CYBER WARFARE – A NON-TRADITIONAL NOTION OF SECURITY

Akash Yogendra Singh, BBA LLB, New Law College, Pune, Bharati Vidyapeeth (Deemed to be University), Pune.

Ms. Shivangi Sinha, Assistant Professor, New Law College, Pune, Bharati Vidyapeeth (Deemed to be University), Pune.

ABSTRACT

"The Supreme art of war of is to subdue enemy without fighting" said by Sun Tzu.

As technologies like artificial intelligence and quantum computing continue to advance, how will they reshape the landscape of cyber warfare, and what implications do these advancements hold for the future of conflict in the digital age? This research paper sparks further inquiry into the multifaceted realm of cyber warfare. The objective of this paper is to study past and current cyber conflicts, analyze them to reflect the probable future threats and to suggest measures to mitigate damages. The importance of learning the modus operandi for a comprehensive strategic preparedness by the nation is well highlighted in the study. Lastly, this paper also suggests some recommendations to nation states to strategize its cybersecurity plan as well as international community to reach an international convention.

Keywords: Cyberwarfare, Cyberspace, Strategic plan, Threats, International community, military, Cybersecurity.

INTRODUCTION

The traditional view of war has gone into paradigm shift emerging new landscape of threats. Advancements in technological arenas have created cyberspace as a medium of target to technologies. Possible cyber threats to financial institutions, military infrastructure, key public infrastructures like power, water, transport etc.

There is ongoing debate over how cyberwarfare should be defined, and no absolute definition is widely agreed upon. 'Cyberwarfare' is used in a broad context to denote interstate use of technological force within computer networks in which information is stored, shared, or communicated online[1]. According to this perspective, the notion of cyber warfare brings a new paradigm into military doctrine. Paulo Shakarian and colleagues put forward the following definition of "cyber war" in 2013, drawing on Clausewitz's definition of war: "War is the continuation of politics by other means". Cyber war is an extension of policy by actions taken in cyber space by state or nonstate actors that constitute a serious threat to a nation's security or are conducted in response to a perceived threat against a nation's security.[2]

CYBER SPACE

Cyberspace is a virtual environment created by the interconnectedness of computer systems and networks. It's a complex global network of communication channel that allows communication, sharing of data, conduct transactions and interact with any sources world-wide. Large domain of the cyberspace and easy access has made it a battleground for conflicts. A unique perspective about cyberspace is its borderless transcending all the geographical boundaries unlike the physical space. Such unique nature poses a special challenge for governance of the cyberspace, requiring cyberspace worldwide co-operations.

CYBERWARFARE

Cyberwarfare refers to use of digital technologies viz. tools, soft wares, information etc to conduct act of war and conflicts in the cyberspace domain. It can be carried out by government, military or other non-state entities. Some types of attacks that are prevalent, are malware attacks, Denial of Service attacks (DOS), Phishing, Advanced persistent threats (APTS). The attackers target critical Infrastructure, Military system, Government network, Private Sector. Attribution challenges that pose a threat to the cyberspace like masking of IP address, employs

[1] Cyber warfare: a multidisciplinary analysis. Green, James A., 1981-. London. 7 November 2016. ISBN 9780415787079.a

[2] Shakarian, Paulo; Shakarian, Jana; Ruef, Andrew (2013). *Introduction to cyber-warfare: a multidisciplinary approach*. Amsterdam: Morgan Kaufmann Publishers – Elsevier. p. 2.

proxies and hacking tools to using of brute forces to find loopholes to target the vulnerable are of the grave concerns. International efforts like Tallinn manual are of less significance as it lacks binding effect. Also, it's difficult to reach a consensus over such issues which every nation wants to exploit for its own interest and gain leverages especially the technologically advanced first world countries.

Dynamic nature of cyberspace with rapidly developing technology makes the space more vulnerable to attacks without a comprehensive legal framework. New methods and tools are constantly developed to increase owns interest and gain leverage over the free lawless, uncontrolled and unregulated cyberspace. This requires players of cyberspace or their governments to rapidly adapt to the dynamics of cyberspace.

If cyberspace continues to operate without a understanding between nations or a legal framework, it can pose threat of escalating tensions of military conflicts or may even prove to be trigger point of wars and conflicts. In absence of such legal framework providing for dispute mechanism through arbitration or mediation, countries may treat violation of their cyberspace as an attack and may or may not without conclusive proof declare war on the attacking nation. Retaliation of cyberattacks through brute physical force of the armed forces will result into loss of innocent life and massive destruction of property.

GLOBAL CONCERN

Technological advancements led to the emergence of cyber space which in turn created room for new strategies, possibilities, threats inter alia. Increasing media coverage made governments aware about the seriousness of the situation. The US President Barack Obama declared "Americas digital infrastructure as national asset" thereby including it in the definition of terrorism, sovereignty and territorial integrity. This declaration made clear that the United States of America reserves right to respond militarily in case of cyber-attack disproportionately using its military force. The US government in 2013 formed 'Cybercom' a division inside Pentagon for specific assignments relating to cyberwarfare.

The United Kingdom invested significantly in its National Cyber Security programme after its officials warned "lack of preparedness in Cyber warfare may cost the nation heavily". The NATO released Tallin Manual stating international laws are applicable to the domain of Cyberwarfare. It advised all the nations to legally operate in this new domain of fight. Above evidence makes it clear that issue of Cyber Warfare is a global concern of 21st century.

TALINN MANUAL

The Tallinn Manual identifies international law principles applicable to cyber-warfare and enumerates ninety-five "black-letter rules" governing such conflicts. Between 2009 and 2012, the Tallinn Manual was written at the invitation of the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence by an international group of approximately twenty experts. In April 2013, the manual was published by Cambridge University Press.[3]

In late 2009, the Cooperative Cyber Defence Centre of Excellence convened an international group of legal scholars and practitioners to draft a manual addressing the issue of how to interpret international law in the context of cyber operations and cyber-warfare[4]. As such, it was the first effort to analyse this topic comprehensively and authoritatively and to bring some degree of clarity to the associated complex legal issues[5].

Three organisations were represented by observers throughout the drafting process: NATO through its Allied Command Transformation due to the relationship of the NATO Cooperative Cyber Defence Centre of Excellence with NATO, the International Committee of the Red Cross because of its "guardian" role of international humanitarian law, and United States Cyber Command due to its ability to provide the perspective of an operationally mature entity[6].

CASE STUDY

To understand the growing landscape of cyberwarfare its crucial to understand the historical glimpses, following are the case views of major cyberwarfare cases that have surfaced in the past four decades,

1) MORRIS WORM (1988)

Hackers attacked public computer system in USA, considered as first public cyber-attack. However, no threats are present today as computers are immune to the Morris code. This attack inspired the generations of hackers to hack the public computers.

2) Operation Anarchist (1998)

The USA and UK hacked Israeli Air surveillance system under the operation, video footage

[3] "The Tallinn Manual". Ccdcoe.org. Archived from the original on 2013-04-24. Retrieved 2013-04-20.
[4] https://link.springer.com/chapter/10.1007/978-3-031-14264-2_3/last visited on 30/01/2024
[5] Schmitt, Michael N (Gen. ed.) (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. New York, United States of America: Cambridge University Press
[6] NATO – Topic: Centres of Excellence". Nato.int. 2012-07-30. Retrieved 2013-04-20.

of IAFs attack in middle east was released later which confirmed this cyber espionage by the state.

3) Operation Desert Storm (1992)

Before the Persian Gulf War, two teenagers Netherlands hacked US Department of Defence's new logistical system and gained control over it.

4) Operation Orchard (2007)

Israel carried out strikes on nuclear facilities In Syria using its electronic warfare capabilities. The IAF Electronic Warfare capabilities took over the Syrian Air defence system, feeder false Sky pictures for the entire period its fighter jets needed to cross and bomb the facilities.

5) Operation Dust Storm (2007)

A massive cyber-espionage campaign targeted the Japanese, South Korean, United States and European Companies for a period of 8 years. By 2015, the operation shifted its target towards critical government infrastructures like electricity grids, finance networks, communication lines transport networks among others.

6) Operation Buckshot Yankee

A Benign 3-year-old worm named "agent btz." Began targeting the US military network via thumb drives soon the major headache was resolved via encryption and strict guidelines to not use the thumb drives in storage of information.

7) Kosovo War

During the war, non-state actors attempted to disrupt the Military operations through hacking.

8) Operation Aurora

Series of cyber-attacks in 2009 to 2010, targeted major US companies like Google, Adobe, Juniper net etc. The US investigation concluded the Chinese involvements into it however China denied such reports.

9) 2011: Duqu

A computer worm in 2011 a relative version of the Stuxnet worm disrupted Iraq's nuclear program. It is alleged that the attack was sponsored by the Israeli efforts.

10) US 2016 Elections

The Russian actors associated with the Russian military intelligence (GRU), hacked email accounts and misused the social media to spread disinformation to serve its geopolitical interest. The impacts of such meddling were the deterioration in the US-Russian relationship, the USA sanctioned the Russia also expelled its diplomat causing further strains in the diplomatic relationship.

11) Russo-Ukrainian War

On its invasion in Ukraine in 2015 the Russian authorities carried out the Cyber-attacks on the Ukrainian power grid. Recently, in 2022 Russian Invasion of the Ukraine Russia carried out multiple cyber-attacks on the Ukrainian government sites.

THREAT ACTORS

NON-STATE ACTOR GROUP

They are Hacktivist and cyber-criminals usually funded by the State to serve their Economic, Political, Geopolitical Interests. Some of the groups are as follows,[7]

a) Anonymous

b) Lizard Squad

c) APT28 (Fancy Bear) / APT29 (Cozy Bear) a state sponsored espionage Russian state Interest.

d) FIN27 (Cabrakan)

e) AyyIldiz Tim a Turkish Nationalist cyber attacker.

f) Dark Overlord

g) The Equation Group alleged to have the links with the USA(NSA) carrying out the cyber espionage to gather the intelligence at its orders.

h) APT33 (Elfin) alleged to have links with the Iranians targets the aerospace and energy sectors primarily located in Israel.

STATE ACTOR GROUP

The State engages in the cyber warfare activities for the intelligence, strategic advances and

[7] Gazula, M.B., 2017. Cyber warfare conflict analysis and case studies (Doctoral dissertation, Massachusetts Institute of Technology).

disruptive purpose among others.

a) USA – The NSA and its cyber command (USCYBERCOM). The advanced capabilities to carry out the cyber espionage, intelligence gathering and cyber operations among others.

b) Russia – GRU and its Federal Security Service (FSB) are the agency cyber espionage and Influence Operations in its political Interests. APT28/APT29 are state associated groups.

c) China – The PLA UNIT 61398 along with the Ministry of State (MSS) targets the Intellectual Property Rights of various western companies for cloning their product manufacturing in their country. Also, it was alleged by the USA for tapping the privileged diplomatic communications through the APT 10/41 (the Chinese associated threat groups)

d) North Korea – Reconnaissance General Bureau (RGB) and financial gain (Wanna Cry) ransomware.

e) Iran – Islamic revolutionary guard corps (IRGC), Ministry of Intelligence and security (MOIS) APT33 targets critical infrastructure of Israel.

f) Israel – Unit 8200 (Israel Intel corps) advanced cyber capability focus intelligence gather and on security operations.

PROBABLE THREATS

Prospect of cyber-attacks voiced across International Community made threats of the weaponry system visible. Assaults aimed at sabotaging and incapacitating the systems, computers, programs that controls weaponry typically through malwares and viruses infiltrate to gain leverages. Such remote access capabilities of attackers provide with the leverages to self-destruct missiles, disable defence mechanisms and may in turn have catastrophic ramifications. Hacked weapons may fire at the instance of the attackers may prove to be disastrous.

Another aspect of the probable threat is of targeting the critical infrastructure. Cyber assailants' assault on strategic corridors, communication channels, logistics network Inter alia may prove a to strategic defeat for the target nation. Transportation routes for military and defence supply movement are critical classified strategically crucial information, whose access may give attackers a strategic leverage.

Other Infrastructures of public importance like highways, railways, airports are dependent on their high technologies for its functioning and operations. As increasing technological dependence may invite risks of cyber threats is a major issue of concern.

Hypothetical situations of cyber strikes on vital transport hub or a power grid system is past historical events as happened in the Ukraine Russian war pose serios consequences like significant transport congestions and power supply shortages respectively. Above all challenges, fundamental responsibilities of the government to protect its Sovereignty and Integrity and maintaining security of state might be questioned.

Another Hypothetical situation might be an attack on "Just in Time" logistics system which can't be underestimated as its based on the accurate timing, which if compromised can be disruptive for the entire supply chain movement.

MITIGATION

A comprehensive cyber strategy policy of a nation is required to protect and maintain the integrity of its cyberspace. Also, to gain strategic leverage in event of the cyberwarfare. Some measures of mitigation that may be part the above document are as follows,

1) Cyberthreat Intelligence

To counter cyber threats nations must share cyber threat intelligence with their allies and partners through cooperative agreements like MOU. Nations also must cooperate with the Cybersecurity organisations and Intelligence agencies to have expert reliance over the project of their cyber space to avoid any probable attacks. Collaborative attempts may further extend to threat hunting. Threat hunting is a concept wherein nations invite individuals and organisations to actively scout and attack their systems by brute forces to check vulnerabilities present in their systems. Such attempts indicate the robustness of the cyber security system towards cyber threats over its system and networks. Such techniques access and neutralize the risks before the actual damage. USCYBERCOM carries such practices withs its allies so as China and Russia cooperate to eliminate such threats present in their systems.

2) Artificial Intelligence

Use of AI/ML algorithms to recognise unusual pattern of network system instantaneously to indicate probable future risks is another mitigation measure to tackle cyberthreats eligible to be part of the document. As the matter of fact, the US Armed

Forces use AI and cybersecurity tools to identify and resolve the potential threats. Russia deploying state of the art technology during cyberwarfare reflects its advanced possession of those. China has reportedly solid comprehensive defensive and offensive cyberwarfare strategic document that protects and guides its interests globally.

3) Command Cyberoperations

India is the classic and recent examples of establishing in the year 2023 a separate command within the Indian Army with the support wings from multi public private sectors to meet its cyberwarfare operational readiness needs. A need for such command aroused in 2020 when several official apprised the importance of having a strategy for future cyberwarfare and conflicts as it can't be ignored in the wake of China which has Cyber offensive warfare strategy. This Unit has been operationalised, several niche technologies have been integrated viz. swarm drones, loitering weapon system, anti-drone gears etc.

4) Cybersecurity strategy

Strategy of cyberwarfare and conflicts shall be the part of the whole defence policy of the Nations in wake of changing modern warfare landscape. India has significantly progressed since 2020 framing and adopting its cyberwarfare strategy to combat data breaches, incursions of malwares and viruses in the public computers to gain access to Information's. The Indian government created a national threat of intelligence Exchange to develop malware responsibilities, conducting baseline audits, organizing awareness events like "Cyber weeks".

CONCLUSION

Cyberwarfare transcends conventional boundaries by operating in the intangible realm of cyberspace where battles are fought with Bits/Bytes/Viruses/Malwares than real bullets and bombs.

Following recommendations are of consideration for Nations to secure a defensive position against the threats of cyberattacks and warfare.

1) Nations must maintain a strategic document inclusive of its real position in case of cyberattacks and its current position of readiness for cyberwarfare. The cumulative assessment of such position will help to plan a strategy and device a future to secure a comprehensive strategic document.

2) A comprehensive national cybersecurity strategy may not be enough given the dynamic nature of the cyberspace. Nations must continuously assess its position and world dynamic to amend the strategies.

3) Cybersecurity demands robust defence mechanism, international collaborations and skilled cybersecurity professional to support the defence policy and its execution. An executive professional body part of the relevant departments of the ministry under the government will support planning and execution of the strategy. Also, the professional body may time to time advice the government regarding steps to be taken in this regard.

Following recommendations are of consideration for international community to secure a defensive position against the threats of cyberattacks and warfare.

1) Cyberwarfare fought in Cyberspace can't just be between Nations as same cyberspace is shared by the whole world. Thus, its assured that every nation will feel the impact of such conflicts which may in turn provoke countries to react by using cyberattacks as a retaliatory countermeasure against the rival nations. Thus, it becomes of vital importance that world community share such concerns and cooperative with each other through mutual understanding.

2) Being a Non-traditional notion of security blurs state and non-state actors capable of carrying cyberattacks. A serious concern that such attacks by non-state actors for committing economic and financial crime worldwide can't be ruled out. This creates a need for at least an international consensus that Nations won't allow use of cyber-attacks on other Nations by non-state actors and would penalize them in accordance with law of their Land.

3) A step towards creation of an independent agency to check, control and regulate such cyber-attacks by nations or non-state actors at their behest.

   Such department maybe part of the United Nations. If proved that parties violated the agreements, of which they are signatory the force of UN like sanctions may be slammed for such violative action. Such agreement which regulates, and controls act of cyber threats and attacks providing preventive, retributive and prohibitive actions for its violation by the independent agency may be named as "International treaty on Cybersecurity".

However, it's unlikely that technologically advanced countries would be signatory to such agreements seeing their own geopolitical interest. Ultimately its unto world leaders to decide on this and highlight this issue on international stage by organizing summits, conferences and dialogues to create an international platform of discussion on such Issues is pressing priority.