CYBER WARFARE

Author: Harini S, V year of B.B.A.,LL.B.(Hons.) from SASTRA University

Abstract

It is hardly an overstatement to say that the advent and global expansion of the Internet may prove to become the fastest and most powerful technological revolution in the history of mankind. In just 15 years, the number of individuals actively using the Internet has skyrocketed from an estimated 16 million in 1995 to more than 1.7 billion in late 2010.1 Today, states, non-state communities, business, academia and individuals have become interconnected and interdependent to a point never imaginable before. At the same time, military reliance on computer systems and networks has increased exponentially, thus opening a "fifth" domain of war-fighting next to the traditionally recognized domains of land, sea, air and outer space. This trend raises the question to what extent can existing international law be transposed to the cyber domain. It is the purpose of this paper to provide an overview: (a) of the potential restraints imposed on cyberwarfare by existing international law, (b) of the most important difficulties and controversies raised in the interpretation and application of international law to cyberwarfare, and (c) of the potential humanitarian impacts of cyber warfare.

Introduction

The use of cyber operations during armed conflicts is a reality. While only a few States have publicly acknowledged using such operations, an increasing number of States are developing military cyber capabilities, and their use is likely to increase in future. Moreover, there have been significant technological advances in offensive cyber capabilities: in recent years, cyber operations have shown that they can seriously affect civilian infrastructure and might result in human harm.

In line with its mission and mandate, the International Committee of the Red Cross (ICRC) is primarily concerned with cyber operations used as means and methods of warfare during an

armed conflict and the protection that international humanitarian law (IHL) affords against their effects.

During armed conflict, cyber operations have been used in support of or alongside kinetic operations. The use of cyber operations may offer alternatives that other means or methods of warfare do not, but it also carries risks. On the one hand, cyber operations have the potential to enable parties to armed conflicts to achieve their military aims without harming civilians or causing physical damage to civilian infrastructure. On the other hand, recent cyber operations which have been mostly conducted outside the context of armed conflict show that sophisticated actors have developed the capability to disrupt the provision of essential services to the civilian population.

By means of cyber operations, it is possible for belligerents to infiltrate a system and collect, exhilarate, modify, encrypt, or destroy data. It is also possible to trigger, alter or otherwise manipulate processes controlled by a compromised computer system. A variety of "targets" in the real world can be disrupted, altered or damaged, such as industries, infrastructures, telecommunications, transport, or governmental and financial systems. Based on discussions with experts from all parts of the world and its own research, the ICRC is particularly concerned about the potential human cost of cyber operations on critical civilian infrastructure, including health infrastructure.

In recent years, cyber-attacks have exposed the vulnerability of essential services. They are reportedly becoming more frequent and their severity is increasing more rapidly than experts had anticipated. Moreover, much is unknown with respect to the most sophisticated cyber capabilities and tools that have been or are being developed, how technology may evolve, and the extent to which the use of cyber operations during armed conflicts might be different from the trends observed so far.

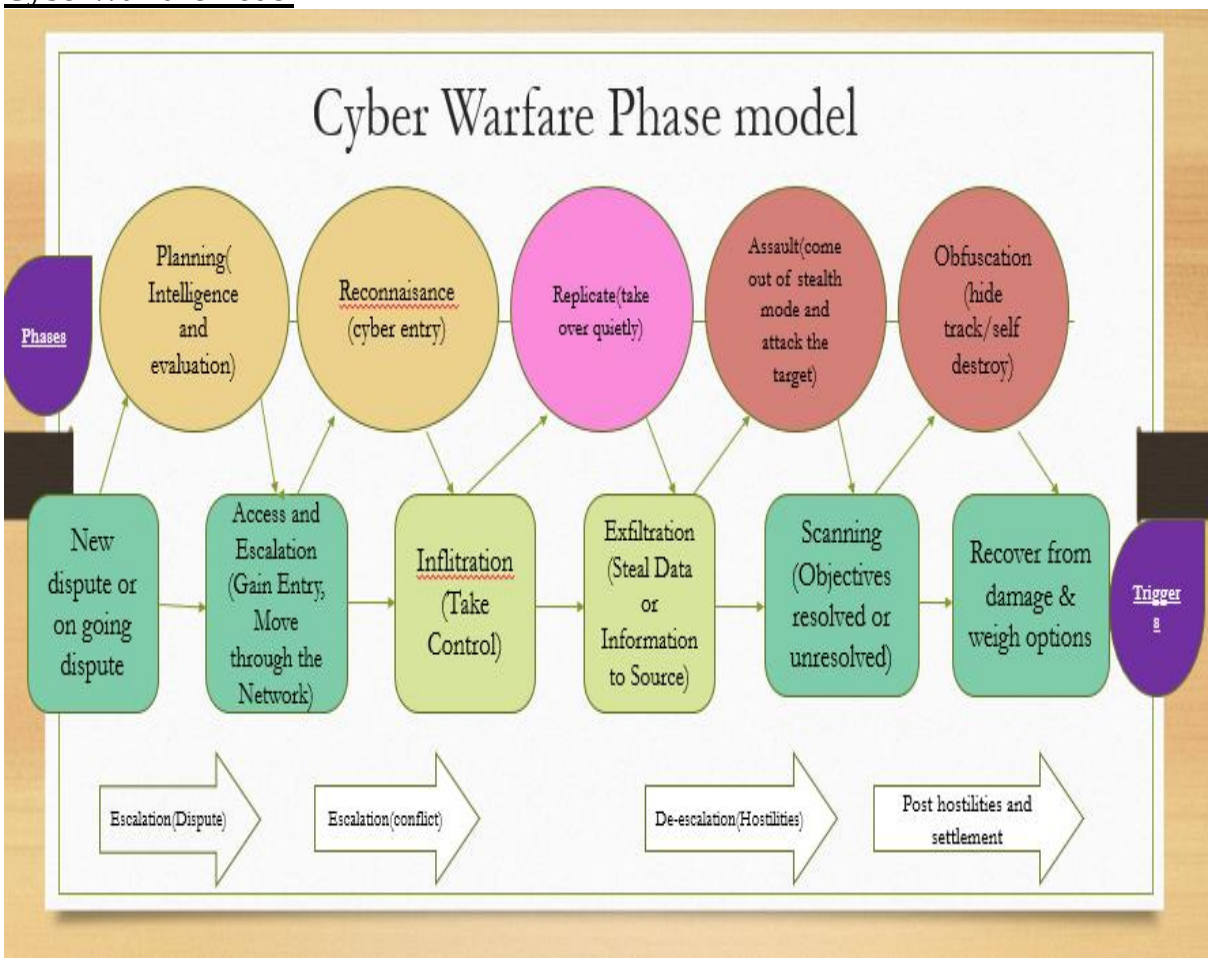
Cyber operations entail a risk for escalation and related human harm for the simple reason that it may be difficult for the targeted party to know whether the attacker's aim is intelligence collection or more harmful effects. The target may thereby react with greater force than necessary out of anticipation of a worst-case scenario. Cyber tools also proliferate in a unique

manner. Once used, they can be repurposed and widely used by actors other than the one that developed or used.

International Law

According to article 2(4) of the UN Charter, "[a]ll Members [of the United Nations] shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations". Although the ordinary meaning of "force" is clearly broad enough to include both armed and unarmed forms of coercion,the overwhelming majority of commentators today consider the term "force" in article 2(4) of the UN Charter as practically synonymous to "armed" or "military" force. The ICJ, prohibits "to any use of force, regardless of the weapons employed". The Tallinn Manual identifies international law principles applicable to cyber warfare and enumerates ninety-five 'black-letter rules' governing such conflicts. This includes the use of cyber operations as an offensive or defensive tool conspicuous examples: cyber operations manipulating target computers systems so as to cause a meltdown in a nuclear power station or disabling a busy airport's air traffic control.

CyberWarfareModel



Timeline of Cyber war

Cyber Warfare is mission focused and the success is largely based on the superiority and sophistication of technology used in the planning phase. The criteria for the mission have to be defined in this phase. Compared to kinetic warfare, where a dispute is the basis for the warfare that escalates to become a conflict, cyber-warfare could originate with or without a conflict. Cyber-Warfare incidents from the past were researched for this thesis, included are a number of prominent and publicized Cyber-warfare cases that involving states.

The Deception Program:

When considering past cases of cyber terrorist attacks arguably the most notorious attacks was during the cold war in 1982, the CIA allegedly found a way to disrupt the operation of a Siberian gas pipeline to the Soviet without using traditional explosive devices such as missiles or bombs. Instead, they caused the Siberian gas pipeline to explode using a portion of a code in the computer system that controls its operation in what they tagged as “logic bomb.” When many people think of Siberia, they imagine freezing temperatures and enormous wasteland; however, Siberia contains a huge supply for natural gas. Conversely, getting this natural gas from the far reaches of the Russian northwest into Moscow posed problematic. The Soviet Union had the skills and knowledge to engineer a solution, although a manual operation would stand too strenuous. Furthermore the Soviet Union did not have the computing expertise to automate more of the processes. Consequently, the KGB (Committee for State Security) sent an operative to a Canadian company to steal the software in order to create the pipeline.The Euro-Siberian gas pipeline under construction, officially called "Rossiya No. 6" by the Soviet Union, was part of a large-capacity, long- distance network originating from the natural gas fields of the Taz Peninsula, in the Western Siberian region of Yamal, north of the Arctic Circle. Rossia No. 6 was to ultimately consist of a double 56-inch wide, 4451 kilometer long pipeline joining Urengoi field to the border town of Uzhgorod, where it is to be connected with the MEGAL pipeline over Czechoslovakia to the West European gas network.

Kosovo War

Tensions on Kosovo started in 1980s with discrimination of both ethnic groups where they were minority. In the mid-1990s, UCK was created, an Albanian militant force.. In 1998, major attack on Yugoslav police and army had started. After the NATO air campaign started, many people in Serbia formed Cyber groups and attacked NATO websites, servers or any infrastructure of NATO or countries that were part of NATO and are exposed on the internet. Modern Black Hand was a hacker group that was quite successful in their attacks. Firstly they started with Kosovo and Albanian websites that spread propaganda. They took down and defaced websites like kosova.com and Swiss

based Albanian news portals zik.com. After NATO bombed China embassy in Belgrade, the things became serious. NATO server was shot down because of denial of service attacks over it. US Navy website was hacked by the Russians. NATO mail servers were non-functional because they were daily they were receiving more than 20 000 emails with malware in attachment. After these 78 intense days conflict ended. With it cyber war ended as well.

Operation Cast Lead

Israel began a military assault on Hamas's infrastructure in Gaza on December 27, 2008, called "Operation Cast Lead." A cyber backlash by Arabic hackers targeted thousands of Israeli government and civilian Websites. When the government of Israel publicly threatened to sever all Internet and other telecommunications into and out of Gaza they crossed a line in the sand. As the former dictator of Egypt, Mubarak learned the hard way - we are ANONYMOUS and NO ONE shuts down the Internet on our watch. To the IDF and government of Israel we issue you this warning only once. Do NOT shut down the Internet into the "Occupied Territories", and cease and desist from your terror upon the innocent people of Palestine or you will know the full and unbridled wrath of Anonymous. This is the first instance of a voluntary botnet ("Help Israel Win") used in a Cyber conflict where individuals voluntarily passed control of their own computers to the botnet host server. Hackers in Gaza have leaked 35,000 credit card numbers of "Zionist civilians" as a "response from the lions to the aggression of the Jews." On 16th november at the Arab hacker group Oujda-Tech Group defaced Israeli websites (non-government) to protest Gaza missile strikes. Later Hamas-friendly websites including ".qassam.ps"and "hamasinfo.net" went down.Unlike other instances of cyber conflicts (Chechnya, Estonia, Lithuania,Georgia, India), this conflict involved both State (Israel and possibly Iran) and Non-State hackers.

DuQu (1.0 & 2.0)

DuQu, was an espionage tool. Duqu looks for information that could be useful in attacking industrial control systems and reported the sensitive data back to the mother ships. DuQu was found to be a child of Stuxnet since its' executables seem to have been developed after Stuxnet because they use the same Stuxnet source code. Central to DuQu was its' ability to capture keystrokes and computer system and network information. Like Stuxnet, Duqu attacks Microsoft Windows systems using a zero-day vulnerability. This spy virus was discovered and linked to several countries, Duqu 1.0 was first installed in 2011 and updated to duku 2.0, it affected over 400 million computers. There were three computers in different hotels that hosted Iran Nuclear talks were targeted by the Duku Virus. Duqu got its name from the prefix "~DQ" it gives to the names of files it creates. This was an incredibly sophisticated virus with 100 modules; each module could do a task. For example there was a video module, a Wifi module, a phone module etc. Each module collects information from its task. It affected over 400 million computers.

The Eastern Railway Defacement

On December 24, 2008, the Whackerz Pakistan Cr3w defaced India's Eastern Railway website with the following announcement: "Cyber war has been declared on Indian cyberspace by Whackerz-Pakistan." The Hack was performed against the action of Pakistani troops, entered Indian territory along the Line of Control in the Poonch sector in Jammu and Kashmir and ambushed a patrol killing five Indian soldiers. The Indian group Guards of Hindustan hacked into the Oil and Gas. Regularity Authority of Pakistan website and placed their organization's logo and the Indian national symbol on the site. The Pakistani organization Pakistan Cyber Army soon answered the attack by hacking the websites of the Indian Institute of Remote Sensing, the Centre for Transportation Research and Management, the Kendriya Vidyalaya of Ratlam and the Oil and Natural Gas Corporation of India. Following this a Pakistani group calling itself Zombie_KSA hacked and defaced the Criminal Investigation Department website, a

cybersecurity unit of the Andhra Pradesh state police, and removed the site's information about 10 most wanted criminals. Soon after the Eastern railways attack, another Pakistani group, which is yet to be identified, hacked an Indian television station and State Bank of India. The website of Bank of India, one of the largest banks in India, was completely down on Christmas Eve.

Shamoon Attack

Shamoon, also known as Disttrack, is a modular computer virus discovered by Seculert in 2012, targeting recent NT kernel-based versions of Microsoft Windows. The virus has been used for cyber espionage in the energy sector. Symantec Kaspersky Lab, and Seculert announced its discovery on 16 August 2012. Similarities have been highlighted by Kaspersky Lab and Seculert between Shamoon and other malware. The Shamoon attack although inflicted on a Saudi Corporation, it is being discussed here as a cyber-warfare case due to its signature of a state sponsored attack. Saudi Aramco is state owned and the attack erased data on three-quarters of its corporate PCs – documents, spreadsheets, e-mails, files – replacing all of it with an image of a burning American flag. Although the US Intelligence pointed to Iran as the perpetrator, there is no specific evidence to support that. TechRadar summarize the virus as a "dropper, wiper and reporter"

Russian Hackers Tracking Ukrainian Artillery

The motive for the intelligence would have likely been used to strike against the artillery in support of Russia-backed separatists in eastern Ukraine. The malware was able to retrieve communications and some locational data from infected devices, intelligence that would have likely been used to strike against the artillery in support of pro-Russian separatists fighting in eastern Ukraine, the report from cyber security firm Crowd Strike found. From late 2014 and through 2016, FANCY BEAR X-Agent implant was covertly distributed on Ukrainian military forums within a legitimate

Android application developed by an Ukrainian artillery officer. A developer App internally developed in the Ukrainian military is installed which had some 9000 users, reduced the time to fire the D-30 from minutes to seconds. Use of trojanized application was later found in the military application. Successful deployment of the FANCY BEAR malware within this application may have facilitated reconnaissance against Ukrainian troops. The ability of this malware to retrieve communications and gross

Locational data from an infected device made it an attractive way to identify the general location of Ukrainian artillery forces and engage them. The hacking group, known commonly as Fancy Bear or APT 28, is believed by U.S. intelligence officials to work primarily on behalf of the GRU, Russia's military intelligence agency. The weapon (malware) was hidden in an Android application used by the Military for quick deployment of a war weapon. DDoS and targeted intrusions in media, financial and political entities in Ukraine. Minski Ceasefire signed but malicious app observed in distribution on Forums.

Solar Wind Attack

Hackers used the operation against SolarWinds, a major US information technology (IT) company, to spy on private companies – such as FireEye, the elite cyber security firm that exposed the breach– as well as US government agencies, including the Department of Homeland Security and Treasury Department. While the Stuxnet operation showed us that, when attackers have sufficient means, it is very challenging to resist thoroughly planned and targeted operations (including, in that case, targeting air-gapped systems), the SolarWinds hack has shown us the massive scale and reach that an adversary can achieve by targeting digital supply chain components that are widely adopted, in this case the security of the software supply chain. The SolarWinds hack was an operation that was ongoing during most of 2020. It was revealed and widely reported in the media at the end of December 2020. It primarily targeted US government agencies and private companies, including the security company that exposed the hack, FireEye. The European Commission confirmed on 13 April 2021 that

fourteen institutions, bodies or agencies of the European Union used SolarWinds/Orion. Six of them were confirmed to have been affected by the hack. The operation is believed by the US intelligence community to be of Russian origin and has been formally attributed by the United States to the Russian Federation. Russia has denied any involvement in the operation. The SolarWinds hack was a "supply chain" type of operation in that it vectored malware through updates of the Orion software product of Solar Winds, which is widely used to manage IT resources along business supply chains. The malicious code creates a backdoor to customers' systems, which enables hackers to install more malware and to spy on their victims. Even at the time of writing, months after the hack was revealed, the full extent of the damage cannot yet be completely mapped. Indeed, according to the CEO of FireEye, Kevin Mandia, the hackers prioritized stealth above all else. It has been estimated that recovering from the Solar Winds hack could take up to eighteen months. It has also been reported that while the Solar Winds hack primarily targeted in-house infrastructure, the breach has morphed into a multidimensional assault on key computing infrastructure, including cloud services". Indeed, it appears that breaching large-scale cloud providers, such as Microsoft, was a primary objective of the operation, and this in turn exposed the customers of such providers to data breaches. Microsoft's president, Brad Smith, has suggested that more than 80% of the victims subsequently targeted were non-government organizations. Microsoft source code was also accessed, and it appears that SolarWinds hackers also accessed the US Justice Department's Microsoft Office 365 email environment.

WannaCry

The WannaCry ransomware attack was a worldwide cyber-attack by the WannaCry ransomware cryptoworm, which targets computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. WannaCry spread across local networks and the Internet to systems that have not been updated with recent security updates, to directly infect any exposed systems. To do so it used the Eternal Blue exploit developed by the U.S. National Security Agency (NSA), which was released by "The Shadow Brokers" two months

before. The attack started on Friday, 12 May 2017, and has been described as unprecedented in scale, infecting more than 230,000 computers in over 150 countries. Parts of Britain's National Health Service (NHS), Spain's Telefónica, FedEx and Deutsche Bahn were hit, along with many other countries and companies worldwide. The WannaCry malware is indirectly loaded and is not directly exposed to the disk. Thus, obfuscating it from anti-virus software analysis.

Cyber Manthan

India Future Foundation (IFF) and United Service Institution (USI) of India held a seminar "Cyber Manthan – Cyber Warfare in the era of Hybrid Warfare and India's Readiness." The observations made in the seminar may be summarized as:

To have a Digital Armed Force so that we can be in a position where we can act and react on any kind of cyber threat, espionage or even war. The Department of Telecommunication (DOT) is working on creating the Computer Emergency Response Team (CERT).Difference between a conventional/traditional war and a cyber-war is that Firepower and mobility remain in the physical space whereas information has shifted in cyberspace.Technology companies has a responsibility to protect the digital systems that underpin the social fabric of our society and promote safe, secure computing environments for every person, wherever they are located.India has always adopted a defensive mode. We need to have those offensive capabilities, as well, to defend ourselves in the event of a cyber war. It should be able to defend its sovereignty in the event of a cyber war.

THE INDIAN APPROACH

India's current approach adopts a reactionary "whack-a-mole" approach rather than creating deterrence. In addition to such a deterrent strategy, India must harden its targets and aim primarily at state-sponsored attacks. India is positioned amongst third-tier countries on a spectrum of cyber warfare capabilities. This position has been allocated based on the strength of the country's digital economies and the

maturity of its intelligence and security functions to how well cyber facilities were integrated with military operations. India is in the final stages of clearing a National Cyber security Strategy, 2020 and has a National Cyber security Policy, 2013. These, however, do not discuss armed conflict or active espionage.

In May 2021, India set up its Defence Cyber Agency (DCA). The DCA works closely with National Technological Research Organisation, India's Research and Analysis Wing, National Security Council, and the Defence Research and Development Organisation. In these capacities, India only addresses cyber security attacks and not cyber warfare. That is, the concern currently is over the importance of civil and military data rather than the use of technology in actual warfare. India needs to employ a strategy that discusses two philosophies of thought: A cyber strategy for offence and defence. India should combine the two in a strategy focusing on deterrence. To allow for this, policies aimed at improving a nation's cyber security would need to increase the amount of information-sharing and real-time threat detection among governments, industry, and academia. Governments, industry, and academia would need to share information about the latest attacks, malware signatures, and vulnerabilities aside from an offensive strategy that would focus on intimidation and expansion of peace-time cyber capabilities.

An effective cyber warfare strategy would discuss developing and employing strategic capability to work in cyberspace, integrated, and coordinated with the other operational domains. It will have to lay down a specific action plan to respond primarily to state-sponsored attacks that threaten national security.

International Humanitarian Law

The conclusion that IHL applies to cyber operations during armed conflict finds further support in the views expressed by the ICJ. In its Advisory Opinion on the legality of the threat or use of nuclear weapons, the Court recalled that the established principles and rules of humanitarian law applicable in armed conflict apply "to all

forms of warfare and to all kinds of weapons", including "those of the future" .Increasing number of States and **international organizations** have publicly asserted that IHL applies to cyber operations during armed conflict. This includes, for example, the **EU and NATO**. Moreover, the Paris Call for Trust and Security in Cyberspace (supported by seventy-eight States as of April 2020) has reaffirmed the applicability of IHL to cyber operations during armed conflict.The heads of government of the **54 Commonwealth States** have committed to move forward discussions on applicable international humanitarian law, applies in cyberspace in all its aspects. The heart of IHL lies the principle of distinction, which requires belligerent parties to always distinguish between legitimate military targets and persons and objects protected against attack, and to direct their operations only against the former.The principle of distinction prohibits cyber attacks directed against civilian objects – such as hospitals, critical civilian infrastructure and civilian public administrations.Article 49 of Additional Protocol I defines attacks as 'acts of violence against the adversary, whether in offence or in defence'.The question of how widely or narrowly the notion of 'attack' is interpreted with regard to cyber operations is therefore essential for the applicability of these rules.

While the principle of necessity defines the margins of lawful self-defence in terms of what is objectively necessary to avert or repel an armed attack, the principle of proportionality determines to what extent the harm to be prevented justifies the harm done by the defensive action. The principle of proportionality prohibits attacks – including cyber attacks – which may be expected to cause excessive incidental harm to civilians and civilian infrastructure. Especially in cyberspace, incidental harm risk being widespread and transcend national borders.

Challenges

Cyber space is challenging the way states or other actors are able to conduct hostilities or able to do hostile act on another state without military forces. A disequilibrium is created on how to connect military forces with non military attacks, military lawyers are not much familiar with digital challenges and cyber war which is generally dealt by economic and foreign affairs ministers. Difficulty in defining what could be termed as use of force for state to qualify cyber-attack and what would amount to force. Geographical scope is a major challenge since it is difficult to differentiate between civilian and combatants.

Conclusion

To regulate cyber attacks the threshold should be low as compared to armed conflicts to cover most cyber operations under cyber-attack. States should address the concerns posed by the increasing integration of cyber operations with other military capabilities during armed conflicts. Existing processes must be adapted to the cyber context to ensure compliance with international humanitarian law (IHL). States must put in place measures to mitigate the risk of civilian harm posed by the use of military cyber capabilities (‘active precautions’). States must put in place measures to protect the civilian population against the dangers resulting from military cyber operations (‘passive precautions’). States should address the risk of civilian harm posed by information operations and grey-zone operations. States and other stakeholders should continue to develop their understanding of the risk of civilian harm posed by new technologies and work towards mitigating those risks