Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Cyber-attack as inevitable kinetic war

Gary Lilienthal [a,*], Nehaluddin Ahmad [b]

[a] School of Law, UUM COLGIS, Universiti Utara, Malaysia
[b] School of Law, (UNISSA) Sultan Sharif Ali Islamic University, Brunei

Keywords:
Cyber-attack
Kinetic war
Stuxnet
Maneuver warfare
Necessity

ABSTRACT

This paper poses the question as to whether a "cyber-attack" by a state against another state might breach of Article 2(4) of the United Nations Charter. Although this question is not new, and the answers to it are either by no means consistent or far too clear for the uncertainty of a military field, this paper expresses significant concerns that some of the basic military issues may have been overlooked in contextualizing cyber-attack in United Nations Charter jurisprudence. Its methodology is delimited to discussing the nature of cyber-attack, but only on a basis between one sovereign state and another sovereign state. The paper is further delimited by reference to Article 2(4) of the UN Charter, and how that article might be considered breached. Interwoven throughout the paper is a proposition that cyber-attack is intended to be a military action in the nature of maneuver warfare as an instance of Aristotelian ethical deliberation and action, and further, it is always intended to have military consequences. The inference from this is that a cyber-attack is intended to have kinetic effects in the same way as fraud and deception infer physical effects, and therefore, is intended to have effects similar to those of conventional warfare. The paper begins with an examination of kinetic precepts underlying cyber warfare. Then, the paper looks at how attacks on information might represent a kind of warfare. With an abiding concern to include practical military thought, to represent the uncertainty of war, the paper discusses the nature of maneuver warfare, based on Lind's practical military discussion of the term. The next phase of the paper surveys the relevant international law and international law precepts, followed by a brief look at relevant case law. The paper concludes with a suggestion that the information operations inherent in cyber-attacks are essentially and necessarily *a priori* to a kinetic consequence.

1. Introduction

This paper asks whether a "cyber-attack" by one state against another might be a breach of Article 2(4) of the UN Charter. This question is not new, and the answers to it are either by no means consistent or far too clear for the uncertainty of a military field. However, this paper expresses concerns that some of the basic military issues may have been overlooked in contextualizing the law of cyber-attack in United Nations Charter jurisprudence. The effects of a breach of article 2(4) through cyber attacks carry significant risk for public safety,

* *Corresponding author*. School of Law, College of Law, Government and International Studies Universiti Utara Malaysia UUM, 06010 Sintok, Kedah Darul Aman, Malaysia.
E-mail address: gary@uum.edu.my (G. Lilienthal).
http://dx.doi.org/10.1016/j.clsr.2015.03.002

nations' security and the stability of the links among the global international community. This suggests an increased likelihood of national armed response as self help.[1]

Its methodology is delimited to discussing the nature of cyber-attack but only on the basis between one sovereign state and another sovereign state. The paper has a further delimitation by reference to Article 2(4) of the UN Charter, and how that article might be considered breached. Interwoven throughout the paper is a proposition that cyber-attack is intended to be a military action in the nature of maneuver warfare, and further, it is always intended to have military consequences. The inference from this is that cyber-attack is intended to have kinetic effects, or effects due to some kind of physical motion, in the same way as deception infers physical effects and, therefore, is intended to have effects similar to those of conventional warfare.

The paper begins with an examination of kinetic precepts underlying cyber warfare, because international actors designed the laws of war in the context of kinetic technologies.[2] Then, the paper looks at how attacks on information might represent a kind of warfare. With an abiding concern to include practical military thought, to represent the uncertainty of war, the paper discusses the nature of maneuver warfare, based on Lind's practical military discussion of the term. The next phase of the paper is to survey the relevant international law and international law precepts, followed by a brief look at relevant case law. Finally, the paper draws relevant conclusions.

The paper is likely to conclude with a suggestion that the information operations inherent in cyber-attacks are essentially and necessarily *a priori* to a kinetic consequence. The Estonian cyber-attacks of 2007 will illustrate this. In that attack, moving the statue of the Bronzed Russian Soldier could have been construed as a perceived attack on sovereignty, naturally precipitating violence. Also, the chain of argument will infer that even when a cyber-attack does not breach Article 2(4) of the UN Charter, application to the United Nations Security Council for remedial action might produce action. That action would be as if the cyber-attack were indeed a breach.

2. Cyber warfare

Parks and Duggan differed from other scholars in that they regarded cyber-attacks as only likely to be kinetic in nature. They examined the theory of kinetic precepts underlying cyber warfare; the word kinetic meaning the kind of force, including the movement of a weapon, which would have physically damaging effects on an enemy recipient.[3] Referring to the ancient text of Sun Tsu on *The Art of War*,[4] they examined what they said were well-understood ancient military principles. These were objective, mass, surprise, offensive, maneuver, economy of force, unity of command, simplicity and security. They conducted their examination with a view to assessing to what extent, if any, these principles applied to cyber warfare. Arguably, an outcome of this exercise would serve to characterise the extent to which cyber warfare was indeed kinetic warfare.

They suggested the kinetic precept of mass was effectively irrelevant to cyber-warfare, unless in the case of denial of service attacks, simulating kinetic warfare. They argued that the kinetic precept of objective was applicable in cyber-warfare since the precept of objective formed part of all types of warfare. They argued that the kinetic precept of offensive was not very relevant to cyber-warfare, in which stealth and surprise were far more important. They noted that, at the Cyber Strategy Workshop in October of 1999, delegates made analogies between cyber-warfare and submarine warfare, and also, analogies between cyber-warfare and special operations. They observed that both analogies were good.[5]

Thus, a submarine could conduct both overt and covert operations, acting in peacetime as a deterrent by performing surveillance operations and information gathering. In times of war, a submarine could carry out surveillance and information gathering, communication of data, landing of special operations forces, attack of land targets, protection of task forces and merchant shipping. It could deny to an enemy certain areas of the seas. Submarines required no vulnerable logistics chain, nor depended for survivability on any mutual defence from other sources.[6]

In the editors' general introduction to *Special Operations in US Strategy*, they cited Tugwell and Charters' proposed description of special operations.[7] As a legal definition, it is arguably unusable:

> *Small-scale, clandestine, covert or overt operations of an unorthodox or frequently high-risk nature could be undertaken to achieve significant political or military objectives in support of foreign policy. Special operations are characterized by either simplicity or complexity, by subtlety and imagination, by the discriminate use of violence, and by oversight at the highest level. Military and non-military resources, including intelligence assets, may be used in concert.*[8]

Isenberg suggested that special operations were a way to maintain low intensity conflict,[9] not inconsistent with the apparent goal of cyber-attack. Putting these views together, special operations appeared to be small-scale risky ventures, of a subtle nature, and probably meaning highly deceptive,

[1] Report of the Group of Governmental Experts on Developments in the Field of Information & Telecommunications in the Context of International Security, 65th Session, ¶1, UN Doc A/65/201, July 30, 2010.

[2] Michael Gervais, Cyber Attacks and the Laws of War, (2102), 30(2) Berkeley Journal of International Law, 526.

[3] Raymond C. Parks and David P. Duggan, 'Principles of Cyber-warfare', (2001) Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point 122, 122–125.

[4] Sun Tsu, *The Art of War* (Dover, 2002).

[5] Raymond C. Parks and David P. Duggan, 'Principles of Cyber-warfare', (2001) Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point 122, 123.

[6] Dan van der Vat, *The Atlantic Campaign*, Harper & Row, 1988.

[7] F. Barnett, B. Tovar, R. Shultz (eds.), *Special Operations in US Strategy*, National Defence University Press, New York, 1988, at p. 9.

[8] Ibid.

[9] David Isenberg, 'Special Forces: Shock Troops for the New Order', 177 *Middle East Report*, (1992), pp. 24–27, at p. 24.