Cyberspace and Information Warfare

Introduction

Cyberspace, along with land, sea, air, and space is now officially recognized as a domain in which war may take place. Sophisticated information and communications technologies (ICTs) are now routinely deployed by military establishments both defensively and offensively. For example, the United States' organization USCYBERCOM "has the mission to direct, synchronize, and coordinate cyber space planning and operations to defend and advance national interests in collaboration with domestic and international partners." (General Paul M. Nakasone, Commanders)[1] The possibility of information warfare being waged either exclusively in cyberspace or in conjunction with other warfare domains raises important questions concerning its just use. In what circumstances may information warfare be justly declared (*jus ad bellum)* and what are the conditions of its just use (*jus in bello)*?

Information Warfare Defined

The term 'information warfare', understood offensively, refers to the use of ICTs to attack an enemy's informational infrastructure to either incapacitate said infrastructure or acquire classified information. Understood defensively, the term refers to the use of ICTs to counter offensive information warfare attacks.

Traditional Warfare versus Information Warfare

There are many differences between traditional warfare and information warfare. Perhaps the most obvious is that information warfare, unlike traditional 'kinetic' warfare does not involve the direct use of physical force against enemy combatants. Cyberattacks need not involve any fatalities nor indeed any permanent damage to the information systems attacked.

This is not to say that cyberattacks might not result in human death or physical damage – think for example what might result if the control systems of nuclear plants were hacked – only that such attacks need not involve the fatalities and deaths of traditional war.

Another important difference is that whereas in traditional warfare the identity of one's attacker is clearly known this is not the case in information warfare. In many instances, it is very difficult and sometimes impossible to know with surety the origin of a cyberattack. This 'attribution problem' applies even in instances where one can know the country of origin of the attack, since the government of that country can often maintain that although the attack originated from within its country it did not authorize the attack.

An additional difference between these two forms of warfare, a difference which further intensifies the attribution problem is that the weapons of information warfare, unlike the weapons of traditional warfare are available to almost everyone. Comparatively few people can gain access to the weapons of traditional warfare, but anyone with a computer and advanced programming knowledge can launch a cyberattack. The weapons of traditional warfare can, with some success, be banned, but this is impossible in the case of computers.

A further difference is that, in contrast to the traditional weapons of war, offensive cyberweapons are largely single use weapons. Once a large-scale cyberattack takes place, opponents are quick to take measures so that identical attacks will not be successful.

There are, however, similarities between traditional war and informational war. In both it is much easier to attack than defend. Effectively defending against cyberattacks is much more difficult and expensive than launching such attacks. This suggests that developing the capacity

to launch offensive cyberattacks needs to be part of a military's defensive strategy in deterring cyberattacks.

A second similarity is that both forms of warfare face the problem that it is difficult to predict with any degree of confidence what distant, destructive, unintended consequences may result from engaging in war. It is true that information warfare avoids the direct physical harms of traditional warfare, but this is no guarantee that information warfare will not result in serious unanticipated distant harms. Despite such possible unanticipated consequences, it appears fair to suggest that information warfare is more like 'cold war' than 'hot war'. An important difference, however, between information warfare and earlier cold wars is that cyberwarfare tends to be multilateral rather than bilateral.

Types of Cyberattacks

It is useful to distinguish between two types of cyberattacks; non-intrusive attacks where the attacker does not gain access to attacked computers' software and data, and intrusive attacks where malware gains access to computers' software and data. The first type of cyberattack takes the form of Denial of Service (DoS) or Distributed Denial of Service (DDoS). In such attacks a site or server becomes paralyzed and unable to function through being overwhelmed by a huge number of requested responses per second. Since these attacks do not actually gain access to hardware or software, they do not damage their targets. In civilian life, such attacks often attempt to extract a ransom from the business or academic institution they target. Once the ransom is paid, the attacks cease, and the institution's system can function normally.

The second type of attack takes the form of computers and networks being infiltrated by malware capable of altering software and data. These ‘viruses’, (programs that attach themselves to another program, file, or email, and which reproduce themselves across computers), and ‘worms’ (freestanding programs that, by travelling through information pathways, exploit vulnerabilities in networks) have a wide application. Among others, their effects include the undetected stealing of classified information, sending misleading communications under a false flag, making software non-functionable, and erasing hard drives.

Information Warfare Targets

Cyberattacks occur on different types of targets. On a communications level they target military chains of command. Such attacks attempt to block information gathering and transmission, generate false reports, or issue wrong commands.

At the level of weapons deployed on a battlefield, cyberattacks target weapons’ information systems. The goal is to cause either temporary or permanent damage that will make the weapons nonfunctional or a liability to their users.

Cyberattacks also target joint use infrastructure, i.e. infrastructure that is used by both the military and civilians. Examples of such joint use infrastructure include oil refineries, global positioning satellites, electricity transmission systems, and water and sewer systems.

Cyberattacks could also, of course, target primarily civilian use infrastructure. This, however, is against international law and what is considered legitimate in war. The previous three types of target are considered lawful to attack in war.

When is Information Warfare Just?

Going to War *(Jus ad bellum)*

On just war theory, the criteria for a war being ethically justified are: 1) there must be a just cause for fighting a war, 2) fighting a war must be a last resort, 3) there must be the likelihood of success, 4) there must be proportionality such that the harms of fighting a war are not outweighed by the harms of not fighting a war, 5) a war must be authorized by proper authority, and 6) a war must be fought with the right intention. These criteria were developed in the context of war understood as necessarily involving bloodshed and physical damage to infrastructure. Given that information warfare does not necessarily involve these features, questions arise concerning the application of just war criteria to information warfare.

The term '*casus belli*' refers to events or actions which justify engaging in war. Traditionally, acts of aggression by one country towards another, such as embargoes or attacks on the targeted country's ships in international waters, have been understood as justifying the targeted country fighting a war against its aggressor. An unprovoked 'soft' cyberattack, i.e. a cyberattack which results in no bloodshed or destruction of physical infrastructure, does not resemble typical instances of *casus belli* and thus raises the question of the proper, i.e. justified response to such attacks. In such instances, the criterion of proportionality needs to be satisfied, such that the response is properly proportional to the effects of the attack. In addition, the traditional understanding of harm needs to be expanded from the traditional categories of bloodshed and destruction of physical infrastructure to include damaging informatic networks. Also, it needs to be clear that the attack was orchestrated, or implicitly or explicitly condoned, by the government of the country in which it originated. Finally, the attack

must have serious consequences in terms of the informational harm it causes; otherwise it cannot be a legitimate reason to engage in war.

The question may be raised of whether a pre-emptive offensive cyberattack could ever be justified under just war theory. At first glance, it may seem clear that the answer is no, since the opponent has not struck first. Two considerations suggest otherwise, however. First, although an enemy has not formally declared war, it may be clear that it intends war, has undertaken active preparation for war and that defeat is likely if one does not strike pre-emptively. As an example, consider the Six Day War of 1967 between Egypt and Israel. Israel was the first to use force and lacking mitigating circumstances would be considered the aggressor and thus unjustified in its actions. There were, however, mitigating circumstances. These included Egypt announcing the closure of the Straits of Tiran to Israeli ships, putting its military forces on maximum alert, expelling the UN Emergency force from the Sinai Peninsula, building up its military along Israel's border, and forming mutual support treaties with Iraq, Jordan, and Syria. Under these circumstances, it seems clear that Israel was justified in striking pre-emptively.

Second, we have noted that information warfare can be waged without bloodshed and damage to physical infrastructure than traditional warfare. This raises the possibility of a pre-emptive cyberattack being justified if it can reasonably be understood to frustrate a country's intended prosecution of a traditional war.

Fighting War (*Jus in Bello)*

In instances where cyberattacks result in serious harm, whether that harm be at the level of bloodshed, physical damage, or compromised informational networks, what conditions

need to be met if the prosecution of war is to be ethically justified? Two key principles apply here as well as in traditional warfare. The first is the principle of discrimination between combatants and noncombatants. This principle requires that noncombatants never be intentionally targeted, that the risks to noncombatants be minimized as much as is possible without compromising legitimate military goals, and that any probable harm to noncombatants must not outweigh expected military benefits. Distinguishing between combatants and noncombatants is often difficult, even in conventional warfare. It becomes even more difficult in information warfare. Could, for instance, a programmer instrumental in developing the programs employed in cyberattacks be legitimately viewed as an enemy combatant? That it is not always easy to distinguish between combatants and noncombatants does not, however, mean that we should not to the best of our ability apply the principle of discrimination.

The second is the principle of proportionality that we have already noted in the requirements of justly going to war. Those engaging in cyberattacks must take into consideration the harm of such attacks such that their harm is proportional to the objective being sought. Given that the harms of information warfare are often less than the harms of traditional warfare it is easier to meet this principle in information warfare than in traditional warfare. It should be emphasized, however, that cyberattacks are not necessarily less harmful than military attacks. For example, compromising the informational system governing a nuclear plant could conceivably cause a nuclear meltdown just as much as bombing the nuclear plant. The principle of proportionality requires careful consideration of the probable effects of cyberattacks, by their users.

Cold Information War

Earlier, we noted that, although informational warfare will play a part in any officially declared war between countries, it, more than conventional domains of war lends itself to use in unofficial 'cold wars.' The potential for unethical behavior in cold wars is large. Such wars are never officially declared and are conducted in secrecy. It is, therefore, much harder for citizens of a country to hold their security agencies and the executive branch of government to account. Although it may be even more difficult to ensure that cold wars are fought ethically than officially declared wars, this difficulty does not extend to knowing the requirements of conducting cold war ethically. The same moral principles apply, it is just more difficult to guarantee that they are observed.

Cold war cyberattacks should not target defensive informational systems. Such attacks should not impose suffering on innocent civilians, and they should not constitute a great enough threat that those targeted would be liable to respond by engaging in traditional kinetic warfare.

Conclusion

Cyberspace has become an important domain in which war is waged. It differs from other domains of war inasmuch as it does not rely on direct applications of physical force. In principle, it allows war to be waged with much less bloodshed and physical damage. Whether or not that will be a practical result of war moving into this new domain remains to be seen. What is clear is that this new domain of war needs to be addressed by careful legal and ethical thinking. International laws need to be put in place and just war theory needs to expand its understanding of harm to include damage to informational systems.

Tallinn Manual

The Tallinn Manual on the International Law Applicable to Cyber Warfare was a three-year project developed by the NATO Cooperative Cyber Defence Centre of Excellence. Located in Tallinn Estonia, the Cooperative is neither a part of NATO (North American Treaty Organization) nor supported by NATO but is part of a broad framework supporting NATO Command arrangements. It is funded by Estonia, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, and the United States.

In 2009, the Cooperative invited a distinguished group of independent international legal scholars whose task was "to produce a non-binding document applying existing law to cyber warfare."[2] The Manual they produced constituted the first comprehensive authoritative examination of the relation of international law to this new form of warfare. Particular attention was paid to complex legal issues involving the *jus ad bellum* and the *jus in bello*.[3] Cyber activities occurring below the level of a 'use of force' as understood in the *jus ad bellum* were not addressed and the legality of cyber intelligence activities were considered only insofar as they involved the *jus ad bellum* understandings of 'use of force' or 'armed attack' or as considered relevant to armed conflict governed by the *jus in bello*. The Manual confines itself to discussing cyber-to-cyber operations, such as the launch of a cyberattack targeting enemy command and control systems and does not consider legal issues concerning kinetic-to-cyber operations such as an aerial attack against a cyber control centre.[4]

A difficulty facing the legal scholars was that there are no treaty provisions that directly deal with cyber warfare.[5] Consequently, it is frequently impossible to appeal to cyber-specific

international laws; the result being that not every assertion in the Manual can be viewed as a statement of international law.[6] The scholars were, however, unanimous in their judgment that both the *jus ad bellum* and the *jus in bello* are applicable.

The Manual set out a series of rules adopted by employing the principle of consensus with the group of legal scholars, with each rule being accompanied by commentary regarding its scope and application. The original Tallinn Manual was published in 2013 by Cambridge University Press. In 2017, an expanded version containing 94 rules (Tallinn Manual 2.0) was published by Cambridge University Press. Although influential and the subject of many scholarly legal publications the Tallinn Manual, both in its original and expanded version, has not been adopted as the official view of NATO or any of the sponsoring nations of the NATO Cooperative Cyber Defence Centre of Excellence.

[1] https://www.cybercom.mil/About/
[2] Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. (New York: Cambridge University Press, 2013) 1.
[3] Ibid. 4
[4] Ibid. 5
[5] Ibid.
[6] Ibid.