Cyber-Warfare

Dilpreet Singh Bajwa

There is no clear definition of "Cyberwarfare". The general conceptualization is that it is a cyber attack or series of cyber attacks through cyber space by one state over another state to deny, manipulate, degrade, disrupt or destroy targeted information systems and networks of the opponents which have an effect equivalent to an armed attack.

It is state sponsored and an action by any nation to penetrate another nation's computer system, networks and critical infrastructure with motive to disrupt and damage it. There has been scattered opinion over the point that whether such operations can be categorized as war but several countries are enhancing their cyber capabilities and also some incident in the past like cyber weapon "stuxnet" use on Iranian nuclear facilities points towards existence of such capabilities and engagement in cyberwarfare. Primarily the countries that are spending their money and efforts rigorously in enhancing their cyberwarfare capabilities are: United States, Russia, China, UK, Israel, Iran and North Korea.

Countries involved in some way in to Cyberwarfare: Following are some examples in which some governments/states were supposed to be involved in cyber-attack or cyberwarfare against their rivals and had achieved their objective or at-least tried for that through cyber operations without shedding any blood.

- Due to anti-chinese riots in Indonesia, the people's republic of china(PRC) hacker community (estimated 3000 hackers) in May 1998 launched attacks against Indonesian government websites in protest.

  Similarly in May 1999, in response to accidental bombardment at Chinese embassy in Belgrade, Yugoslavia by NATO jet, the Chinese red hacker alliance launched a series of cyber attacks against hundreds of US Government websites.

In 2001 when over the South China Sea a Chinese fighter plane collided with a US fighter aircraft then in response over 80,000 hackers from China were engaged in act like of cyberwar against US and the New York Times also referred to it as "World Wide Web War-I".

- During the Russian-Chechen conflict from 1997 to 2001 both sides were engaged in cyber operations to control and shape public perception. In Oct 2002 after officially end of war, the Russian Federal Security Service (FSB) even then attack and shutdown two main Chechen websites.

  In April 2007 Estonian government blames Russia for cyber attacks which includes DDOS attack against government websites, websites belonging to Estonian banks and communication networks . Although there is no reliable evidence available in support of these claims but Konstantin Goloskokov, a prominent Russian youth leader has admitted his involvement in these attacks in protest of Estonian government's decision to relocate "The Bronze Soldier of Tallinn" statue which was dedicated to the former Soviet Union soldiers who had died in battle.

  In 2008, Georgia act against separatists in south Ossetia, in response Russia invaded Georgia and at the same time a fully coordinated attack was initiated against Georgian government websites and other valuable infrastructure including US and UK embassies websites. Cyber attacks include SQL inection, crosssite scripting and DDOS.

- "Stuxnet" is the first ever cyber weapon. It is a sophisticated malware specifically programmed to target the Iran's nuclear facility. The stuxnet malware is believed to be joint venture of America and Israel intelligence agencies under operation called "Operation Olympic Games" but neither country openly admitted it.

- In Dec 2008, a cyber war erupted between Israel and Arabic hackers due to Israel's Operation Cast Lead against Palestine. The point to be focus on here is that mainly state sponsored hackers were involved in these attacks. Israel Defense forces cyber professionals hacked in to Hamas TV station Al-Aqsa.

- In 2009, several US government websites including white house experience DDOS attack and few days later same type of attack experienced by south Korean government websites. The Democratic People's Republic of Korea (DPRK) was prime suspect in this case but there is no evidence to support this.

Although the word cyberwarfare has been around for more than a decade but still it has not been defined properly and till this writing there is no international law clearly and specifically refers to cyberwarfare but cyberwarfare is a reality and poses a high threat. Due to lack of proper definition, rules and guidelines, in case of any online conflict between nations, there is high risk that the situation can go out of control or can cause lots of destruction.

So how a cyberwarfare scenario actually looks like: The computer system, networks, critical infrastructure like: nuclear facility, command and control system of army, transportation facilities, power grids, banking and financial systems are the real targets in case of cyberwarfare because all systems are at some point are controlled or managed through computer systems, networks and internet. For example if you shutdown the power system of a region or in worst case all of a country then there is situation of mass panic, computer system and networks go down, banking system and stock market collapse, hospitals and machines can't work, command and control system of army cannot be able to work properly if not completely collapse which in turn poses new threats, challenges and may be cause of loss of lives.

What makes the cyberwarfare more lucrative than other modes of traditional warfare:

- Cyberwarfare is cheaper in terms of cost, effort and loss of soldier lives in comparison to other traditional warfares.

- Cyberwarfare is easy to control and stealth in nature because can be initiate from anywhere via internet.

- Tools are easy to build, cheap can also be openly available on internet. Even the tools/software are increasing day by day without any control and don't face any legal hurdle because same tools set and techniques are part of cyber defense mechanism.

- Even small countries or non- significant actors can cause high damage.

- Cyberwarfare is initiated through cyberspace and the attacker remains anonymous because it is very difficult to trace the origin of attack.

- Cyberwarfare can be initiated within short term which also gives less time to opponent for preparation.

- Cyberwarfare save precious life of soldiers and casualties of any nation but still has equivalent effect of any otherwarfare mean.

- Cyberwarfare can't be dependent on distance and physical boundaries.

- Enable a nation to achieve its political or strategic objectives without disclosing its identity and without any armed conflict.

- Cyberwarfare can also attacks country's critical infrastructure like banking system, power grid etc which in turn also influence the lives of common man and create a situation of mass panic, that also gives you a psychological advantage.

- As mentioned above that cyberwarfare attacks country's critical infrastructure which may also includes nuclear facilities, army command, control system and power system on which the army is dependent for their traditional warfare which in turn gives you a strategical advantage over enemy.

- The vulnerabilities and complexity of the opponent's interconnected system provides more opportunity to the attacker and the victim's has to invest considerably to neutralize the threat.

Conclusion: Cyberwar can be fought exclusively but the chances are more common that future wars are a combination of tradition warfare and cyberwarfare where cyberwarfare either use to disrupt or damage the opponent military capability and to enhance your own capability. Cyber soldiers are more likely to be integrated with conventional army commands or a separate new command can be established like Land, Air, Navy commands with name like cyber command. Countries around the world are enhancing and developing their cyber strategies and cyberwarfare capabilities. They understand its significance and the strategic advantage it can provide during actual war. Even small countries that in actual can't afford to compete with rival countries in traditional warfare can take a lead through cyberwarfare.

Sources:

https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/.

Book: Inside Cyberwarfare by Jeffrey Carr, OWeiley Publications.

https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf.