How India Will Win Cyber War- A Mini Review

Dr. Kanchan Mishra

Associate Professor, Department of Defence and Strategic Studies, V.S.S.D. College, Kanpur, Uttar Pradesh, India

ABSTRACT: Cyber power is slowly becoming the new value addition to a country's strength. We have been witnessing increased cases of espionage, cyber warfare, bot attacks and strong surveillance systems to monitor people. Given that India's border tensions with China have soured in recent times, how much power does India hold in cyberspace. Harvard University's National Cyber Power Index currently ranks China second in cyber power. Meanwhile, India is among one of the most cyber targeted countries in the world. And for China, India is the number one target. Nevertheless, the cyber domain does not lend itself to leaving the initiative to the adversary and remaining defensive as it has its costs, simply because exploitable opportunities to attack in the cyber domain are fleeting. Forces are kept in reserve to use in the future works for other domains and weapons systems, not the cyber domain. For instance, today's cyber tools cannot be used tomorrow. Preparing an attack takes time as it requires constant presence in adversary networks, involving surveillance, intelligence collection, and understanding the operational environment of a given network in cyberspace to deliver an attack.

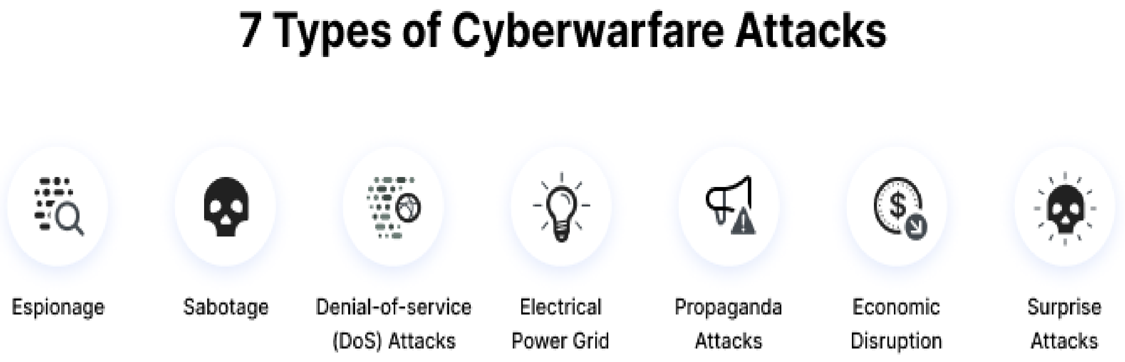
KEYWORDS: cyber, war, India, threat, country, cyberspace, networks, attack, tools

I. INTRODUCTION

Cybersecurity is a term almost all have heard about but can't exactly grasp the holistic meaning of. Cybersecurity refers to the technologies and processes made to protect networks and devices from attack, damage and/or unauthorised access.

A simple analogy; no cybersecurity is like having all of your valuables in a house that has no doors or windows. Indian firms, especially startups, are incorporating more of machine learning, artificial intelligence, data analytics and cloud computing in their everyday functions. All sectors face persistent and serious threats to India's security. Incidents can include data leaks, malware, terrorist-driven activity, the spread of extremism, illicit trafficking and radicalisation. Action needs to be taken.[1,2]

India has a solid and well-deserved reputation as one of the leaders in the global IT industry. This makes it all the more surprising that, until recently, Indian authorities had paid relatively little attention to introducing cyber technologies in the country's governance system and using them to combat cyber threats posed by hackers acting out of personal, economic, and political motives.



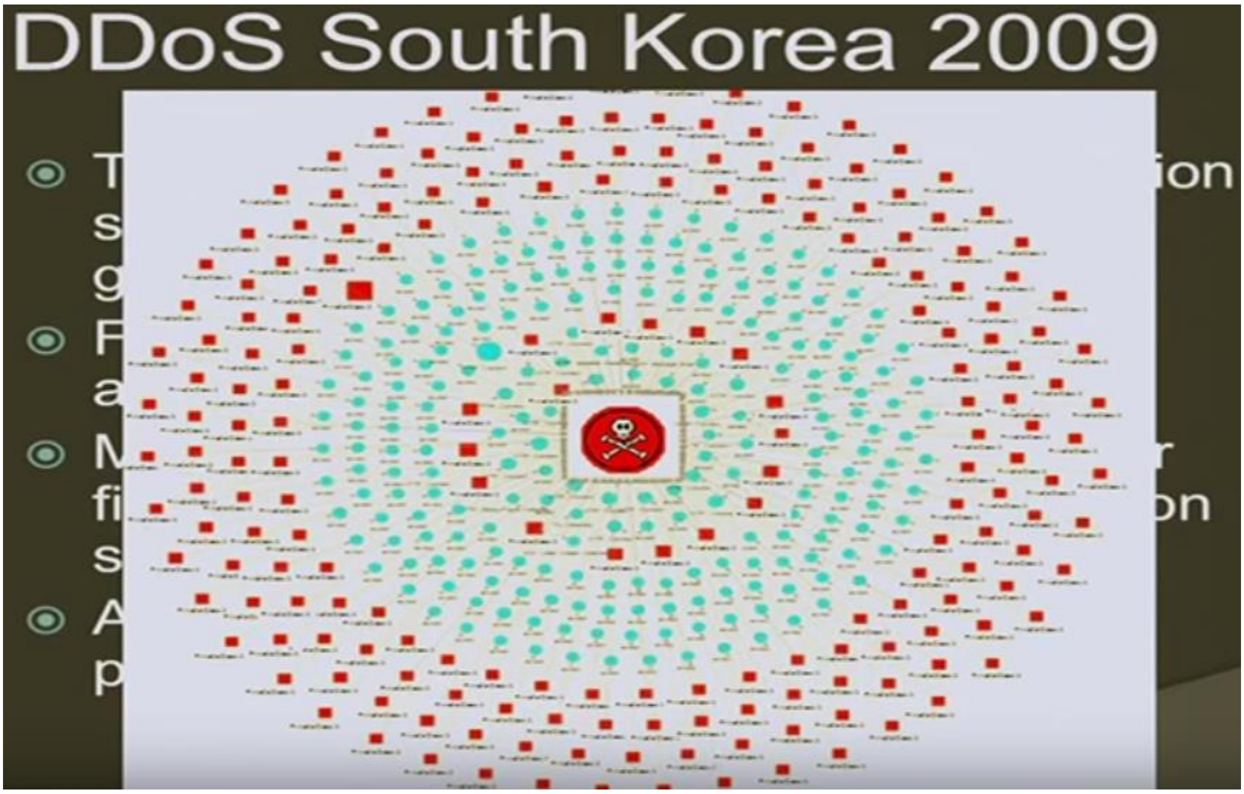
There are several reasons for this. The main factor is that India's leadership has underestimated the scale of confrontation in cyberspace, believing that other great powers limit themselves to negligible operations that aim to collect information at best.

Serious difficulties have emerged due to the specific features of Indian governance as such; it is characterized by an extreme abundance of red tape and inertia in areas that are not considered a priority. While India's bureaucracy exhibits its best qualities in priority areas such as ensuring the rapid concentration of resources, personnel mobilization and motivation, minimizing expenses, and a high level of oversight, thus making it possible to achieve outstanding successes with minimal expenses (India's space program is a prime example), areas believed to be of secondary importance are plagued by chronic problems.[3,4]

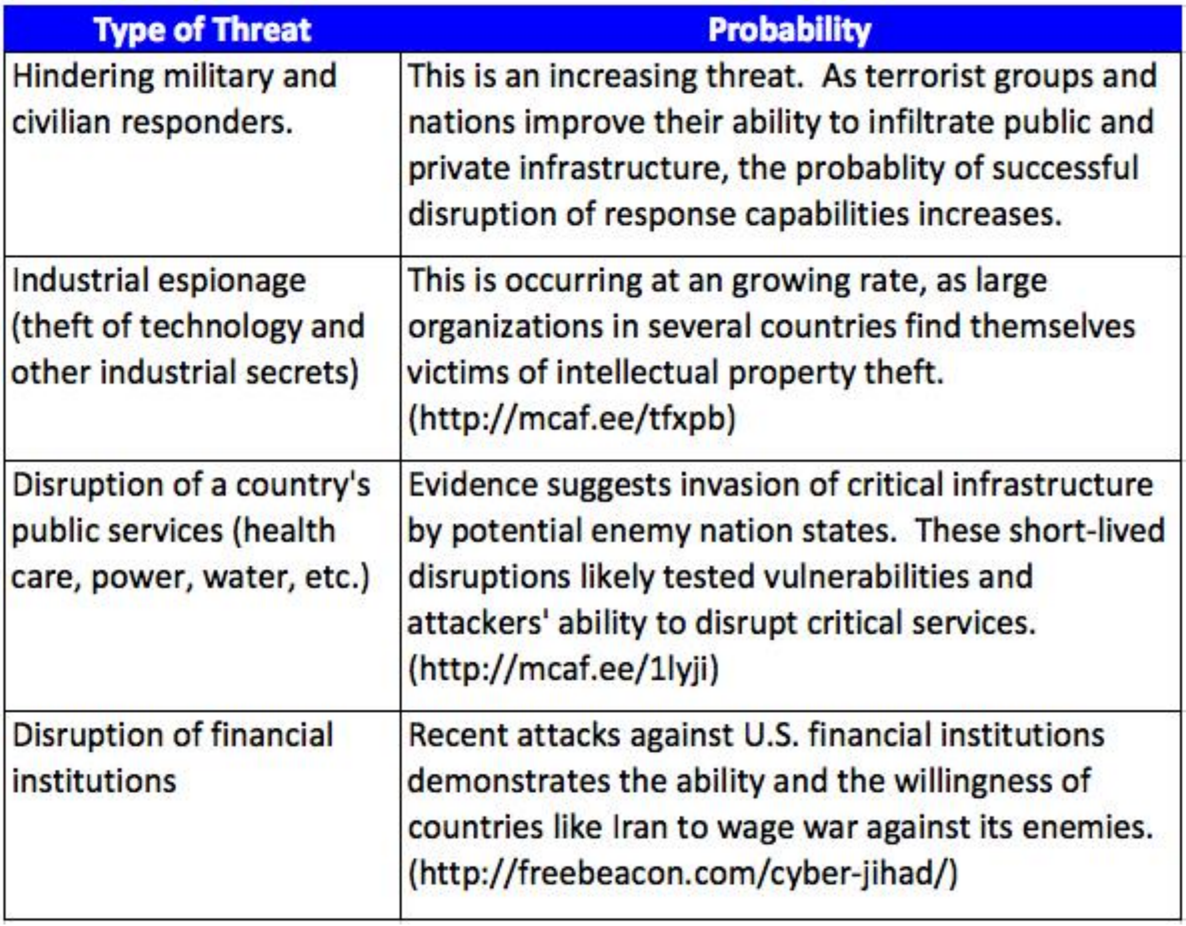
II. REVIEW

In July 2009, there were a series of coordinated denial of service attacks against major government, news media, and financial websites in South Korea and the United States. While many thought the attack was directed by North Korea, one researcher traced the attacks to the United Kingdom. Security researcher Chris Kubecka presented evidence multiple European Union and United Kingdom companies unwittingly helped attack South Korea due to a W32.Dozer infections, malware used in part of the attack. Some of the companies used in the attack were partially owned by several governments, further complicating attribution.

In July 2011, the South Korean company SK Communications was hacked, resulting in the theft of the personal details (including names, phone numbers, home and email addresses and resident registration numbers) of up to 35 million people. A trojaned software update was used to gain access to the SK Communications network. Links exist between this hack and other malicious activity and it is believed to be part of a broader, concerted hacking effort.



With ongoing tensions on the Korean Peninsula, South Korea's defense ministry stated that South Korea was going to improve cyber-defense strategies in hopes of preparing itself from possible cyber attacks. In March 2013, South Korea's major banks – Shinhan Bank, Woori Bank and NongHyup Bank – as well as many broadcasting stations – KBS, YTN and MBC – were hacked and more than 30,000 computers were affected; it is one of the biggest attacks South Korea has faced in years. Although it remains uncertain as to who was involved in this incident, there has been immediate assertions that North Korea is connected, as it threatened to attack South Korea's government institutions, major national banks and traditional newspapers numerous times – in reaction to the sanctions it received from nuclear testing and to the continuation of Foal Eagle, South Korea's annual joint military exercise with the United States. North Korea's cyber warfare capabilities raise the alarm for South Korea, as North Korea is increasing its manpower through military academies specializing in hacking. Current figures state that South Korea only has 400 units of specialized personnel, while North Korea has more than 3,000 highly trained hackers; this portrays a huge gap in cyber warfare capabilities and sends a message to South Korea that it has to step up and strengthen its Cyber Warfare Command forces. Therefore, in order to be prepared from future attacks, South Korea and the United States will discuss further about deterrence plans at the Security Consultative Meeting (SCM). At SCM, they plan on developing strategies that focuses on accelerating the deployment of ballistic missiles as well as fostering its defense shield program, known as the Korean Air and Missile Defense.



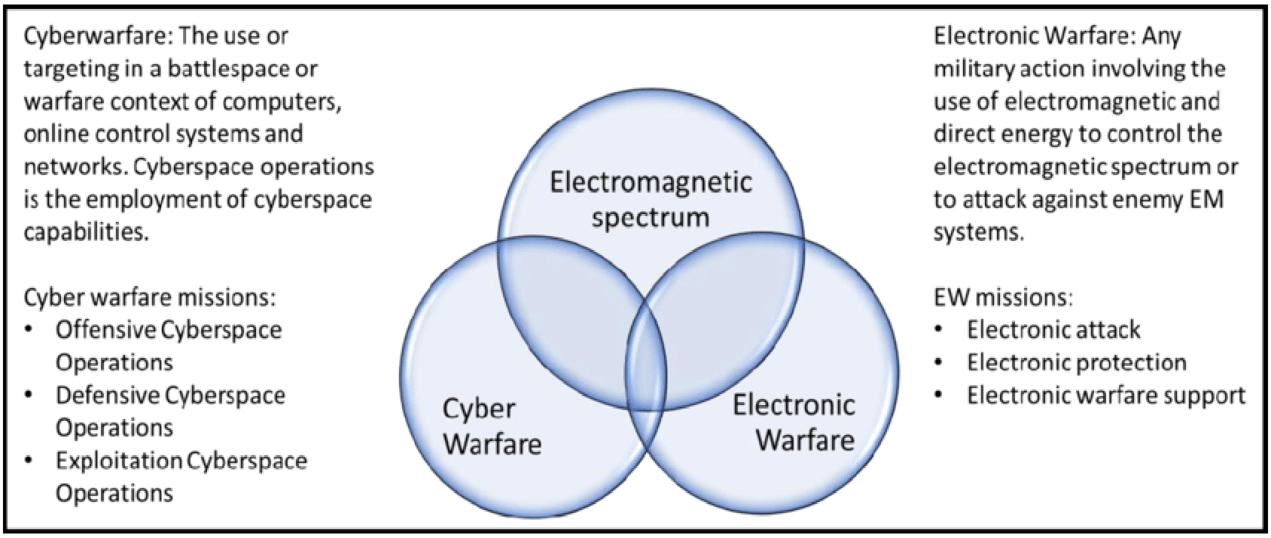
Type of Threat	Probability
Hindering military and civilian responders.	This is an increasing threat. As terrorist groups and nations improve their ability to infiltrate public and private infrastructure, the probablity of successful disruption of response capabilities increases.
Industrial espionage (theft of technology and other industrial secrets)	This is occurring at an growing rate, as large organizations in several countries find themselves victims of intellectual property theft. (http://mcaf.ee/tfxpb)
Disruption of a country's public services (health care, power, water, etc.)	Evidence suggests invasion of critical infrastructure by potential enemy nation states. These short-lived disruptions likely tested vulnerabilities and attackers' ability to disrupt critical services. (http://mcaf.ee/1lyji)
Disruption of financial institutions	Recent attacks against U.S. financial institutions demonstrates the ability and the willingness of countries like Iran to wage war against its enemies. (http://freebeacon.com/cyber-jihad/)

III. DISCUSSION

Until recently, cybersecurity was not one of the Indian government's top priorities, and consequently, the relevant departments in state agencies were, as a rule, staffed residually. Since work in this area was not considered important or prestigious, employees working in IT security were paid relatively little and their in-house status was lower than those of employees working in other departments. As a result, these positions were filled with underqualified and poorly motivated people. A positive discrimination system intended to advance members of lower castes had an adverse effect in this regard; underqualified employees hired to fill the quotas were placed with cybersecurity departments.[5,6]

Consequently, many agencies outsourced their cybersecurity while hiring specialized organizations to handle those matters. Since India does not have enough specialized organizations, foreign organizations were brought in, in particular, American ones, which, for obvious reasons, was not conducive to strengthening cyber protection. Since Pakistan and China were traditionally considered to be India's principal adversaries on the cyber front, this state of affairs was considered acceptable.

Plans for the agency call for over providing some 1,000 experts who will ensure the cybersecurity of the military, the navy and the air force as well as conducting offensive operations in cyberspace. In the future, this agency should be transformed into a full-fledged cyber command.[7,8]



Cyberwarfare: The use or targeting in a battlespace or warfare context of computers, online control systems and networks. Cyberspace operations is the employment of cyberspace capabilities.

Cyber warfare missions:

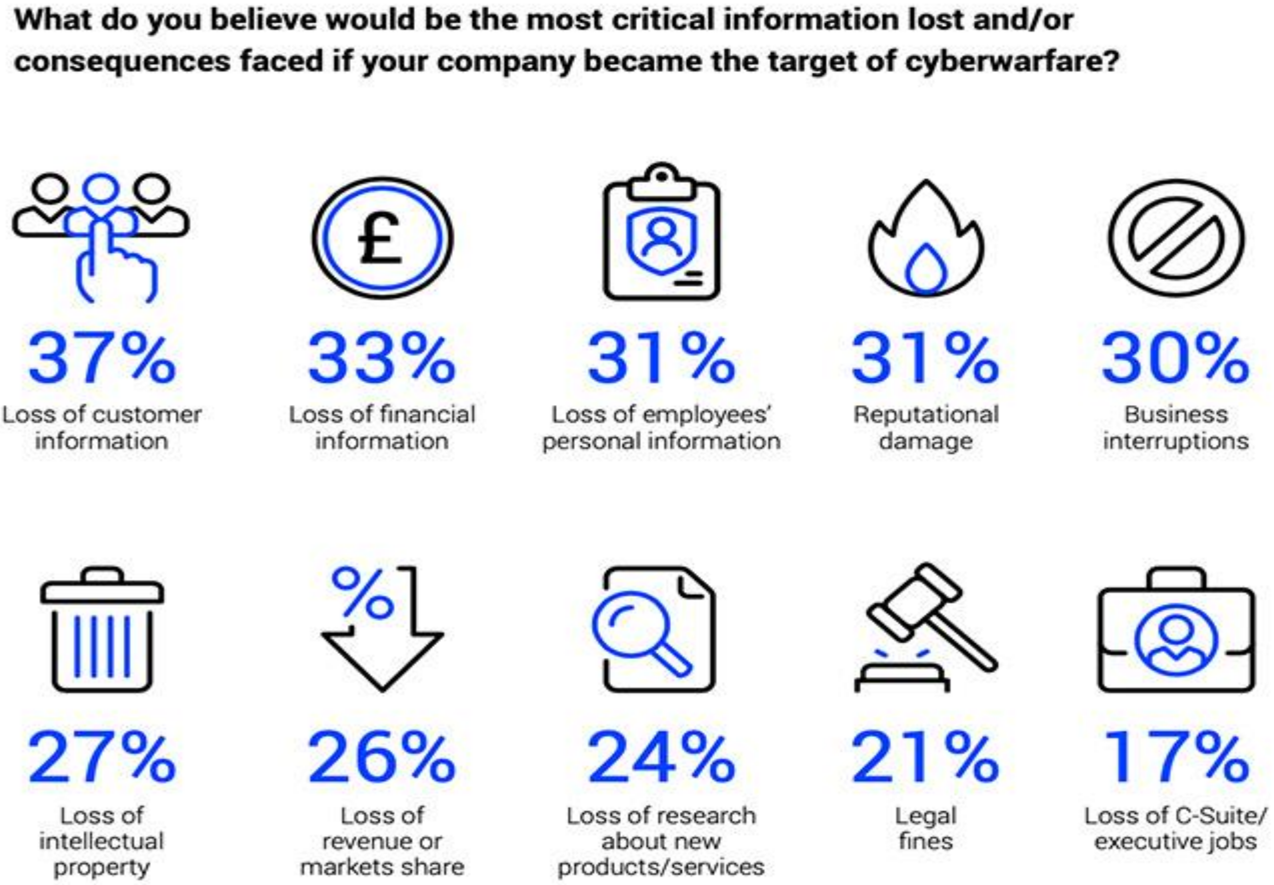
- Offensive Cyberspace Operations
- Defensive Cyberspace Operations
- Exploitation Cyberspace Operations

Electronic Warfare: Any military action involving the use of electromagnetic and direct energy to control the electromagnetic spectrum or to attack against enemy EM systems.

EW missions:

- Electronic attack
- Electronic protection
- Electronic warfare support

The newly-created body was called the Defence Cyber Agency (DCA). Rear Admiral Mohit Gupta was appointed as its commander. At present, its head and his executive office are working on developing a cyber ops doctrine. Thus far, it is hard to say how effective the DCA will be, given the traditional autonomy of the navy, the air force, and the military, which are reluctant to share operational information with each other and the difficulties of developing their own software. A previous attempt to introduce a specialized operating system called Bharat Operating System Solutions (BOSS), which was developed by the Centre for Development of Advanced Computing, ended in failure and the Indian military was forced to go back to using Windows OS.



What do you believe would be the most critical information lost and/or consequences faced if your company became the target of cyberwarfare?

37%	33%	31%	31%	30%
Loss of customer information	Loss of financial information	Loss of employees' personal information	Reputational damage	Business interruptions
27%	26%	24%	21%	17%
Loss of intellectual property	Loss of revenue or markets share	Loss of research about new products/services	Legal fines	Loss of C-Suite/ executive jobs

| ISSN: 2582-7219 | www.ijmrset.com |

| Volume 1, Issue 1, November 2018 |

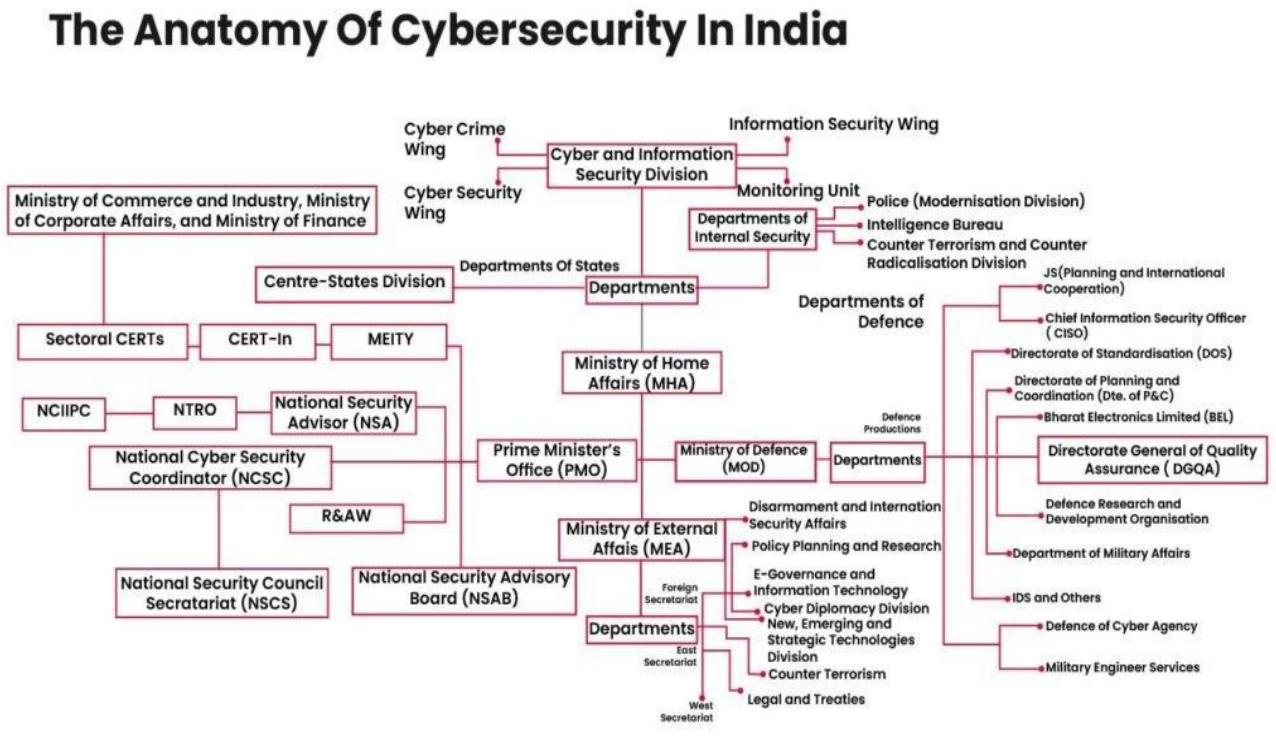
Given the absence of the requisite products created by governmental organizations, the Indian authorities will have to turn to private firms. Back in 2018, the Central Reserve Police Force (CRPF) and the Border Security Force (BSF) signed a contract with Innefu, a start-up headquartered in New Delhi. This company's products had previously passed a test of sorts: the company was given about 1,500 documents, including social media profiles of protesters and posts about planned actions. Based on this data, Innefu managed to trace connections between protesters, determine the nature of their interaction, and predict possible actions very soon.

Innefu now offers a complete set of ready-to-use solutions called Prophecy. It includes several tools that monitor social media, which provide big data analytics, facial recognition, and object identification, and detect faces and objects in real-time.

Thus, Indian IT specialists have created a product that may be used to process massive amounts of information for the purposes of intelligence and counter-intelligence. It has already been tested: according to the Indian media, police used it to successfully prevent several protests by analyzing the social media activity of certain individuals and to find roughly 3,000 children missing in New Delhi.

IV. RESULTS

Now India's leadership has acknowledged possible threats and is developing the necessary response means that take into account the realities of cyber warfare that is being conducted without regard for existing borders and for pacts and treaties regulating military action; cyber warfare also allows states to conceal their complicity in a cyberattack against another state. The Indian authorities are paying more and more attention to conducting defensive and offensive operations in cyberspace while striving to reduce the country's dependence on tools developed aboard and giving preference to forward-looking India-made products.[9,10]


The Anatomy Of Cybersecurity In India
Cyber Crime Wing
Information Security Wing
Cyber and Information Security Division
Cyber Security Wing
Monitoring Unit
Ministry of Commerce and Industry, Ministry of Corporate Affairs, and Ministry of Finance
Departments of Internal Security
Police (Modernisation Division)
Intelligence Bureau
Counter Terrorism and Counter Radicalisation Division
Departments Of States
Centre-States Division
Departments
JS(Planning and International Cooperation)
Departments of Defence
Chief Information Security Officer (CISO)
Sectoral CERTs
CERT-In
MEITY
Ministry of Home Affairs (MHA)
Directorate of Standardisation (DOS)
Directorate of Planning and Coordination (Dte. of P&C)
NCIIPC
NTRO
National Security Advisor (NSA)
Bharat Electronics Limited (BEL)
Defence Productions
National Cyber Security Coordinator (NCSC)
Prime Minister's Office (PMO)
Ministry of Defence (MOD)
Departments
Directorate General of Quality Assurance (DGQA)
R&AW
Disarmament and Internation Security Affairs
Defence Research and Development Organisation
Ministry of External Affais (MEA)
Policy Planning and Research
Department of Military Affairs
E-Governance and Information Technology
National Security Council Secratariat (NSCS)
National Security Advisory Board (NSAB)
Foreign Secretariat
Cyber Diplomacy Division
IDS and Others
Departments
New, Emerging and Strategic Technologies Division
Defence of Cyber Agency
East Secretariat
Counter Terrorism
Military Engineer Services
Legal and Treaties
West Secretariat

Source: National Cyber Security Coordinator

Inc42

At present, Pakistan, China, and the U.S. are India's key adversaries in cyberspace. Pakistan's capabilities for waging cyberwar are fairly limited: as a rule, Pakistani secret services either hack the websites of Indian agencies and companies connected with the government (such operations cause relatively little damage), or they pose on the Internet as young girls wishing to meet young officers in order to recruit current employees of Indian law enforcement, military, and secret services.

China is conducting large cyber operations against India which have reached such a scale that some analysts characterize them as a full-fledged cyberwar. This war takes on various forms: from hacking Indian networks to providing various rebel groups with hosting services on China's servers; nonetheless, the large-scale cyber ops have not prevented Beijing and New Delhi from strengthening their political and military relations.

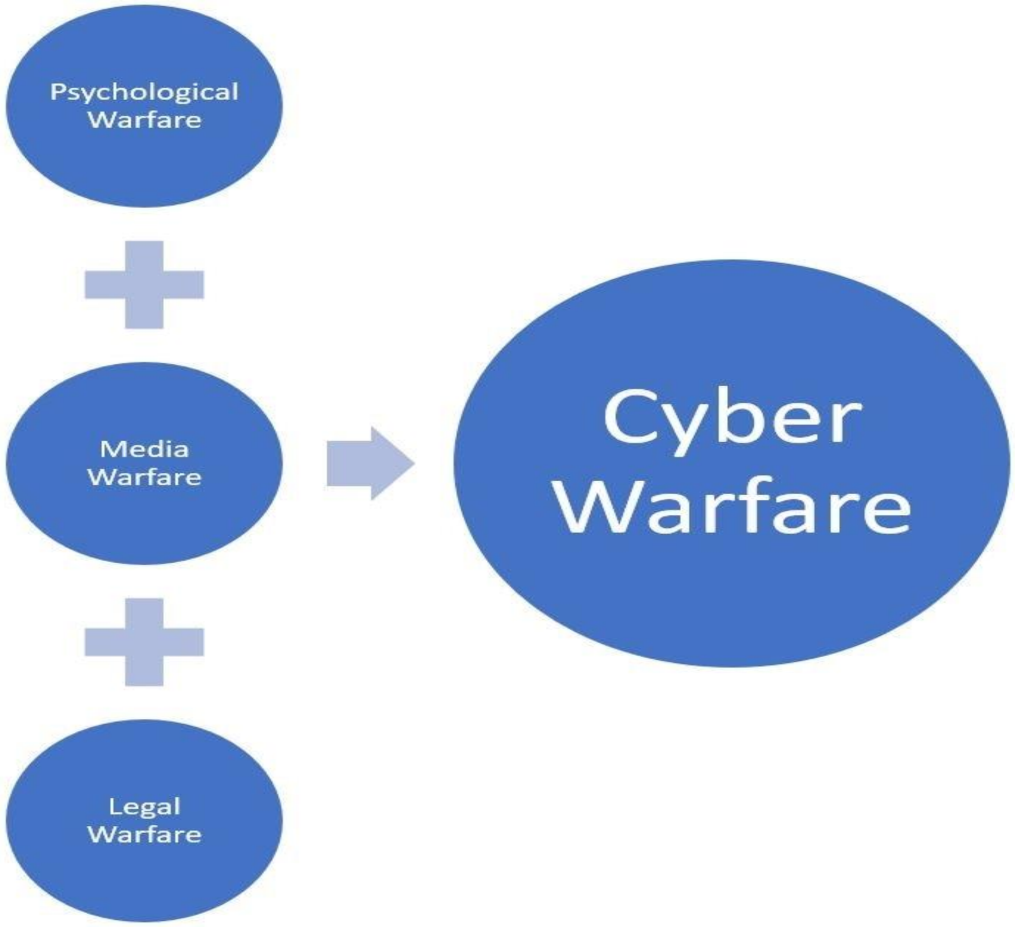


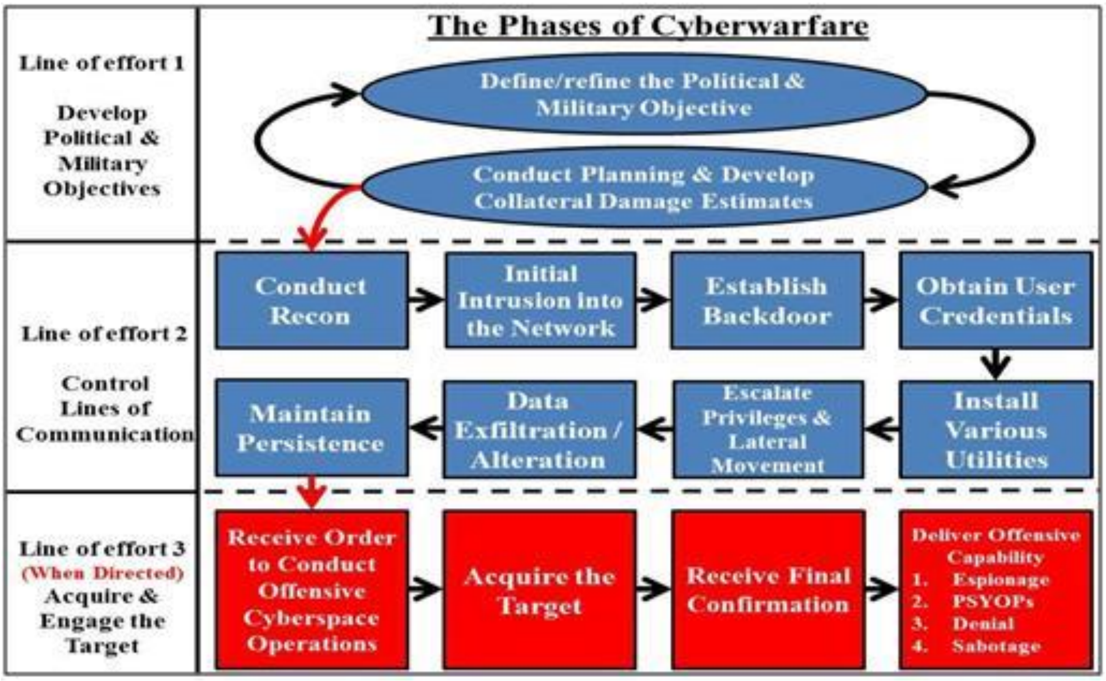
Figure: Warfare tools of CMC
Compiled by @saikirankannan

Relations with the U.S. are complex. On the one hand, Washington publicly calls India its key partner in the Indian Ocean region; on the other hand, U.S. secret services continue to conduct cyber ops that threaten India's national security.

Russia is one of the few great powers that has interests in the region and does not attack India in cyberspace. This is due primarily to the fact that there is no conflict between the two countries as well as Russia's general interest in establishing cooperation with Eurasian states to form a common trade space. Thus, Russia currently has a favorable opportunity to bolster its interaction with India in this regard and conclude a cyberspace non-aggression pact and, in the future, coordinate efforts with New Delhi to this end.[11,12]

V. CONCLUSION

Compared to China's cyberwarfare capabilities, India has a lot of catching up to do on both offensive and defensive fronts. Experts in the cybersecurity space believe India's preparedness is almost non-existent, even in defensive measures, let alone offensive. [13] To develop these capabilities, India needs to invest in infrastructure, funds, cryptography capabilities, developing indigenous tools, and, most importantly, talent. All the talent that exists today is private hackers with little to no capabilities outside the government. China has been preparing its cybersecurity strategy for over two decades, and India is still making baby steps. [14,15]


The Phases of Cyberwarfare
Line of effort 1
Develop Political & Military Objectives
Define/refine the Political & Military Objective
Conduct Planning & Develop Collateral Damage Estimates
Line of effort 2
Control Lines of Communication
Conduct Recon
Initial Intrusion into the Network
Establish Backdoor
Obtain User Credentials
Install Various Utilities
Escalate Privileges & Lateral Movement
Data Exfiltration / Alteration
Maintain Persistence
Line of effort 3
(When Directed)
Acquire & Engage the Target
Receive Order to Conduct Offensive Cyberspace Operations
Acquire the Target
Receive Final Confirmation
Deliver Offensive Capability
1. Espionage
2. PSYOPs
3. Denial
4. Sabotage

The rise of cyber as a warfighting domain has led to efforts to determine how cyberspace can be used to foster peace. For example, the German civil rights panel FIfF runs a campaign for cyberpeace − for the control of cyberweapons and surveillance technology and against the militarization of cyberspace and the development and stockpiling of offensive exploits and malware. Measures for cyberpeace include policymakers developing new rules and norms for warfare, individuals and organizations building new tools and secure infrastructures, promoting open source, the establishment of cyber security centers, auditing of critical infrastructure cybersecurity, obligations to disclose vulnerabilities, disarmament, defensive security strategies, decentralization, education and widely applying relevant tools and infrastructures, encryption and other cyberdefenses.The topics of cyber peacekeeping and cyber peacemaking have also been studied by researchers, as a way to restore and strengthen peace in the aftermath of both cyber and traditional warfare.[15]

REFERENCES

1. Singer, P. W. (Peter Warren) (March 2014). Cybersecurity and cyberwar : what everyone needs to know. Friedman, Allan. Oxford.
2. ^ Smith, Troy E. (2013). "Cyber Warfare: A Misrepresentation of the True Cyber Threat". American Intelligence Journal. **31** (1): 82–85.
3. ^ Shakarian, Paulo. (2013). Introduction to cyber-warfare : a multidisciplinary approach. Shakarian, Jana., Ruef, Andrew. Amsterdam [Netherlands]: Morgan Kaufmann Publishers, an imprint of Elsevier.
4. ^ Clarke, Richard A. Cyber War, HarperCollins (2010)

5. ^ Blitz, James (1 November 2011). "Security: A huge challenge from China, Russia and organised crime". Financial Times.
6. ^ Arquilla, John (1999). "Can information warfare ever be just?". Ethics and Information Technology. **1** (3): 203–212.
7. ^ Parks, Raymond C.; Duggan, David P. (September 2011). "Principles of Cyberwarfare". IEEE Security Privacy. **9** (5): 30–35.
8. ^ Taddeo, Mariarosaria (19 July 2012). An analysis for a just cyber warfare. Cyber Conflict (ICCC), International Conference on. Estonia: IEEE.
9. ^ "Latest viruses could mean 'end of world as we know it,' says man who discovered Flame", The Times of Israel
10. ^ "White House Cyber Czar: 'There Is No Cyberwar'". Wired, 4 March 2010
11. ^ Deibert, Ron (2011). "Tracking the emerging arms race in cyberspace". Bulletin of the Atomic Scientists. **67** (1): 1–8.
12. ^ "A Note on the Laws of War in Cyberspace", James A. Lewis, April 2010
13. ^ Rayman, Noah (18 December 2013). "Merkel Compared NSA To Stasi in Complaint To Obama". Time.
14. ^ Devereaux, Ryan; Greenwald, Glenn; Poitras, Laura (19 May 2014). "Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas". The Intercept. First Look Media.
15. ^ Schonfeld, Zach (23 May 2014). "The Intercept Wouldn't Reveal a Country the U.S. Is Spying On, So WikiLeaks Did Instead". Newsweek.