Journal of Politics and Law; Vol. 9, No. 4; 2016
ISSN 1913-9047 E-ISSN 1913-9055
Published by Canadian Center of Science and Education

International Humanitarian Law: Attack of the Binary Bullet?

Helen Wilson[1] & Patrick van Esch[2]

[1] School of Law, Charles Darwin University, Northern Territory, Australia

[2] Department of Economics and Business, Moravian College, Bethlehem, Pennsylvania, United States

Correspondence: Patrick van Esch, Department of Economics and Business, Moravian College, 1200 Main Street, Bethlehem, PA 18018, United States. E-mail: vesch54@hotmail.com

Received: February 27, 2016 Accepted: March 21, 2016 Online Published: May 29, 2016

doi:10.5539/jpl.v9n4p110 URL: http://dx.doi.org/10.5539/jpl.v9n4p110

Abstract

Cyberspace has emerged as the 5th domain combat zone from which large scale cyber-attacks are launched at an adversary anonymously in milliseconds, by a single stroke on a computer keyboard or mobile device. Such cyber-warfare operations deliberately seek to deceive, degrade, destroy or disrupt computer systems and networks in a battle-space that transcends borders, under the shroud of secrecy to the attacker's identity or source (Herbert, 2012). Unlike past armed conflicts between nations, conventional weaponry, warring combatants and military objectives were readily identifiable features of the conflict. Cyber-warfare, is asymmetric and can be deceptively and expeditiously instigated by States, Non-State actors, organised groups or sole operators targeting computer networks (e.g. Estonian attack in 2007, Stuxnet attack in 2010).

Keywords: international humanitarian law, cyber-attack, jus in Bello, cyber warfare

1. Introduction

1.1 What Constitutes an Attack in Cyber-Warfare?

The UN Charter (Note 1) is mute as to the meaning of such terms as 'use of force', 'threat of force' or 'armed attack', which allows ambiguity to exist until International Humanitarian Law (IHL) is modified to mirror contemporary technological advances. The International Criminal Tribunal for the former Yugoslavia (ICTY) provided a definition of armed conflict as existing whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organised armed groups between such groups within a State (Note 2). While the ICTY's definition allows for characterization of cyber-attacks as being either of an international nature between States, their affiliates or of a non-international nature perpetrated by non-State actors, organised groups or individuals; the ambiguity still remains surrounding at what point the threshold is reached transforming the attack into an armed attack.

Currently, the enormity of the decision rests with individual States to determine when the armed attack threshold has been breached, which illustrates a disturbing flaw in *Lex lata* IHL. Article 49(1) AP I (Note 3) defines 'attack' as an act of violence against the adversary, whether in offence or in defense. It can be argued that cyber-attacks are synonymous with the determination applied by the International Court of Justice regarding nuclear weapons, in that coercive force is analogous regardless of whatever the type of weapon is used (Note 4). Computer network attacks (CNA) using the various methods of infiltration such as viruses, worms, logic bombs and sniffer packets, which are representative of virtual weapons, constitute physical acts of violence that cause damage, death or injury to persons, or the destruction of civilian objects and infrastructure. Therefore, the use of a devise(s), computer instructions or malware codes that are used to cause excessive loss of life and destruction, normally associated with kinetic operations, irrespective of whether such destruction involves physical damage, functional harm, or a combination of both, such acts should be deemed to constitute an attack under an IHL interpretation.

2. Gaps in Lex lata

2.1 When Is IHL Activated?

Lex lata IHL applies whenever a cyber-network attack can be attributed to a specific State that was intended to cause damage, death, destruction or injury (Schmitt, 2012). The principle of attribution in cyber warfare is problematic and whilst there are scientific findings presented which maintain that cyber fingerprints deduced

from ethnic overlays that allow State CNAs to be readily identified (Note 5), cyber experts argue that the current internet architecture and the dynamic governance systems make the attribution of cyber-attacks extremely challenging at best. This is largely due to sophisticated users being able to modify information forging the source addresses in IP packets that are essential to protecting anonymity (Reitch et al. 2010). Cyber operations that manipulated computer networks so as to cause a meltdown in a nuclear reactor, or opening the floodgates of a dam above a densely populated area, possess potentially horrendous consequences in terms of death, destruction and injury and therefore, representative of an armed attack.

In order to overcome a cyber-attack that is not deemed an armed attack and therefore not subject to AP II (Note 6), a consequence based solution for such circumstances is recommended. This would entail implementing a typology of cyber-attacks ranging from low level nuisance type activism and disruptive hacktivist's activities to the more serious cyber-crime, cyber-terrorism and full effect cyber-warfare (Schmitt, 2012). An additional recommendation would be to expand the terminology of AP 1 Article 52(2) (Note 7) to include terms such as cripple, hamper, hinder, inhibit or neutralize which are more readily associated with cyber-attacks, rather than the more kinetic based terminology of 'kill, injure or destroy the target'. This would allow not only a standardized terminology to be inducted into the law of armed conflict (LOAC), which currently adds to the ambiguity and lack of clarity in IHL, but it would provide a clear delineation of civilian, governmental, military and national responsibilities in response to cyber-attacks (Note 7).

2.2 Cyber Warfare's Challenge to the Principle of Distinction

AP I involving armed conflict and its overarching principles of *jus ad bellum* and *jus in Bello*, succinctly details the obligations the parties to the conflict must adhere to without derogation. There must be respect for and protection of the civilian population and civilian objects at all times, and to distinguish between the civilian population and combatants, and between civilian objects and military objectives. Furthermore, combatants must direct their operations only against military objectives, and the foreseeable military advantage must be real and not theoretical (Note 8). Further obligations contained in Article 57(2)(a)(i) require the parties to the conflict to conduct military operations with the necessary degree of constant care to spare the civilian population and civilian objects (Note 9). Precautions must be taken prior to any attack to include, factoring in the feasibility as to determining the nature of the target, the choice of weapons to be employed in the attack and the foreseeable incidental loss of life and injury to civilians and civilian objects (Note 10). Where practicable, an advanced warning should be given to minimize civilian losses (Note 11). Such regulations, while seemingly clear cut and echoing the humanitarian values underpinning LOAC, were devised for conventional theatres of war strategies, and now require contemporary modification to cope with the nuances of cyber-warfare and the inter-connectivity between civilian and military functions and facilities.

2.3 Inter-connectivity between Military and Civilian Infrastructure

The International Committee of the Red Cross (ICRC) has expressed concern that cyber operations could have serious ramifications for civilian infrastructure due to the civilian population's increasingly universal reliance on computer systems (Droege, 2012). Critical civilian infrastructure, such as air traffic systems, banking, dams, hospitals, irrigation systems, nuclear power plants, rail-roads and water treatment plants; all of which have a heavy reliance upon acquisition and distributed control systems, data collection and are therefore vulnerable to a CNA. The increasing inter-connectivity between military and civilian capacities has resulted in a greater reliance of military networks upon civilian commercial computer infrastructure, comprising of undersea fiber optic cables, satellites, routers, or nodes. Civilian shipping, air traffic controls and civilian motor vehicles are increasingly equipped with navigation systems relying on global positioning system (GPS) satellites, co-used by the military. The emergence of symmetric warfare illustrates the increasing difficulty to distinguish between purely military and purely civilian facilities, participants and targets.

The principle of discrimination is of paramount importance in preventing damage to civilians and civilian property during warfare. The principle of discrimination is expressed in AP I Article 51 (4) (Note 12), indicates that indiscriminate attacks which are not directed at a specific military objective, and have the potential to strike civilians or civilian objects without distinction, are prohibited (Note 13). Indiscriminate attacks (e.g. unintended consequences) are more likely to occur with CNAs than with kinetic warfare by virtue of computer codes turning indiscriminate over widespread re-transmission, and the increasing inter-connectivity between military and civilian systems (Schmitt, 2012).

3. Discussion

3.1 The Tallinn Manuals Proposed Solution to the Distinction Enigma

In addressing the problematic area of inter-connectivity of cyber-infrastructure the International Committee of Experts (Note 14) determined that as matters of law, status as a civilian object and a military objective cannot co-exist, therefore the object is either one or the other (Note 15). Thus, any use or future use contributing to military action renders an object a military objective pursuant to Rule 38 (Note 16), taking required precautions in an attack, and the principles of proportionality (Note 17) being a doctrine embedded in Customary International Law (CIL) that is binding on all States. Military Commanders must balance the foreseeable incidental loss of civilian life, injury and damage to civilians and civilian objects or a combination thereof, to the concrete and direct military advantage anticipated (Note 17). Ideally the principle of proportionality is to ensure there is a nexus between means to an end in the conduct of hostilities, requiring that even unintentional harm, or collateral damage, must still be proportionate.

Interestingly, cyber-operations pose both unique challenges and possible perceived benefits (Kelsey, 2008), so arbitrarily designating all dual use facilities as military, poses that a kinetic attack would potentially cause significant unlawful civilian casualties whereas a cyber-code may be injected as a payload to totally destroy, disable or neutralize that specific part of the military network recognized as a legitimate military objective (Note 18). The Stuxnet worm designed to destroy networks that operate electrical grids, oil refineries, pipelines and other utilities, delayed Iran's development of nuclear weaponry, and achieved in a single cyber strike what five years of discussions between States and the UN Security Council had failed to resolve (Tyagi, 2013). The collateral damage associated to the Stuxnet malware virus was estimated to have infected 100,000 inter-connected host networks, and while this is an unintended consequence it must be weighed against the benefits of significantly delaying the nuclear plant's operational capabilities (Tyagi, 2013).

4. Conclusion

The explosion of technological advancements in computer architecture and software applications has seriously questioned the historical tenets underpinning the law of armed conflict. Ideally, the release of the Tallinn Manual 2.0 in 2016 will address in a regulative rather than an interpretative method, similar to Air and Missile Warfare (Harvard Guide to Air and Missile Warfare) and Naval Warfare (San Remo Manual), the issues arising from a non-standardised terminology glossary, the failure to clarify what constitutes an armed attack and how humanitarian norms are to be ensured considering the increasing inter-connectivity between military and civilian infrastructure due to their dual purpose use.

Cyber-weapons have low procurement, operational and maintenance costs compared to conventional weaponry, and present a viable option to the lesser developed States as the 'first choice' weapons. As the threat of a massive CNA increases, so to do the reasons for stringent agreements to be negotiated to thwart the potential peril that hides within an encrypted cyber code. Therefore, a treaty like that adopted to monitor, regulate and prohibit the use of biological, chemical and nuclear weapons should be formulated to address the insidious threat that a major cyber-attack poses to the international community. Interestingly, major States (e.g. China, Russia, USA) are more likely than not to resist any moves to impose restraints on their alleged cyber-operational supremacy that decreases their military advantage over potential combatant States.

References

Droege, C. (2012). Get off my Cloud: Cyber Warfare, International Humanitarian law, and the protection of civilians. *IRRC, 94*(886). http://dx.doi.org/10.1017/s1816383113000246

Herbet, L. (2012). Cyber Conflict and International Humanitarian Law. *IRRC, 94*(886), 515. http://dx.doi.org/10.1017/S1816383112000811

Kelsey, J. T. G. (2008). Hacking Into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare. *Michigan Law Review, 106*, 1431.

Reitch, P. C, Weinstein, S., Wild, C., & Cabanlong, A. (2010). Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents, and the Dilemma of Anonymity. *European Journal of Law and Technology, 1*(2), 1-58.

Schmitt, M. (2002). Wired warfare: Computer network attack and jus in Bello. *IRRC, 84*(846), 375. http://dx.doi.org/10.1017/s1560775500097741

Tyagi, R. K. (2013). *Understanding Cyber Warfare and its Implication for Indian Armed Forces.* New Delhi: Vij Books, India, Ch.11, p. 250.

Notes

Note 1. United Nations Charter of 1945 <http://www.un.org/en/sc/repertoire/principles> accessed 06/02/2016.

Note 2. *The Prosecutor v Tadic, (*Jurisdiction Appeal*)* ICTY-94-1-AR72 (2 October 1995) para 76.

Note 3. First Additional Protocol to the Geneva Conventions of 1977 (AP 1), Article 49(1).

Note 4. ICJ, Legality of the threat or use of Nuclear Weapons Advisory Opinion of 8 July 1996 - General List No. 95 (1995-1998).

Note 5. Emma Lovett, *International law and Cyber Warfare*, Adelaide University MOOC, <https://www.youtube.com/watch?v=Am4gOf-KDG0> accessed 24/01/2016.

Note 6. Second Additional Protocol to the Geneva Conventions of 1977 (AP II), Article 1. (Organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol).

Note 7. First Additional Protocol to the Geneva Conventions of 1977 (AP 1), Article 52(2).

Note 8. First Additional Protocol to the Geneva Conventions of 1977 (AP 1), Article 48.

Note 9. First Additional Protocol to the Geneva Conventions of 1977 (AP 1), Article 57(2)(a)(i).

Note 10. First Additional Protocol to the Geneva Conventions of 1977 (AP 1), Article 57(2)(a)(i).

Note 11. First Additional Protocol to the Geneva Conventions of 1977 (AP 1), Article 57(2)(c).

Note 12. First Additional Protocol to the Geneva Conventions of 1977 (AP 1), Article 51(4).

Note 13. The Iraqi SCUD missile attacks directed at densely populated areas in Israel during the 1991 Gulf War were deemed indiscriminate attacks.

Note 14. NATO Cooperative Cyber Defence Centre of Excellence, <https://ccdcoe.org/>, accessed 06/02/2016.

Note 15. Tallinn Manual, Rule 39(1).

Note 16. First Additional Protocol to the Geneva Conventions of 1977 (AP I), Article 52(1).

Note 17. First Additional Protocol to the Geneva Conventions of 1977 (AP 1), Article 51, para 5b.

Note 18. First Additional Protocol to the Geneva Conventions of 1977 (AP I), Article 52(1).