National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CYBER "WAR" – IS IT?

Cdr Bryan Price

JCSP 43 DL

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 43 AD

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 43 DL – PCEMI 43 AD
2017 – 2018

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

CYBER "WAR" – IS IT?

Cdr Bryan Price

Word Count: 2833

Compte de mots: 2833

CYBER "WAR" – IS IT?

Introduction

The emergence of Cyber as the fifth domain of warfare has brought it squarely into the consciousness of military thinking, planning and operations. This is reflected in many ways and places in militaries globally, with a useful omnipresent definition coming from the United States (US) which includes it as a constituent part of their overall defense goal of "full-spectrum superiority."[1]

However, this new domain is at odds with the other four warfare domains in that military activity within it does not fit neatly into what has been, and is, accepted as constituting war. Many attacks in the Cyber domain originate from disparate actors that do not meet the criteria for acts of war. Cyberattacks have not demonstrated significant violent effects in the physical world, have not demonstrated effects related to an overall end nor have they been easily or readily attributable to identifiable adversaries. When this is juxtaposed against the prevailing guiding principles of war in western countries derived from Carl von Clausewitz (Clausewitz) and his tome *On War*, conflict and confusion exists as to whether or not the Cyber domain fits into the military consciousness in the context of war.

With this landscape in mind, this paper will show that although Cyberwar does largely conform to Clausewitz's definition of war, in the current paradigm it does not meet the criteria to be considered as such. This will be done by providing background and analysis of the current understanding of Cyberwar within the larger Cyber domain. Then, to analyse this domain in

[1] Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms 8 November8 2010 (As Amended Through 15 February 2016***)**, JP 1-01, (Washington, D.C.: Joint Chiefs of Staff, 2016), 95-96.

Clausewitzian space, a brief outline of key precepts will be undertaken and then compared to the populist notions of Cyberwar and past Cyberattacks as assessed by other authors.

Discussion

The evolution of the Cyber realm traces back to the late 1980s and began in earnest in the 1990s through the emergence of systems and users becoming interconnected through global networks like the Internet. This new environment became known as "Cyberspace"[2] and as it became ubiquitous, threats to its security soon emerged.

The first self-propagating virus, the Morris worm, was launched in the 1980s that initiated the phenomenon of the Denial of Service (DoS) attack. The forms of attack expanded over time to include Advanced Persistent Threats (APTs), malware and others along with an overall increase in frequency, durability and potency. These "Cyberattacks," can be summed us as "Cyberspace actions that create various direct denial effects in cyberspace (i.e., degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains"[3]

The meteoric rise of the interconnected nature of the world has made "Cyberspace operations"[4] core to the efficient and effective functioning of all aspects of the modern world including; banking and finance, commercial activities, health care, personal information management, and security and defense apparatus. The commensurate ability to ensure security from attack has become paramount, necessitating a strong focus on building competencies and

[2] A definition of Cyberspace is included in Appendix A.

[3] Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12(R), (Washington, D.C.: Joint Chiefs of Staff, 2013), II-5.

[4] A definition of Cyber operations is included in Appendix A.

capabilities in what is termed "Cybersecurity."[5] Examples of these kinds of threats occur constantly in the world today where the boundaries between individuals, non-governmental organisations, security organisations, commercial entities, nations and states are often blended together. A salient example of this was a warning by the US FBI of a malware threat from the Sofacy Group, which was suspected of being connected with the Russian GRU. This threat was purported to affect over 500,000 individual routers used by individuals, businesses and larger organisations in 54 countries.[6]

The ability to contend with external Cyber threats is critical no more so than for militaries as they work to defend against Cyberattacks and prosecute adversaries' Cyber capabilities as necessary. As with the noted example, attacks in military Cyberspace come from a spectrum of entities and a variety of state and non-state actors. Further, a significant portion of these attacks are well outside of being considered an act of war in a legal or theoretical sense. These attacks range from criminal acts by individuals with rudimentary equipment and capabilities, through terrorist attacks by transnational or distributed groups, espionage by foreign powers to acts-of-war by evolved and capable adversaries.

The wide-ranging threat environment for military Cyber operations and the rapid development of it as a military discipline over the last two decades has seen it grow from an area of limited consideration and scope to being held on par with the other four domains of warfare.

Two examples of the profile and position that the Cyber domain has in the military nexus are with the US and China. In the US, the military activities in Cyberspace fall under the auspices of the Department of Defense (DoD) and more specifically, US Cyber Command

---

[5] A definition of Cybersecurity is included in Appendix A.

[6] Louis Lucero II, "The FBI is making an urgent request: Reboot your Internet routers to thwart Russian malware," *The New York Times*, 28 May 2018.

(USCYBERCOM). From its inception as a sub-unified command under the US Strategic Command (USSTRATCOM) in 2009, USCBYERCOM grew in scope and importance prior to being elevated as a full Unified Combatant Command in early May, 2018.[7] It has overall responsibility for Cyberspace defence and it activities are driven by a higher order US DoD Cyber Strategy that reinforces the importance of Cyberspace defence as a key part of the DoD's mandate of defending the US territory and its associated interests.[8]

China too has demonstrated the importance that military Cyberspace activities have in its defence framework. In 2014, after a legacy of categorically denying that the Chinese military was involved in offensive Cyberspace activities, it was revealed through the release of the People's Liberation Army's (PLA's) Academy of Military Sciences (AMS) Science of Military Strategy (SMS) document that the Chinese military has a three-tier Cyberattack capability consisting of:[9]

- Specialized military network warfare forces
- PLA-authorized forces
- Non-governmental forces

The importance of these two examples is not limited to the fact that these significant capabilities exist and that they are positioned as a key part of their respective military capabilities. Equally significant is that their existence has been made known with an expectation that any attacks will be defended against with a more implied message that retaliatory or pre-emptive strikes could and may also be effected.

---

[7] Warren Strobel, "Pentagon's Cyber Command get upgraded status, new leader." *Reuters* (4 May 2018) last accessed 28 May 2018. https://www.reuters.com/article/us-usa-defense-cyber/pentagons-cyber-command-gets-upgraded-status-new-leader-idUSKBN1I52MS

[8] United States. Department of Defense. *The DoD Cyber Strategy*. (Washington, DC: U.S. Government Printing Office, April, 2015), 2.

[9] Joe McReynolds. "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy." *China Brief* Vol. XV, no. 48 (April 17, 2015): 4.

Notwithstanding the strong commitment to building military Cyber capabilities and the clear threat profile that exists, clouding the issue is the fact that there have been few publicly known instances of events that can be regarded as being within a nexus of what could be considered as acts of war. Those that are typically held up as examples include; the disabling of the Syrian air defense system prior to an attack on a nuclear reactor site in 2007, the Distributed Denial of Service (DDoS) attacks on Estonian websites in 2007 and in Georgia in 2008 and the Stuxnet worm attack on Iranian nuclear facilities in 2009.[10]

The amorphous nature of the Cyber domain, its rapid evolution and a dearth of baseline war-centric events has meant that it is difficult to discern exactly where defence and security against non-act-of-war-related threats and attacks ends and those related to Cyberwar begin. Adding to this ambiguity is the fact that Cyberwar has no defined term in law or legal convention.[11] This lack of clarity extends through to the military realm as well, with a key example being that the terms Cyberwar or Cyberwarfare are notably absent from even the US military lexicon.[12]

Regardless of the semantic paradox and notwithstanding the lack of nationally or universally agreed upon definitions of Cyberwar, attempts have been made to ring-fence the concept to bring some measure of clarity to the discussion. Included in Appendix A are three examples of definitions of Cyberwar that are illustrative of the multiplicity of them that do exist. These three definitions approach the topic differently with obvious discrepancies including the

---

[10] Jeppe Teglskov Jacobsen, "Clausewitz and the Utility of Cyberattacks in War." *International Journal of Cyber Warfare and Terrorism.* Vol. 4, No. 4 (Oct-Dec 2014): 1.

[11] Lisa Brownlee, "Why 'Cyberwar' Is So Hard To Define," Forbes, 16 July 2015, last accessed 26 May 2018, https://forbes.com/sites/lisabrownlee/2015/07/16/why-cyberwar-is-so-hard-to-define/#68f75fd631f1

[12] The terms "Cyberwar" and "Cyberwarfare" do not occur in US DoD documentation relating to Cyberspace, including; The DOD Cyber Strategy, Joint Publication 3-12 (R) Cyberspace Operations and Joint Publication 1-01 Dictionary of Military and Associated Terms 8 November8 2010 (As Amended Through 15 February 2016)

variation of the terms used to describe the phenomenon; Cyber warfare, Cyber Warfare Operations and Information Warfare. However, on closer examination key similarities are also evident in that each of them:

1. References attacks or hostile acts intended to cause a definitive negative outcome, or harm to adversaries, their systems and information.
2. Postulates scenarios where Cyber capabilities are used against cyber capabilities
3. Articulates that action(s) are a result of a conflict between adversaries
4. Contains a politically motivated aim
5. Has conflict occurring between nations or states

These practical definitions (the Practical Definitions) and their associated characteristics provide a basis for analysis of Cyberwar with respect to the key principles of war as postulated by Clausewitz. To provide context to this, the analysis will follow the methodology that is used by two different authors. Thomas Rid and Jeppe Teglskov Jacobsen analyse Cyberwar and Cyberattacks in terms of the principles articulated in *On War* by comparing them to the Cyberwar events noted earlier herein. The two authors have differing views but both postulate that to be considered an act of war three key criteria must be met; political nature, instrumental character and violent character.[13]

The first criterion is espoused in Clausewitz's oft-quoted phrase "war is merely the continuation of policy by other means."[14] In this, war emerges as a result of political motivation and intent to act, taking on different forms as political requirements dictate.[15] This political motivation, or will, to act is what enables war as being the means to do so. However, in order for

[13] Thomas Rid.7-8 and Jeppe Teglskov Jacobsen. 5 - Jacobsen defines them as "Clausewitzian political, tactical and physical nature of war."

[14] Clausewitz, Carl von. On War. Translated by Michael Howard and Peter Paret, edited by Michael Howard and Peter Paret. (Princeton: Princeton University Press, 1976). 87.

[15] Antulio J. Echevarria II, *Clausewitz and Contemporary War.* (Oxford: Oxford University Press, 2007). 69.

the political objective to be achieved, this also needs to communicated to, and understood by, an adversary to ensure cognizance as to whether the consequences of having the means applied against them are more palatable than acquiescing.

This sentiment is reflected in the Practical Definitions by their reference to Cyberwar activities as being politically motivated actions between nations or states. However, in the first two definitions there is no articulation of communication between adversaries as to intent and will. It is in the third definition where the use of the word confrontation indicates that the adversaries will be known to each other, thus satisfying Clausewitz's first criterion.

In Rid's analysis of this criterion against past Cyberattacks, the fundamental gap is associated with attribution. He makes particular note of the DDoS attacks in Estonia (2007) and Georgia (2008) for which Russian involvement was likely and there was extant political motivation for the attacks. However, with no admission of responsibility and no definitive proof as to the perpetrators of the attacks[16] his assessment is that the tenets of the first criterion were not met.

However, as Jacobsen argues, conclusive attribution is not necessarily a limiting factor. The key instead is consideration of Clausewitz's idea that war is a series of reciprocal actions between two adversaries. So, when there is a power imbalance and lack of ability to retaliate without significant downside risks, the weaker adversary may acquiesce. In fact, as circumstances have shown in other instances, such as with the invasions Iraq and Afghanistan, the requirement for conclusive attribution is not a required condition.[17] Under this scenario if the roles were reversed and Russia was the aggrieved party with the same level of indication that

[16] Thomas Rid. 14.
[17] Jeppe Teglskov Jacobsen. 8.

Estonia or Georgia had propagated the attacks, the likelihood of a retaliatory strike would be extremely high.

The second criterion relates to the means required to achieve the ultimate end of compelling the enemy to accede to the aggressor's will, "…physical force … is thus the means of war; to impose our will on the enemy is its object."[18] The combination of both the means and the end are the figurative book-ends that make an act of war instrumental in nature.

It is only the second of the Practical Definitions that reflects both the means (network-based capabilities) and the ends (disrupt, degrade…) in a manner consistent with the tenets of this criterion. The other two definitions do have mention of ends but lack the key enabler of means in order to complete the continuum associated with the instrumental character of war.

Rid's approach for this criterion is to illustrate several scenarios where the ends could potentially be achieved through the use of various means of Cyberattack under specific conditions. He does, however, illustrate that notwithstanding the possibility of the Cyberattack means being causal for the political end, the probability of it occurring is very low.[19]

Although Jacobsen's descriptors differ for this criterion, the intent is the same in that the "tactical aims" (means) are the key requirement to achieve the "political objective" (ends). In his treatise he illustrates that the different Cyberattacks have varied levels of alignment between means and ends. In the Estonian example the Russians were using the available means in aid of a realistic end while in the Israeli example the disabling the air defence radar system was not

[18] Clausewitz, Carl von. *On War.* 75.
[19] Thomas Rid. 10.

causal in assisting them to reach their political end of the destruction of the Syrian nuclear facility.[20]

The last of the three criteria is drawn from the beginning of *On War*, where it is defined that, "war is an act of violence meant to force the enemy to do our will"[21] Key to this is to be reminded that violence is "the use of physical force so as to injure, abuse, damage, or destroy."[22] In the Cyber realm, the use of physical force in an attack is a component that is notably absent or minimized. Although physical outcomes from a Cyberattack are possible, they are rare. In Cyberwar, the destructive measure is in the form of non-physical information theft, controlling computers or networks and / or denying users the ability to access websites or networks.[23]

For the Practical Definitions, the fulfillment of will is implied through the description of conduct or participation in conflict by one nation or state attacking another nation or state. However, with the lack of application of physical force extant in Cyberattacks a discrepancy exists. The Practical Definitions do refer to destructive or disabling attacks but in two of the three of them the effects are non-physical, where it is only information and websites that are "destroyed." It is only the in the second definition where physical destruction, in this case "computers and networks themselves," is described.

Rid's analysis is consistent with the stated definition of violence and the need for it to be aligned with Clausewitz's precepts. His very literal view is that the measure of the violence of

---

[20] Jeppe Teglskov Jacobsen. 6.

[21] Clausewitz, Carl von. *On War.* 90.

[22] Miriam-Webster. "Violence" last accessed 28 May 2018: https://www.merriam-webster.com/dictionary/violence

[23] rapid7. "Common Types of Cybersecurity Attacks," last accessed 28 May 2018: https://www.rapid7.com/fundamentals/types-of-attacks/

war is in the explicit loss of life, injury or physical damage, all of which have not yet been demonstrated as a result of Cyberattacks.[24]

The review by Jacobsen is consistent with Rid's analysis. He amplifies that conflict without physical threats or at least attempted physical destruction is out of alignment with Clausewitz. As an example, in the case of the Estonian DDoS attack, the lack of any physical destruction ultimately negated potential NATO Article 5 invocation.

The one event that both authors congruent on in terms of the application of physical destruction that could meet was Stuxnet. In this, the ability of the Cyberattack to have effected damage to equipment in the nuclear facility does demonstrate support to the notion that it meets this third criterion.

Conclusion

The phenomenon of Cyberwar resides at an interesting juncture. When assessed against a purely theoretical lens, it becomes apparent that there is no clear definition as to what it is and where the dividing line between the "war" and "non-war" exists. This ambiguity becomes particularly important for states that have a requirement to defend against attacks from adversaries in the first part and retaliate appropriately.

In the analysis, the fundamental disconnect of a Cyberwar construct is that it currently fails to demonstrate the capacity to *consistently* provide the required physical effect necessary to be able meet the overall aim of war from the Clausewitzian perspective, namely to impose a

[24] Thomas Rid. 11.

proponents will on an adversary. Without this ability, Cyberwarfare as a domain is then inexorably linked to other domains to be able to provide the necessary effect to do so.

The Cyber domain is connected by way of physical and network infrastructure with the other four domains which effectively makes it an extension of them. In this, although under the current construct Cyberwar does not generally fulfill the requirements of the definition of war as Clausewitz had intended, it is not to say that it can't today or won't tomorrow.

Regardless as to whether Cyberwar exists in a comprehensive and explicit sense today, the threat that Cyberattacks pose to states and their interests does not diminish the requirement to defend against them. As illustrated, countries like the US and China regard military Cyber capabilities as being critical to defend against attack and provide a capacity to retaliate or give the capability to execute a pre-emptive strike as and when required.

As the Practical Definitions illustrated and Jacobsen and Rid validated, notwithstanding individual shortcomings in particular instances, the ability for Cyberattacks to fulfill the definition of an act-of-war is possible. This is particularly salient when considering Cyberattacks and war's violent character, that they *can* provide effect in the physical realm. As technology and its application evolve these scenarios will not only become more prevalent, they will become ubiquitous. When that occurs the ghost of Clausewitz will nod knowingly as he sees his original thesis come to life in a medium that he could never have imagined would even exist.

Appendix 1 – Definitions

Cyberspace definitions

> Cybersecurity — Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (DODI 8500.01)[25]

> Cyberspace — A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12)[26]

> Cyberspace operations — The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. (JP 3-0)[27]

Definitions of Cyberwar

> Cyber warfare is internet-based conflict involving politically motivated attacks on information and information systems. These types of attacks can disable official websites and networks, disable services and steal or change classified data. Cyber warfare occurs between nations and most commonly targets corporations and government institutions.[28]

---

[25] Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms 8 November8 2010 (As Amended Through 15 February 2016***)**, JP 1-01, (Washington, D.C.: Joint Chiefs of Staff, 2016), 57.

[26] Ibid. 58.

[27] Ibid. 58.

[28] Upper Midwest Security Alliance (UMSA), "What is cyber warfare?" (blog), 21 February 2017, https://umsa-security.org/what-is-cyber-warfare/

Cyber Warfare Operations - the use of network-based capabilities of one state to disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves, of another state.[29]

From the Shanghai Cooperation Organization that defines - "information war" in part as a "confrontation between two or more states in the information space aimed at… undermining political, economic, and social systems [or] mass psychologic [sic] brainwashing to destabilize society and state."[30]

[29] Major Arie Shaap, "Cyber Warfare Operations: Development and Use Under International Law," *The Air Force Law Review, Cyberlaw Edition* 64 (2009): 127.

[30] Tom Gjelten, "Shadow wars: Debating Cyber Disarmament" *World Affairs*, 173(4) (November-December 2010): 36.

Bibliography

Brownlee, Lisa, "Why 'Cyberwar' Is So Hard To Define," Forbes, 16 July 2015, last accessed 26 May 2018, https://forbes.com/sites/lisabrownlee/2015/07/16/why-cyberwar-is-so-hard-to-define/#68f75fd631f1

Clausewitz, Carl von. On War. Translated by Michael Howard and Peter Paret, edited by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1976.

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

Gjelten, Tom, "Shadow wars: Debating Cyber Disarmament" *World Affairs*, 173(4) (November-December 2010): 33–42.

Jacobsen, Jeppe Teglskov. "Clausewitz and the Utility of Cyberattacks in War." In *International Journal of Cyber Warfare and Terrorism.* Vol. 4, No. 4 (Oct-Dec 2014): 1-16.

McReynolds, Joe. "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy." *China Brief* Vol. XV, no. 48 (April 17, 2015): 3-6.

Miriam-Webster. "Violence." Last accessed 28 May 2018: https://www.merriam-webster.com/dictionary/violence

rapid7. "Common Types of Cybersecurity Attacks." Last accessed 28 May 2018: https://www.rapid7.com/fundamentals/types-of-attacks/

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

Shaap, Major Arie, "Cyber Warfare Operations: Development and Use Under International Law," *The Air Force Law Review, Cyberlaw Edition* 64 (2009): 121-174.

Strobel, Warren, "Pentagon's Cyber Command get upgraded status, new leader." *Reuters* (4 May 2018) last accessed 28 May 2018. https://www.reuters.com/article/us-usa-defense-cyber/pentagons-cyber-command-gets-upgraded-status-new-leader-idUSKBN1I52MS

United States. Department of Defense. *The DoD Cyber Strategy*. Washington, DC: U.S. Government Printing Office, April, 2015.

United States. Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12(R). Washington, D.C.: Joint Chiefs of Staff, 2013.

United States. Joint Chiefs of Staff. *Dictionary of Military and Associated Terms 8 November8 2010 (As Amended Through 15 February 2016),* JP 1-01. Washington, D.C.: Joint Chiefs of Staff, 2016.