Understanding Cyber Weapons

Colonel Sanjeev Relia[@]

Introduction

A weapon is any device used in order to inflict damage or harm to living beings, structures, or systems. Weapons are used to increase the efficacy and efficiency of activities such as hunting, crime, law enforcement, self-defense, and warfare.[1] In a broader context, weapons may be designed to include anything used to gain a strategic, material or psychological advantage over an adversary. Simple as well as complex products can be used both for peaceful purposes and as arms or weapons depending on the intentions of the user. So is the case with Information Technology tools. While the internet was never designed to wage a war, cyber space today is on the threshold of being the fifth domain of warfare.

A lot is being spoken about attacks in the cyber space and cyber weapons. Nations like the USA, Russia and China have gone ahead and raised cyber units and even cyber commands. Although, we in India lag behind a little in this facet of warfare, however measures have been initiated to bridge the gap. The defence minister of India, Shri AK Antony in May 2013 announced that India too will soon form a cyber command to handle the online threats being faced by the country. He further said that we have already got a mechanism for cyber security but we are augmenting it further and the forces are finalising a proposal for a cyber command.[2] Does this mean that we have entered into an era where our defence forces will be fighting in the cyber domain? Does it also imply that we will need to create new kind of weapon systems to ensure territorial integrity of our nation and that we will have to create new units of computer geeks in uniform who will control cyber weapons and employ them when the need arises?

What are Cyber Weapons?

When a weapon is spoken or written about, a distinct perfect shape of the weapon system emerges in the mind. Whatever be

[@]**Colonel Sanjeev Relia** was commissioned into the Corps of Signals on 20 Dec 1986. Presently, he is a Senior Research Fellow at the Centre for Strategic Studies and Simulation, United Service Institution of India, New Delhi.

Journal of the United Service Institution of India, Vol. CXLIII, No. 594, October-December 2013.

the weapon system, the IHS Jane's Defence Weekly would clearly spell out the destructive powers of each of the system with a few glossy pictures leaving little doubt in the mind what the weapon platform or system can do. But as the concept of cyber weapon is abstract, these weapons find no such mentions in any of such glossy journals. Besides, what can be made out of a printout of a software programme claiming to be a deadly cyber worm capable of destroying the command and control system of an Air Defence Network? A trained military mind finds it difficult to comprehend how an innocent looking laptop or desktop could cause havoc in the battlefield and perhaps may cripple the critical infrastructure of a nation. Therefore, there is a need for the men in uniform to critically analyse the concept and capabilities of Cyber Weapons.

The definition of a kinetic weapon fails to capture the essence of what are generally regarded as cyber weapons. This is because most of the malicious computer codes, may it be Virus, a Trojan or a Worm that would fall within the parameters of a cyber weapon are designed to have an indirect kinetic outcome which may, or may not, result in inflicting damage or harm to living beings, structures, or systems. To define a cyber weapon in the specific context of conflicts, it is necessary to first differentiate a cyber weapon from a malware, typically used for criminal purposes or an information tool used to perform espionage in the cyber space. To reach a definition of cyber weapon, it is therefore necessary to focus on three essential elements. As Thomas Rid explains it, a computer code as a cyber weapon has to first "weaponise" the target system in order to turn itself into a weapon.[3]

(a) The Context. It must be the typical context of a cyber warfare act. This concept may be defined as a conflict among actors, both national and non-national, characterised by the use of technological information systems, with the purpose of achieving, keeping or defending a condition of strategic, operational and/or tactical advantage.

(b) The Purpose. Causing, even indirectly, physical damage to equipment or people, or rather sabotaging or damaging in a direct way the information systems of a sensitive target of the attacked subject.

(c) The Mean/Tool. An attack performed through the use of technological information systems, including the Internet.

Based on the above, Stefano Mele defines a cyber-weapon as: "A part of equipment, a device or any set of computer instructions used in a conflict among actors, both national and non-national, with the purpose of causing, even indirectly, a physical damage to equipment or people, or rather of sabotaging or damaging in a direct way the information systems of a sensitive target of the attacked subject."[4]

Thomas Rid defines a Cyber Weapon as a subset of weapons more generally as computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living things.[5] The spectrum of cyber weapon system therefore becomes very large and hence there is a need to spell out the important facets of such weapons such as their lethality, its effect and their employment.

Aspect of Lethality

One aspect which clearly emerges from both the above definitions is that cyber weapons are built with lethal intent although the lethality of such weapons is not quantifiable. For instance, for a nuclear strike with 20 KT weapon, the extent of damage that will be caused on any particular type of target can easily be tabulated. For a cyber weapon, such predictions can never be accurately made. How lethal is a cyber weapon, depends on its ability to cause the following to a network :–

(a) Disruption of the network services.

(b) Denial of services of the network to its users.

(c) Degradation of the performance of the network, thereby degrading the efficiency/ performance of the overall system.

(d) Destruction of critical components of the network thus rendering the entire system useless.

The easiest way to check the above capabilities of a cyber weapon would be by carrying out a live test fire, like an underground nuclear test for a nuclear weapon. However, no such tests of a cyber weapons are possible on actual networks as not only the damage caused may result in loss of property or revenue but also may be seen as an act of aggression. Stuxnet, a cyber worm attack in 2009 from an unknown origin (probably collaboration of the US and Israel) on a highly protected nuclear site at Natanz, in

Iran is perhaps the only example which clearly indicated the extent of damage that a cyber weapon can cause. Although a large number of scholars till date still debate on Stuxnet as a cyber weapon, it did attack the nuclear centrifuges that operated with a Supervisory Control and Data Acquisition (SCADA) system using Siemens software and is believed to have caused a setback of at least one year if not more to the Iranian Nuclear Development Program.[6]

To establish the lethality and destructive power of cyber weapons and the network security aspects against such attacks, the US Defence Advanced Research Projects Agency (DARPA) is developing the National Cyber Range (NCR) to provide realistic, quantifiable assessments of the Nation's cyber research and development technologies.[7] The NCR will provide fully automated range management and test management suites to test and validate leap-ahead cyber research technologies and systems. It will test technologies such as host security systems, and local and wide area network (LAN and WAN) security tools and suites by integrating, replicating or simulating the technologies. Seven large-scale cyber experiments for multiple US Department of Defence (DoD) organisations were executed on the range during a one-year beta operation phase that ended in Nov 2012.[8]

Effect of Cyber Weapons

Cyber weapons and cyber attacks offer a means for potential adversaries to overcome overwhelming advantage of a nation in conventional military power. The other most important aspect of a cyber weapon is that they need not necessarily target a military objective. In fact more often than not, the objective of a cyber attack will be a non-military target. Critical national infrastructure such as the power grid systems, telecom networks, the air traffic control system, economy sector to include banking and other financial institutions and railways could be such possible targets as all these sectors heavily rely on automation and networking. The payload of a cyber weapon could vary from a programme that copies information off a computer and sends it to an external source; or an altering and manipulating programme to either take control of the system or to alter the way in which it works. It could also be a code which could convert a computer into a botnet[#] and employ the machine in a Distributed Denial of Service[##] (DDoS) at

a later stage or even cause destruction of a physical process which the computers of the SCADA system controls like it happened with Stuxnet. Various effects of a cyber weapon attacking a network have been summarised by Dr Roland Heickerö in an Effect matrix as shown at **Figure 1**.[9]

	Physical arena (land, air, maritime, space)	Information Arena	Cognitive domain (cognition, perception, emotion)
Physical Effects	Interruption, destroy electronics and sensors, affect transmission and access links, derive robots, system failure	Interrupted communication, denial of services; DOS	Fragmented communication, decreased amount of information, reduced analysis capability
Syntax Effects	Hacking, cracking virus, Mistrust against system Trojans, spam, interception, exploit, bugging illegal misuse of information system	Attack logic of system, delay and distortion of information	Mistrust against system
Semantic Effects	Mass medial manoeuvers, planted information, mutilation of sensor data	Deception and manipulation of information (disinformation)	Changed situation awareness, mistrust against and questioned of information, inability for decision making

Figure 1 : Effect Matrix of Cyber Weapons

A botnet (also known as a zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet.

A DDoS attack is one in which a multitude of compromised systems attack a single target like a server, thereby causing denial of service for users of the targeted system.

A single cyber weapon may not be able to impact the physical arena, information arena and the cognitive domain and hence a multi-pronged cyber attack may be necessary if all the three spheres are to be addressed simultaneously. Key for success in cyber space is to understand prerequisites for conducting operations in the information arena and cognitive domain of the enemy. Cyber weapons do not create the same spectacular visual that a nuclear or even conventional missile does, which makes them weapons of stealth. Also before being hit, a network is unlikely to get any advance warning of an incoming cyber attack. Not knowing what the next attack is going to be or when it will happen has a profound effect on the victim and makes cyber weapons unique amongst all possible coercive systems. Another characteristic of cyber weapons is that for the first time in history, this technology gives small states with minimal defence budgets the capability to inflict serious harm on a vastly stronger foe at extreme ranges.

Employment of Cyber Weapons in a Conventional War

The US Air Force has designated six cyber tools as weapons to help normalise military cyber operations and keep up with rapidly changing threats in the newest theatre of war.[10] This clearly indicates that time has now come that the armed forces around the world gear up to employ as well as defend against cyber weapons. The 2008 cyber-attacks on Georgia is the first case in history of warfare when cyber space domain attacks were synchronised by Russia with major combat actions in the other war fighting domains. Although denied till date by the Russian Government, the Russian naval and land operations against Georgia were preceded by large scale DoS attacks on Georgian Military and Government networks. The attacks continued as the Russian tanks and troops were crossing the border and bombers were flying sorties.[11] The impact : Georgian citizens could not access websites for information and instructions while the nation was being invaded.

When employed in conjunction with conventional operations, cyber weapons increase the cost of conflict for adversaries as he has to now protect the National Critical Infrastructure against cyber weapons besides the conventional and nuclear threat of the enemy. Imagine, if India was involved in a conflict situation and the adversary through pre-emptive cyber attacks crippled the movement of trains and air traffic and the civil telecom network at the mobilisation stage itself. The problems that would arise for movement of troops and logistic supplies would be phenomenal. Similarly, if the major oil refineries were to be shut down because of failure of its SCADA system, it could create a critical situation for the defence forces embroiled in a conventional war. Hence, like the lines of communication have to be protected during the war, in a similar manner in the cyber age, the Critical National Infrastructure will have to be protected against enemy cyber attacks both before the outbreak of hostilities as well as during the hostilities, thereby increasing the cost of war fighting. However, cyber weapons are unlikely to influence beyond a point the national security policy when core national interests are at stake.[12]

Like the civil infrastructure, cyber weapons can target the military networks too. Although our defence networks enjoy the advantage of being segregated from internet, however this does not make them immune to cyber weapons. Most of our defence

equipment is imported and most hardware today is produced in and around China. Also, there exists no agency in the country to sanitise the network equipment when it is being imported against malware pre-embedded in them. Therefore, a cyber attack could yet be initiated during critical periods of the battle employing Embedded Devices and Trapdoors.[13] Any network in the battlefield is perhaps therefore as vulnerable to a cyber attack as a civil target is. However, developing and deploying potentially destructive cyber weapons against hardened military targets will require significant resources, hard-to-get and highly specific target intelligence, time to prepare, launch and execute an attack. Hence, the deterrence value of such weapon systems against military targets is negligible.

India too could employ such weapon systems during the preparatory as well as the contact stages of a battle to weaken the enemy's war waging potential by targeting their critical national infrastructure. After all, cyber weapons are a cheap way to build a global strike capability against networked states and armies and our potential adversaries are well on their way to create such networks, if already not existing. Therefore, the time has now come to take charge of the cyber space and develop offensive cyber capability as part of the overall national security policy. After all, like in a battlefield, even in the cyber space, offence is the best form of defence.

Conclusion

We once lived in a world in which wars were fought by brave soldiers who faced each other in furious combat in a way that today we would find it hard to believe. In the last decade, the concept of war and war fighting has changed considerably. The massive introduction of the technology component in all spheres of warfare has ensured that cyber weapons and cyber attacks too become activities undertaken by governments to degrade the enemy's war waging capabilities.

End Notes

1. Definition of Weapons as given in Wikipedia

2. Cyber Command for Country Soon: Antony TNN May 26, 2013, 03.09AM IST

3. Thomas Rid, Cyber War Will Not Take Place, 2013

4. Stefano Mele,Cyber Weapons: legal and strategic aspects Version 2.0, June 2013.

5. Thomas Rid and Peter McBurney, Cyber Weapons published in The Rusi Journel

6. Stuxnet Effect: Iran Still Reeling, Industrial Safety and Security Source, August 3, 2011, Link: http://www.isssource.com/stuxnet-affect-iran-still-reeling/

7. The National Cyber Range: A National Test bed for Critical Security Research http://www.whitehouse.gov/files/documents/cyber/DARPA%20-%20NationalCyberRange_FactSheet.pdf

8. ibid

9. Some Aspects on Cyber War Faring in Information Arena and Cognitive Domain http://www.dodccrp.org/events/11th_ICCRTS/html/presentations/157.pdf

10. US Air Force designates cyber weapons Apr 10, 2013. http://www.itnews.com.au/News/339234,us-air-force-designates-cyber-weapons.aspx

11. David Hollis, Cyberwar Case Study: Georgia 2008, available at smallwarsjournal.com

12. Ross M Rustici, Cyber Weapons: Levelling the International Playing Field http://webcache.googleusercontent.com/search?q=cache:http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/2011autumn/Rustici.pdf

13. Trapdoor : also referred to as backdoors, are bits of code embedded in programmes by the programmers to quickly gain access at a later time, often during testing or debugging phase.