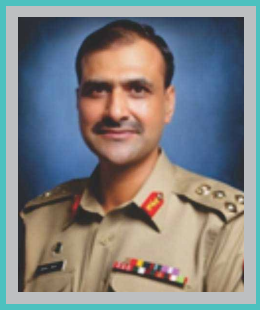
CYBER WARFARE: PREPARING FOR THE NEXT BIG WAR



Brig Dr Abdul Rauf

Brig Dr Monis Akhlaq

ABSTRACT

Global cyberspace has evolved so swiftly over a period of time that its extents have become difficult to grasp and the dynamics of cyber environment a decade from now are hard to forecast. However, it can be predicted with surety that anyone controlling the cyberspace would rule the world. Cyberspace can be visualized as something analogous to the physical world, where everything from real life is replicated in one form or the other. This similarity implies that other than the warfare types in the actual world, there exists a battlefield in the cyberspace as well with its own peculiar techniques, called cyber warfare. Cyber warfare is not a new warfare, rather it has been termed as an important dimension of modern war, where its diminuendos change as quickly as that of the cyberspace itself. Therefore for any nation staying abreast with the subtleties of cyber warfare is the need of the time. In this backdrop, the article presents a concise overview of cyber warfare conceptual paradigm, the prevalent threat spectrum and some pertinent lessons from contemporary states in order to highlight a strategic perspective coupled with crisp implementation modalities.

Key Words: Cyber Warfare, National Security and Cyber Defence.

With the introduction of IoT and 5G there is going to be an exponential growth in connected devices and expansion of cyber world by manifolds. The price of entry into internet world is extremely low

Conceptual Paradigm

News about cyber incidents are persistently on the rise nowadays with novel cybercrimes and associated techniques discovered each day. Computer users continually hear about the latest cyberattacks attempting to steal credentials, hacking, malware, adware, botnets, ransomware, insider threats, dark web, zero-day attacks, privacy, identity thefts, data protection, wireless, Wi-Fi & IoT security vulnerabilities, deepfakes, smartphone hacking, SIM-jacking, cloud-jacking, AI poisoning, cyber espionage, cyber sabotage etc, and now its all-encompassing Cyber Warfare.[1]

The speedy deployment of Information and Communication Technology (ICT) is effecting the entire world. The idea of cyberspace, cyber power and the related danger of cyber war is the result of the infiltration of ICT in almost every field of life. Cybersecurity has emerged as a new element of national security and correspondingly cyber power is acknowledged as a new building block of national power. Many nations are actively defining and building their cyber defensive and offensive capabilities. Activities of cyber reconnaissance, espionage and probing missions both by the state and non-state actors are on the rise. World may be spending more financial, academic and research capital in digging out how to carry out cyber warfare rather than on activities focused at how to thwart it. Today, approximately over 140 countries are emerging in offensive cyber warfare potential.[2]

In this era of global connectivity, our dependency on internet based technologies is on the rise and is continuously increasing with each passing day. With the introduction of IoT and 5G there is going to be an exponential growth in connected devices and expansion of cyber world by manifolds. The price of entry into internet world is extremely low. Furthermore the gains or profit of attacking someone in cyber world are much higher than the investments and risks. This is what is motivating people to invest in cyber domain. We need to develop our cyber defensive and cyber offensive capabilities not only to prepare for the next cyberwar but actually to defend ourselves in the ongoing cyberwar.

"Cyber power is the ability to use cyber-space to create advantages and influence events in other operational environments and across the instruments of power"

Defining Cyber Warfare

Cyberspace. Today, the number of computer systems is more than two billion (and increasing every minute) including IT servers, network routers, switches connected through optical fibre, copper cables and over the air using wireless communication to make these IT infrastructures interact and collaborate. These mutually dependent and unified IT networks and systems exist at once in both physical and virtual space without any restrictions of geographic borders. The concept of Net Centric Warfare (NCW) would not be possible without cyber based potential. Targeting the necessary information by the tool and then trusting real-time updates to accurately reach the target from the GPS satellite can only be achieved through cyberspace.

Cyber Power. As described by Stuart H Starr "Cyber power is the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power". Hence, cyber power is the ability to use cyberspace stage.[3]

Cyber Warfare. Cyber warfare may be defined as the use of cyber power either to impose sentence to

an opponent or to get political aim without the enemy's consent. Cyber warfare is a harmonized digital harass on a state by another. The act by a nation to penetrate another nation's computer systems and networks for the purpose of break or interruption of ICT services. Cyber warfare can be described as attacks between sectors, from terrorist groups, or just attacks by persons (hackers), who seem as war like, in their intention. The US Department of Defence (USDOD) describes cyber warfare as "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace." As defined in UN Security Council Resolution, "Cyber warfare is the use of computers or digital means by a government or with explicit knowledge of or permission of that state against another state, or private property within another state including; intended access, interception of data or damage to digital and digitally controlled infrastructure and production and distribution of devices which can be used to undermine domestic activity".[4,5,6,7]

Cyber Warfare as Computer Network Operations (CNOs)

Cyber Warfare is the new type of operations where the nations / groups / individuals conduct CNOs to get their goal. CNOs can be commenced either alone or in combination with the Kinetic Operations. These are basically combination of the following:

Computer Network Attack (CNA). The operations planned to interrupt, refute, degrade or demolish information occupant in computer systems and computer networks. The fresh developments in which the computer systems can thwart with the physical systems have offered the CNOs with very effective capacity to attack the vital infrastructure of the opponent.

Computer Network Exploitation (CNE). It is recovering intelligence rank data and information from the computer systems of an opponent by using ICT. This technique is used by nations, groups and persons for getting information to make data base for further use or for sabotage.

Intranet and internet based technologies have widened the threat domain with no limits; offensive could be launched from anywhere, any platform and towards any target

Computer Network Defence (CND). All procedures essential to defend own ICT systems and networks and infrastructures against antagonistic CNA and CNE. It is a luxurious and prolonged activity, needs a huge expertise and vigilant human resource.

Prevailing Threat Spectrum Emerging Scenario

Digital revolution has necessitated usage of Information Technology (IT) in all domains of life. The transformation has witnessed great dependence upon connectivity of user end devices to the networks like communication, internet or intranet. All of these networks bare similarity in technology standards and protocols in which the backbone communication medium is either offered or influenced by internet protocols. Today, prime objective for technology researchers and providers is to widen the connectivity spectrum of internet by offering robust and performance oriented networks, thus making the developing countries like Pakistan to have more dependency on technology acquisition, rather development. The span of internet technology has not only influenced economic and social sectors but also has influenced defence and national security. The virtual world of cyber has actually being manifested in physical world by technology advancements, adoption and benefits offered. The unfortunate part is that developing nations are mostly neglecting the associated threats and fail to ascertain the spectrum of cyberspace and cyber warfare for national security.

Threat Domains

Discussion here would focus upon the grey areas in understanding cyber warfare threat domains and their possible implications.

In today's digital world SMNs are considered life line for internet users however these are also being misused for religious extremism, harassment, blackmailing and even sexual exploitation

Versatile threat actors. Intranet and internet based technologies have widened the threat domain with no limits; offensive could be launched from anywhere, any platform and towards any target.

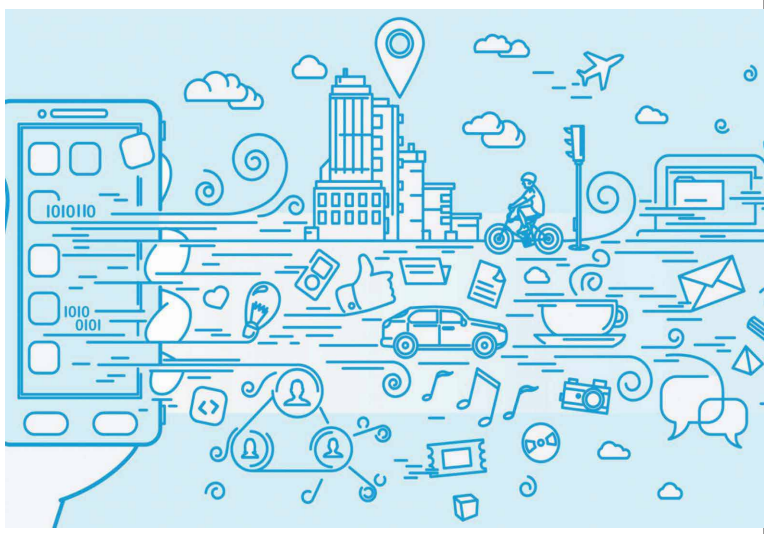
Social Media and Over-The-Top (OTT) Applications. Freely available applications have totally engulfed internet community globally, getting away and operating carefully on these platforms seems impossible, hidden implications of these applications are discussed as follows:[8,9,10]

- **Data Collection.** Users wilfully share personal data, identify family/friends, identify liking/ disliking, chats and calls etc. Just imagine, how much efforts would be required to get all of this information at such a massive scale. Preparation of individual's personal profile could take no time as mostly information shared by a person is available online over different social media platforms.
- **Data Analytics.** Recent advancements in Big Data analytics using Artificial Intelligence technologies have paved the way to analyse the massive data stored. Identification of groups / national trends and psychology is no more difficult. Advanced algorithms would take minutes to discretely analyse the national perspective / opinion on critical issues to ascertain national cohesion, stability, security and state of preparedness (readiness / support to military efforts against hostile nations/ groups, acceptance / rejection of state policies, national morale etc.).
- **Conduit for Hostile Propaganda.** Extensive usage of social media has empowered hostile agencies / groups and individuals, a comparatively easier platform to explode nefarious agenda – with no effective provision to stop the propagation or even to identify the source. Strong resistance from internet users' community also restricts any preventive effort. The seriousness would increase manifolds in the presence of hostile actors creating hostile environment.
- **Restricts Intelligence Efforts.** User privacy policies, protection acts and treaties have limited the efforts of intelligence agencies. Use of advanced encryption technologies has also allowed the hostile / subverted groups, individuals and agents to remain undetected.
- **No Control on Users.** In today's digital world SMNs are considered life line for internet users however, these are also being misused for religious extremism, harassment, blackmailing and even sexual exploitation. Ethical and cultural issues generated through these networks are difficult to address due to identity issues, lack of cooperation from service providers, legal restrictions and hectic complaint resolution procedures involved. SMNs offer excellent medium to create law and order / anarchy in the society where it would be difficult for the stakeholders to control / block its usage due to strong resentment from the digital rights activists and even from the online community as a whole.

Cybersecurity and Technology. Cybersecurity is heavily dependent upon technology including high performance operating systems, user end devices, network switches / routers, data storage security systems and devices. Significant concerns in this regard are as follows:[11,12]

- **Auto Discloses Network and Security Architecture.** Network and security devices need certification / authentication from Original Equipment Manufacturer (OEM). Mostly the

Cybersecurity is heavily dependent upon technology including high performance operating systems, user end devices, network switches / routers, data storage security systems and devices

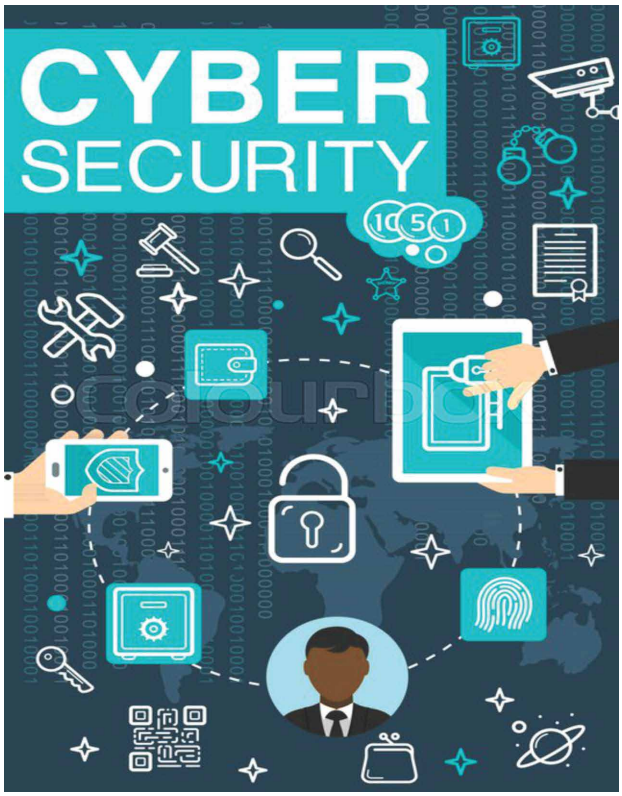


Cyber Security has witnessed tremendous progress, developments in IT have always brought new dimensions to security. The primary factor is "dependence brings vulnerabilities which create opportunities to exploit"

Technology giants are immune from any blames/responsibilities incurred due to any security breach, as they say, "no network/system is totally secure, security is dependent upon vigilant monitoring by humans and who are prone to errors"

mechanism is ensured by exchange of certain security credentials such as certificates, equipment IDs etc. Online connectivity of these devices could provide network design information to OEM, hostile usage of which is a great concern.

- **Live Cyber Threat Sharing.** Sharing of live threat/ attack detection with OEM is the significant feature of most security systems and devices (antivirus, firewall, Intrusion Detection Systems etc.). The mechanism has the hostile exploitation possibility associated such as covert sharing of attack information with intruders, providing information about level of protection offered (what all attacks are and can be detected) and even lower the guards. Such exploitation is of no surprise in cyber warfare scenarios.
- **Dependence on Regular Updates.** Proactive Cyber Security is a necessity, however, the concept is implemented in a reactive mode. Cyber Security OEMs creates patches and updates of their systems and devices on detection of some errors / flaws in products, operating systems or even on identifying novel successful attacks. These patches if applied in time could prevent a breach, however failing to do so could lead to significant damage. Intent based manipulation of such act cannot be ruled out. Transparency in this process becomes extremely important in air-gapped networks in which any delay or unauthorized acts (injection of hacking code, denial of service or even network sabotage etc.) could be catastrophic. Patch management in closed network is also a difficult task and requires evaluation process and record keeping. Mismanagement in the process could also result into system loss or compromise.
- **No Liability on OEM in Case of Security Loss.** Technology giants are immune from any blames / responsibilities incurred due to any security breach, as they say, "no network / system is totally secure, security is dependent upon vigilant monitoring by humans and who are prone to errors". Large number of cybersecurity incidents happen daily, knowingly not a single OEM (technology) was held responsible for the breach, and technology users (network designer and security expert) always got penalized.
- **Cyber Security Progression Continues.** Cyber Security has witnessed tremendous progress, developments in IT have always brought new dimensions to security. The journey has started from antivirus and passed through many phases of security software and hardware products development, the journey still continues with no end point or finish line. The primary factor is "dependence brings vulnerabilities which create opportunities to exploit".
- **R&D Collaboration of International OEM's with India.** The country has offered better infrastructure and cheaper trained workforce in cyber and cyber security. Many reputed firms have established R&D bases in Indian universities and other public / private sector organizations / firms. Indian hegemonic influence to these companies for strategic and tactical gains by exploitation of our national cyberspace cannot be ruled out.



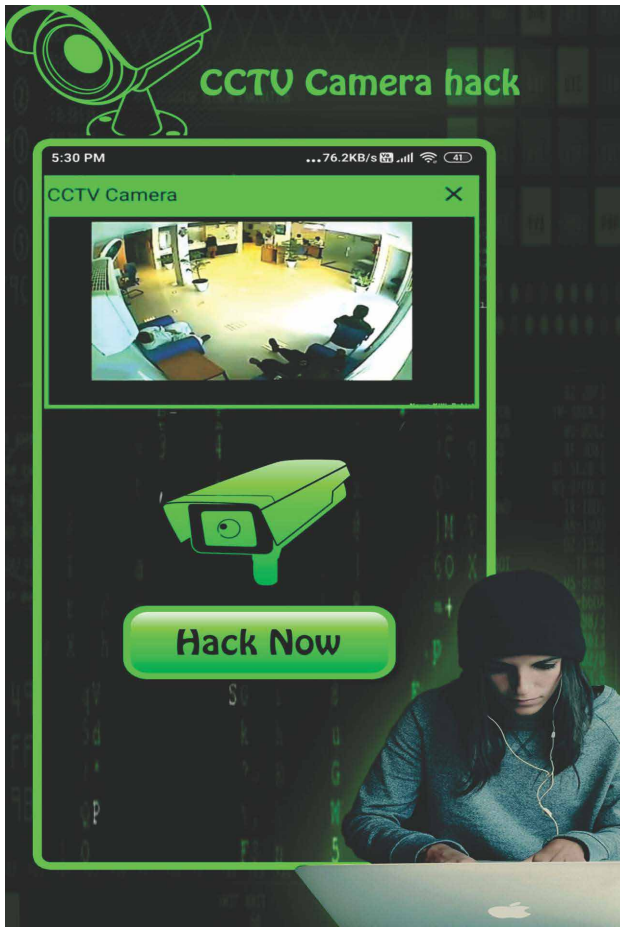
Benefits has made internet the backbone communication media even for critical national assets banking/ finance, power/ energy, communication, diplomacy etc. Internet connectivity has increased the threat spectrum

- **National Certification and Accreditation Process.** Limited control has been implemented by Pakistan Telecommunication Authority (PTA) on usage of mobile phones in Pakistan. Mobile phones are approved by PTA on completion of customs and taxation formalities. The process is incomplete and do not include technical evaluation of mobile phones to identify bugs/ implants and hacking software installed, probability of presence for hostile purpose is quite high. Certification and Accreditation process has been adopted by most of the countries, standards are formulated to ensure procurement of requisite technology for civil and military purposes. The process also includes evaluation of other ICT systems and devices such as laptops, computers, storage devices, network and security devices etc.

Vital National Assets on Internet. High bandwidth, speed, coverage, connectivity, availability, lower cost and other benefits has made internet the backbone communication media even for critical national assets banking/ finance, power/ energy, communication, diplomacy etc. Internet connectivity has increased the threat spectrum, few concerns associated are discussed below:[13]

- **National Cyber Security Policy.** Efforts are in place since long to develop a consensus based cyber security policy in the country but unfortunately could not be materialized so far. Absence of such a critical policy has created the strategic vacuum in cyber security landscape of the country.
- **National Firewall.** Cyber Security is the collective responsibility in which every tier from user to network security administrator, organization to service provider and relevant national stake holders have to perform certain tasks in which most important is the security technology adoption / usage. The task is mostly being performed at organizational and lower levels – absence of appropriate technology at service provider and national levels has increased the threat spectrum to critical assets.
- **Emergency and Incident Response.** National level IT crisis management is an important responsibility domain, mostly Computer Emergency Response Teams (CERT) are created at all levels to handle the crisis. Collective effort is needed among all teams to generate comprehensive response, absence of CERT at national level has created a vacuum and any unfortunate incident could affect performance and availability of critical assets. Absence of effective national level CERT has also compounded the threat spectrum.
- **Monitoring Mechanism.** Mostly organizations relying on ICT have developed mechanisms for protection of data and ensure availability of resources, however, lack of policy defining necessity of audit and monitoring of security parameters by independent (third party) organizations has created a vacuum.

Risk associated with CCTV cameras of home / office or property available through internet on a mob phone devices, control of security systems and house hold devices need consideration

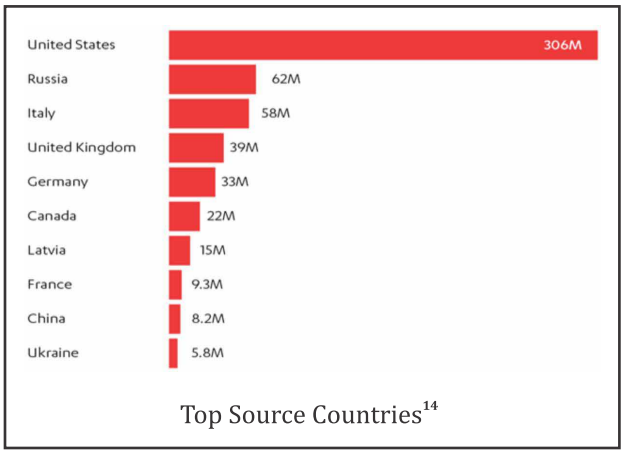


Russian successful experiment of 'sovereign internet', where in an emergency situation, national internet can work independently, irrespective of the global connectivity could bring some lessons for us to ponder upon

- **Future Technologies.** High speed internet technology 5G and IoT have already demonstrated the strength of internet for house hold purposes etc. Risk associated with CCTV cameras of home / office or property available through internet on a mob phone devices, control of security systems and house hold devices need consideration.
- **Implications of Internet Unavailability.** Hostile security environments due to internal disturbances or trans-frontier aggressions could result into digital isolation in which Pakistan cyberspace could be disconnected from global internet. The situation must be detrimental due to massive dependence upon the internet media by government and private sectors (education, economic, finance, communication etc.). The situation is further aggravated due to a single landing site at Karachi offering connectivity to international submarine cables. Russian successful experiment of 'sovereign internet', where in an emergency situation, national internet can work independently, irrespective of the global connectivity, could bring some lessons for us to ponder upon.

Cyber Warfare Around the World

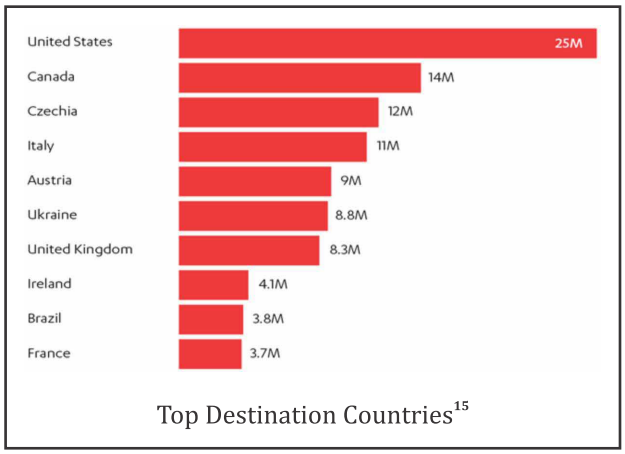
It is always interesting is to have a look at which countries' IP spaces attacks came from and which countries they were directed at.



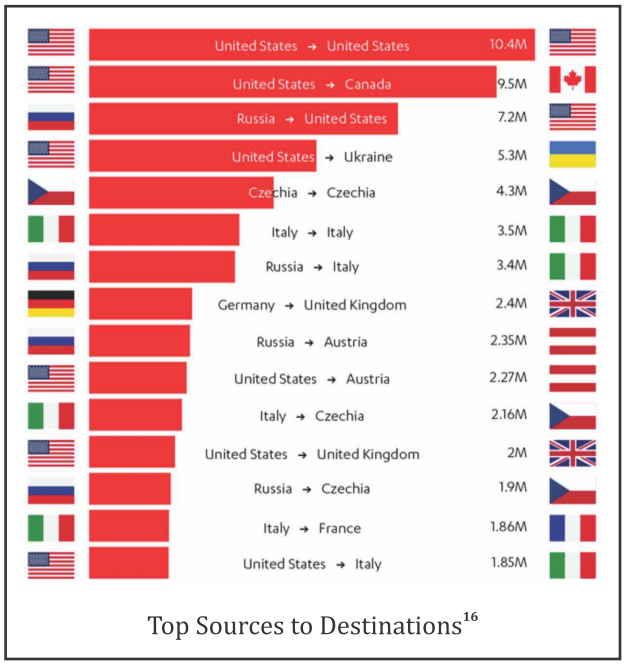
Top Source Countries[14]

Traffic originating in the US IP space grabbed the largest share at this time, with Russia coming second, at a far distance. Of course, as we always point out, there is no way of knowing whether the attacks are actually conceived in a given country, since cyber criminals route their attacks through proxies to avoid detection. They may employ VPNs, Tor ('The Onion Router', free and open-source software for enabling anonymous communication), and compromised machines or infrastructure in different locations to evade law enforcement.

The list of countries is not meant to imply that this is predominantly a nation state behaviour. The motivation behind the majority of these attacks is likely financial and instigated by common cyber criminals who are carrying out Distributed Denial-of-Service (DDoS) attacks and sending malware, etc. What we can be more certain of, however, is the attack destinations, and these are the countries who attracted the most interest from attackers.



Top Destination Countries[15]



Top Sources to Destinations[16]

Cyber warfare bare similarity to different strategies of conventional war, in which similar objectives could also be identified to destroy or disable war fighting capability, economic, power, communication and government sectors of the target nation or region

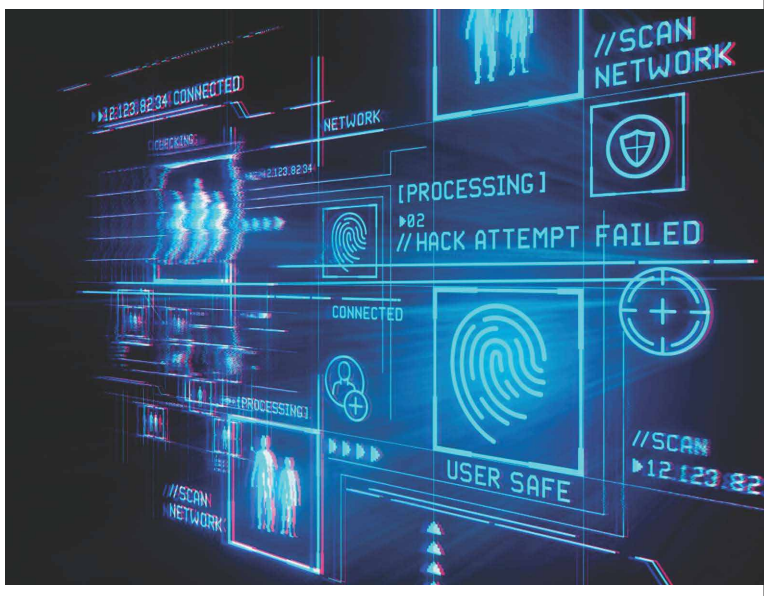
Strategic Aspects and Implementation Modalities
Cyber Warfare Strategies

Cyber warfare must be seen in the context of war in general. Conventional war involves different categories of actions falling within ambit of strategic, tactical and operational activities. These categories are primarily differentiated by impact required from a military action and employment of forces and weaponry. Cyber warfare bare similarity to different strategies of conventional war, in which similar objectives could also be identified to destroy or disable war fighting capability, economic, power, communication and government sectors of the target nation or region. Actors involved in such acts are state sponsored cyber criminals to trained cyber soldiers. Terrorists and rogue criminals could also be employed in cyber domain to attain military benefits. Following are the different strategies of Offensive and Defensive Cyber Warfare:[17,18,19]

A well trained and equipped military cyber force is required for attacking and destruction. Preferably, force comprised of military and civilian experts progressively groomed over years

Catastrophic Cyber Offensive. A well planned and organized cyber offensive activities to totally destroy adversary's military ICT capabilities (communication, battle field management systems and decision support/ making networks), ICT dependent government and private sectors (economic, financial, communication, development etc.), create a nation-wide impact and making recovery of the ICT assets impossible or exceeding planned timeframe. Factors affecting execution of such operations are:-

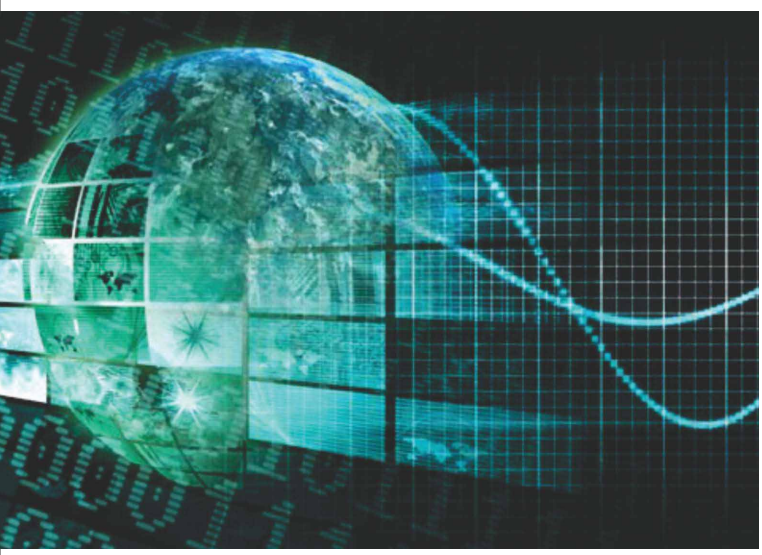
- A well trained and equipped military cyber force is required for attacking and destruction. Preferably, force comprised of military and civilian experts progressively groomed over years.
- Necessitated specialized skillset, mental capabilities and in-depth understanding of ICT programming, software / hardware knowledge, cyber security technology and vulnerabilities identification.
- Proactive target identification, reconnaissance, penetration and persistence are needed with absolute accuracy. Objective is to create strategic / tactical imbalance by striking, damaging and destroying when ordered.
- Kinetic effects are foreseen, mostly the attacks are launched to achieve destruction through cyber sabotage, system malfunction (misguide friends and foe), prolonged denial of service / networks unavailability and either making information/ data unavailable or tempered.
- Backdoor channels, connection with underworld (deep and dark web), objective intelligence efforts seems essential in force development and execution.
- Could be executed in isolation or in support to conventional military strive.
- Identification of zero-day vulnerabilities and development of Advance Persistent Threats (APTs) fall in this strategy.
- In few situations, assistance from ground forces is mandatory to attain results (filling the gap of air gapped networks).
- Such activities are extremely heavy on finances as millions of dollars are required for specialized skills development / trainings, sustenance, technology development etc. – very few nations could afford to execute this strategy however this could be considered as a benchmark to attain excellence.



Well planned and organized cyber offensive activities to cripple or damage selected adversary's military ICT capabilities, ICT dependent government and private sectors create a regional/ zonal impact and making recovery of the ICT assets difficult not impossible

Extensive Cyber Offensive. Well planned and organized cyber offensive activities to cripple or damage selected adversary's military ICT capabilities (communication, battle field management systems and decision support/ making networks), ICT dependent government and private sectors (economic, financial, communication, development etc.), create a regional/ zonal impact and making recovery of the ICT assets difficult not impossible. Factors affecting execution of such operations are:-

- This is a level below Catastrophic Cyber Offensive. It has reduced kinetic impact and may cause prolonged outage of critical systems and infrastructure.
- Well trained work force on ICT programming, software / hardware knowledge, cyber security technology and vulnerabilities identification is needed.
- Cyber warriors selected for the higher level are primarily filtered at this stage. Critical decisions are required for progression towards higher level because of complexity and finances involved there. Deciding factor could be whether the strategy fulfils the operational requirements or has given the expected outcome.



Open source resources provide quite good offensive tools to cyber stalkers in targeted operations. Major effort required is to bypass the antivirus detection and conceal footsteps

- Proactive target identification, reconnaissance, penetration and persistence are needed with absolute accuracy. Objective is to create tactical imbalance by striking and damaging when ordered.
- Preferably the strategy could be developed and executed for intelligence based objectives and in coordination with military endeavour.
- Foreseeable impacts are partial unavailability and critical delays, losing trust on deliverance and accuracy (decision support systems) and persistent foot hold for data espionage.
- Strategy is suitable against nations and militaries dependent upon ICT for operational tasks.
- Comparatively less financial heavy approach and most suitable for developing nations / militaries.

Targeted Cyber Offensive. A well planned and organized cyber offensive activity for covert data/ information acquisition, data modification or create denial of service and system/ resource unavailability. The objectives of strategy could be acquisition of critical documents and letters, official and personal data research and trade secrets, military operational plans and financial data. The act is conducted by military, intelligence agents, state sponsored cyber activists and hired hackers. Factors affecting execution of such operations are:-

- Conventional hacking strategy to attain ingress into personal / official systems and networks connected over the internet.
- Trojans and Malware are major arsenals in this strategy. Techniques employed are social engineering, spear phishing, phishing and similar attacks.
- Technologies employed in this are from low to moderate levels. Open source resources provide quite good offensive tools to cyber stalkers in targeted operations. Major effort required is to bypass the antivirus detection and conceal footsteps.
- Comparatively less financial resources are required in this. The strategy also offers outsourcing of Trojans/Malware developments and even assigning the intrusion tasks.

Sometimes gains acquired from targeted cyber offensive are of immense strategic value and could jeopardize national and military security, personal privacy and even repute

- Mostly cyber security firms focus on detection of this offensive strategy, quite often reports have been published on detection of attack signatures and identification of source of attacks.
- Sometimes gains acquired from targeted cyber offensive are of immense strategic value and could jeopardize national and military security, personal privacy and even repute etc.
- Applicable in internet based environments, no limits and boundaries involved.

Sporadic Cyber Offensive. Activities of cyber criminals, terrorists or rogue elements for personal, financial and subversive gains. The target of activity could be persons (common, military, government etc.), government and private sector ICT systems/ resources. The impact foreseen ranges from data acquisition (espionage), denial of service and system unavailability. Factors affecting execution of such operations are:-

- Less expensive than targeted cyber offensive and mostly does not require hired workforce, training and sustenance.
- Techniques and technologies required are mostly similar to targeted cyber offensive.
- They have little lasting impact on organizations except network / system unavailability may cause functional delays and disclosure could affect the repute.
- Mostly, criminal and terrorists attempts for personal and financial gains are the prime objectives in this strategy however, support from intelligence agencies on selected targets cannot be ruled out. Political motivation could also be a factor for this strategy.
- Cyber stalkers, launching pads and targets are mostly located within geographical boundaries.

Collective Impermeable Cyber Defence (CICD). A well planned and organized defensive effort involving all national stakeholders to prevent military ICT networks/ capabilities (communication, battle field management systems and decision support/ making networks), ICT dependent government and private sectors (economic, financial, communication, development etc.) from destruction or damage by hostile cyber offensive from aggressor nation/ state, cyber criminals, state/ non state actors, terrorists or rogue elements. Factors affecting execution of such operations are enumerated below:

Military could be assigned the responsibility to operate and manage central monitoring organization

- Well planned and organized layered cyber defence architecture involving all national stakeholders. Requisite technology and human resources is employed at each layer to detect, prevent and respond to cyberattacks.
- Requires well established organization and specific cyber security skill set of employees. The layered defence is centrally monitored at the national internet gateway to have better visibility of cyber offensive against critical ICT infrastructures. In CICD military could be assigned the responsibility to operate and manage central monitoring organization.
- Financially heavy strategy, continuous investment in technology and HR capability building (training and sustenance) is necessary.
- Strategy is mostly suitable for countries developing ICT technology having large reliance on ICT in all sectors and has capability to develop indigenous ICT and security systems and products (mostly in developed part of the world).
- Regional or international cooperation and alliances could be a part of this strategy (support / assistance between national and regional / international CERTs).

In absence of national level organization and cyber defence collaboration among stake holders the strategy follows the principle of collective impermeable cyber defence and take over the first/ top security tier

CCD is a offensive defensive strategy to facilitate the defender by giving a befitting response to the offensive strive of adversary by gaining access and acquiring control of their critical systems and networks and attain a strong negotiating posture

Organized Cyber Defence. A well planned and organized defensive effort of individual stakeholders of a national cyberspace (military, government and private sectors) to prevent dependent ICT networks from destruction or damage by hostile cyber offensive from aggressor nation/ state, cyber criminals, state/ non state actors, terrorists or rogue elements. Factors affecting execution of such operations are enumerated below:

- Organization / institution based cyber defence strategy falls at the second tier of cyber defensive efforts and primarily meant to ensure confidentiality, integrity and availability of ICT networks and resources.
- In absence of national level organization and cyber defence collaboration among stake holders, the strategy follows the principle of collective impermeable cyber defence and take over the first/ top security tier.
- Suitable for the countries in which few critical sectors are having reliance on ICT for operational requirements, however, the country / nation have moderate level ICT usage for operational purposes.
- Provide adequate protection to critical infra-structure/systems by adoption of security architecture model such as air-gapped network (connected through own dedicated communi-cation links and not through internet).
- Preferable for those countries making progression in ICT R&D and cyber security, availability of trained workforce could also benefit the strategy.
- Comparatively less financialy heavy and more reliance on credible ICT systems developers and providers.

Counter Cyber Defence (CCD). A well planned defensive-offensive effort to cripple or disable military ICT networks/ capabilities (communication, battle field management systems and decision support/ making networks), ICT dependent government and private sectors (economic, financial, communication, development etc.) in response to aggressive endeavour to attain a strong negotiating posture over aggressor nation/ state or force. Factors affecting execution of such operations are enumerated below:

- CCD is a offensive-defensive strategy to facilitate the defender by giving a befitting response to the offensive strive of adversary by gaining access and acquiring control of their critical systems and networks and attain a strong negotiating posture.
- Collective impermeable and organized cyber defence strategies (both) seems mandatory in successful execution of this, any failure can have a drastic impact over this effort.
- Well organized and trained workforce is needed. Extensive cyber offensive strategy could be the component of this strategy.
- Well thought-out plan incorporating cyber and ground intelligence resources seems mandatory. Long term strategic planning and consistency of efforts seem necessary in it.
- Selection of target (strategic / tactical), acquisition of persistent ingress and attaining exploitation capability well before the hostility breakout would provide necessary advantage.
- Comparatively financially heavy (developing

Prevailing local laws / instructions on the subject also enhance the defence mechanisms and thwart criminal activities

workforce and technology acquisition), extremely dependent upon ICT support from manufacturer and developer.

Sporadic Cyber Defence. Organized and well planned cyber defence activities to thwart hostile attempts of cyber criminals, terrorists or rogue elements to destroy, damage or cripple adversary's military ICT capabilities (communication, battle field management systems and decision support/ making networks), ICT dependent government and private sectors (economic, financial, communication, development etc.). Factors effecting execution of such operations are enumerated below:

- Well organized effort to secure non-military targets in which cyberattacks are mostly executed to acquire secret / classified data, trade secrets, personal information etc. from computers and mobile phones. Cyber stalking has also been identified as a new offensive activity with respect to this defensive technique.
- The offensive activity could be conducted by novice hacker or an expert resource depending upon the target involved.
- The effort includes development of Trojans and launching these through Social Engineering, Smear Phishing/ Phishing techniques.
- Adherence to organizational/ institutional policies for secure computer and mobile phone usage, antivirus / malware solutions and cyber security awareness could enhance the effort.
- Prevailing local laws / instructions on the subject also enhance the defence mechanisms and thwart criminal activities.

Conclusion

Cyber warfare is a fast-changing warfare due to dynamic nature of cyberspace, therefore the techniques mastered in this warfare are never all-encompassing. Every now and then newer techniques emerge due to emerging technologies. With the boom of social media, AI, crypto currencies and hyper-connectivity etc, new vistas come up periodically. Future wars cannot be won without supremacy in the field of cyber warfare.

NOTES

1. J. Andress and S. Winterfeld, Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. USA: Elsevier Syngress 2011.
2. S. Mukherjee, "Cyber Warfare and Implications," doi: http://dx.doi.org/10.2139/ssrn.3431676.
3. R. A. Clarke and R. Knake, Cyber War: The Next Threat to National Security and What to Do About It. Harper Collins Publishers, 2010.
4. Joint Publication 3-12, Cyberspace Operations. (2018). Joint Chief of Staff, Armed Forces of the United States.
5. S. Winterfeld and J. Andress, The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice. Elsevier Inc., 2012.
6. P. W. Singer and A. Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2014.
7. I. Bernik, Cybercrime and Cyberwarfare. John Wiley & Sons, Inc., 2014.
8. Y. Riahi and S. Riahi, "Big Data and Big Data Analytics: Concepts, Types and Technologies," International Journal of Research and Engineering, no. 9, pp. 524-528%V 5, 2018-11-06 2018, doi: 10.21276/ijre.2018.5.9.5.
9. Mazarr et al., "Hostile Social Manipulation: Present Realities and Emerging Trends." [Online]. Available: https://www.rand.org/pubs/research_reports/RR2713.html
10. A. Ali, A. K. Malik, M. Ahmed, B. Raza, and M. Ilyas, "Privacy Concerns in Online Social Networks: A Users' Perspective," International Journal of Advanced Computer Science and Applications, vol. 10, no. 7, 2019, doi: 10.14569/IJACSA.2019.0100780.
11. "Cyberattack Trend Analysis - 2019 Security Report," Check Point Software Technologies Ltd, San Carlos, USA, 2019, vol. 01. [Online]. Available: http://snt.hr/boxcontent/CheckPointSecurityReport2019_vol01.pdf
12. A. Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Countermeasures," Procedia Economics and Finance, vol. 28, pp. 24-31, 2015/01/01/ 2015, doi: https://doi.org/10.1016/S2212-5671(15)01077-1.
13. "Seminar Report "Cyber Secure Pakistan – Policy Framework"," Center for Global and Strategic Studies, Islamabad, Pakistan, 2018.
14. M. Michael. "Attack landscape H2 2018: Attack traffic increases fourfold." https://blog.f-secure.com/attack-landscape-h2-2018/ (accessed 4-9-2020.
15. Ibid
16. Ibid
17. U. K. Singh, C. Joshi, and D. Kanellopoulos, "A framework for zero-day vulnerabilities detection and prioritization," Journal of Information Security and Applications, vol. 46, pp. 164-172, 2019/06/01/ 2019, doi: https://doi.org/10.1016/j.jisa.2019.03.011.
18. D. Galinec, D. Možnik, and B. Guberina, "Cybersecurity and cyber defence: national level strategic approach," Automatika, vol. 58, no. 3, pp. 273-286, 2017/07/03 2017, doi: 10.1080/00051144.2017.1407022.
19. M. Erbschloe and J. R. Vacca, Information Warfare: How to Survive Cyber Attacks. Osborne/McGraw-Hill, 2007.