National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CYBER WARFARE, THE LAW OF ARMED CONFLICT, ROE AND THE SUFFICIENCY OF INTERNATIONAL LAW

LCdr D.M. MacInnis

JCSP 40

Exercise *Solo Flight*

Disclaimer

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

PCEMI 40

Exercice *Solo Flight*

Avertissement

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

Canada

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

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

CYBER WARFARE, THE LAW OF ARMED CONFLICT, ROE AND THE SUFFICIENCY OF INTERNATIONAL LAW

LCdr D.M. MacInnis

Word Count: 3085

Compte de mots: 3085

Introduction

In 2007, Estonia suffered a series of denial of service (DoS) attacks during a period of heightened tensions with Russia.[1] Similar tactics were used during Russia's involvement in the Abkhazia and South Ossetia crises of 2008 which saw one of the first uses of cyber attack in support of military operations against Georgia.[2] Finally, it is suspected that the United States used computer network attacks (CNA) against Iran in 2010 to disable elements of Iran's nuclear development program, which was followed by cyber "preparation" of the battle space in advance of the bombing campaign over Libya in 2011.[3] Cyber Warfare had clearly moved from the realm of the theoretical when it was first conceived in the late 1990's, to the domain of the operational.

Despite the evolution of an "operationalized" or militarized internet, it has been argued by some legal scholars that the legal regime that governs cyberspace has not kept pace. The commander of US Cyber Command told Congress in 2010 that there was a mismatch between the ability to conduct cyber operations and the laws that should govern such activity.[4] In 2011, Jeffery Addicott, an authority on cyber-law, asserted that international laws associated with use of force and cyber warfare were woefully inadequate.[5] And as recently as 2012, Oona Hathaway of the Yale Law School opined that a new legal framework, both international and domestic, was required to deal with aggressive and illegal action in cyberspace.[6]

It is my contention that these critics are overstating their case. Hathaway's analysis centres on the phenomenon of "cyber attack" across a spectrum of activities, ranging from criminal, hacktivist and

[1] William Boothby, *The Law of Targeting*, (Oxford: Oxford University Press, 2012) at 378.
[2] *Ibid* at 379.
[3] *Ibid.*
[4] Charles Dunlap Jr., "Perspectives for Cyber Strategists on Law for Cyberwar", (2011) Spring, Strategic Studies Quarterly, 81 at 81.
[5] *Ibid*.
[6] Oona A. Hathaway et al, "The Law of Cyber Attack" (2012) 100 no. 4 Cal L Rev 817 at 817

up to and including conflicts between states. In short, she was concerned about the lack of a comprehensive legal regime that encompassed all areas of national security.[7] While an all-encompassing cyber treaty regime may be desirable, from a military perspective it is not necessary. The scope of Hathaway's argument tends to exaggerate the challenges facing operational commanders and practioners in the field of International Humanitarian Law (IHL) / the Law of Armed Conflict (LOAC). Like Charles Dunlap Jr.[8] and Michael Schmitt,[9] I believe that existing international legal structures are sufficient to govern the use of force in cyberspace.

This paper will look at the formulation of rules of engagement (ROE) for cyber operations from both a general and Canadian context. The aim is to show that existing control mechanisms for the use of force can be adapted without creating an entirely new body of international law. It will not be so broad as to provide a definitive list of all possible cyber ROE but it will serve as a "think piece" to chart a way ahead for future research. With the publication of NATO's *Tallinn Manual on the International Law Applicable to Cyber Warfare* in 2013,[10] a legal basis for the use of cyberspace to support or even form the vanguard of military operations was established. The next step is to find a means of operationalizing it. To this end, I will look at the requirement for cyber ROE and some of the major legal issues engaged. This discussion will be followed by an examination of a sample of NATO ROE as an example of how existing control mechanisms can be adapted to meet the legal constraints of cyberspace. In doing so, it will become readily apparent that LOAC applies equally to cyber and kinetic operations.

---

[7] *Ibid*. at 826-828.
[8] Dunlap 81.
[9] Michael Schmitt, "International Law in Cyberspace: the Koh Speech and Tallinn Manual Juxtaposed", (2012) 54 Harv Int'l LJ 13 at 15.
[10] Michael Schmitt general ed, *Tallin Manual on the International Law Applicable to Cyber Warfare*, (Cambridge: Cambridge University Press, 2013)

The Necessity for "Cyber" ROE

Given that there are a range of activities in which a state may participate in during times of peace and conflict, it comes as no surprise that in some instances, the military may employ cyber methods to support its operations. Furthermore, the Government may call on the military to engage in cyber activities in order to further national interests or achieve policy goals.[11] As will be seen below, there are some cyber activities that constitute use of force. When cyber use of force reaches the level of lethality or destructiveness of traditional kinetic weaponry, regardless if during conflict or in self-defence, then the law of armed conflict becomes engaged. Only military personnel enjoy the protection of "combatant privilege, which means in some instances, cyber operations must be conducted by *cybernauts* in uniform. [12]

Rules of engagement exist in order to achieve two things. First, they are designed to ensure that use of force complies not only with LOAC but all applicable laws relative to the operational context.[13] In some circumstances this may even mean domestic laws.[14] Second, they are a means of controlling the use of force.[15] Furthermore under Canadian doctrine, there is an absolute requirement for the control of the use of force.[16] Therefore, the requirement for "cyber" ROE stems from the need for lawful use of force and the requirement that the use of cyber instruments when employed by members of the CAF, be controlled.

---

[11] Chris Masden, "Use of Force" in *Military Law and Operations* (Ontario: Canadian Law Book, 2008) 7-1 at 710; Department of National Defence, *CFJP-5.1 Use of Force for CF Operations* (Ottawa: Strategic Joint Staff, 2008) at 2-5.
[12] Dunlap 91.
[13] Boothby 481.
[14] Clearly this applies within Canada. Domestic law governs domestic operations but the *NDA* s 273 also allows for the extraterritorial application of domestic laws like the *Criminal Code* to CAF members when they are operating abroad.
[15] Masden, at 7-3; *Use of Force Manual* at 2-4.
[16] *Use of Force Manual* at 1-1; *The Law of Armed Conflict – An Operational Approach*, Geoffrey Corn et al eds, (New York: Wolters Luwer Law & Business, 2012) at 128.

The Relevance of the Tallinn Manual

Throughout this paper, regular reference will be made to the *Tallinn Manual*. It is a seminal document in that it is the first serious attempt to show how various aspects of cyber operations and cyber warfare can be analyzed under the lens of LOAC. Furthermore, it represents a consensus view by legal scholars and military lawyers from within the Atlantic Alliance on cyber use of force issues.[17] Although not binding, it is at least the beginning of a journey to explore how the extant norms of international law will apply in cyberspace.[18] Simply put, it connects the dots and acts a lens for assessing actions in cyberspace permissible under international law. This in turn can be used to formulate ROE.[19]

LOAC Issues that engage ROE

The legal issues that ROE embrace centre around two main themes: *what* and *when*. The *what* deals largely with matters of definition of what constitutes certain cyber activities. The *when* deals with the three instances where cyber operations are governed by law: domestic operations, *jus ad bellum* (the law before hostilities which largely deals with issues of self-defence); and *jus in bello* (the laws of war).[20] Domestic operations and criminal law will not be discussed here as the primary focus of the paper is on LOAC issues.

Our point of departure for the definition discussion is *what constitutes cyber use of force*? The governing law on this question is the UN *Charter,* Article 2(4) which prohibits the use of force between states. This prohibition clearly extends to cyber operations but when does the operation cross the

[17] Canada was represented by Capt (N) Genvieve Bernatchez.
[18] Schmitt at 37.
[19] Boothby at 841 (And as previously noted, ROE must conform to international law.)
[20] Masden at 7-8.

threshold to use of force?[21] Key to making a determination is to look at the physical effects of the activity. According to *Tallinn*:

> a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force…[a]cts that injure or kill persons, or damage or destroy *objects* are unambiguously uses for force.[22]

Clearly events cyber incidents that result in a nuclear plant meltdown or the disabling of an air-traffic control system could be classified as cyber uses of force.[23] However, there are instances when cyber events may not have a kinetic parallel. An example would be the introduction of a virus into a stock exchange which resulted in financial chaos that ruined a state's economy. Such non-kinetic events can be assessed on a case-by-case basis using eight criteria as agreed upon by the group of international experts at Tallinn. Of these, the most important was severity of the result closely followed by temporal proximity.[24]

Jus ad Bellum

The second definition engages *jus ad bellum* by determining what constitutes an *armed attack*. Under the UN *Charter* article 51, a state can only act in self-defence if its sovereignty is violated by an armed attack. Again, scale and effects matter: while all armed attacks are uses of force, not all uses of force can be equated to armed attacks.[25] The "serious injury" test discussed above was once again seen as the threshold combined with severity of the result both kinetic and non-kinetic. Furthermore, probing could be viewed as an armed attack if the cumulative effect crosses the use of force threshold, is directed against the same object, and is conducted by the same individual or entity. [26] It should be

[21] Schmitt at 18.
[22] *Tallinn Manual* at Rule 11. (An *object* can be military or civilian in nature and represents both infrastructure and persons)
[23] Schmitt at 19.
[24] *Tallinn Manual* at R 11.
[25] Schmitt at 22.
[26] *Ibid* at 23.

noted that an armed attack may also be assumed if a state provides the means of conducting a cyber attack (i.e. malware or hardware).[27] However, other material support would not qualify.

Another *jus ad bellum* issue is *anticipatory self-defence.* States need not wait to take the first hit. The right to use force in self-defence (cyber or kinetic) exists if a cyber *armed attack* is imminent.[28] The ultimate test for when anticipatory self-defensive action can be taken is "when a failure to act results in a state being unable to defend itself".[29] *Preventative* self-defence remains proscribed even in the cyber world. If a prospective adversary has the capability to conduct a cyber attack, but has not demonstrated intent, cyber defensive action is not permitted.

A final consideration with respect to *jus ad bellum* is whether *non-state* actors can be considered capable of launching a *cyber* armed attack as a matter of law.[30] The short answer is yes and largely stems from the collective response to 9-11. From a practical perspective, the ability to act in self-defence against non-state actors is vitally important since in contemporary conflict these groups regularly attempt to conduct cyber attacks. The consensus was that if an act was attached to an organized group, generated the consequences associated with the requisite scale and effects of armed cyber attack, and directed against a state, then action in self-defence could be used.[31]

Jus in Bello

Once actual hostilities have begun,[32] the word *attack* does not have such a loaded meaning. "Attacks" merely refer to "acts of violence against an adversary whether in offence or defence."[33] From a cyber perspective, an attack occurs when there are violent kinetic effects that result in physical

[27] Dunlap at 86.
[28] *Tallinn Manual* Rule 15.
[29] *Ibid.*
[30] Schmitt at 24.
[31] *Ibid*.
[32] The word hostilities or conflict is used because since 1945 with the advent of the UN system, War is technically illegal.
[33] Geneva Conventions, Additional Protocol I (AP I), article 49 (1) as cited in Boothby at 384.

damage. However, effects that hamper the usage of network and computers can also be considered a cyber attack. The *Tallinn Manual* requires to factors in this regard. First, the functionality of the affected system must be impaired or ceased. Second, restoration of functionality must entail some form of physical repair.[34] The implication of this interpretation of LOAC is significant. It allows attacks against civilian IT systems and networks so long as the functionality is not affected. Therefore, Denial of Service (DoS) attacks would be valid in a conflict as a harassing measure. A proportionality analysis would not be included in a proportionality of such attacks. It also envisages that certain cyber activities are lawful. For example, cyber espionage and surveillance activities could be considered permissible.[35]

A key concept for *jus in bello* is ***Necessity***. It permits the lawful use of force to bring the enemy to submission or to achieve a valid military objective.[36] A military object is a valid object for attack because it offers some form of military advantage if it is destroyed or neutralized. Therefore, dual use infrastructure such as networks could be attacked if they have a military nexus, so long as collateral damage to civilian objects is reasonable.

This is where the concept of ***Proportionality*** is engaged. The *Tallinn Manual* gave an explicit definition of "Cyber proportionality": a cyber attack that causes incidental loss of civilian life, injury or damage to civilian objects that is excessive in relation to the military advantage engaged, is prohibited under LOAC.[37] There are two implications for cyber operations resulting from this definition. First, attacks that create inconvenience or stress would not be considered disproportional and active cyber harassment campaign is a valid tactic. Second, loss of data would not be considered disproportionate

[34] *Tallinn* at Rule 30.
[35] Corn at 221. It should be noted that if such activity took place within the boundaries of the target country, the protections of the Geneva conventions would no longer apply to a military member engaged in such activities.
[36] *Ibid.* at 116.
[37] *Tallinn Manual* at Rule 51.

unless it affected the functionality of a computer network or system.[38] This interpretation of LOAC would therefore allow cyber attacks that destroyed militarily vital data such as intelligence or mapping coordinates, so long as the integrity of the network was maintained. The *Tallinn* group of experts as looked at collateral damage. In light of modern interconnectivity and the ubiquitous nature of computer enabled control systems, the potential for unforeseen consequences from a cyber attack looms large. Therefore collateral damage assessments prior to an attack must take into account direct effects and indirect affects.[39]

The LOAC concept of ***distinction*** which requires civilian persons & objects to be distinguished from combatants & military objects, is problematic within cyberspace. Determining who conducted attack and who may own the infrastructure is difficult because of the dual use nature of the internet and the ability of advanced users to mask their identities or to take-over infrastructure in a third country in order to launch an attack.[40] Still civilians can be targeted if it can be proven that they are directly participating in hostilities and civilians that acting a continuous combat function. The implication for the CAF is that civilians that facilitate CAF cyber operations may lose their immunity under LOAC and become valid targets. [41] However, it does provide a legal basis for action against individuals supporting organized terror or insurgent groups who engage in cyber attacks against Canada and her allies.

Although this coverage of some of the key aspects of LOAC was not in-depth, it is nonetheless important. Even a rudimentary exposure to these issues allows for the development of an analytical framework from which we can unpack ROE as they pertain to cyber operations.

---

[38] Boothby at 386.
[39] *Tallinn Manual* at Rule 51.
[40] Hathaway at 855-856.
[41] *Ibid* at 853-854.

NATO ROE

At first it may seem counter-intuitive to focus on NATO ROE as a framework for discussing cyber ROE issues. However, as Boothby noted, the necessity for most ROE systems to be classified prevents us from doing otherwise.[42] Furthermore, the parallels between Canadian national ROE and NATO ROE allow the latter to act as a close proxy for the former.[43] Therefore, NATO ROE allow for the best approximation given the unclassified nature of this discussion. Only a representative sample will be taken as space precludes a detailed examination. Furthermore, there are only a limited number that are directly applicable within the cyber environment. The most appropriate starting point is the ROE that directly engage use of force, seeing how it was an issue of central importance to the discussion above.

33 USE OF FORCE IN DESIGNATED OPERATIONS

The purpose of this ROE is to authorise the use of force under specified circumstances. It is used to prevent interference with mission accomplishment and either designates the amount of force to be used or provides a general permission to use force.[44] During Peace Support Operations (PSOs) and humanitarian ops, the key issue is not use cyber capabilities in such a way so as to raise their use to the level of an armed attack. Even during a period of heightened tensions such as what now exists between Russia and much of the rest of the world, this threshold must not be crossed. Activities should remain limited to: i) cyber espionage; ii) cyber deception; iii) hacking; iv) cyber enabled psyops and v) cyber sabotage the causing inconvenience as opposed to damage.[45] Even during actual conflict, the use of cyber force should be limited. Necessity will limit the number of targets that should be

[42] Boothby at 481.
[43] Masden at 7-11; *Use of Force Manual* at vii. (While the *Manual* is unclassified, the annexes containing the actual ROE are not)
[44] NATO, MC 362-1 *NATO Rules of Engagement* (2003) at A-15.
[45] Boothby at 381.

engaged and difficulties with cyber identification makes the job of distinction difficult. Given the potential for misidentification, unforeseen 2nd and 3rd order effects, not to mention for possible reprisals,[46] cyber use of force should be limited to specific objectives specified within specific constraints in terms of time and space.

42 Attack

The purpose of this ROE is to control attacks to accomplish NATO missions during NATO/NATO led operations.[47] There are 10 listed ROE in this series ranging from a complete prohibition to only minor limits on a commander's ability to decide when to attack. Many of the caveats permitting an attack are premised on actions first taken by the adversary. For instance, 421 and 423 are both predicated on the enemy showing *hostile intent*. But what does this mean in cyber terms? Clearly cyber Indications and Warning intelligence (I & W) derived from both espionage and surveillance, is required to make such an assessment. Possible indicators might be increased internet traffic; the taking offline of critical infrastructure controlled by SCADA computerized control systems;[48] and/or rerouting of "packets" from suspected adversary servers contrary to normal traffic flow. But as noted previously activity is not the deciding factor. Not only must an enemy have the capability, he must also have intent. While this may be ascertained through public pronouncements, more likely it will have to be ascertained via HUMINT and COMMINT, and to mention the capture of adversary email traffic. Further, any anticipated cyber attack must have the potential to cause death, serious injury or damage, and the defending party must has a reasonable apprehension that this will occur.[49]

ROE 422 and 424 deal with the right to attack (in self-defence) when an enemy commits a

[46] Boothby at 389. (AP I allows for this and reprisals can be done by cyber means)
[47] MC 362-1 at A-19.
[48] Boothby at 385. (SCADA – Supervisory Control and Data Acquisition)
[49] *Use of Force Manual* at GL-3.

hostile act. It should be remembered that not all CNA constitute a hostile act. In order to reach this threshold, the attack must either destroy the network or its infrastructure, or significantly reduce it functionality. Finally there is ROE 426 – First in a series, which allows a Commander to attack entities that he assesses may continue subsequent attacks. In a cyber context, this may apply to known hacking facilities within a specific country or individuals known to have supported the organization conducting the first CNA.

36 Information Operations

The purpose of this series is to authorize and control the use of information operations.[50] It is through this group of ROE that an observer can see the most obvious and direct link to cyber operations. 361 & 362 authorize taking control of enemy information distribution systems in order to use them to persuade and influence target audiences. In the internet age, the most readily available means is through clandestine cyber activity. 363 & 364 envisage a direct response to any computers or computer systems that have intruded into NATO computers and networks. Finally, 366 authorizes the conduct of CNA against a designated adversary.

Conclusion

As can be seen by the preceding analysis, Hathaway's apprehensions about the limits of current law to deal effectively with cyber aggression between states are misguided. The both streams of the LOAC regime have the means to control the use of cyber capabilities both outside and during armed conflict. Architectures for control already exist as demonstrated by the discussion on NATO ROE. While there is always room for improvement, the current legal regime is sufficient and it provides a launching point for research and negotiations of cyber treaties in areas beyond the purview of LOAC.

[50] MC 362-1 at A-15.

BIBLIOGRAPHY

I. Statutes

Criminal Code, RSC 1985, c C-46

National Defence Act, RSC 1985 c N-5

II. Government & Official Publications

CFJP-5.1 Use of Force for CF Operations Department of National Defence - Canada (Ottawa: Strategic Joint Staff, 2008)

Tallin Manual on the International Law Applicable to Cyber Warfare, Michael Schmitt general ed (Cambridge: Cambridge University Press, 2013)

III. Secondary Material: Monographs

Boothby, William. *The Law of Targeting*, (Oxford: Oxford University Press, 2012)

Corn, Geoffrey et al eds. *The Law of Armed Conflict – An Operational Approach*, (New York: Wolters Luwer Law & Business, 2012)

IV. Secondary Material: Articles

Dunlap Jr., Charles. "Perspectives for Cyber Strategists on Law for Cyberwar", (2011) Spring, Strategic Studies Quarterly, 81

Hathaway, Oona A. et al, "The Law of Cyber Attack" (2012) 100 no. 4 Cal L Rev 817

Masden, Chris. "Use of Force" in *Military Law and Operations* (Ontario: Canadian Law Book, 2008) 7-1

Schmitt, Michael. "International Law in Cyberspace: the Koh Speech and Tallinn Manual Juxtaposed", (2012) 54 Harv Int'l LJ 13