as a low risk alternative to conventional warfare.

> This also means new channels for warfare. Indeed, a target in cyberspace is more appealing than conventional physical targets, since the aggressor would not need to incur the expense and risk of transporting equipment and deploying troops across borders into enemy territory, not to mention the political risk of casualties. Cyberweapons could be used to attack anonymously at a distance while still causing much mayhem.[20]

Cyberwarfare is not a riskless affair to the user. A characteristic of cyberspace is that it is very difficult to determine the follow-on effect of actions taken in cyberspace and even more difficult to try to control these effects. Physical weapons are tangible; they can be inventoried, expended and destroyed if required. When cyberweapons are used in cyberspace the user may not always be able to contain the weapon's effects or control its use and eventual destination. This can have three very negative consequences:

[19] Thomas Rid and Peter McBurney, "Cyber-Weapons," *Rusi Journal* 157, no. 1 (2012).
[20] Patrick Lin, "Is it Possible to Wage just a Cyberwar?" *The Atlantic* (2012).

Firstly, a state's cyberweapon will not necessarily discern enemy from friendly in cyberspace. A launched cyberweapon could seep into the attacker's networks and infect the systems of the employer resulting in negative consequences. Conventional weapons effects are observable and finite. It is not easy to tell what kind of damage a cyberweapon has done or where a virus ultimately ends up. When a state loses control of the effects of its weapons, the attacking state could do more damage to itself that to the intended target. Consequences of cyber blowback would not be contained to defense systems and would include the technologies that are integral to the state's citizens. Major efficiencies and economic production could be compromised. The secondary effects caused by engaging in cyberwarfare could undermine a state's citizen's trust in cyberspace well into the future.

Secondly, a country that uses and creates advanced cyberweapons will need to be very reliant on IT systems. This serves to increase a state's vulnerability to the very cyberweapons it is producing. It also increases the attractiveness of that state to other states wishing to employ cyberattack.[21]

Thirdly, the most lucrative targets and typically most vulnerable in cyberspace are non-military. Attempting to defeat the adversary by attacking the economy and industry of a country through cyber will have global consequences given the interconnectedness of the world. Power generators and communications networks are intertwined with other cities and countries. IT infrastructure and private networks are connected globally.[22] Due to the interconnectedness of the financial systems, a successful attack against for example Wall Street will more than likely

[21] James Adams, "Virtual Defense," *Foreign Affairs* 80, no. 3 (2001).98.
[22] Andrew Krepinevich, "Cyberwarfare: A "Nuclear Option"?" *Centre for Strategic and Bugetary Assessments* (2012).65.

have negative consequences to an attacker's allies and the country itself. Interdependencies are not always obvious in cyberspace.[23]

PART II

Cyberdeterrence

Threat and deterrence are unique psychological aspects within the concept of war. The aim of deterrence is to persuade an adversary not to initiate action for fear the retaliation would not be outweigh potential benefits.

> A state deploys a deterrent strategy to protect an interest. To keep adversaries from attacking the interest, a state makes a deterrent declaration, 'Do not do this, or else that will happen.' This is any adversary action that would threaten the [state's] interest. That includes either denial measures, penalty measures, or both.[24]

There is a significant body of knowledge that shows wars have been averted due to the perception of strength or perception of powerful weapons that were in reality not as powerful as they appeared.[25] If arguing for cyberwar as a legitimate form of war, it would be rational to assume that the associated negative costs and risks of engaging in cyberwar could act as a deterrent. Will Goodman who has served as an advisor to US Defense dept. argues cyberwarfare can be used as an effective deterrent. He states that "Cyberdeterrence proves easier in practice than it seems to be in theory because cyberattacks are ultimately inseparable from the physical domain, where deterrence has a long-demonstrated record of success".[26]

Cyberwarfare however does not represent an effective means to apply the functions of deterrence. Deterrence requires two key elements: a credible threat and ability to communicate

---

[23] S. Borg, "Economically Complex Cyber Attacks," *IEEE Security and Privacy* 3, no. 6 (2005).
[24] Will Goodman, "Cyber Deterrence," *Strategic Studies Quarterly* (2010)., 105-106.
[25] Geoffrey Blainey, *The Causes of War* (New York: Free Press, 1973).35-56
[26] Goodman, *Cyber Deterrence*102.

the threat. Cyber unfortunately does neither effectively. Cyber coercion cannot compel like physical means can. A physical force in a tangible environment is still preferred.

Known cyberwarfare capability on its own is not compelling. “All publicly known cyberweapons have far less ‘firepower’ than is commonly assumed”.[27] To deter, you need to make the adversary believe that an attack will cause some level of pain and suffering. Though the Stuxnet example might be an example of how physical damage can be delivered via cyber (albeit indirectly), for now it is the exception rather than the rule in cyberwarfare. The cyber attacker in reality is very limited in what can be achieved. Interrupting a state’s industry or military communications network are irritating notions and could weaken the state temporarily, they are however temporary and any resulting destruction could be fixed fairly quickly as previous examples have indicated. Retired US Marine General James Cartwright has been urging the US military to be more overt with their cyber capability.

> We've got to step up the game; we've got to talk about our offensive capabilities and train to them; to make them credible so that people know there's a penalty to this," said Cartwright. "You can't have something that's a secret be a deterrent. Because if you don't know it's there, it doesn't scare you.[28]

Cartwright is correct, if you want to deter, having the capability is important but you also need to communicate to your enemy your ability. What Cartwright fails to realize, is how hard this is to do in cyberspace. When it comes to deterrence, actions speak louder than words. In cyberwarfare deterrence is difficult.

Pointing to one’s ability to use cyberweapons effectively in the past would not necessarily be all that compelling. If a computer virus was launched in the past and discovered, it can be safe to say an attack employing an identical or similar virus and using similar

[27] Rid and McBurney, *Cyber-Weapons*
[28] Shane McGlaun, "DARPA Wants More Money for Cyber Weapons," *Daily Tech Magazine,* 2011, .

vulnerabilities would be nearly impossible to deliver again. Additionally the cyberweapon design utilized will have been dissected and access points patched. As soon as Stuxnet was discovered it was globally "outted" and neutralized.

> Once you know that it's there it's not that difficult to reverse engineer. Neutralization of Stuxnet, once its operation is understood, would not be that difficult as it was precisely engineered to disrupt a specific item of machinery, once Stuxnet' s signature is identified it can be eliminated from a system .[29]

Launching a lesser show of force attack like overtly probing an enemy's servers or causing minor network disruptions to illustrate a capability would work well in an observable world, but not so much in the virtual world. By conducting a show of force you telegraph your intent to use cyberwarfare. Lupovici sees this as a significant drawback stating, "exposing the offensive capabilities as the consequence of repeated attacks may serve as the basis of knowledge or inspiration for the challenger, it is also likely to allow enemies to prepare for a future threat."[30]

Attribution is another challenge in cyberdeterrence. The advantage of easily being anonymous in cyberspace has its benefits and drawbacks. When trying to coerce in cyberspace it is a drawback. Cyberspace is not an exclusive club where all members are known, like the 'nuclear club' of the Cold War. The majority of the world is operating in cyberspace.[31] This poses a problem in deterrence as the sender of a cyberdeterrence message may not be known. When the sender is not known the message can be misinterpreted, misread, misidentified or perhaps not even detected. There is a difference between a cyberattack that originates from a domestic hacker and one that is external and state sanctioned. The attack against Estonia in 2007 used hundreds of thousands of computers from 178 countries against 90% of the key information

---

[29] Peter Sommer, "Experts Say, Iran has Neutralized Stuxnet," *YNet News- Middle East,* 2012, .
[30] A. Lupovici, "Cyber Warfare and Deterrence: Trends and Challenges in Research," *Military and Stategic Affairs* 3, no. 3 (2011).55.
[31] J. Nye, "Cyber Power," *Belfer Centre for Science and Int'L Affairs Harvard Kennedy School* (2010).4.

systems in the country.[32] The origin of the attack could not be determined; without knowing who was attacking it is difficult to determine what the purpose of the attack even is. Estonia is an example of how difficult it might be to attribute what the message is and where it is coming from.

Cyberspace is not a good venue to achieve deterrence. Physical weapons and their effects are observable and their effects are understood making deterrence compelling. Deterrence through cyber is not effective as one cannot effectively communicate the threat in which one should fear.

Cyberpower

Could cyberpower replace conventional military means in other domains? Cyberpower, as a new form of warfare has been compared to the emerging airpower theory of the 20th century. Andrew Krepinevich states, "in the context of the historical analogies discussed, the state of cyber weapon development appears to most closely approximate that of airpower during the 1930s."[33] He further states that a "cyberattack on an advanced state's critical infrastructure achieves results more similar to those of the strategic bombing campaigns of World War II"[34]It is argued that cyberweapons can strike at strategic targets like industry supporting the war effort and the state infrastructure so crucial in holding the will of the people together. Conceptually, there are obvious similarities between airpower and cyberpower, however the domains of cyberspace and air are vastly different. The most glaring difference is in the potential to create destruction. During WWII, Allied aerial bombing campaigns could effectively strike deep into Nazi Germany, degrading support to the war effort.

[32] Charles Clover, "Kremlin Backed Group Behind Estonia Cyber Blitz," *Financial Times- Europe* (2009).
[33] Krepinevich, *Cyberwarfare: A "Nuclear Option"?*79.
[34] Ibid.65.

> The German experience suggest that even a first class military power- rugged and resilient as Germany was- cannot live long under full-scale and free exploitation of air weapons over the heart of its territory. By the beginning of 1945, before the invasion of the homeland itself, Germany was reaching a state of helplessness. Her armament production was failing irretrievably, orderliness in effort was disappearing, and total disruption and disintegration were well along.[35]

Bombing campaigns targeted civilian targets like transportation, electricity and manufacturing infrastructure that enabled war production. Assessment reports post Second World War determined irreparable physical damage needed to occur to inflict strategic victory over the means of production.[36] Cyberattacks cannot achieve destruction of infrastructure like conventional weapons can. Networks can be disrupted temporarily but the hardware and machines that enable cyberspace will still be intact. "Because cyberwar does not involve bombing cities or devastating armored columns, the damage inflicted will have a short-term impact on targets".[37]

Another effect of aerial bombardment is the immediate delivery of shock and destruction. It is seen and felt. Cyberweapons are incapable of delivering this sensation. Empirical evidence shows that a cyberweapon has never caused immediate direct damage and destruction on the same level as bombs. Stuxnet took many months to damage Iranian nuclear facilities.[38]

Aerial bombardment can be overwhelming on first strike, but usually requires multiple waves and re-attack to achieve strategic goals. This was noted in the US Strategic Bombing Survey, "no indispensable industry was permanently put out of commission by a single attack. Persistent re-attack was necessary."[39] Attacks were rarely successful on the first attempt and if

---

[35] . *The United States Strategic Bombing Surveys, Summary Report* (Maxwell Airforce Base, Alabama: Air University Press,[1945]).37-38.
[36] *Ibid.*
[37] Eric Gartzke, "The Myth of Cyberwar," *International Security* 38, no. 2 (..57.
[38] Langner, *Cracking Stuxnet: A 21st Century Cyberweapon*
[39] . *The United States Strategic Bombing Surveys, Summary Report*39.

they were, the German industry was very capable of replacing and rebuilding infrastructure.[40] Persistent attacks is not a luxury in cyberwarfare.

Cyberattacks "are most effective as an opening salvo in war".[41] Once an attacker has infiltrated a network the defender will quickly move to patch the vulnerability and perhaps even close the network from the outside. For a re-attack to occur, another vulnerability in the system would need to be found. The more attacks that are launched against a system the harder it becomes to find future vulnerabilities.

Though cyberattacks can achieve disruption of critical industry in depth for minimal expenditure, they are not a replacement for airpower as they are incapable of delivering the carnage of bombs and cannot be employed persistently. The more pragmatic use of cyberweapons is in a combined force environment which may be alongside strategic bombing campaigns but always synchronized with conventional warfare assets.

Can Cyberwar replace conventional war?

> The chief reason warfare is still with us is neither a secret death-wish of the human species, nor an irrepressible instinct of aggression, nor, finally and more plausibly, the serious economic and social dangers inherent in disarmament, but the simple fact that no substitute for this final arbiter in international affairs has yet appeared on the political scene.[42]

The ultimate argument for cyberwarfare being the alternative to conventional warfare would be if cyber conflict could achieve the decisiveness of war. Proponents of cyberwarfare as the future replacement of warfare have gone so far as to propose strategic cyberwar as the future

[40] Ibid.38.
[41] A. Liff, "Cyberwar: A New Absolute Weapon? the Strategic Proliferation of Cyberwarfare Capabilities and Interstate War," *War of Strategic Studies* 35, no. 3 (2012).
[42] Hannah Arendt, (New York: Harcourt, Brace, 1970). 2.

of war. Tim Mauer argues that cyberwar would benefit society as cyberattacks limit the damage that can occur and does not put people at risk compared to conventional war.[43]

Would it be possible for a cyberwar to achieve similar decisiveness to that of conventional war?

A key element of war is its finality. Wars usually come to an end when one side is victorious or the warring parties become weary of further conflict. For this to occur there needs to some persuasive reason to cease conflict. "The fighting force must be destroyed: that is, they must be put in such a condition that they can no longer carry on the fight."[44] Destroy implies that there needs to be some level of physical destruction. It might be hard to convince a country to capitulate if there is no observable death or destruction and lifestyles are only mildly inconvenienced. Can cyberwarfare cause destruction?

Stuxnet was an example of how cyber was able to penetrate a system and damage sensitive nuclear equipment. It however led to no loss of life and no one claimed responsibility. Though it is widely agreed Stuxnet set back the Iranian nuclear program 1-2 years, it did not cause irreparable damage or eliminate the Iranians capability.[45] Thomas Rid equated the act to sabotage- antagonistic perhaps, but not warfare.[46]

The Stuxnet example highlights another characteristic of cyberattack, its effects are short-lived. Up to date there has been no cyberattack that has resulted in any kind of lasting damage to an adversary. Even the 2007 attack on Estonia as holistic and complex as it was caused no

---

[43] Tim Maurer, "The Case for Cyberwarfare," *Foreign Policy*, 2011, .
[44] Carl von Clausewitz, *On War* (New York: Oxford University Press, 1976)..32.
[45] David Albright, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment," *ISIS Reports* (2010).
[46] Rid, *Cyber War Will Not Take Place*

significant damage to the economy or loss in GDP.[47] Conversely the cyberattack committed against the Saudi oil company ARAMCO erased the hard disks of 30 000 computers causing a degree of economic damage, but nothing enduring. The attack certainly was not capable of destroying physical hardware or harming humans.[48]

If something operates in cyberspace or depends on cyber to function, it will almost always have fail safes or redundant processes. "A cyberattack carried out against a military today can at worst, return it to its pre-networked condition (as long as it has something to revert to)."[49] In order to attain a certain level of decisiveness, cyberweapons need to be able to not only attack single targets but also the backup capabilities to the targets as well. If the targeted can simply flick the switch to the backup, the cyberattack will not be all that useful unless combined with some other strike.

Cyberwar conjures a vision of two states fighting each other with computers in cyberspace. The word cyberwar implies that there would be no need for war in any other domain. Could a hypothetical cyberwar be contained to its singular cyberspace domain?

An issue with the notion of a contained cyberwar is that there is no rule in war that says a cyber-participant cannot at any time, *breakout* the conventional weapons. A nation's desire to fight a war solely in cyber may not be known or adhered to by their opponent; there is nothing constraining the adversary to retaliate with conventional weapons in a different domain. The cyberwarrior won't be much of a match for effective kinetic warfare. "Plutonium trumps bytes in a shooting war."[50] A single cyberattack is not decisive like a nuclear attack could be and will not

[47] Clover, *Kremlin Backed Group Behind Estonia Cyber Blitz*
[48] Thomas Rid, "Cyberwar and Peace," *Foreign Affairs* (2013b).
[49] Libicki, *Why Cyber War Will Not and should Not have its Grand Strategy*29.
[50] William Jackson, "Fuss Over Cyber War Distracts from Real Threats, Security Pioneer Says," *GCN* (2012).

end a conflict before a retaliation would occur. "Cyberattack would not be the first choice of a competent military commander because the commander's biggest concern is preventing counterattacks, and unless they primarily target a country's military, they will receive counterattacks."[51] It is almost a given that an enemy under attack, in any domain would not hesitate to respond within any other means under their power.

Another issue is that cyberwar is impeded by the ambiguity of cyberspace. Cyberspace unlike air, sea, land and space is created by machines and many cyberspaces can be created. Due to this lack of singularity it is difficult to discern what is being contested and by whom. How is it possible to reach any degree of finality in such an environment? A hacker shut down and neutralized one day, can be up and running the next on a different server in a different domain. Furthermore, damage to physical servers and infrastructure can be easily repaired and replaced thanks to an abundance of cheap and readily available hardware.[52]

During the 2007 attacks against Estonia, Estonia had evidence the attacks originated in Russia. But as author Miska Rantanen points out, Russian government computers could have been infected by a virus that in turn launched the denial of service attacks. The attacks actually could have been committed by anyone.[53] If one cannot positively identify the attacker how can one retaliate and exchange blows- a necessary element of war. The Moonlight Maze example illustrates this problem. The moonlight maze incident involved a group of unknown hackers whose actions were thought to be authorized by the Russian Government. They infiltrated the US NIPRNET and other networks and stole sensitive defense material. It was believed the attackers were Russian given the IP addresses, but IP addresses are not reliable to determine origin. The

[51] Neil Rowe, "The Ethics of Cyberweapons in Warfare," *International Journal of Cyberethics* 1, no. 1 (2009).4.
[52] Martin Libicki, *Conquest in Cyberspace*Cambridge University Press, 2007).84-85.
[53] Miska Rantanen, "Virtual Harassment, but for Real," *Helsingin Sanomat* (2007).

Pentagon wanted to “hack back” but was unsure who the attacker was and retaliating against the Russians who may not even be the perpetrators, could be perceived as an act of war.[54]

The Brazilian power outages of 2005 and 2007 re-iterate the attribution problem and add another layer of ambiguity in that what was thought to be a hacker may just have been a technical glitch. In 2005 and 2007 Brazil suffered power losses in many cities, affecting millions. The US stated credible sources indicated a cyberattack.[55] However later it was determined the culprit might have been a glitch in the grid at the Itapúa dam [hydroelectric dam].[56] If simple infrastructure failures could be confused for an act of war in cyberspace, it is likely any actions in cyberspace could be widely interpreted. This makes the domain of cyber an undesirable place to settle anything of significance.

Future conflicts between states will have a cyberspace element. The element however will be part of the aggregate military operation and projection of force and not the deciding part of the war. The future of war is not ‘cyberwar’ but wars rather that will utilize cyberweapons in combination with other means to wage war. Without an enduring effect on the balance of power, attacks in cyberspace serve only to irritate or disrupt. They are not effective in breaking the will of a state or the will of the fighting force.

PART III

Cyber as a Force Multiplier

Cyberweapons will never replace conventional weapons and the reality of a cyberwar is a distant fantasy. However, combined with conventional warfare, cyberweapons can have an

[54] Vernon Loeb, "Pentagon Computers Under Assault," *Washington Post*2001.
[55] Graham Messick, "Cyber War: Sabotaging the System," *CBS News*2009.
[56] Loeb, *Pentagon Computers Under Assault*

advantageous if not devastating result. As was argued in this paper, a cyberattack in isolation has little value and when used in isolation it will very likely result in a retaliatory kinetic attack. Cyberattack should always be executed in combination with other forms of warfare.

Cyberwarfare is effective in hybrid warfare in that all other domains have some residual dependency on cyberspace to function, hence cyberwarfare can be applied against actors in all domains, so long as they are vulnerable in cyberspace. Cyberweapons can be conducted simultaneously to conventional attacks to amplify the chaos and also sequentially, perhaps as a preliminary condition setter to make a larger subsequent conventional attack more devastating.

Israel was able to apply this combined concept in 2007 when they effectively blinded Syrian Air Defense stations while conducting a bombing raid on a suspected nuclear research site. It is believed they used the 'Suter' network attack system produced by BAE:

> The technology allows users to invade communications networks, see what enemy sensors see and even take over as systems administrator so sensors can be manipulated into positions so that approaching aircraft can't be seen, they say. The process involves locating enemy emitters with great precision and then directing data streams into them that can include false targets and misleading messages algorithms that allow a number of activities including control.[57]

Similar to how land forces might integrate artillery or Information operations into their operational manoeuvre; the Israelis were able to effectively integrate cyberattack into a combined effort attack. This is an excellent illustration of the combat enhancing capability of cyberweapons.

Disrupting Lines of Communication and Information

[57] Sharon Weinberger, "How Israel Spoofed Syria's Air Defence System," *Wired*, Oct 2007, .

In chapter 16 of his book, Clausewitz describes the importance of lines of communication- attacking lines of communication at any point in a conflict can severely degrade the enemy's ability to make decisions and manoeuvre.[58] Country's reliance on networks to enable these lines of communication makes them a particularly vulnerable. Because cyberattacks cause only temporary disruption, an attack would need to be combined with some other means. Cyberattacking lines of communication alone would not have a devastating effect. "Effects would not be immediate and troops like to think they can fight just fine without system administrators."[59]

A cyber blockade similar to its naval equivalent could deny a state freedom of movement and an ability to support operations in cyberspace by denying or disrupting internet access. Used in early phase shaping operations a belligerent could degrade the resolve of an adversary's populace by targeting social media and public relations sites before forces have engaged in physical war. This application is compelling as it can be done without violence or physical harm. The fact so many are reliant on internet connections for everything they do amplifies this type of attack considerably. "There are alternatives to banks, but there is only one Internet."[60]

Deep Battle

When weak armies meet strong ones in contemporary battle, the weaker force is not able to take advantage of the deep battle. An advanced state will have few vulnerabilities that will permit a foe to penetrate in depth. The creation of cyberspace has opened the possibility of a smaller state attacking a stronger foe in depth. Cyberspace creates advantages for a technologically advanced state like the USA, but it also creates challenges. Cyber offers "means

[58] von Clausewitz, *On War*
[59] Rowe, *The Ethics of Cyberweapons in Warfare*3.
[60] Ibid.12.

that include unconventional or inexpensive approaches that circumvent strengths exploit vulnerabilities and confront the country in ways that cannot be matched in kind."[61]Cyberweapons may offer the only affordable option of a non-state or small state to strike a stronger, more geographically distant country at home. An adversary that is capable of conducting attack in depth in combination with fighting the near fight will always be able to mount a more effective offense. Cyberwarfare alone may not be able to defeat the enemy, but it can increase the perception of an adversary's strength by changing a force's appearance to that of one that is not conventional, one whose operational structure is dissimilar to their own.

The Frontline

It is theoretically possible to attack the networks that support front-line fighting vehicles and soldiers systems. However tactical level systems are rarely connected to the internet and can usually be manually overridden. A more effective means of attack might be to target not only military networks but public and private sector as well. Creating cyber chaos at the target location before a kinetic attack could enhance the damage caused by conventional weapons.

A joint attack was conducted by Russia against Georgia in 2008. Russian launched a three pronged cyberattack into Georgia prior to their invasion. Russia defaced government websites, launched denial of service attacks against the private and public sector and distributed malicious software to Russian sympathizers living in Georgia with the idea they would diffuse viruses throughout the country's networks.[62] The effect was minimal as Georgia was only minimally connected and dependent on the internet. The primary damage was to

[61] Office of the Chairman, Joint Chiefs of Staff, *National Military Strategy* (Washington, D.C: , 1997).9.
[62] Jose Nazario, "Politically Motivated Denial of Service Attacks," *Arbor Networks* (.

communications systems that limited the Georgians to execute an effective public affairs plan.[63] Though cyber was not a crucial factor in this conflict, it does illustrate how cyber could be employed in the future. As countries become more connected this tactic will become more effective.

CONCLUSION

Cyberwarfare is an emerging military capability that has been presented as an alternative means to wage costly and risky physical warfare. It is omnipresent in all other warfare domains which gives it the appearance of being a possible alternative to other forms of warfare. While it is true, cyberwarfare can permit a belligerent to strike targets from great distance affordably; what the attacker is actually able to achieve is limited and the associated risks in using the weapon can be surprisingly high

Cyberweapons are not alternatives to conventional weapons. Possession of a militarized cyber capability is not compellingly coercive due to the ambiguities of cyberspace and its inability to cause physical harm. Though it is possible and cheap for anyone to enter cyberspace, what one is able to do there is dependent on preparation time, funding, expertise and exploitable vulnerabilities in the enemy's network. Due to the number of factors that need to be simultaneously in place to conduct successful cyberwarfare, it is evident that cyberweapons will never be alternatives to conventional ones and cyberwarfare will not replace physical warfare.

Furthermore, cyberwar should not be considered as an alternative to conventional war. Physical war is destructive and decisive. Known cyber capabilities do not possess an ability to

[63] Rid, *Cyber War Will Not Take Place*14.

destroy. Add to that the fact the enemy can revert to conventional means at any point negates the notion of a singular cyberwar.

Conflict in cyberspace is a future reality; however the notion that contemporary physical wars will be replaced by cyberwars in the future is a gross exaggeration and based on false assumptions and sensationalism. Future warfare will not revolve around a single capability or means. Recent limited cyberwarfare incidents show that cyberattack will not be used by itself but always in conjunction with other means. Future warfare will be joint and all joint warfare will have a cyberwarfare component.

- Ryan Stimpson

GLOSSARY

Cyberattack

-"actions taken through the use of computer networks to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and the networks themselves." It will not include criminal cyberattack (vandalism, fraud, etc.) nor will it include cyber-espionage.

Cyberpower

- "the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power."[64]

Cyberspace

-The novel 5th space of warfare after land, sea, air and space. Includes all computer networks in the world and everything they connect and control via cable, fiber-optics or wireless.[65]

Cyberwar

- Warlike conflict conducted in virtual space with means of information and communication technology and networks. Cyberwar aims at influencing the will and decision making capability of the enemy's political leadership and armed forces.[66] One would conduct cyberwar to achieve the same war aims identified by von Clausewitz's.

Cyberwarfare

[64] Daniel Kuehl, "From Cyberspace to Cyberproblem: Defining the Problem," in *Cyberpower and National Security*, Vol. 48, 2009).
[65] Fred Schreier, "On Cyberwarfare," *DCAF Horizon* (2015).10.
[66] Ibid.25.

-"use of computers or digital means by state or non-state, with explicit knowledge or approval by that actor against another state or private property within another state that includes: intentional access, interception of data, damage to digital and digitally controlled infrastructure."[67]

Cyberweapons

- "is seen as a subset of weapons more generally: as a computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings."[68]

War

- The metric definition we will use in order to determine if an action is fulfilling the requirements of the purpose of war will be from Clausewitz's On War. "War is nothing but a duel on a larger scale, an act of force to compel our enemy to do our will"[69]. Clausewitz does not imply at any point that total destruction of the enemy is a requirement, however there needs to be a reason of some kind that compels the enemy to physically and/or morally capitulate.[70]

[67] *Resolution 1113*, (2011): .
[68] Rid and McBurney, *Cyber-Weapons*
[69] von Clausewitz, *On War*13.
[70] Ibid.31-44.

BIBLIOGRAPHY

"Major Power Failures Hit Brazil." *BBC News*,2009.

The United States Strategic Bombing Surveys, Summary Report. Maxwell Airforce Base, Alabama: Air University Press, 1945.

Adams, James. "Virtual Defense." *Foreign Affairs* 80, no. 3 (2001).

———. "Virtual Defense." *Foreign Affairs* (2001).

Albright, David. "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment." *ISIS Reports* (2010).

Arendt, Hannah. On Violence. New York: Harcourt, Brace, 1970.

Blainey, Geoffrey. *The Causes of War*. New York: Free Press, 1973.

Borg, S. "Economically Complex Cyber Attacks." *IEEE Security and Privacy* 3, no. 6 (2005).

Clover, Charles. "Kremlin Backed Group Behind Estonia Cyber Blitz." *Financial Times- Europe* (2009).

Devost, Matthew and Neal Pollard. "Taking Cyber-Terrorism Seriously." *Terrorism Research Centre* (2002).

Gartzke, Eric. "The Myth of Cyberwar." *International Security* 38, no. 2.

Goodman, Will. "Cyber Deterrence." *Strategic Studies Quarterly* (2010).

Gray, C. S. *Another Bloody Century, Future Warfare*. London: Phoenix, 2005.

Hart, Liddell. *Strategy*. New York: Penguin Books, 1991.

Hesseldahl, A. "Computer Worm may be Targeting Iranian Nuclear Sites." *Bloomberg* (2010).

Jackson, William. "Fuss Over Cyber War Distracts from Real Threats, Security Pioneer Says." *Gcn* (2012).

Joint Publication 3-13, Joint Doctrine for Info Ops (2006).

Kirschner, S. "I Love You...Not." *Popular Science.* (2000).

Krepinevich, Andrew. "Cyberwarfare: A "Nuclear Option"?" *Centre for Strategic and Bugetary Assessments* (2012).

Kuehl, Daniel. "From Cyberspace to Cyberproblem: Defining the Problem." In *Cyberpower and National Security*. Vol. 48, 2009.

Langner, R. *Cracking Stuxnet: A 21st Century Cyberweapon.* Anonymous 2011. (Ted.com).

Lee, M. and L. Hornby. "Google Attack Puts Spotlight on China's "Red" Hackers." *Reuters* (2010).

Libicki, Martin. *Conquest in Cyberspace* Cambridge University Press, 2007.

———. "Why Cyber War Will Not and should Not have its Grand Strategy." *Strategic Studies Quarterly* (2014).

Liff, A. "Cyberwar: A New Absolute Weapon? the Strategic Proliferation of Cyberwarfare Capabilities and Interstate War." *War of Strategic Studies* 35, no. 3 (2012).

Lin, Patrick. "Is it Possible to Wage just a Cyberwar?" *The Atlantic* (2012).

Loeb, Vernon. "Pentagon Computers Under Assault." *Washington Post,*2001.

Lucas, George R. "Postmodern War." *Journal of Military Ethics* 9, no. 4 (2010).

Lupovici, A. "Cyber Warfare and Deterrence: Trends and Challenges in Research." *Military and Stategic Affairs* 3, no. 3 (2011).

Maurer, Tim. "The Case for Cyberwarfare." *Foreign Policy* (2011).

McGlaun, Shane. "DARPA Wants More Money for Cyber Weapons." *Daily Tech Magazine* (2011).

Messick, Graham. "Cyber War: Sabotaging the System." *CBS News,*2009.

Nakashima, Ellen. "Defense Officials Discloses Cyberattacks." *The Washington Post,*2010.

———. "US Cyberweapons had been Considered to Disrupt Gaddafi's Air Defenses." *The Washington Post,*2011.

Nazario, Jose. "Politically Motivated Denial of Service Attacks." *Arbor Networks*.

Nye, J. "Cyber Power." *Belfer Centre for Science and Int'l Affairs Harvard Kennedy School* (2010).

O'Donnell, B. T. "Humanitarian Law:Developing International Rules of The Digital Battlefield." *Journal of Conflict and Security Law* 8, no. 1 (2003).

Office of the Chairman, Joint Chiefs of Staff. *National Military Strategy*. Washington, D.C: 1997.

Rantanen, Miska. "Virtual Harassment, but for Real." *Helsingin Sanomat* (2007).

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (2012).

———. *Cyber War Will Not Take Place*. London: Hurst and Company, 2013.

———. "Cyberwar and Peace." *Foreign Affairs* (2013).

Rid, Thomas and Peter McBurney. "Cyber-Weapons." *Rusi Journal* 157, no. 1 (2012).

Rowe, Neil. "The Ethics of Cyberweapons in Warfare." *International Journal of Cyberethics* 1, no. 1 (2009).

Rustici, Ross. "Cyberweapons: Leveling the International Playing Field." *Strategic Studies Institute* (2011).

Schmitt, M. "Wired Warfare: Computer Network Attack and Jus in Bello." *International Review of the Red Cross* 84, no. 846 (2002).

Schneier, Bruce. "Want to Evade NSA Spying? Don't Connect to the Internet." *Wired* (2013).

Schreier, Fred. "On Cyberwarfare." *DCAF Horizon* (2015).

Sommer, Peter. "Experts Say, Iran has Neutralized Stuxnet." *YNet News- Middle East* (2012).

Suciu, Peter. "Why Cyberwarfare is so Attractive to Small Nations." *Fortune Magazine* (2014).

UNSC Resolution 1113 (2011).

von Clausewitz, Carl. *On War*. New York: Oxford University Press, 1976.

Weimann, Gabriel. "Cyberterrorism: How Real is the Threat?" *USA Institute of Peace* (2004).

Weinberger, Sharon. "How Israel Spoofed Syria's Air Defence System." *Wired* (Oct 2007).