Cyber Weapons – The New Weapons of Mass Destruction?

Lieutenant General Davinder Kumar, PVSM, VSM and Bar (Retd)*

Introduction

In this Information Age, while Cyber Space has been accepted as the new domain of warfare, it still does not have an internationally accepted definition. The same is true for cyber weapons. The US Government security expert, Richard A Clarke, in his book, *Cyber War defines Cyber Warfare as actions by a nation state to penetrate another nation's computers or networks for the purpose of causing damage or disruption.*[1] Cyber Weapons, accordingly, are the tools for conducting cyber warfare.

Weapons, in their simplest form, could be considered as, *"instruments of harm".* Since the dawn of time, humans have used weapons to hunt and demonstrate or acquire power. The types of weapons and their range, lethality and precision have increased substantially with the advancement of technology and the need to obviate the perceived threat. *The weapons thus have evolved with time.* The time taken to translate the concept into a product/weapon has been reducing in consonance with the pace of development of technology and its engineering into production. Cyber weapons are also evolving just as the conventional weapons albeit at a much faster pace. In the cyber world, the technological advancements happen in days or even hours with the emergence of corresponding new threats. *The most significant development has been the reach of cyber weapons in the real physical world* as demonstrated by the Stuxnet attack on the Iranian Nuclear facility.[2]

Definition

We need to define cyber weapons correctly as the same has significant political, security and legal consequences. This is an urgent and important requirement - for being able to assess both

* **Lieutenant General Davinder Kumar, PVSM, VSM and Bar (Retd)** was commissioned in the Corps of Signals in December1965 and retired as Signal Officer-in-Chief in September 2006. Post retirement he has worked in the Corporate Sector, contributed extensively in professional journals and has been a member of National IT Task Force and a number of Committees.

Journal of the United Service Institution of India, Vol. CXLII, No. 591, January-March 2013.

the level of threat from a cyber attack and the consequent political and legal responsibilities attributable to the attacker. Two definitions, one by a security expert and the other with legal overtones are given below:

> *"Cyber Weapon could be defined as a 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 beings."*

> *"A device or any set of computer instructions intended to unlawfully damage a system acting as a critical infrastructure, its information, the data or programmes therein contained or thereto relevant, or even intended to facilitate the interruption, total or partial, or alteration of its operations."*

The above definitions imply that cyber weapons may span, in theory, a wide range of possibilities: from Denial of Service attacks (which typically have a low level of penetration) to, "tailored" malware like the Stuxnet characterised by high intrusiveness and a low rate of collateral damages. It may be prudent, therefore, to evaluate cyber weapons from its domain of relevance, cyber space, with the distinct possibility to cross the virtual boundaries and extend to the real world.

Classification [3]

With the above idea in mind, cyber weapons can be classified according to the following four parameters as shown at Figure 1 :–

(a) Precision - That is the capability to target only the specific objective and reduce collateral damages.

(b) Intrusion - the level of penetration inside the target.

(c) Visibility - the capability to remain undetected

(d) Ease of Implementation - a measure of the resources needed to develop the specific cyber weapon

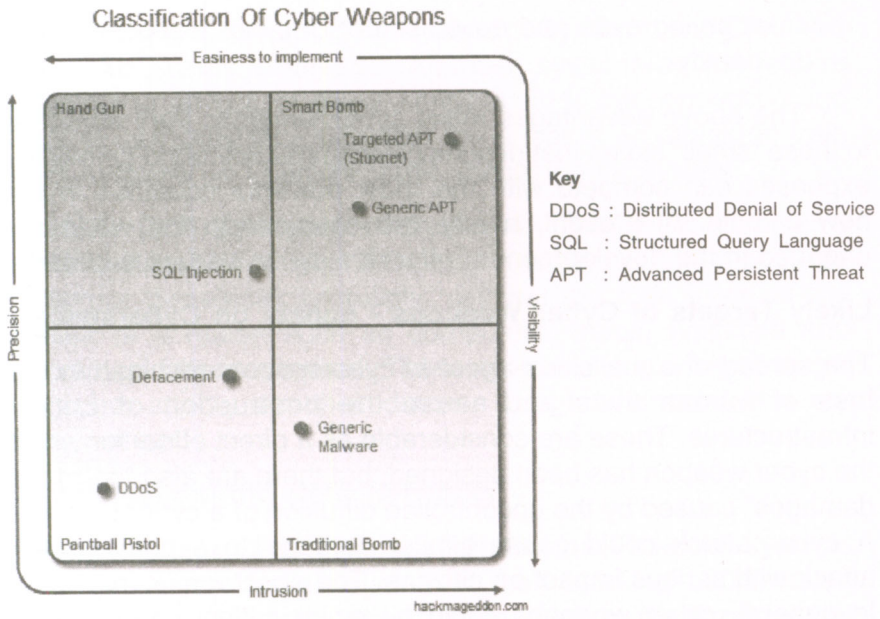

Figure 1

Why Cyber Weapons? [4]

Use of cyber weapons is complementary to conventional military strikes. It could be possible to:-

(a) Support offensive operations by destroying enemy's defence/critical infrastructure

(b) Probe the technological capabilities of the adversary by evaluating the ability of an agent to infect the enemy system.

(c) Cyber weapons are more efficient and less expensive.

(d) The attack is carried out at the speed of light.

(e) Cyber weapons are less noisy (stealth weapons) - no one wants to acknowledge the vulnerabilities of their system.

(f) Attribution is very difficult - the possibility to operate under cover makes cyber weapons very attractive.

(g) Cyber weapons are offence dominant and ideal weapons for asymmetric warfare - the warfare of 21st century

(h) Preparation phase of cyber weapons is easy to hide

from prying eyes and development of cyber weapon is hard to identify.

The above advantages make cyber weapons very attractive to those "small" states that despite having reduced funds for military expenses can compete with the most powerful countries in the new domain. At present, nearly 140 countries in the world are engaged in the development of offensive cyber warfare capability.

Likely Targets of Cyber Weapons - Impact on Cyberspace [5]

The spread of a malicious agent in cyberspace could lead to the loss of human lives and cause the destruction of critical infrastructures. These are considerable as a direct effect for which the cyber weapon has been designed, but there are also "collateral damages" caused by the uncontrolled diffusion of a cyber weapon. A cyber attack could cause similar damage to a conventional attack with serious impact on citizens. The spectrum is very wide. In general, cyber weapons could hit every critical infrastructure and vital systems of a country such as:-

Electronic National Defence Systems. By hacking a defence system of a country it is possible to control its conventional weapons, for example there is the possibility to launch a missile against the state itself or other nations. Similarly, Command and Control systems of the adversary can be degraded substantially by interfering/disrupting the defence communication networks

Hospitals. Electronic systems present in hospitals and health centres could be exposed to cyber attacks that can compromise their functioning, causing serious consequences.

Industrial Control Systems (like Supervisory Control and Data Acquisition (SCADA) System or Programmable Logic Controllers (PLC) of Critical Facilities. A cyber attack could compromise the management system of a chemical plant, dams, energy production plants or a nuclear site, altering production processes and exposing large areas to risk of destruction.

Water Supply. Water is an essential resource for the population. Interruption of the supply might leave large areas without water. The alteration of the control system might allow it to be functional but vulnerable to a successive attack such as water poisoning.

Fully-automated Transportation Control Systems and Civil and Military Air Traffic Controls. All those systems do not require conductors or drivers, or give a sensible aid to the conduction and control of transportation. Consider the effect of an attack on train control systems or to an air traffic management system.

Electricity Grid Management Systems. This target represents the vital system of a country. Attacking these systems, it is possible to interrupt the electricity supply, causing the total block of the activities of a nation such as computers, trains, hospitals and telecommunications services. These represent a privileged target for a cyber attack, and their defense is a fundamental in every cyber strategy.

Communication and Data Networks

Banking Systems and Financial Platforms. Financial systems are critical assets for a nation and their blocking could cause serious problems. Despite being unable to cause the direct loss of human lives, a cyber attack could cause the financial collapse of a nation through interference/blocking of all economic activities. The scenario is worrying - if we think that global finance today is strictly dependent on the economy of each single state, a cyber attack against a state could cause serious and unpredictable consequences to the entire economic system.

Limitations of Cyber Weapons

One of the most dangerous effects of the use of a cyber weapon is the difficulty to predict its diffusion since cyber space has no boundaries. This means : –

(a) Cyber weapons could hit in unpredictable ways other systems and networks that are not considered targets. In extreme cases, there is a possibility that it attacks the systems of host nation in a sort of "boomerang effect".

(b) Presence of cyber weapons in cyberspace could open up the possibility of reverse engineering of its source code by ill-intentioned individuals. Foreign governments, cyber terrorists, hactivists and cyber criminals could be able to detect, isolate and analyse the agents, designing and spreading new cyber threats that are difficult to mitigate.

(c) Cyber weapons have limited shelf life since they are designed to exploit a particular vulnerability.

(d) Span of attack and extent of damage is inversely proportional to the sophistication of the cyber weapon

Generations of Cyber Weapons[6]

Cyber weapons, like any other weapon system are evolving with time, technological advances and threat perception. The three generations of cyber weapons could be defined as follows:

Generation 1. Physical or (Anti) radiation electronic warfare weapons that can blind, cripple, degrade or incapacitate through physical attack or traditional electronic warfare means. These are effectively command and control weapons. The criterion is the level of effect delivered. Traditional effects are degradation, disruption of communication with very closely controlled deployment and targeting. Examples are the blowing up of the Siberian oil pipe line in 1982; destruction of Iraq's power grid by deploying carbon fibers to short the electric grid; blowing up of Baghdad telephone system in the Gulf war and so on.

Generation 2. Software and hardware derived technical implementations that allow for vulnerabilities to be exploited in the systems of systems or specific targets. These are characterised by their requirement that somebody has an exploitable feature in systems design, configuration, or software implementations. This is further characterised by heavy reliance on network infrastructures though they may not be the primary mechanism of exploitation. There is varying levels of barrier to entry. Traditional characteristics are of espionage and sabotage with varying level of sophistication and control of deployment. Estonia[7] and Georgia[8] incidents would qualify.

Generation 3. Fusions of generation 1 and 2 weapons then become point and shoot weapons that can destroy, degrade or disrupt the adversary's systems without requiring the vulnerabilities to be exploited. The adversary is no longer required to make a mistake. These kinds of weapons simply destroy the command and control, (communication and coordination) behaviours of cyber infrastructures. Emerging characteristics are of selective targeting and speed of deployment.

Generation 1 weapons primarily work against the availability of systems and the inherent infrastructures that they operate upon. Generation 2 weapons tend to operate at the logical layers against the protocols and applications that run on top of the network. Finally, Generation 3 weapons appear to be destined to work against the entirety of the systems of systems infrastructures inclusive of the human being.

Another interesting way to define cyber weapons would be based on the contemporary threats and their classification.[9] The current state of threats is best represented as a pyramid. The base of the pyramid is made up of all kinds of threats – what we call 'traditional' cybercrime. Its distinguishing features include a reliance of mass attacks targeting ordinary users. Cyber criminals' are mostly interested in launching these attacks for direct financial gain. This accounts for over 90 per cent of all contemporary threats.

The second tier is made up of threats aimed at organisations. These are targeted attacks, which include industrial espionage, as well as targeted hacker attacks designed to discredit their victims. The attackers are highly specialised and work with a specific target in mind or for a specific client. The goal is to steal information or intellectual property. Financial gain is not the attackers' primary goal. This group of threats also includes a variety of malicious programmes created by certain companies at the request of law enforcement agencies.

The third tier, which is the top level of the pyramid, includes malware which can be categorised as true cyber weapons. *These include malware created and financed by government-controlled structures. Such malware is used against citizens, organisations and agencies in other countries.*

To summarise, we can identify three main groups of cyber weapons based on threats:-

(a) **Destroyers.** These are programs designed to destroy databases and information as a whole. They can be implemented as 'logic bombs' that are introduced into victim systems either in advance and then triggered at a certain time, or during a targeted attack with immediate execution. The most notable example of such malware is Wiper.[10]

(b) **Espionage Programmes**. This group includes cyber weapons (malware) like Flame, Gauss,[11] Duqu[12] and miniFlame[13]. The primary purpose of such malware is to collect as much information as possible, particularly very highly specialised data (e.g. from Automated Computer Aided Design (Autocad) projects, SCADA systems etc.), which can then be used to create other types of threats.

(c) **Cyber Sabotage Tools.** These are the ultimate form of cyber weaponry – threats resulting in physical damage to targets. Naturally, this category includes the Stuxnet worm. Threats of this kind are unique and require adequate intelligence and R&D resources. Some developed and networked countries are devoting more and more effort to developing this type of threat, as well as defending themselves against it.

Cyber Weapons – The New WMDs[14]

Just as the industrial revolution brought about a fundamental change in warfare, the Information Age is ushering in a new, low cost option for strategic defence in the form of cyber warfare in general and cyber weapons in particular. These can now accomplish most of the strategic tasks that once required air superiority or nuclear capability. The situation is similar to the time when early nuclear theory wrestled with many of the similar issues that we now face in attempting to understand cyber weapons. Some of the important issues are:-

(a) The long range strike capabilities of cyber warfare have the potential to be extremely effective when employed as an anti-coercion weapon (power projection capability at minimal cost).

(b) A strong cyber capability is a deterrent force that will largely mitigate outside interference in domestic and regional affairs.

(c) Cyber weapons have the potential to become an equalising force because they require a fraction of investment compared to nuclear weapons or the strategic air power and yet would be able to execute most of similar missions and that too with limited or no collateral damage. While a cyber

weapon can cause a total black out of the electric grid for the operationally desired duration, the same can be restored just by a click of a switch!

(d) Given the speed and precision with which a cyber attack can be carried out, these weapons can be used for anything from a warning shot to signal an adversary to a catastrophic strike that could cost trillions of dollars and an unspecified discomfort to the people.

The wide range of issues mentioned above make the cyber weapons unique. The fact that a cyber arsenal is also exceedingly cheap means that the available destructive capacity for poor and weak States vis-à-vis a developed and networked State is unprecedented. The ability to strike quickly and on such a scale with no possibility of retribution makes cyber weapons uniquely terrifying. A well executed cyber campaign coupled with careful public relations has the potential to traumatise a society in ways not seen after Nagasaki. *Cyber weapons are a cheap way to build a global strike capability against networked states.*

Implications[15]

Curtailing of Inter-State Coercion. Just like large and capable conventional forces, cyber weapons present a strong deterrent for a potential attacker. While very few countries have the capability of intervention at the regional or global levels, any country with a network connection may be able to launch an effective retaliatory strike. Consequently, interventionist foreign policies will become exceedingly expensive both in the material and human cost. The new dangers that the fifth domain of warfare creates will limit the behaviour of bigger nations. There is a school of thought that the Iraq war would have to be fought differently if Iraq had cyber weapons.

Derailment of Human Security Issues. The cost of intervention increases in direct proportion to the target state's ability to launch a strategic cyber attack. Accordingly, not many nations would like to intervene to prevent humanitarian crises.

Alteration of Conventional Force Structure. Cyber weapons present the possibility of altering conventional force structure in a fundamental way. For example, there are multiple comparative advantages of cyber weapons over air strikes. The first and the

most compelling is cost. The second is the temporary nature of the effect of cyber weapons and finally negligible collateral damage caused by cyber weapons.

Cyber Deterrence

The above implications mean that cyber deterrence is capable of reducing the incidents of violence in the International system. At the same time, it is also likely to make the world a safer place for corrupt and abusive regimes. Cyber weapons and their value may not rival that of nuclear weapons at present, but they certainly have greater deterrence force than conventional systems. These have the potential of increasing the transactional cost of war to such an extent that developed nations will be far less willing to use force internationally based on ideals or a perception of marginal regional balance of power.

Failure of Deterrence[16]

There are, however, glaring issues regarding deterrence in cyber space and these are:-

(a) Unlike nuclear weapons or any other conventional capability, it is almost impossible to demonstrate cyber power.

(b) It is very easy to develop this capability with an exceedingly small foot print.

(c) The technical nature of cyber weapons requires a pre-existing vulnerability in the software or the ability to assume the identity of a trusted user to carry out an attack (Identity theft when viewed in this context becomes extremely serious).

(d) The shelf life of a cyber weapon is limited to the presence of the particular vulnerability. Further, a near perfect defence against a cyber weapon can be brought in a matter of days or weeks against the use of that particular exploit.

(e) Cyber weapons, at present, can only penetrate network defences if there are exploitable flaws in those defences (It is in this context that probing attacks on the networks are to be viewed seriously and reported).

(f) Most of the technology and material needed to develop sophisticated cyber weapons are commercially available and

completely unregulated. Consequently, traditional technology and arms control regimes are impossible to create and verify.

(g) Currently, the only way we can correctly estimate the cyber capabilities of another actor is by measuring the frequency and sophistication of attacks emanating from a source/state.

The world has dealt with the threat of Weapons of Mass Destruction, commonly known as WMD, in the past. However, in the world of Cyber Space, we are now confronted with a new WMD threat: *Weapons of Mass "Disruption".*[17] If we do not prepare now, we could, one day, face a cyber attack that could cripple our government, our economy and our society. We need to formulate and announce our Doctrine regarding Cyber Warfare and develop demonstrable Cyber Defence and Cyber Attack capabilities to act as an effective deterrent.

In the nuclear domain, the nuclear weapon states have promulgated their respective doctrines and have built or are in the process of building a strategic triad of land, sea and airborne capabilities of launching nuclear weapons. Consequently, the nuclear deterrent has held thus far. In the Digital Age, we need a, *'Cyber Triad'*[18] that will deter cyber attacks on our information infrastructure by employing *Weapons of Mass Disruption.* The various legs of the 'Cyber Triad' are as under : –

(a) **Resilience (First Leg).** Cyber resilience would mean such things as Redundancy of critical connectivity; the ability to handle increased traffic loads under the most stressed conditions; and the ability to protect and secure sensitive and private information.

(b) **Attribution (Second Leg).** Our continued inability to attribute attacks tantamount to an open invitation to those who would like to harm us, irrespective of their motives. If the adversary can attack our networks and systems without leaving finger prints, they can attack without consequences and that means they cannot be countered or deterred; a serious matter indeed. To deter cyber attacks, we need to improve our capability to attribute these attacks to their ultimate source and display a very strong political will that we will respond in the most devastating manner. Concurrently,

we need to announce our likely response to probing or cyber espionage attempts by any player.

(c) **Offensive Capabilities (Third Leg).** Just as in the kinetic weapons, the adversary must know that the nation has an effectively balanced defensive and offensive cyber capabilities backed by a very strong political will. The nation's strategic doctrine must clearly state both the likely response to a cyber attack and the response that the same would invite. For example, many countries have promulgated that an electronic attack on their assets will be construed as an act of war and would attract appropriate response.

Development of credible cyber deterrence would have to be a national effort that would involve the government, industry, academia and most of all the people. At the same time, we will have to work very closely with the international community to develop a forum for peaceful co-existence in the cyber space, the corresponding legal framework; the development of secure products and services and the likely international response to a cyber attack on a nation state. We need to work harder on fostering international alliances and be an active member in the formulation of best practices and a code of conduct in the cyber space.

Conclusion

Information and Communication Technology (ICT) has created a virtual world with no boundaries where the rules of engagement are being constantly defined by the world community with very little interference from the government. This virtual world called the, "cyber space" has not only opened new avenues for interaction, development and exchange of views but as a natural corollary, it is also becoming more hostile. Worldwide, people and in some cases, the governments are engaged in the exploitation of the cyber space for illegal activities like espionage, theft of technology, financial frauds and so on. They have, accordingly, developed means and methods to carry out such activities by way of viruses, root kits, malware and so on. These are the initial steps in the evolution of cyber weapons which till date do not have a formal definition. This evolving threat to society as a result of these cyber weapons and their capability to disrupt networks, systems and their functionality; their suitability for the conduct of asymmetric warfare, coupled with the all pervasive application of ICT in the

Military and civilian domains, have opened a new dimension of warfare.

The recent critical development wherein ICT has enveloped the physical space has led to both the weaponisation of cyber space and the consequent threat to the Critical Information Infrastructure (CII). While blowing up of the Siberian oil pipeline in 1982 indicated *the possibility;* the destruction of Iraq's power grid by deploying carbon fibres to short the electric grid in Gulf war, the interference of financial system in Estonia and effective neutralisation of the war fighting capabilities in Georgia displayed the emergence; the Stuxnet attack on the Iranian Nuclear facility and the recent discussions in the Pentagon of possible option of taking out the Libyan Air Defence system by cyber weapons are pointers to both the emanating threat and coming of age of cyber weapons. While the USA, Russia, China, North Korea and Iran are said to have developed effective cyber weapons, many other nations are engaged in developing the same. The challenge is to stop their development and proliferation or at least regulate them through generating trust and confidence. There is an urgent need to have international treaties for limiting the use and proliferation of cyber weapons, independently or as part of expanded role of the United Nations. India, while participating in the international efforts, must enter into alliances - bilateral, multi-lateral or regional to secure her national interests and sovereignty. She must formulate a national doctrine and develop credible cyber offensive and defensive capabilities. Notwithstanding our strength in the field of ICT, such capabilities, skill sets and the much needed synergy amongst all concerned in the nation would take a long time; assuming that we have and can display political will and resolve. A few initial steps have been taken but we have a long way to go. The nation urgently needs to develop a credible cyber deterrence through promulgation of a doctrine, development of the skill sets, a dedicated organisation and demonstrable cyber defensive and offensive capabilities.

Endnotes

1. The rise of Cyber Weapons and Related Impact on cyberspace. Resources.infosecinstitute.com dated Oct 5,2012

2. Stuxnet: A malware said to have been created under a special programme, "Operation Olympic Games" jointly by the USA and Israel and used to damage the centrifuges at the Natanz nuclear facility of Iran.

3. What is a cyber weapon ? Paolo Passeri, April 22, 2012. Hackmageddon.com

4. Ibid, endnote 1.

5. Ibid.

6. Generations of Cyber Weapons. Selil.com/archives/3152, July 10, 2012

7. Estonia : In the spring of 2007, a cyber attack on Estonia blocked websites and paralysed the country's entire internet infrastructure.

8. Georgia: In August 2008, Russian planners tightly integrated cyber operations with the kinetic, diplomatic and strategic communication operations and achieved cyber disruption at the moments they needed those disruptions to occur.

9. Kaspersky Security Bulletin 2012 : Cyber Weapons

10. Wiper: One of the world's most powerful data snatching cyber espionage virus targeting computers in Iran, Israel and middle eastern countries. The worm has allegedly been used in state sponsored espionage.

11. Gauss : A new cyber surveillance virus found in West Asia that can spy on banking transactions and steal log-in information from social net working sites, e-mails and instant messages. Discovered as part of United Nation backed effort to reduce the global impact of cyber weapons.

12. Duqu: A new virus which can leak data from any computer it infects – particularly leaking data from power plants, oil refineries and pipe lines. Data acquired by this virus is used for creating new cyber weapons.

13. miniFlame: A small and highly flexible malicious programme designed to steal data and control infected systems during targeted cyber espionage operations. It is a high precision surgical attack targeted cyber weapon used as the second wave of cyber attack.

14. Cyber weapons: Leveling the International Playing Field. Ross M Rustici

15. Ibid, endnote 3.

16. Ibid.

17. Global Cyber Deterrence- East West Institute. www.ewi.info/system/files/CyberDeterrence.pdf Cyber Weapons by P Paganini, April 3, 2012, Hacker News

18. Ibid.