JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Beyond the Firewalls: A Deep drive into the Cyberwarfare strategies.

Puloma Pal
Student and Researcher
Amity Institute of International Studies,
Amity University, Noida, India

Abstract: Cyberwarfare has become a significant issue in the modern geopolitical landscape, with complex tactics such as APTs, zero-day vulnerabilities, and social engineering methods being used. The landscape is complex, with roles of non-state actors, government agencies, and unidentified cyber mercenaries in executing cyberattacks. It is essential to comprehend these goals in order to foresee and handle future cyberattacks. The influence of offensive cyber operations on international relations, global economy, and national security is also examined in this paper. The process of recognizing assaults and creating defences is made more difficult by the differences between digital espionage, cyber sabotage, and cyberwarfare. A comprehensive plan combining offensive and defensive strategies is needed to mitigate risks related to digital warfare. This article contributes to the discourse by highlighting the subtle aspects of digital warfare strategies and advocating for proactive cybersecurity.
Keywords - Cyber Warfare, APTs and Zero day Vulnerability, International relations, Cybersecurity, Geopolitics

I. INTRODUCTION

Modern geopolitics and Cyber warfare - In contemporary geopolitics, cyberwarfare has grown to be a powerful force that is erasing the distinction between real-world and virtual conflicts. The combination of cyber operations and conventional military techniques has resulted in coordinated cyberattacks that have affected institutions all around globe. Enormous DDoS assaults, a rise in malware operation, focused scams involving phishing, misinformation efforts, and cyber-physical system risks to critical systems are all part of the danger environment (Proctor, 2022). Cyberwarfare is a global issue, and energy firms in China and Germany are taking advantage of this to spread threats. Globally, organizations have reinforced their defences against threat information and incident handling skills, examined and restricted the strategies of recognized threat actors, and prioritized awareness of security and communication in addition to taking cybersecurity action (Ribeiro, 2024).

The Traditional defensive mechanism like firewall and its inadequacy - In the ever-changing cybersecurity world, conventional protection techniques like rule-driven barriers and detection based on signatures confront difficulties. Firewalls find it difficult to dynamically adjust to new concerns or quickly evolving attack patterns since they filter network traffic according to pre-established criteria. Although detection via signatures depends on well-known trends, hackers can simply circumvent identification by changing their attack strategies or taking use of zero-day attacks. Cyber-attacks nowadays are complex and multidimensional, using methods like payload encryption, obfuscation, and polymorphism. In order to tackle these obstacles, scholars have employed Deep Reinforcement Learning (DRL) frameworks to mimic cyberattacks (Fruhlinger, 2022), utilizing real-world circumstances to augment realism. The actor-critic algorithms fared better than the others, with a 0.78 rate of success and greater effectiveness.

The Offensive Cyberwarfare strategies - In contemporary combat settings, offensive cyber warfare strategies—which involve proactive actions to disrupt or impede harmful cyber activity—are essential. "Defence forward" was an idea first presented by the US Department of Defence to combat threats and support victims of ransomware (Brumfield, 2022). Technical command and control, exploit development, malware payload creation, operational oversight, vulnerability research, training, and assistance are some of these tactics (DeSombre, et al., 2021). Determining what exactly qualifies as an act of war in cyberspace is still difficult, though, because the Law of Armed Conflict permits quick physical reactions to cyberattacks {1}. Since offensive cyber is a political decision driven by national cybersecurity objectives, striking a balance between attack and defence is crucial to preserving security in cyberspace.

II. LITERATURE REVIEW

Evolution - The dynamic nature of digital combat has led to a major evolution in cyber warfare tactics and technology (Baloch, 2019 - 2020). The early strategies focused on disrupting or stealing data from specific systems or networks. Sophisticated methods like as spear phishing, zero-day attacks, and social engineering have been used over time (Check Point, 2024). The integration of hybrid warfare techniques with conventional military tactics has enabled the execution of synchronized assaults in several sectors. In cyberwarfare, nation-state actors have become major players, utilizing assets and expertise to launch massive strikes. Smaller entities can confront larger opponents through asymmetric warfare. Data weaponization is becoming a common strategy in contemporary digital warfare. The use of cutting-edge technology in cyberwarfare has been further revolutionized by

AI, machine learning, and quantum computing (Check Point, 2024). Global ramifications result from the growth of cyberwarfare, which calls for constant innovation, cooperation, and adaptation.

What motivates the cyber attackers? - Hacktivist, insiders, organized crime organizations, sabotage and disruption, geopolitical purposes, and espionage are some of the reasons behind cyberattacks (Nershi & Grossman, 2022). Nation-state actors, frequently backed by the government, carry out espionage to learn about the military prowess, economic secrets, and political or commercial objectives of their adversaries; they also carry out cyberattacks, sabotage, and disruption to compromise vital infrastructure. Financially driven criminal syndicates extort funds from victims, especially weaker enterprises, by using ransomware assaults. Hacktivist, such as Anonymous, employ cyberattacks to spread awareness and further their causes, while insiders like Edward Snowden, who have access to private information may use it for retaliation or personal gain (Startup defense, 2023). For cybersecurity measures to be successful, it is important to comprehend these reasons.

Implication - Offensive cyber missions have a significant impact on national security and international relations, changing the security environment, diplomatic dynamics, and strategic planning (Skingsley, 2019). These actions have the potential to undermine international cooperation and confidence, raise the danger of escalation, undermine accepted standards and codes of interaction, and alter the balance of power in geopolitics. States with sophisticated cyber capabilities have the potential to exert an outsized impact on global events, influencing the dynamics of international relations and alliances of strategic importance.

Critical infrastructure is vulnerable, making it possible to conduct clandestine collecting data and monitoring operations over foreign enemies, endangering national security. National security is also at risk from cyber terrorism and hybrid warfare as they target government facilities, vital infrastructure, and civilian populations.

The likelihood of cyberattacks leading to escalation and counter-escalation in a vicious cycle that intensifies instability and insecurity gives rise to fears of escalation and reprisal. It is challenging to place blame and hold criminals accountable for digital crimes because to their anonymous and defendable nature, which raises important questions about culpability.

III. METHODOLOGY

Research Methods: With an emphasis on Iran specifically, this study uses a qualitative research methodology to examine and comprehend offensive cyberwarfare tactics. The selection of qualitative methodologies facilitates a comprehensive investigation of the topic, encompassing the reasons behind, strategies employed, and consequences resulting from Iran's cyber operations.

Choice of Case Study: Iran is chosen as the major case study because of its growing importance in the field of cyberwarfare and its substantial influence on the dynamics of global cybersecurity. The decision was made after a review of the body of research, reports, and expert evaluations that demonstrated Iran's engagement in cyber operations against a range of targets, including persons, countries, and organizations.

Approaches for Gathering Data:

Literature Analysis: To learn more about Iran's digital warfare capabilities, past cyberattacks, and its diplomatic objectives, a thorough analysis of scholarly journals, research papers, official publications, and reliable news items is carried out.

Professional Analyses: To get nuanced viewpoints and confirm findings, insights from professionals in cybersecurity, analysts, and practitioners specialized in Iranian cyber operations are taken into consideration.

Case Studies: An analysis of strategies, methods, and results is conducted by looking at pertinent case studies that detail particular cyber occurrences involving Iran.

Government publications: To learn the official line on Iran's cyber activities and reactions, one should reference official publications and announcements from government authorities, such as the departments of cybersecurity and intelligence.

Intelligence that is Open-Source (OSINT): To add to the findings of the study and give more context, publicly accessible data is evaluated, such as cybersecurity forums, blogs, and social media debates.

Resources:

Peer-reviewed scholarly journals, reliable research papers, government publications, trustworthy news sources, and professional analyses from respectable cybersecurity groups are only a few of the sources that were used in this study. When it comes to reporting on cybersecurity and foreign relations, sources with a track record of accuracy and dependability are given particular consideration.

The Analysis of the Data:

To find recurrent themes, trends, and important insights from the gathered data, thematic analysis is used. The analysis aims to comprehend Iran's offensive cyber abilities strategies, and goals, as well as the effects of its cyber activity on global relationships and the state of cybersecurity globally.

Authenticity and Accuracy:

Various sources are compared, and methods of triangulation are used where appropriate to guarantee the accuracy and dependability of the results. To improve the reliability of the study findings, critical assessment of the reliability of sources and cross-referencing of data from various angles are done.

Ethical issues:

The entire study deals with the ethical issues are crucial. Academic credibility and honesty are preserved by adhering to ethical rules guiding research concerning delicate themes, respecting intellectual property rights, and properly citing sources. Furthermore, endeavor are undertaken to exhibit results truthfully and impartially, circumventing partiality or fabrication of data.

IV. CASE STUDY: IRAN

Since the latter part of 2022 campaign, when it launched the 24-operation Cotton Sandstorm campaign, Iran has greatly stepped up its attempts to wage digital warfare (The Iran Primer, 2023). This illustrates Iran's capacity to utilize cyber skills for disturbances, espionage, and coercion—all strategic goals. Iranian hackers proved their capacity to target critical systems in other countries when they broke into the Bowman Avenue Dam in New York in 2013. 2019 saw Iranian hackers showcasing their extensive cyber espionage efforts by targeting the Trump campaign, American officials, the media, and Iranian expatriates. Destructive malware and ransomware have been used in Iran's recent state-sponsored cyber operations, endangering the vital infrastructure of the United States and perhaps resulting in extensive disruption and monetary losses. This emphasizes the necessity for prospective targets to exercise more caution and implement strong cybersecurity safeguards.

International security is becoming increasingly concerned about Iran's cyber capabilities (Daragahi, 2023). The nation has been shown creativity and agility as it has been strengthening its cyberwarfare, espionage, and sabotage capabilities. Iranian cyber forces target financial institutions, media organizations, government institutions, and military facilities with offensive operations such as spear phishing, DDoS assaults, online defacement, and data tampering (CyberSecurity & Infrastructure Security Agency., n.d.). These actions, motivated by resentment and an ambition for influence in the area and beyond, are consistent with Iran's larger security policy. It is recommended that organizations prioritize the remediation of vulnerabilities that are exploited and establish fundamental cybersecurity procedures.

Despite not ranking among the top cyber powers, Iran has made great progress in strengthening its cyber capabilities (Rashid, 2016). The nation's understanding of cyberspace as an asymmetric tool for enhancing national power, evading global penalties, transforming the economy, upending regional rivals in the Middle East (IronNet Threat Research and Intelligence Teams., 2021), retaining custody over the Ayatollah's government, and penalizing and disproving ideological opponents, is the driving force behind its cyberwarfare strategy and organization. Iran uses its cyber abilities especially in the face of possible protests similar to the Arab Spring, to counter the influence of rival states, stifle dissent, and retain control over its populace. The evolution of cyber power is a reaction to both the ongoing battle and Iran's weaknesses.

Iran employs a combination of diplomatic manoeuvres, defensive postures, and punitive measures in reaction to global cyber threats. It uses intrusion detection systems, makes investments in cyber protection, and pursues diplomacy through global fora like the UN. Iran may launch its own cyberattacks in retaliation, using non-state actors or proxy organizations to carry out cyber operations on its own. In order to sway public opinion and undermine enemies, it may also participate in digital warfare and propaganda operations. Cyber espionage activities improve awareness of situations in cyberspace by gathering intelligence on the cyber skills and risks of other countries. Iran's strategic goals, worries about national security, and attempts to protect its own interests in cyberspace in the face of growing hostilities and geopolitical rivalry are all reflected in these replies.

V. DISSCUSSION.

The networks and data of the United States and its allies are seriously threatened by Iran's expanding cyber capabilities and aggressive actions. Establishing Cyber Performance Goals and prioritizing exploit vulnerability mitigation should be top priorities for organizations. Iran's influence operations, facilitated by cyberspace, facilitate geopolitical shifts by providing low-cost deterrent and external threat management. Top Iranian cyberattacks use PowerShell, disguised documents or data, and credential dumps. Comprehending Iran's aggressive tactics is important for efficient defence and global collaboration.

Iran's cyber abilities have a big impact on national security, international relations, and cybersecurity overall. They can threaten vital infrastructure, increase hostilities, and make it difficult to assign blame for assaults. Countries need to set guidelines, work together to share information, and improve cyber resilience in order to reduce these dangers.

The security of US and partner networks and data is seriously threatened by Iran's aggressive cyber activities. The necessity for strong defences and preventative measures is highlighted by recent state-sponsored actions in Iran, such as ransomware and damaging malware campaigns. Patching risks, putting Cyber Performance Goals into practice, and disclosing unusual activities to CISA or the FBI are examples of mitigation techniques. Iranian cybercriminals take advantage of weaknesses in a number of industries, such as intrusions into government networks, cyberattacks on Albania, as well as information extraction and ransom schemes using U.S. wastewater and water supply facilities. Iran sees cyberspace as an asymmetric weapon for spying on other governments, businesses, educational institutions, non-governmental organizations, and its own people. To solve these issues and lessen the global effect of cyber threats, international collaboration and legislative frameworks are essential.

VI. CONCLUSION

In the digital era, preventative cybersecurity measures are essential since cyber threats are ever-changing and can affect a country's economic, national security, data security, and global interconnectivity. In order to create an extensive national cybersecurity plan that involves government agencies, the business sector, educational institutions, and civil society, Iran's leaders and practitioners should take a holistic approach. In order to effectively combat cyber threats, they should work with other countries to develop operational incident response teams, implement and enforce cybersecurity rules and regulations, encourage public-private collaboration, invest in cybersecurity training, education, and skill development for professionals, and inform citizens and organizations about cyber risks and secure practices.

Future research prospects for cyberwarfare methods in Iran include hybrid warfare, digital standards and international law, cyber-physical integration, active defensive strategies, sophisticated threat prediction, behavioral analytics, and attribution techniques. Iran can bolster its resilience, safeguard its people, and promote global cyber stability by adhering to preventive cybersecurity. An understanding of Iran's cyber future and possible dangers may be gained from reading research papers on the nation's cyber capabilities and reactions to cyber threats.

VII. WORKS CITED

1. Middle East Institute (MEI). (2021, February 23). Iran’s cyber future. https://www.mei.edu/publications/irans-cyber-future
2. Siboni , G., & Kronenfeld, S. (2012, October 15). Iran’s Cyber Warfare. Institute of National Security Studies (INSS). https://www.inss.org.il/publication/irans-cyber-warfare/
3. Microsoft Security: Freedom to innovate. (2023, June 14). Microsoft special report: Iran’s adoption of cyber-enabled influence operations. CSO Online. https://www.csoonline.com/article/575581/microsoft-special-report-iran-s-adoption-of-cyber-enabled-influence-operations.html
4. Shayda Pendleton, C., & Bucala , P. (2015, November 24). Iranian Cyber Strategy: A View from the Iranian Military. Critical Threats; Critical Threats. https://www.criticalthreats.org/analysis/iranian-cyber-strategy-a-view-from-the-iranian-military
5. Connell, M. (2014). Deterring Iran’s Use of Offensive Cyber: A Case Study. In Indian Strategic Knowledge. Indian Strategic Knowledge. https://indianstrategicknowledgeonline.com/web/DIM-2014-U-008820-Final.pdf
6. Lewis, J. (2019, June 25). Iran and Cyber Power. Csis.org. https://www.csis.org/analysis/iran-and-cyber-power

7. Zvelo. (2023, September 20). Defense-in-Depth: A Layered Strategy for Modern Cybersecurity. Zvelo. https://zvelo.com/defense-in-depth-layered-strategy-for-modern-cybersecurity/
8. Dragoo, H.M. (2021). Exploring the Spread of Offensive Cyber Operations Campaigns. In: Kosal, M.E. (eds) Proliferation of Weapons- and Dual-Use Technologies. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-030-73655-2_9
9. Check Point Researchers. (2024). 2024's Cyber Battleground Unveiled: Escalating Ransomware Epidemic, the Evolution of Cyber Warfare Tactics and strategic use of AI in defense – Insights from Check Point's Latest Security Report. In Check Point Research. CPR. https://research.checkpoint.com/2024/2024s-cyber-battleground-unveiled-escalating-ransomware-epidemic-the-evolution-of-cyber-warfare-tactics-and-strategic-use-of-ai-in-defense-insights-from-check-points-latest-security-re/
10. Kastelic, A. (n.d.). International Cyber Operations: National Doctrines and Capabilities. In United Nations Institute for Disarmament Research. International Cyber Operations Research Paper Series. https://unidir.org/files/2021-05/International%20Cyber%20Operations%20Series%20-%20Paper%201%20-%20Final.pdf
11. Baloch, R. (2019 - 2020). Cyber Warfare Trends, Tactics and Strategies: Lessons for . Journal of Development Policy, Research & Practice, 3 and 4 (January – December 2019 - 2020), 51 to 71. Retrieved from https://pdfs.semanticscholar.org/7803/ff63e484935d0ba240b7ed13f88535863dc2.pdf
12. Brumfield, C. (2022, 9 13). U.S. government offensive cybersecurity actions tied to defensive demands. Retrieved from CSO: https://www.csoonline.com/article/573597/u-s-government-offensive-cybersecurity-actions-tied-to-defensive-demands.html
13. Check Point. (2024). 2024'S CYBER BATTLEGROUND UNVEILED: ESCALATING RANSOMWARE EPIDEMIC, THE EVOLUTION OF CYBER WARFARE TACTICS AND STRATEGIC USE OF AI IN DEFENSE – INSIGHTS FROM CHECK POINT'S LATEST SECURITY REPORT. Tel Aviv: Check Point. Retrieved from https://research.checkpoint.com/2024/2024s-cyber-battleground-unveiled-escalating-ransomware-epidemic-the-evolution-of-cyber-warfare-tactics-and-strategic-use-of-ai-in-defense-insights-from-check-points-latest-security-re/
14. CyberSecurity & Infrastructure Security Agency. (n.d.). Iran Cyber Threat Overview and Advisories. Retrieved from CyberSecurity & Infrastructure Security Agency.: https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran
15. Daragahi, B. (2023, 5 24). Iran is using its cyber capabilities to kidnap its foes in the real world. Retrieved 2024, from Atlantic Council: https://www.atlanticcouncil.org/blogs/iransource/iran-cyber-warfare-kidnappings/
16. DeSombre, W., Campobasso, M., Allodi, D. L., Dr, Shires, J., Work, J., . . . Herr, D. T. (2021, 03 01). A primer on the proliferation of offensive cyber capabilities. Retrieved from Atlantic Council: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/a-primer-on-the-proliferation-of-offensive-cyber-capabilities/
17. Fruhlinger, J. (2022, 7 28). Defense in depth explained: Layering tools and processes for better security. Retrieved 03 20, 2024, from CSO: https://www.csoonline.com/article/573221/defense-in-depth-explained-layering-tools-and-processes-for-better-security.html
18. IronNet Threat Research and Intelligence Teams. (2021, 4 12). Strategic goals behind Iranian cyber attacks. Retrieved from Iron Net: Despite not ranking among the top cyber powers, Iran has made great progress in strengthening its cyber capabilities. The nation's understanding of cyberspace as an asymmetric tool for enhancing national power, evading global penalties, transforming the e
19. Nershi, K., & Grossman, S. (2022). Assessing the Political Motivations Behind Ransomware Attacks. Central Bank bahamas, 5 to 39. Retrieved from https://bahamasamlconference.centralbankbahamas.com/assets/images/pdf/conferences/2023/nershi-grossman_ransomware.pdf
20. Proctor, P. (2022, 6 10). How Geopolitics Impacts the Cyber-Threat Landscape. (M. Rimol, Interviewer) Gartner. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2022-06-10-how-geopolitics-impacts-the-cyber-threat-landscape
21. Rashid, B. (2016, 05 02). Iranian Capabilities in the Field of Cyber Warfare. Retrieved from International Institude for Iranian Studies: https://rasanah-iiis.org/english/centre-for-researches-and-studies/iranian-capabilities-in-the-field-of-cyber-warfare/
22. Ribeiro, A. (2024, 02 18). Growing convergence of geopolitics and cyber warfare continue to threaten OT and ICS environments in 2024. Retrieved from Industrial cyber: https://industrialcyber.co/features/growing-convergence-of-geopolitics-and-cyber-warfare-continue-to-threaten-ot-and-ics-environments-in-2024/
23. Skingsley, J. (2019). Offensive cyber operations: States' perceptions of their utility and risks. Chatam House, 3 to 5, 7 to 13,14 to 25. Retrieved from https://www.chathamhouse.org/sites/default/files/2023-09/230919-offensive-cyber-operations-skingsley.pdf
24. Startup defense. (2023, 6 1). Understanding the Motivations and Goals of Cyber Attackers: A Guide for Security Practitioners. Retrieved from Startup defense: https://www.startupdefense.io/blog/understanding-the-motivations-and-goals-of-cyber-attackers-a-guide-for-security-practitioners
25. The Iran Primer. (2023, 7 31). Iran Accelerates Cyberattacks. Retrieved from The Iran Primer: https://iranprimer.usip.org/blog/2023/may/03/report-iran-accelerates-cyberattacks