The Applicability of the Laws of War to Cyberspace: Exploration and Contention

Xu Longdi

Recent years have seen a profusion of Internet security-related incidents, with the situation becoming increasingly serious. Internationally, there has been an endless succession of calls and proposals to make rules on cyber security in order to tackle online threats. In this discourse the issue of the applicability of existing laws of war to cyberspace has become a focus of the international debate.

Ⅰ. The diverse nature of online activity and the contested existence of cyber warfare

1. The diverse nature of online activity

There is a huge amount of variety among the type and nature of online activities, and also differences among people's understanding of cyber activity, cyber threats and cyber security. For example, some people believe online threats can be divided into four levels: cyber intrusion, organised crime, ideological and political extremism, and cyber invasion originating from countries. Others believe cyber attacks include hacking, distributed denial of service (DDoS), and Trojan malware. Still others believe cyber attacks include cyber terrorism, cyber warfare, cybercrime, and cyber espionage. Among these, although terrorist organisations do have an online presence, true cyber terrorism is still extremely rare, while true cyber warfare is also yet to take place. In contrast, cybercrime and cyber espionage are the most pressing problems. In brief, because of the complex and ever-changing nature of online activity, and the wide range of cyber threats, it is imperative to formulate rules to tackle these threats and safeguard cyber security.

Cyber warfare is the extreme form of online threats and cyber attacks, and is receiving an increasing amount of attention. In fact, since the inception of the Internet, internationally, there has been constant debate about cyber warfare, with different countries contesting the 'dominance' over the net. In the 1991 Gulf War, 1999 Kosovo War and 2003 Iraq War, cyber tools came into their own. In recent years, many countries have taken various measures, unveiled rafts of cyber policy, formulated cyber strategies, set up cyber commands and strengthened the building of cyber forces as if cyber warfare was about to break out at any time.

Some of the cyber attacks that have taken place in recent years seem to have provided further evidence of the arrival of cyber warfare. The 2007 attack on Estonia and the 2010 Stuxnet virus are seen as the newest cases of cyber warfare. The

former was described by the Estonia's Defence Minister as the "unnoticed Third World War". Western cyber warfare specialists also called it the first cyber war in its true sense. The Stuxnet virus did not disable Iran's nuclear facilities, but it did cause approximately 20% of Iran's centrifuges to be scrapped and caused huge delays to Iran's nuclear plans. The appearance of the Stuxnet virus signified the inception of yet another type of cyber weapon and a new phase of cyber warfare.

2. The contested existence of cyber warfare

People have different ways of defining and understanding warfare. Similarly, there are also different understandings of cyber warfare. On the whole, at present there is still no consensus as to the existence of cyber warfare, with opinion generally divided into two camps: one group maintains that cyber warfare exists and, indeed, has already occurred; the other school of thought contends that cyber warfare does not exist and will not occur.

As early as 1993, John Arquilla and David Ronfeldt of the Rand Corporation claimed 'Cyber warfare is coming!' In 2010, US Deputy Secretary of Defense, William Lynn III, wrote "although cyberspace is a man-made domain", in terms of military action, it has become "as important as land, sea and air". The White House's former cyber 'czar', Richard Clarke, believes the threat posed by cyber warfare dwarfs that posed by terrorist attacks such as 9/11 and has called for the adoption of a raft of measures "to begin to prevent the catastrophe of cyber warfare". In February 2011 the then-Director of the CIA, Leon Panetta, also warned "the next Pearl Harbour may well be a cyber attack". Of course, some believe this is a kind of 'cyber paranoia' and an overreaction to cyber attacks.

In contrast to this 'cyber paranoia', Thomas Rid at King's College London believes that although there have been numerous cyber attacks, there has not yet been a cyber war. There has not been one at present and neither is it possible that one will occur in future. This is because one form of aggressive action must satisfy a number of conditions before it constitutes an act of war. According to Carl von Clausewitz's definition, war must be violent, instrumental and political or, that is to say, any act of war must be potentially fatal, instrumental and political. However, among cyber attacks that have already taken place, regardless of the scale, none have satisfied these conditions and thus cannot be said to constitute an act of war. In contrast, all past and present political cyber attacks can be attributed to three relatively complex forms of activity, which are as old as warfare itself: subversion, espionage and sabotage.

Ⅱ. Factors influencing the definition of 'cyber warfare'

Faced with a lack of consensus on the concept of cyber warfare, it is beneficial for an accurate definition and understanding of the issue by clarifying the parameters of the term, including attackers and targets, and objectives and consequences.

1. Attackers and targets

Put simply, attackers can be divided into three levels of actors: individuals, groups and states. These can be configured in six pairs as: individual-individual, individual-group, individual-state, group-group, group-state and state-state. In terms of these configurations, it is only the state-state attacks that can be described as acts of war, whereas it would be very hard to describe attacks among the other five pairs in this way. Of course, if an individual or group is authorised or instructed by a state, this could also constitute an act of war. However, because of the unique nature of cyberspace per se, it is difficult to trace the origins of an attack. Therefore, it is very hard to identify the attacker, and to infer whether cyber warfare does actually exist.

In terms of attackers' targets, these often include: computer operating systems and software and hardware; soft resources and computer information such as personal information, corporate secrets and intellectual property; and critical infrastructures such as banking system, airlines, communications, dams and power stations. These targets may be individual, group or state assets, of different levels and of different value. Therefore, it is very difficult to determine the existence of cyber warfare from just one factor/criterion. This is also a Gordian knot in defining cyber warfare from the perspective of attacker or target.

2. Objectives and consequences of cyber attacks

Just as with the different types of cyber activity, there is a huge variety of objectives of cyber attacks. Some attacks are purely borne out of the attackers' interest and curiosity, or to demonstrate their computer talents and abilities - the majority of early 'hacking' falls into this category. Some attacks are to gather corporate secrets, gain economic advantage or perpetrate online fraud. Some are for sabotage, including: corrupting or deleting information from a target computer, corrupting or paralyzing the target computer's software and operating system or corrupting the computer's hardware or information infrastructure. Of course, some cyber attacks are also intended to launch cyber warfare, in both its limited and unlimited forms.

Related to this, attacks with different objectives will also bring about different consequences, including: loss of personal and commercial information, theft of intellectual property rights, sabotage of computer hard- and software, corruption of computer's operating system, destruction of key information infrastructure or even human casualties. Apart from the latter, i.e. human casualties, all of these other consequences have occurred, but it is very difficult to see them as constituting cyber warfare. Even if attacks result in casualties, these still have to be differentiated according to whether they were caused directly or indirectly. These factors all influence the decision as to whether cyber warfare has already taken place or whether it even exists.

Simply put, when analysing and evaluating the nature of cyber incidents, one must take an overview of the above mentioned factors in a comprehensive manner. One must make an objective analysis of the specific situation, including the originator and victim of the attack, and the objectives, as well as possible consequences. We should not exaggerate or overlook facts, and should avoid oversimplifying cyber warfare by lumping all cyber attacks together under the rubric of 'acts of war'.

Ⅲ. The codification of cyber warfare and the laws of war

1. How to codify cyber conflict and cyber warfare

There are two key approaches in codifying cyber warfare: first is formulating new international laws and regulations, and signing new international treaties, such as the *International Code of Conduct for Information Security* (hereinafter referred to as *the Code*) proposed by China, Russia and other countries. Second is amending the existing norms of international law so as to make them applicable to cyberspace and cyber warfare. This latter approach has been supported by western countries and organizations, such as the US and NATO.

On 12 September 2011, China, Russia, Tajikistan and Uzbekistan jointly submitted a letter to UN Secretary General, Ban Ki-moon, asking him to make *the Code* a formal document to be distributed at the 66th UN General Assembly, and calling upon all member states to discuss the document within the UN framework, in order to reach consensus on international norms on information and cyberspace at the earliest possible date and regulate state behaviour. This was the first time the international community had put forward a fairly comprehensive and systematic document on international regulations for information and cyber security. However, *the Code* was "largely dismissed by the US and its western allies". Recently, the Jimmy Carter administration's senior adviser Amitai Etzioni said, "if you didn't know which countries submitted this draft, it would be very easy to think that 95% of it was

written by the western nations lead by the US". This is a clear indication of the universal significance of *the Code*.

In contrast to this approach, western countries and international organisations such as the US and NATO believe that current international law can be applied to cyberspace and that there is no need for new legislation. At the US Cyber Command Interagency Legal Conference in September 2012, the legal advisor to the US State Department, Harold Hongju Koh formally set out this position. In the same month, after three years of research, NATO also released *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (hereinafter referred to as *the Tallinn Manual*). In the course of drafting, *the Tallinn Manual* collated the opinions of dozens of experts from fields such as international law, international relations and cyber security. Member states also sent representatives to act as observers to related discussions.

The Tallinn Manual put forward 95 rules that could be applied to cyber warfare. These related to issues such as the rights and responsibilities of states in cyberspace and the use of force. Each rule also included an accompanying comment. These reflected the consensus and debate that occurred in the process of formulating *the Tallinn Manual*. As a kind of handbook, it is extremely comprehensive. Of course, NATO also stated that *the Tallinn Manual* does not represent its official view, but the views of the various experts. While the existence of cyber warfare is still being debated, not only does the US clearly believe the existent international law is applicable to cyberspace, NATO has even taken a lead in codifying cyber warfare by compiling a detailed manual.

2. The dual objectives of the laws of war

Apart from regulations which specify the legitimacy of the use of force, such as Article 2 and Article 51 of the UN Charter, international law which is exclusively used to define acts of war also includes the four Geneva Conventions[i] and their additional protocols. These are the so-called 'laws of war', also called the 'law of armed conflict' or 'International Humanitarian Law'. In terms of cyberspace, apart from formulating specific international regulations for cyber warfare, there is a greater need to discuss the possibility of applying the laws of war to cyberspace. However, current discussions in this regard often overlook the original objective of the laws of war.

No matter whether it is formulating new rules or applying existing international norms to cyber warfare, we cannot forget the original objective of the laws of war: firstly, protecting non-combatants (such as civilians, and army medical or religious

personnel) and servicemen and - women who have ceased to be involved in combat (such as casualties, those who have had their vessel sunk, those who are sick and prisoners-of-war). Secondly, to limit the means (especially weapons) and the methods (such as military tactics) of waging war, so as to reduce the impact of armed conflicts. The laws of war forbid means and methods of waging war that can lead to the following consequences: making it impossible to distinguish between combatants and non-combatants (such as civilians), its objective is to protect the lives and property or civilians; to cause excessive harm or unnecessary suffering; or to cause serious or long-term damage to the environment. Clarification of the objectives of the laws of war can make related discussions more focussed and, thus, more relevant and effective.

Ⅳ. The applicability of the basic principles of the laws of war in cyberspace, and associated difficulties

Taking into account the dual objectives of the laws of war, they should also be applicable to cyberspace, i.e., the protection of non-combatants in cyber warfare and the limitation of cyber weapons. However, when applying the basic principles of the laws of war to cyberspace, we also face difficulties. When specifically using the basic principles of the laws of war, a number of difficult questions arise.

1. The threshold of cyber warfare and the principle of legitimate self defence

Article 2 (4) of the UN Charter states, “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.” However, in cyberspace what type of cyber attack constitutes ‘use of force’ and ‘armed attack’? This relates to the issue of the threshold of cyber warfare or what kind of cyber attack constitutes cyber warfare. Because the majority of malicious cyber activities cannot be classed as cyber warfare - but are instead cybercrime and cyber espionage - the threshold for cyber warfare should be set high rather than low. Otherwise, not only will this cause conceptual confusion and countries to be overloaded with cases classed as cyber warfare, it will also cause confusion in the application of international law.

Article 51 of the UN Charter stipulates that, nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. However, what conditions are necessary for self defence in cyberspace? What means can be

employed for self defence? Can conventional weapons be used as retaliation? These questions all require further clarification. In addition, because cyber attacks are, among other things, anonymous, asymmetrical, instantaneous and sudden, they are often seen as weapons of the weak and, therefore, the principle of declaring war is not easily applied to cyberspace. Otherwise, if war is declared, the effect of cyber attacks will be greatly diminished.

2. The principles of differentiation and proportionality

According to the principle of differentiation within the laws of war, even if an attack occurs in cyberspace, in principle, it should only be directed at military networks. Military and non-military targets should be differentiated, as should civil and military facilities, combatants and non-combatants, and civilians and armed forces. However, in today's Internet world, it is not easy to do this. This is because the majority of Internet infrastructure is often civilian/military dual use and cannot be completely separated. However, once the target has been confirmed, military personnel and civilians can both initiate attacks, making it difficult to distinguish between combatants and non-combatants.

The principle of proportionality requires that collateral damage caused by military action cannot exceed the specific direct or indirect military advantage that may result from such action. In cyberspace, it is possible to carry out 'precision' cyber attacks in order to reduce unnecessary harm as much as possible, and it is still possible to evaluate the advantage that may be gained from a cyber attack. However, it is extremely difficult to limit collateral damage from cyber attacks. This is because this kind of collateral damage may relate to various different aspects, including military, economic and social impacts, with consequences that are often hard to calculate. Therefore, as general principles of the laws of war, the principles of differentiation and proportionality in cyber attacks should be respected, but in practice, this is problematic.

3. The principle of neutrality and the interests of neutral countries

The legal rights and interests of neutral countries are protected under international law, and cyberspace is no exception. As I have noted before, cyber attacks take many forms and it is extremely difficult to trace their origins. Cyber attacks such as DDoS require the mobilisation of a large number of computers linked together to form a 'zombie' network. In cyber warfare, it is easy for the computer systems and resources of neutral countries to be used by one side involved in warfare to attack the other, while leaving the neutral country unaware. Therefore, on one hand it is

very easy for neutral countries to become scapegoats for cyber attacks, while the actual originator of the attack remains outside the law. On the other hand, because the origins of a cyber attack are hard to attribute, protecting the rights and interests of neutral countries is out of the question. Therefore, the principle of neutrality in cyberspace is also problematic.

4. The principle of Internet sovereignty

The principle of sovereignty is a cornerstone of the modern international system and international relations. Regardless of whether it is the white paper on *the Internet in China*, issued by the Chinese government in June 2010, the aforementioned *International Code of Conduct for Information Security*, the *Declaration of the Geneva Principle* issued as a result of the UN World Summit on the Information Society in December 2012 or the 2005 *Tunis Agenda for the Information Society*, they all recognise a country's Internet sovereignty.

As noted previously, Harold Hongju Koh pointed out in his speech that all countries conducting activities in cyberspace must consider other countries' sovereignty, this also includes the context of non-armed conflict. He pointed out that the physical infrastructure that supports the Internet and online activities is often located within sovereign territory and is under the jurisdiction of that country. Because of the interconnected and interoperable nature of cyberspace, actions directed at one country's Internet and information infrastructure many affect another country. No matter when a country considers carrying out activities in cyberspace, they must always consider other countries' sovereignty.

NATO's *Tallinn Manual on the International Law Applicable to Cyber Warfare* states that no country can declare that it has sovereignty over cyberspace per se. But, States can exercise their sovereignty over any Internet infrastructure within its territory and related activities, including: personnel involved in Internet activities within its territory, Internet infrastructure located within its territory and the right of 'extraterritoriality' as enjoyed under international law.

Simply put, the principle of Internet sovereignty includes: the rights of jurisdiction over the Internet infrastructure within a given country, individuals and groups and their Internet activities, and the right to formulate public policy for the Internet. The principle of Internet sovereignty means all countries can enjoy equal status in cyberspace. This is beneficial for countries in protecting their own online security and interests. In theory, it should be relatively easy for countries to reach consensus on the issue of Internet sovereignty. However, in practice there may be divergence

on how the meaning and content of Internet sovereignty is interpreted.

5. The application of the laws of war to cyber warfare: possible scenarios

As a new domain, cyberspace still contains many uncertainties, and applying the laws of war to cyberspace poses a number of difficulties. However, this in no way means international law cannot be applied to cyberspace. Nor does it mean we should be indifferent and do nothing when faced with new situations and problems. On the contrary, in order to avoid only enjoying perspicacity with the benefit of hindsight, we should explore the applicability of the laws of war to cyberspace. We should not first have to go through the horrors of wars we have seen historically before finally drawing up relevant rules and codes of conduct. For that matter, apart from discussing which basic principles of the laws of war can be applied to cyberspace, we should also explore under what circumstances they can be applied.

From many previous discussions it seems a consensus is gradually emerging: firstly, when war breaks out, the laws of war are applicable. Secondly, when there is heavy loss of life, the laws of war are also applicable. When war breaks out, cyber warfare is only a part of wider war and the Internet is only one tool and means of waging war among many which can be used. The laws of war can, therefore, naturally be applied. However, at present, discussion of serious loss of life has mainly focussed on major incidents and the loss of life they may cause, such as a 'Cyber Pearl Harbour' or 'Cyber 9/11'. However, the question of what kind of human casualties constitutes 'serious loss of life' still requires further discussion.

---

[i] The Geneva Conventions are a series of treaties on the treatment of civilians, prisoners of war (POWs) and soldiers who are otherwise rendered hors de combat, or incapable of fighting. The 1949 versions of the Conventions, along with two additional Protocols, are in force today.

Convention I: This Convention protects wounded and infirm soldiers and medical personnel against attack, execution without judgment, torture, and assaults upon personal dignity (Article 3). It also grants them the right to proper medical treatment and care.

Convention II: This agreement extended the protections mentioned in the first Convention to shipwrecked soldiers and other naval forces, including special protections afforded to hospital ships.

Convention III: One of the treaties created during the 1949 Convention, this defined what a Prisoner of War was, and accorded them proper and humane treatment as specified by the first Convention. Specifically, it required POWs to give only their name, rank, and serial number to their captors. Nations party to the Convention may not use torture to extract information from POWs.

Convention IV: Under this Convention, civilians are afforded the protections from inhumane treatment and attack afforded in the first Convention to sick and wounded soldiers. Furthermore, additional regulations regarding the treatment of civilians were introduced. Specifically, it prohibits attacks on civilian hospitals, medical transports, etc. It also specifies the right of internees, and those who commit acts of sabotage. Finally, it discusses how occupiers are to treat an occupied populace.

Protocol I: In this additional Protocol to the Geneva Conventions, the signing Nations agreed to further restrictions on the treatment of "protected persons" according to the original Conventions. Furthermore, clarification of the terms used in the Conventions was introduced. Finally, new rules regarding the treatment of the deceased, cultural artefacts, and dangerous targets (such as dams and nuclear installations) were produced.

Protocol II: In this Protocol, the fundamentals of "humane treatment" were further clarified. Additionally, the rights of interned persons were specifically enumerated, providing protections for those charged with crimes during wartime. It also identified new protections and rights of civilian populations.