29th ASIA-PACIFIC ROUNDTABLE

1 - 3 JUNE 2015, KUALA LUMPUR, MALAYSIA

ISIS MALAYSIA

ASEAN-ISIS

PS 5 (b)

PLENARY SESSION FIVE
2 JUNE 2015

DEBATE: “CYBER CONFLICT IS SIMPLY A QUESTION OF WHEN, NOT IF”

Measuring Cyber Warfare

by

Dr XU Longdi
Director
Center for Cyber Security & Research Fellow
China Institute of International Studies (CIIS)

SPONSORS

UEM

The Embassy of
The People's Republic of China
in Malaysia

Konrad
Adenauer
Stiftung

JAPANFOUNDATION

NEW ZEALAND
FOREIGN AFFAIRS & TRADE

Measuring cyber warfare

Xu Longdi, China Institute of International Studies

Over the past years, there have been a lot of discussions and debates about cyber warfare, but few consensus have been reached among officials, scholars and technical experts. Therefore, a measuring of cyber warfare is still needed in this context.

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, -threats and -security. For example, some people believe online threats can be divided into four levels: cyber intrusion, organized 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 organizations 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 -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 strategy, set up cyber commands and strengthened the building of cyber forces as if cyber warfare were 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 twenty per cent 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 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 soft- 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.

Conclusion

There might be no simple answer to the definition of cyber warfare, but when we analyse and evaluate the nature of cyber incidents, we have to take an overview of the above-mentioned factors in a comprehensive manner. We must also 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’.