Evolution of Cyberwars

1. Abstract

The art of cyber-warfares have undergone tremendous changes and improvements with the innovations that has taken place in the the field of technology. Number of growing innovations with technologies and their impact on the war techniques have given birth to different strategies and techniques such as nuclear weapons, bio-weapons, stealth aircrafts/ submarines, radio-electronic combat systems, etc. Intelligence units and Information gathering wings of the military have adopted new methods to fetch details about the enemies, analyze the enemy strategies and counter attacks schemes resulting a military revolution. All these have given a clear cut indication of cyber-warfares dominating the future wars. In this paper we discuss about the evolution of cyberwars with some examples, their implications and the future issues that could arise because of cyberwars.

2. What is Cyberwar?

Cyberwars can be loosely defined as cyberspying and controlling the other country's technological resource through network communication and computer systems to cause some sort of damage or loss to the enemy country. It is often motivated by political or military forces. Cyberwars are carried out according to the military operations and information related principles. It involves destructing the resources or disrupting the services of information and communication systems with the help of modern day technologies. It may also imply developing new doctrines for the politics/military about to how to cause loss to the enemies by analyzing what kind of computers, sensors, networks, databases and physical war weapons are used by them.

Cyberwar is could be seen as a variant of netwar. Netwars are defined as information related conflict at a grand level between nations or societies [1]. It may occur between the governments/military forces of rival nation-stations; between governments and non-government bodies (such as terrorist groups, activists. Most of the times netwars are non - violent (without causing death), but in worst cases, it could combine low intensity losses. For example activists by the group named "Anonymous", has hacked Websites for government departments, India's Supreme Court and two political parties [2], making it unavailable till their demands getting fulfilled. On the other hand, cyberwars are intended to cuase death and physical harm (en example could be Stuxnet cyberwar malware) and hence are more various variant of netwars though strategies and technique used in both of these warfares are almost same.

3. Evolution of Cyberwars

The strategy where one would try to destroy the enemy's communications and make sure of their own safety can be found throughout the history of wars. The shows that cyberwars does not depend on modern day technologies and also it shows the evolution of cyberwar over time with thought process of conflicts and strategic interaction.

3.1 Mongolian cyber-warfares(12th -13th century):

Mongols, in one of their greatest wars against the Muslim empire of Khwarizm in 13th century(which is located in the current day territories of Iran, Iran and central Asian republic of earlier soviet union) demonstrated the use of cyberwar strategies and that could be seen as the origin of such war strategy. The Mongol army comprising of more than 100 thousand soldiers attacked the enemy force which is about half a million and having same amount of war resources of them right in the heart of the enemy territory, without even letting know the enemies that there could be one such attack that too in the heart of the territory. The Mongols noticed the linear and forward disposition of the enemy troops, and they avoided them. But they worked around the defending approach where sudden attacking troops (some sort of guerrilla experts) of messengers moving to and fro between the capital of enemy kingdom and the Mongol army fronts. The king of Khwarizm - "Muhammad Ali Shah" did not have any information about the Mongol army approaching their territory for a war against them until one of the informers informed him that he has seen the Mongol troops patrolling near the capital "Samarkand". But it was a shock to him as the Mongols had crossed all the strong military protection of the borders and it is too late to have a winning strategy of winning the war against them. It would not have been possible if the Mongols made sure that no communication of the Khwarizm's would inform the king or the military about them approaching the capital for a war.

In terms of strategy, Mongols aimed to disrupt the communications of the enemy before striking their capital. They depended on approach which was about breaking the plans and control of the enemies. A sophisticated command, control, communication and intelligence are the clear success factors for the Mongols in this war. They gave preference to the decentralized command in the war field, where as the enemy foes waited for the order from their capitals. In the earlier wars, the Mongols had used terror tactics where they would inform before war that they will attack a particular city, and they would attack after that. Any resistance by the people would get them slaughtered or raped before getting killed. In those cases surrendering from the enemy country's people was plentiful. Some analysts think that Mongol war strategy in their war against Khwarizm was an early experiment of blitzkrieg [3], but some argue that there were differences between cyberwar and blitzkrieg, and the Mongol war was different than them.

3.2 Blitzkrieg - People’s War:

Warfare experts state that Blitzkrieg [4] (which in German language means "lightning war") is a warfare strategy where initial attacks are carried out by dense concentration of mechanized and armored infantry wings which is supported heavily by air-force. Then the Blitzkrieg wings will break through the enemies border of control through continuous short and fast yet powerful attacks. After they are in the enemy territory, they would disperse them. The blitzkrieg doctrine emphasizes on trying to destroy the balance of the enemy, with continuously changing war formation and cutting down the enemy's source of communication, which results in a difficult situation for them to reciprocate efficiently.

The doctrine of German blitzkrieg during the world war II can be seen as the predecessor of modern day cyberwar techniques - as it resulted in disruption of enemy communications and control. It had an explicit goal at tactical and strategic levels. Most of the German tankers were provided with radios as a tactical force multiplier strategy in their war against Soviet Union, whose troops had such communication medium only for the commanders. Destroying the central communications and control unit of the Soviet army by capturing Moscow was the main strategy used by the Germans, as that would completely make the Soviet's lose their communication channel.

3.3 Modern day cyber/netwars – Stuxnet and Anonymous group :

With the advancement in modern technology, we can see a lot of changes in day to day life. The affect of such technologies can also be seen in the art of warfare where various countries (ethically or non ethically) is use softwares as weapon. It is beyond the imagination of common man that how a software can be powerful enough to destroy a nation or disrupt the services that normal citizens of a country could avail.

Stuxnet - It is computer worm which infected many industrial plants in Iran including the Uranium enrichment plant. The existence of such deadly virus which is powerful enough to destroy a nuclear centrifuge was discovered in June 2010. The virus was designed in a way such that it can spread rapidly from one computer through other with or without the Internet unlike the normal computer viruses. Stuxnet was crafted in such a way that it is quite impossible to predict and stop. Stuxnet stealthily spreads between the computers running on windows even without Internet connection, through USB drives. Since it is much unsuspected that anyone could spread a worm in this way, it was unpredictable till the actual damages were reported. The authors of Stuxnet have not been identified officially [5]. But looking at the code size, complexity and the development efforts that has been put up build this lethal weapon, it is quite evident that it is impossible without the help of sponsorship of a nation-state. Though no one has officially come forward to claim the ownership responsibilities, many reliable sources strongly believe that it is a joint effort by United States of America and Israel. This is visualized as a modern day cyber-warfare weapon and experts believe that more of this kind of weapons could be seen in the future wars.

Anonymous group **[6]-** "Anonymous" is a group of activists with great computer skills, claiming to working for a cause without revealing their identity. They gained attention from the world by publicity stunts and distributed *denial-of-service* (DDoS) attacks on government, religious, and corporate websites. The group calls itself as "an Internet gathering" with decentralized command structure which operates on ideas and not on any directives unlike military or political cyber - warfare wings. Though the warfare of the anonymous group cannot be called as cyberwars, it is definitely a netwar where the activists disrupt the services (more often online) by attacking them and making then unavailable to its legitimate users. Anonymous group is active since 2003 and they gained more attention with their protest (named " Project Chanology") against "Church of Scientology" focusing on collaborative international issues on religion and church. Another famous protest carried out by Anonymous was the Internet war they declared against anti-digital piracy campaigns by motion picture and recording industry trade associations.

Starting from 2003 till date, this group has carried out wars in the internet world against many government organizations, private companies to spread across a message which they think as "creating awareness" of which some are of global interest and they have been genuine issues. Who is behind Anonymous – is yet unknown, yet anonymous.

5. Concluding remarks

Cyberwars and netwars have evolved as more than just operational techniques. It has emerged as a new mode of warfare with new approaches to plans, strategies and new forms of doctrine. Cyberwars are adaptive to many contexts and they do not represent a single or structured approach. Another important aspect of Cyberwars is that it can be fought offensively or defensively. It can take place at strategic levels or tactical levels. The definition of Warfield in the context of these kind of wars, where they do not rely on geographical terrain; instead they rely on cyberspace, where the electronics and computers speak [7]. Cyberwars are aided by open electronic spectrum, speed flow of communication and information in the real world as the intension of such wars are not just causing destruction to the enemies. Including new technologies in the old ways might create inefficiencies in some of the military doctrines, but some have been very efficient. Though some of the military bodies are lagging behind in technology adaptations because of their dependency on hierarchical traditions; slowly and steadily they will be competitive enough as business and government bodies, which also influence cyberwars have been adopting new technology trends. All these clearly implies that the cyberwars dominating the future wars with the advancement of technology.

References:

[1] Arquilla , John , and David Ronfeldt. "Cyberwar Is Coming!." Comparative Strategy: 141-165.

[2] "Anonymous attacks Indian websites." BBC News. http://www.bbc.com/news/technology-18114984 (accessed May 10, 2014).

[3] Curtin, Jeremiah. The Mongols: a history. Cambridge, MA: Da Capo Press, 2003.

[4] Fanning, William, Jr. (April 1997). "The Origin of the term "Blitzkrieg": Another view". Journal of Military History 61 (2): 283–302. doi:10.2307/2953968

[5] Kushner, David. "The Real Story of Stuxnet" ieee.org. IEEE Spectrum. Retrieved 25 March 2014.

[6] Halupka. M., Star. C. (2011)The Utilization of Direct Democracy and Meritocracy in the Decision Making Process of the Decentralized Virtual Community Anonymous. Presented at the Australian Political Studies Association conference.

[7] Grier, Peter, “The Data Weapon,” Government Executive, June 1992, pp. 20–23.