Cyber Warfare and the Laws of War*

Wing Commander UC Jha, PhD (Retd)@

Introduction

Today, computers control much of our civilian as well as military infrastructure, including communications, power systems, banking and healthcare. The Internet provides nearly universal interconnectivity of computer networks, with no distinction being made between civilian and military uses. It has the capacity to carry data across the countries, continents and oceans of the world. The Internet has expanded rapidly at a global scale and has been the most powerful technological revolution known in the history of mankind. In just 18 months, between December 2010 and June 2012, the number of individuals actively using the Internet increased from an estimated 36 million to more than 2.4 billion. There has also been a phenomenal growth in military reliance on computer systems. This has introduced a "fifth" domain in which wars may be fought, besides the conventional domains of land, sea, air and space. Given the increasing reliance on information systems in general and access to the Internet in particular, critical military and civil infrastructure is growing more and more vulnerable to cyber attacks. Some have even likened the potential of cyber weapons to inflict damage to that of nuclear weapons.

Cyber warfare, unlike nuclear warfare, is not just the province of the industrial nation-state. Terrorist groups, whether state-sponsored or independent, domestic or international, as well as organised crime syndicates and individuals, are equipped with cyber technologies with which they can launch cyber attacks. The potential of cyber capabilities to cause serious harm to an adversary is no longer theoretical. During the Cold War, the Central Intelligence Agency (CIA) allegedly gained unauthorised access to a Soviet computer to install a malicious code, called a logic bomb, which the CIA subsequently used to destroy a Soviet natural gas pipeline in 1982. An expertly conducted cyber attack could destroy a nation's economy and deprive much of its population of basic services, including electricity, water, sanitation, and health. Cyber attacks and cyber warfare undoubtedly present new and difficult legal problems.

Cyber Warfare

Cyber activities can span from cyber crime to cyber espionage to cyber terrorism and all the way to cyber attacks and cyber warfare. The term cyber warfare refers to warfare conducted in cyberspace through cyber means and methods. Warfare is commonly understood as the conduct of military hostilities in situations of armed conflict. Cyber attacks comprise efforts to alter, disrupt or destroy computer systems or networks or the information or programs on them. They may vary in terms of target (military versus civilian, public versus private), effect (minor versus major, direct versus indirect), and duration (temporary versus long-term).

Cyberspace is a global domain consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers. It is the only domain which is entirely man-made. It is created, maintained, owned and operated collectively by public and private stakeholders across the globe and changes constantly in response to technological innovation. It is not subject to geopolitical or natural boundaries, and is readily accessible to governments, non-state organisations, private enterprises and individuals alike.

Cyber Warfare and the Use of Force

The most important source of the body of law, i.e., jus ad bellum, which governs the "use of force" by States in their international relations, is the UN Charter.1 Article 2(4) of the Charter provides that all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations. The "use of force" constitutes an internationally wrongful act entailing the international responsibility of the State, and also allows the victim State to take counter-measures against the perpetrator. The Charter allows for two exceptions to this prohibition; the right to self-defence in case of an armed attack as well as the use of force authorised by the UN Security Council. A state-sponsored cyber operation would qualify as a use of force against another State and may also trigger an international armed conflict. A cyber operation amounting to an armed attack would permit the attacked state to exercise its inherent right to self-defence. However, a cyber operation that merely causes inconvenience or irritation would not qualify as use of force.

Action in Self-defence

A State that is the target of a cyber operation which is equivalent to an armed attack may exercise its inherent right of self-defence. Whether a cyber operation qualifies as an armed attack depends on its scale and effects. It would be immaterial whether the cyber attack is against a military target or civilian objects. It would be considered an attack against the State. However, a cyber attack on any civilian infrastructure cannot be considered an armed attack. Though there are no agreements on what is critical infrastructure, the UN General Assembly (A/RES/58/199 of 23 December 2003) has recognised that "each country will determine its own critical information infrastructure". The UK, the US and Australia include agriculture, food, water, public health, emergency services, government, defence industrial base, information and telecommunication, energy, transportation (aviation, maritime and surface), banking and finance, chemicals and hazardous materials, and postal system among critical infrastructure. However, this is not conclusive; any system related to a State's economic prosperity, public safety and national defence would constitute a critical infrastructure.

The action of a State in self-defence against a cyber attack must meet the requirements of necessity, proportionality and immediacy. This means the use of force is the last resort, only if the matter cannot be settled by peaceful means. Further, there is an obligation to identify the author and verify that the cyber attack was not accidental. The same rules apply to cyber capabilities as to traditional kinetic weapons. A State could also resort to

anticipatory self-defence against an imminent attack through conventional means.

Cyber Attack: Legal Obligations

The 1977 Additional Protocol I (AP-I) to the Geneva Convention illustrates the principle of distinction to protect civilians during armed conflict. Under this principle, parties to an armed conflict must always distinguish between civilians and civilian objects on the one hand, and combatants and military targets on the other. Under AP-I civilians and civilian objects cannot be targets of attack. The treaty bars belligerents from rendering useless those objects that are indispensable to the survival of the civilian population, such as foodstuff, agricultural crops, livestock, drinking water installations and supplies, and irrigation works. Further, the States must never use weapons that are incapable of distinguishing between civilian and military targets. In the conduct of military operations, belligerents have the duty (i) to exercise constant care to minimise the loss of civilian lives and damage to civilian objects; (ii) to protect the natural environment and protect works and installations containing dangerous forces, such as dams and nuclear power plants; and (iii) not to undertake attacks that have the primary purpose of spreading terror among the civilian population.

In planning a cyber attack, military commanders must comply with the principle of distinction as well as proportionality. There are a few situations where the principle of distinction could be easily applied to cyber attacks, such as when the target is a military air traffic control system and the attack causes a troop transport to crash. If properly executed, the result of the cyber strike would be the same as a conventional bombing. However, often it may be nearly impossible to distinguish between combatants, civilians directly participating in hostilities, civilians engaged in a continuous combat function, and protected civilians in the context of cyber attacks. The obligation of legal review of new weapons, means or methods of warfare are contained in Article 36 of AP-I. These obligations are a part of customary international law2 and applicable to cyber weapons too.

Non-international Armed Conflict

Sophisticated non-State actors can also launch severe cyber attacks against the government, affecting the economy and communication. Non-State actors committing cyber crime and economic cyber espionage do pose serious threats; however, till date there are no reports of highly devastating cyber attacks launched by non-State actors against a State. With technical advancement and the proliferation of malware tools; or with support from a technically advanced State, the possibility of non-State actors carrying out sophisticated cyber operations cannot be dismissed. For instance, hijacking of drones by insurgents in future conflicts cannot be ruled out. Some students in Texas recently managed to take a ship completely off-course (off Italy) by interfering with GPS signals.3

The Status of Cyber Warriors

Cyber warriors could be classified into four major categories; namely, combatants, contractors and civilian employees of the armed forces, levee en masse, and civilians. Cyber operations are generally carried out by highly specialised personnel. To the extent that they are members of the armed forces of a belligerent State, their status, rights and obligations are no different from those of traditional combatants. According to the laws of war, the armed forces of a belligerent State comprise all organised armed forces, groups and units which are under a command responsible to that State for the conduct of its subordinates. This broad and functional concept of armed forces includes essentially all armed actors belonging to a belligerent State and showing a sufficient degree of military organisation.

In the last two decades, belligerent States have increasingly employed private contractors and civilian employees to perform a variety of functions traditionally performed by military personnel. This includes the support, preparation and conduct of cyber operations. As long as such personnel assume functions not amounting to direct participation in hostilities, they remain civilians. In case they are formally embedded in the armed forces in an armed conflict, they would be de facto irregular members of the armed forces and entitled to prisoner of war status in case of capture.

The concept of a levee en masse is that during the initial invasion, the civilian population of unoccupied territory can spontaneously ‘take up arms against the invading army’ in order to forestall an occupation. The mobilisation of a levee en masse is patriotic zeal coupled with the initiative of the citizen-soldier under emergency until the enemy has been defeated or repelled. The law of war recognises the concept and protects those who participate in a war and ‘carry their arms openly’ by granting them combatant status under the Geneva Convention of 1949. While this category of persons has become ever less relevant in traditional warfare, it may well come to be of practical importance in cyber warfare. In cyber warfare, territory is neither invaded nor occupied, which may significantly prolong the period during which a levee en masse can operate. Also, cyber space provides an ideal environment for the instigation and non-hierarchical coordination of spontaneous, collective and unorganised cyber defence action by great numbers of “hacktivists”. The only problem foreseen in this case is that in the context of cyber space, how would the requirement of “carrying their arms openly” be interpreted?

Under the laws of war, civilian means all persons who are neither members of the armed forces of a State or non-State party to an armed conflict, nor participants in a levee en masse. As civilians, they are entitled to protection against the dangers arising from military operations and against attack. In cyber warfare, this category is likely to include most non-State hackers not belonging to the armed forces. If and for such time as their operations amount to direct participation in hostilities, civilians lose their protection and may be directly attacked as if they were combatants. They do not benefit from immunity from prosecution for lawful acts of war and, therefore, can be punished by their captor for any violation of national law.

Tallinn Manual

One of the problems with cyber warfare is the lack of uniformity in concepts, definitions, rules, policy and law. In many instances, not only is uniformity lacking, but there is simply a void. As a result, there is no general international consensus on how to treat cyber warfare. Attempts have been made, however, to create concepts, definitions, rules,

policy and law regarding cyber warfare. The Tallinn Manual on the International Law Applicable to Cyber Warfare has been prepared by experts working with the Cooperative Cyber Defense Center of Excellence (CCDCOE), an institute based in Tallinn, Estonia, that assists NATO with technical and legal issues associated with cyber warfare. The Manual, released in 2013, is particularly concerned with jus in bello (the law of war) and jus ad bellum (the set of rules to be consulted before engaging in war) and does not deal with cyber crime in general or cyber terrorism. It is intended as a reference for legal advisers for government agencies.

The Manual consists of 95 rules reflecting customary international law and has been adopted unanimously by an International Group of Experts. It defines a cyber attack as "a cyber operation, whether offensive or defensive that is reasonably expected to cause injury or death to persons or damage or destruction to objects." The definition makes it clear that a cyber attack is an act of violence either against a person or object and that the focus is on the consequences and not the initiating act itself. Thus, the consequences of a cyber attack must generate some violence to some person or property. Therefore, it is not the act itself, but rather the subsequent consequences thereof that matter. The Manual has been criticised for being "an exercise of academic debate, restating what has been the practice, but failing to address the central issues raised by the emerging technical landscape." Developing international law for cyber warfare is a complex challenge and will take many nations coming to an agreement over a substantial period of years.4 It is not possible to base it on some basic and fundamental concepts, definitions and rules created by some influential countries, especially when it relates to the safety and security of a State.

The Future

Governments as well as industries have established both formal and informal mechanisms for countering rapidly increasing cyber threats and operations. More than 100 militaries in the world have dedicated cyber-attackers and defenders and have built some kind of cyber military units. These include the establishment of the US Cyber Command, China's People's Liberation Army General Staff Department's 3rd Department, Iranian Sun-Army and Cyber Army, Israel's Unit 8200, and the Russian Federal Security Service's 16th Directorate. India may soon have an independent Cyber Command to protect the nation's cyber domain and vital infrastructure.

There are varying opinions on how to tackle the issue of cyber warfare. While few are in favour of an international convention, others have opposed efforts to create a new treaty and have argued that the current laws of war can be applied to cyber warfare by analogy. It is clear, however, that States must develop a cyber warfare doctrine (CWD) to regulate the use of cyber weapons in war. India has been a major target of cyber attacks and the frequency and intensity of such attacks is increasing. There have been numerous incidents of sensitive government and military computers being attacked by unknown entities and information being stolen. India should be prepared for a cyber attack and stand ready to launch a counter-offensive. We must find answers to issues such as what activities must be undertaken in the case of a cyber attack against our nuclear power plants; what would be the appropriate response in the case of such an attack; and the attack threshold that would constitute an act of war. The CWD must be based on our current legal doctrine and precedents.

Conclusion

Compared to the weapons that threatened States in the past, modern technology has made the tools of cyber warfare cheap, readily available and easily obtainable. Legal norms are emerging in cyber warfare, but many questions about what is legal and what is not in this "fifth domain of warfare" need to be answered. The implication of future cyber warfare is uncertain. Cyber weapons, while targeting military objectives, may also attack civilian objects such as railways, air traffic, hospitals, and power plants, causing massive collateral damage and civilian casualties. In addition to the legal regulation of cyber warfare, cyber espionage, theft of intellectual property, and a wide variety of criminal activities in cyberspace pose real and serious threats to all States, as well as the corporate world and private individuals. An adequate response to issues related with cyber crimes requires national and international measures. It is important that States be aware not only of their legal duty to examine whether new weapons and methods employed in cyber warfare would be compatible with their obligations under existing laws of war, but also of their moral responsibility towards generations to come.

Endnotes

1. Jus ad bellum is the Latin term for the law governing the resort to force i.e. when a State may use force within the constraints of the UN Charter framework and traditional legal principles. The modern jus ad bellum has its origins in the 1919 Covenant of the League of Nations and the UN Charter.

2. The customary international law requirement for legal review of a weapon to ensure its use will be lawful in conflict stems from the 1868 St Petersburg Declaration, the 1899 Hague Declaration Concerning Asphyxiating Gases, the 1899 Hague Declaration Concerning Expanding Bullets and the 1907 Hague Convention IV Respecting the Laws and Customs of War on Land. These international instruments address the issue of whether a weapon causes superfluous injury in violation of the laws and customs of warfare. Additionally, in 1996, the International Court of Justice confirmed this customary international law status in its Nuclear Weapons Opinion.

3. Civilian GPS is vulnerable to being spoofed, 14 August 2013. Available at: http://www.technologyreview.com/news/517686/spoofers-use-fake-gps-signals-to-knock-a-yacht-off-course/, accessed 23 January 2014.

4. James E McGhee, Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy, Vol. 2 (1), Journal of Law & Cyber Warfare, Spring 2013, pp. 64-103, at p. 93.

*Edited text of a Talk delivered by Wing Commander UC Jha, PhD (Retd) on 26 Feb 2014 at USI, with Lieutenant

General SP Kochhar, AVSM**, SM, VSM (Retd) in the Chair.

@Wing Commander U C Jha, PhD (Retd) served in the IAF for 24 years and took premature retirement in 2001. He is an independent researcher in the field of environmental law, human rights, international humanitarian law and military law. He has authored a number of books, the latest one being, “Drone Wars : Ethical, Legal and Strategic Aspects”, a USI publication.

Journal of the United Service Institution of India, Vol. CXLIV, No. 595, January-March 2014.