National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CYBERWARFARE

Maj J.S. MacDonald

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*

CYBERWARFARE

Maj J.S. MacDonald

Word Count: 2750

Compte de mots: 2750

CYBERWARFARE

The term "cyberwarfare" captures the imagination with images of a nation's armed forces capable of utterly defeating its opponent without firing a shot; a modern vision of Sun Tzu's principle that, "…supreme excellence consists in breaking the enemy's resistance without fighting."[1] Cyberwarfare understandably appeals to Western armies as Western countries generally enjoy broader access to and use of computers and associated technology. This provides these countries with a natural launching point for the adoption of many of these technologies to military use. However, this paper will demonstrate that cyberwarfare is, far from a silver bullet to war, merely another tool with both advantages and disadvantages that accompany any other; for every measure there is a counter-measure. Canadian doctrine notes that, "[t]echnology on its own is not a capability; it is its interaction with people (through doctrine and training) that transforms it into something capable of dominating the adversary."[2]

While Colin S. Gray has stated, "…notwithstanding the 'Cybergeddon' catastrophe scenarios that sell media products, it is clear enough today that the sky is not falling because of cyber peril," this conclusion is driven in part by his rather narrow definition.[3] Technology and the will to use it for military purposes risks outracing any deliberate and thoughtful strategy for its use and integration. This poses a significant risk that Canada will find itself devoting resources to the tools associated with cyberwarfare without the institutional ability to achieve the country's strategic goals towards which all

---

[1] Sun Tzu, *The Art of War*, tr by Lionel Giles, http:www.classics.mit.edu/Tzu/arwar.html; Internet; accessed May 20 2015.

[2] Department of National Defence, *No-Man's Land: Tech Considerations for Canada's Future Army* (Kingston: Army Publishing Office, 2014), 1-1.

[3] Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling*, (Carlisle, PA: U.S. Army War College Press, 2013), xi.

military power should be directed. Furthermore, while the cyber domain itself is merely another environment in which to fight, it is the possibility of linking weapons platforms through the domain that carries the greatest military risk. Gray's assertion that the sky is not falling may be more appropriate for the civilian sector, but is not applicable to the military due to his definitional limitations and the ongoing advances of networked weapons systems.

What is "Cyberwarfare?"

Cyberwarfare has taken its place as another domain of warfare alongside land, sea and air although the CAF Integrated Capstone Concept also proposes space and human as additional domains.[4] Perhaps its intangible nature and its novelty have contributed to the perception that it is predominant rather than simply another domain in which militaries should be prepared to fight. As one author noted, "cyber power 'catches the wave'…of an American official and public mood that strongly wishes the country to substitute stand-off power, kinetic and electronic, for boots on the local ground across oceans."[5] The cyber domain is so novel, that as of the publication of the Canadian Army Land Warfare Centre's ("CALWC") *No Man's Land: Tech Considerations for Canada's Future Army*, they acknowledge that there is no CAF doctrinal definition of "cyber".[6] The CALWC proposes that there are only five distinct domains and what has been termed "cyber" is in reality better described as the Electromagnetic ("EM") domain.[7] This is generally enough in accord with the two definitions of cyberspace relied on by Colin Gray.[8]

---

[4] Department of National Defence, *No Man's Land*:…, 5-2.
[5] Gray, *Making Strategic Sense of Cyber Power*:…, 6.
[6] Department of National Defence, *No Man's Land:…*, 5-6
[7] *Ibid.*, 5-7.
[8] Gray, *Making Strategic Sense of Cyber Power:…*, 9.

Cyberwarfare, however, is more nuanced. As Gray notes, there are serious consequences to calling an activity cyberwarfare versus another label.[9] For example a hacktivist group (hacktivist being an amalgam of "hacker" and "activism" and meaning "promoting or resisting some kind of political or societal change through nonviolent but often legally questionable cyber means of protest") that leaks military secrets has engaged in cyber activity, or as Gray would say, exercised "cyber power" but it has not, as a non-state actor, engaged in cyberwarfare.[10]

While widespread computer use is the norm, attacks against institutions such as banks or movie studios, while causing widespread panic and economic harm, are not the real threat to national security. Certainly broader economic cyber-attacks serve to assist in an overall warfare, but these types of attacks can generally be recovered from and rarely work twice. These types of attacks may just as easily be cyber-crime such as an attempt to hack a bank and steal financial information or the actions of hactivists who seek to serve their own agenda. Such actions, while meeting Gray's definition of "cyberpower" fall short of cyberwar. What then is cyberwar? As only one domain in which we fight, the definition of cyberwar is not fundamentally different than the concept of war we are more familiar with, "[w]hether it be war on land, at sea, or in the air, or now in cyberspace, war always has a political goal and mode (which distinguishes it from crime) and always has an element of violence."[11] The violence however must manifest itself on the physical plane, which is where Gray's definition of the cyber domain falls short. Some less precise definitions seem to use the terms "cyberspace" and "internet"

---

[9] *Ibid.*, 10.

[10] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014) [kindle edition], Part II.

[11] *Ibid*.

interchangeably which is both incorrect and dangerous.[12] The US government's definition of a cyber-attack, or an exercise of cyber power which would meet the criteria for cyberwarfare is that it is, "proximately result in death, injury or significant destruction."[13] Again, the result of the actions executed through the cyber domain must impact on the physical. Here the Canadian definition of cyber-attacks risks a dangerously narrow understanding as it focusses on, "the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information." This definition is perhaps more appropriate to the civilian sector but it risks being perceived as networks and their computers, instead of all devices linked to the network and that can have a physical effect. The difficulty with cyber-attacks is figuring out when they actually began, as the effects may not be discovered in time and of a greater concern is the issue of attribution, so that the appropriate actions can be directed at the appropriate actor.

Attribution

Whereas in earlier times an act of war by a nation state was relatively clear, actions taken in cyberspace are far less so. Fielding an army or navy or manufacturing nuclear weapons were the guarded domains of nation states, subject perhaps to the selling or theft of a nuclear weapon. Even the September 11th, 2001 al-Qaeda planned attacks on the US were eventually discovered to be the actions of a non-state terrorist organization. However, within the cyber domain access to the tools needed to exert cyber power are near ubiquitous in comparison. Computers and access to networks are so common in the

[12] Myriam Dunn Cavelty, "Cyber-security," in *Contemporary Security Studies, 3rd ed.*, (Oxford: Oxford University Press, 2013), 364.

[13] Singer and Friedman, *Cybersecurity and Cyberwar.*

vast majority of elementary schools, high schools, universities and workplaces that the average citizen spends a considerable portion of their day on-line. One factor of cyber weaponry, such as malware, is that it, "…can be detected only after it has been released, and by that time it becomes even more difficult to link it with the person or organization that actually released it."[14] Of course this difficulty can also make cyberwarfare attractive to nation states who can subsequently deny their involvement in any attack. Perhaps the most well-known such example is the Stuxnet virus directed squarely at Iran's Natanz nuclear facility and subsequently identified as having been a joint operation between US and Israeli governments, but only discovered by chance by a German computer specialist.[15]

The Cyberwarfare Threats and Advantages

Having looked at what cyberwafare is we can now look at what the threats and advantages are, for as with any other tool, the cyber domain is a double edged sword. The greatest threat from cyberwarfare is not on the cyber domain itself, but in the physical. This is tacitly recognized by the CALWC when they note that cyberwarfare is increasingly becoming a matter of the convergence of Computer Network Operations and Electronic Warfare. The more physical weapons systems such as air defence systems, ISR platforms and communications and computer systems become networked, the greater the vulnerability of cyber-attack. Whether this is truly cyberwarfare will greatly depend on the definition of "cyber" as discussed above. There are some who would argue that cyberwarfare can only take place in the cyber domain, which as described by the CALWC is solely along the EM spectrum. However, to look at the above noted

[14] Department of National Defence, *No Man's Land*:…, 5-14.
[15] Singer and Friedman, *Cybersecurity and Cyberwar.*

examples, a coordinated attack using malware to defeat or overtake the systems in an air defence battery and a drone equipped with an ISR pod would have to be considered distinct attacks on the land and air environments. Instead, I propose that the fact that the initiating attack is launched from the cyber domain is the overriding characteristic and that cyberwarfare can, and very likely will, have carry over effects on the physical domains. This is where Gray's view is somewhat constrained as he views cyber as "an extreme case of non-kinetic agency" akin to economic warfare.[16] This is primarily due to his definition of cyber, but this definition then serves to show how dangerous it can be to ignore the full spectrum of cyberwarfare possibilities. His limited scope is somewhat surprising given that one of the definitions he draws on for "cyberspace" includes the computers as well as computer networks.[17] Gray himself goes on to agree that cyber power "has to be expressed as, in, and through networks with physical architecture."[18] It would appear then that he was live to the issue of the need for a physical manifestation at the start and/or end of a cyber-attack yet it remains his view that cyber power only constitutes information.[19] He did not state, however, whether it was the reading and interpretation of this information by humans that transformed the cyber to the physical, or whether if another computer could interpret, and possibly act, on that information the actions stayed in the cyber domain or were then transformed into the physical. The main limitation with Gray's view is that he sees computers and their networks as the only physical ends to cyber, but one need only look around their house today to realize that everything is a computer. The battlefield is no different.

---

[16] Gray, *Making Strategic Sense of Cyber Power:…*, 14.
[17] Gray, *Making Strategic Sense of Cyber Power:…*, 9.
[18] *Ibid.*, 19.
[19] *Ibid.*, x.

What is far more likely in true cyberwar is that nation states will use cyberwarfare at its most effective: as only part of a larger campaign of war. This recognizes the fact that war is ultimately a political endeavour, as Clausewitz said, "a continuation of political intercourse, carried on with other means," and a contest of wills and therefore not to be won solely through the use of cyber.[20] However, the greatest threat comes from an increased reliance on connectivity through the stated move towards Adaptive Dispersed Operations and the consequential reliance on computer networks, as well as networked sense and weapons platforms themselves. While it is possible that one way to degrade an enemy's attack is to rely less on the cyber domain, the reality is that the obvious advantages offered by such reliance means that Western nations will simply not do so.[21] As *No Man's Land* notes, this actually establishes a vulnerability for other countries to exploit, with minimal fear of a cyber-retaliation, although the threat that cyber-aggression would bring about a physical retaliation would have deterrent value.[22] The Chinese view of cyberwar specifically notes that enhanced reliance on computer networks in fact establishes a vulnerability.[23]

While there is some recognition of the risks imposed by a reliance on network enabled operations, there is also a failure to adequately recognize the full threat. In *Future Networks: A Concept for the Army of Tomorrow*, characterizes the risk of threat forces essentially ignores the threat from a peer force, suggesting, "NEOps and NCW may very well optimize the Canadian Army's ability to operate against peer or near peer

---

[20] Carl von Clausewitz, *On War*, ed. And trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1989), 87.

[21] Department of National Defence, *No Man's Land*:…, 5-17.

[22] Department of National Defence, *No Man's Land*:…, 5-17.

[23] Singer and Friedman, *Cybersecurity and Cyberwar.*

competitors but may not function quite so well against an asymmetric threat."[24] In fact, others have argued, rightly, that the reverse is true because a massive act of cyber terrorism is beyond the "intellectual, organizational, and personnel capacities of even the most well-funded and well-organized terrorist organization, as well as those of even the most sophisticated international criminal enterprises."[25] This is due in large part to the requirement for a cyber-attack to cross over into the physical domain. Merely hacking infrastructure is irrelevant if you do not know how the infrastructure works so that you can inflict damage to achieve the desired effect. The clearest example is the Stuxnet virus which damaged the Iranian nuclear facility. It was not merely a malicious code written by a computer specialist that did the damage. The code was the means by which the physical damage was achieved, but that required individuals knowledgeable in "nuclear physics and engineers familiar with a specific kind of Siemens-brand industrial equipment."[26] Thus it is argued that Gray is incorrect when he states that the only real threat to cyber-attack is information.[27]

Reliance on computerized networks as avenues to link devices is only intended to grow. The Canadian Army's vision of the future way it expects to fight has been laid out in part in *Land Operations 2021: Adaptive Dispersed Operations*.[28] Essentially, the army envisions leveraging an ability to carry out actions "faster than the adversary can respond while maintaining the ability to respond to changes in the adversary actions faster than he

---

[24] Department of National Defence, *Future Networks: A Concept for the Army of Tomorrow* (Kingston: Army Publishing Office, 2013), 35.

[25] Singer and Friedman, *Cybersecurity and Cyberwar.*

[26] Singer and Friedman, *Cybersecurity and Cyberwar.*

[27] Gray, *Making Strategic Sense of Cyber Power:…*, x.

[28] Department of National Defence, *Land Operations 2021: Adaptive Dispersed Operations. The Force Employment Concept for Canada's Army of Tomorrow* (Kingston: Army Publishing Office, 2007).

can exploit these changes."[29] The forces able to do this will be dispersed throughout the physical dimensions of the battlespace and through time, yet able to synchronize their effects at a time and location of our choosing. Key to controlling this synchronization is the concept of Network-enabled operations (NEOps).[30] The crux of NEOps is networking, resulting in integrated "information systems, weapons and other effects-producing platforms" in order to leverage maximum integration.[31] This reliance on networking, however, also serves to open the number of physical platforms subject to cyber-attack. If every direct and indirect fire system in an Area of Operations is networked in order to leverage dispersion on the battlefield and in an attempt to synchronize effects, then the entirety of an army's direct and indirect fire systems are vulnerable. Further advances attempting to link sense to fire systems such as an unarmed drone, or in current nomenclature Remote Piloted Aircraft ("RPA") only serves to further extend the vulnerability. Antithetical, though perhaps precautionary, to defensive cyberwarfare might be to establish insulated nodes of systems or groups of systems so that a successful cyber-attack onto one node does not compromise a wider system.

Finally, two obstacles to the development of appropriate doctrine on cyberwarfare are the speed with which technology is changing and the familiarity with senior leadership with computers. First, the most oft-cited quantifiable measure of technological advance is Moore's law, which roughly states that computer processing power will double every two years.[32] Rapid advances in what we can do make it difficult to decide what we should do as a best strategy which should guide armed forces over a longer

---

[29] *Ibid.*, 18.
[30] *Ibid.*, 22.
[31] *Ibid*.
[32] "Moore's Law or how overall processing power for computers will double every two years", www.mooreslaw.org; Internet; accessed May 16, 2015.

period of time. Second, today's youngest soldiers have never lived in an age when home computers were not a reality. They understand technology far more intuitively, yet at the same time are that much more reliant on it. Conversely, those in the senior ranks of the military are far less likely to be familiar and comfortable with technology, risking a slower adoption rate. In essence, those who can have the greatest impact on cyber strategy and cyberwarfare are those least well versed in it.

Conclusion

As a battle of wills, warfare will always be a human endeavour. Regardless of how attractive technology and the cyber domain may be, they can no more guarantee quick, unilateral victory than any other military invention. Neither the machine gun, the tank, nor the atomic bomb have served to end war, let alone any other point on the spectrum of conflict; "[the] computer used as a military weapon is just a tool. Just as with the spear, the airplane, or the tank, it simply aids in achieving the goals that are part of any military operation."[33] To take a broader view, Western countries have gotten so good at waging war, certainly at the tactical level, that armies have forgotten that war is a tool itself intended to be part of a larger political strategy; "[o]ur subject ultimately, as it was for Clausewitz, is war, not the waging of war."[34] Excellence in cyberwarfare, offensive or defensive not only forms parts of a more comprehensive war plan, but the war plan itself must be tied to political goals. Cyber does pose what can be regarded as unique benefits and risks given its ubiquity, particularly the fact that the technology to do harm is in the hands of individuals, and that it cuts across the both military and civilian organizations.

---

[33] Singer and Friedman, *Cybersecurity and Cyberwar.*
[34] Gray, *Making Strategic Sense of Cyber Power*, 30.

Ultimately, however, cyber is far more of an evolution in military affairs than a true revolution.

BIBLIOGRAPHY

1. Canada. Department of National Defence. *Future Networks: A Concept for the Army of Tomorrow*. Kingston: Army Publishing Office, 2013.

2. Canada. Department of National Defence. *Land Operations 2021: Adaptive Dispersed Operations. The Force Employment Concept for Canada's Army of Tomorrow*. Kingston: Army Publishing Office, 2007).

3. Canada. Department of National Defence. *No-Man's Land: Tech Considerations for Canada's Future Army*. Kingston: Army Publishing Office, 2014.

4. Cavelty, Myriam Dunn. "Cyber-security." Chap. 25 in *Contemporary Security Studies, 3rd ed.* Oxford: Oxford University Press, 2013.

5. Gray, Colin S. *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling*. Carlisle, PA: U.S. Army War College Press, 2013.

6. "Moore's Law or how overall processing power for computers will double every two years." www.mooreslaw.org; Internet; accessed May 16, 2015.

7. Singer, P.W and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2014. [kindle edition]

8. Tzu, Sun. *The Art of War*. Translated by Lionel Giles. http:www.classics.mit.edu/Tzu/arwar.html; Internet; accessed May 20 2015.

9. von Clausewitz, Carl. *On War*. Edited and Translated by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1989.