Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

The Cyber-Geopolitical Nexus: Conflicts, Impact and Global rules

Gaurang Neha Vishwajit Marathe
Dept. of Computer Science
Dr. D. Y. Patil ACS College, Pimpri
Pune, India

Atharva Rajendra Tambe
Dept. of Computer Science
Dr. D. Y. Patil ACS College, Pimpri
Pune, India

Abstract **- The paper explores the complex features between geopolitics and cyberwarfare links, highlighting their growing impact on international relations and security. It examines the occurrences for state-sponsored cyberattacks, including economic disruption, political turmoil, and espionage, and provides prominent examples, such as SolarWinds, Iranian cyberattacks on Israel, and electoral interference in Romania. The paper discusses the difficulties of responsibility and accountability brought on by the use of proxies and anonymity in cyber operations, as well as how cyberwarfare increases tensions and impacts international relations. The absence of strictly followed cybersecurity norms is researched as well, highlighting the critical need for global norms and international collaboration. In order to reduce the risks associated with this modern threat to peace and security, the study highlights the significance of strong cybersecurity measures and cyber diplomacy.**

Keywords - ***Cyber Security, Cyber Warfare, Geopolitics, Diplomacy.***

I. INTRODUCTION

The rapid growth of technology in the current digital era has given international disputes new dimensions. Among these, cyberwarfare is especially important as an adverse impact that affects the way countries operate, influence and power. The primary focus of this study is the increasing connection between geopolitics and cyberwarfare. The study specifically looks at how state-sponsored cyberattacks have replaced traditional combat as the main means of accomplishing strategic goals. These operations, in which the criminals remain anonymous, attack vital infrastructure, affect operations, and increase tensions between nations.

Studying how cyberwarfare works as a tool of geopolitical strategy and the challenges it presents for global governance and accountability is the main research subject. This paper is unique because it examines the multiple effects of cyberattacks, which are frequently examined separately, on both a technological and political level. This study aims to address a significant knowledge gap about the integrated nature of cyberwarfare and its greater consequences for global security and diplomacy by integrating multiple points of view. The study is important because it highlights an important global issue and provides information that is essential for finding solutions and encouraging global collaboration to counter this modern threat.

II. METHODOLOGY

A. Research Design

As cyberwarfare involves deep political, strategic, and safety concerns that cannot be entirely analyzed, this study utilizes a qualitative and exploratory method with supporting quantitative insights. A comparative case study approach is utilized to examine several cyber warfare cases that have occurred in recent years. These cases involve state-sponsored cyberattacks that target critical infrastructure including the IT sector, power supply, water systems, healthcare facilities, democratic elections and more. This method helps in identifying repetitive patterns, strategic goals, and geopolitical effects of modern cyberwarfare.

B. Tools and Technologies Used

This study is based on secondary research and does not involve experimental tools or simulations. The following tools and resources were used:

- Reputed cybersecurity and threat intelligence reports published by trusted organizations.
- Various academic research databases and papers.
- Digital documentation and reference management tools for organizing data and citations
- The Global Cyber Security Outlook Report 2025 published by the World Economic Forum.

III. RESULT

The Three Main Features of Cyber-Geopolitical Nexus:

1. State-Sponsored Cyberattacks

   State-sponsored cyberattacks are majorly an important aspect of modern geopolitical conflicts. Governments are increasingly using cyber capabilities as strategic tools to achieve their political, military, and economic objectives. These cyber operations typically confidential, making it difficult to find and punish the offenders. Unlike conventional warfare, cyberattacks do not require direct military involvement; instead, they target government agencies, private businesses, and critical infrastructure,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

disrupting critical functions and causing significant damage.

Various well-known cyberattacks represent powerful cases of how nations use cyberspace as a battlefield to achieve their geopolitical aims. These attacks can involve anything from economic and military damage to political influence and espionage.

Here are a few significant cases that highlight how cyberwarfare shapes world geopolitics:

- SolarWinds (2020): A supply chain intrusion connected to Russian hackers that affected several U.S. government organizations.
- Iran-Israel Infra Attacks (2024): Increased cyber operations targeting Israel post-Gaza war, impacting critical infrastructure and defence systems.
- Influence campaign in Romania Elections (2024): A major attempt to interfere in the country's presidential elections using the social media platform TikTok, and with a series of cyber-attacks.
- ESET Claims Attacks on Systems (2025): Israeli organizations hit by a cyberattack spreading pro-Hamas propaganda amid hostage return process.
- Norway dam sabotage (2025): Russian hackers took access of a dam in Bremanger, western Norway and opened a flood gate to release 500 litres (i.e. 132 gallons) of water per second for 4 hours.
- Cyber Attack on Polish Power Grid (2025): A Russian state-sponsored hacking group, 'ELECTRUM,' was alleged to be the perpetrator of the coordinated cyberattack that targeted numerous locations around the Polish power grid.
- Crimson RAT attempt (2025): Using the emotional impact from the terror attack in Pahalgam in April 2025, Pak-based APT36 group used Crimson RAT as a specific bait to breach Indian government and defence networks using phishing and social engineering techniques.

An absolute ironical part was a historical advocate of the Palestinian cause, and member of the Palestinian Liberation Organization (PLO), had himself fallen victim of hackers targeting Israeli cyberspace in solidarity with Palestine.

State-sponsored cyberattacks can be motivated by various motives, including data collection, financial damage and political dominance. Cyberattack is a unique approach for geopolitical manipulation as compared to traditional warfare, they enable countries to take down rivals without engaging in direct battle.

The ongoing conflict between Russia and Ukraine is one of the most prominent scenarios of cyberwarfare influencing global events. Ukraine has been the victim of frequent cyberattacks since 2014 that have targeted its banking system, communication networks, and electrical grid. These attacks have resulted in the disruption of public services, the spread of false information, and a surge in tensions between the two nations. In 2015 and 2016, Russian hackers launched cyberattacks that resulted in severe blackouts in Ukraine, demonstrating the capacity of cyber operations to create major disruptions.

In the same way, China was accused of cyber espionage against the United States and its allies, especially targeting technological organizations, research institutes, and defence personnel. The goals of these breaches were to collect military intelligence, steal intellectual property, and boost China's technological development.

The Graph below shows the response of various businesses over the world about the influence of geopolitical tensions on their cybersecurity strategies.

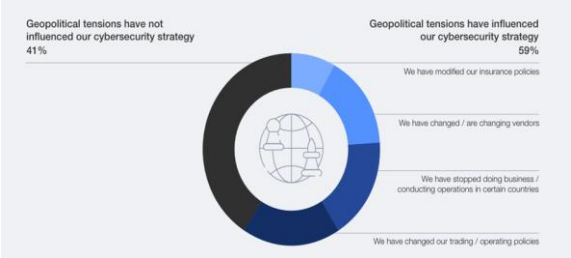

Fig. 1. Influence of geopolitical tensions on cybersecurity strategies (Reference: Global Cyber Security Outlook Report 2025 by World Economic Forum)

2. Impact on International Relations

A notable example of cyberwarfare impacting global affairs is the suspected Russian involvement in the 2016 U.S. presidential election. In order to influence public opinion, cyber agents suspected of being connected to Russian intelligence services planned a massive distraction operation, broke into email accounts belonging to political parties, and purposefully released private material. This cyberattack increased tensions between the US and Russia in addition to raising doubt on the legitimacy of democratic processes. The United States responded by dismissing diplomats, enforcing penalties against Russian people and organizations, and improving cybersecurity defences against future election interference.

The case of Romania's 2024 presidential election shows the increasing relations between geopolitics and cyber-influence operations. The results were scrapped because of allegations that TikTok was used to influence voter opinions and promote political campaigns. TikTok and other platforms allow for targeted campaigns that use algorithmic streaming of videos to improve political propaganda. It looks like Romanian political candidates have taken advantage of the platform to interact with

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

younger people. However, when these tools are used to spread false information, problems happen.

Cyber influence in elections sometimes links with international relations. Larger concerns about how foreign entities or opponents can use social media platforms to influence election results in their favour are raised by claims in Romania. This resulted to even more criticism, especially when it comes to ties between Western countries and nations like China and Russia, which have been accused of using similar tactics in the past.

The difficulty of defining proper responses and getting precise connection is the primary challenge for efficiently combating cyberwarfare. Cyberattacks frequently contain layers of deception, as compared to traditional battles when acts of aggression can be directly connected to certain states or entities. To avoid detection, attackers commonly use strategies including hiding digital footprints, utilizing proxy servers, and launching attacks from hacked third-party networks. This uncertainty makes it difficult to apply preventive measures or tactics and poses a major challenge to accountability. Targeted countries find it difficult to defend retaliatory measures in the lack of clear evidence connecting cyberattacks to particular criminals, creating an endless loop of uncertainty and rising tensions.

3. Challenges in Responsibility and Accountability

One of the most challenging aspects of tackling cyberwarfare is identifying attackers. Cyberattacks regularly use proxies, false flags, and anonymity tactics, making detection more difficult. In fact, there is substantial evidence connecting the Russian government to the SolarWinds attack, though the full technical details remain classified.

Cybercriminals frequently have proxy networks and third-party hacking groups to mask their involvement. These third parties can be independent hacking networks, cybercriminal associations, or professional groups hired by governments to carry out activities on their side. The technique enables states to achieve their political aims while effectively denying their involvement. Because attackers may purposely leave fake evidence to suggest other nations or organizations and distract attention away from the actual operators, false flag operations make detection much more challenging.

The lack of internationally accepted regulations and standards for digital operations increases the issue. Policies like the Tallinn Manual make suggestions, but they are not legally binding. Because there is no worldwide agreement on cybersecurity legislation, states are free to exploit the gaps in international law. Finally, because geopolitical conflicts limit cooperation, governments usually place their strategic goals ahead of universal safety.

IV. DISCUSSION

The rise in cyberwarfare has drastically changed the nature of international relations by introducing new challenges to global governance, security measures, and diplomatic interaction. Because cyberwarfare takes place in the virtual world, it is more challenging to identify, attribute, and react to attacks than traditional forms of conflict, which depend on physical force and prominent aggression. As a result, states looking to influence others, provoke enemies, or threaten political stability without committing to straight military conflict now prioritize cyber operations.

International organizations like NATO and the QUAD alliance, which consists of the United States, India, Japan, and Australia have made cybersecurity a top priority as a crucial component of international security policies in recognition of the growing threat posed by cyberwarfare. Significant efforts have been made by NATO, in particular, to integrate cyberwarfare into its defensive strategy. The strategic importance of digital security was highlighted in 2016 when NATO officially acknowledged cyberspace as an operational region alongside land, air, and sea. Additionally, cyberattacks are now included as possible triggers for collective defence measures under NATO's Article 5, which declares that an attack on one member is considered an attack on all. This change demonstrates how cyberwarfare is increasingly influencing military alliances and geopolitical plans.

Measures to create legal frameworks for countering cyberthreats include the UN Charter or even Tallinn Manual which is an in-depth study of the application of international law to cyber activities of 3 versions. However, enforcement is still difficult because there are no legally binding international norms, and many countries still use cyberspace as a grey area for espionage activities.

Cyberwarfare's influence on international relations will only grow as it develops stronger. Global stability is at risk due to the rise of state-sponsored hacking, technological influence operations, and cyber espionage, which calls for closer diplomatic ties. Developing internationally accepted guidelines for cyberspace, improving cyber resilience, and encouraging openness in cyber defence efforts are all tasks that nations must undertake. The lines between digital and physical combat get blurred in international conflicts until there is a coordinated worldwide effort to combat the growing cyber threat.

V. CONCLUSION

A complex combination has emerged in the modern world as a result of the integration of cyberwarfare and geopolitics. Strong cybersecurity measures and international cooperation are essential in light of state-sponsored cyberattacks, their effects on international relations, and the challenges involved in responsibility and accountability. The overdependency on internet for essential services could have adverse impacts on international peace and security if preventive measures are not taken. Countries must acknowledge the importance of cyber diplomacy and cooperate to properly solve these issues.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

Strong cybersecurity measures and international cooperation are now essential due to the growing frequency and complexity of attacks. Updating cybersecurity policies are necessary to strengthen nation's cyber defence, incorporating several strategic solutions that can be implemented. Some solutions that should be considered include enhancing the capacity of human resources in cybersecurity, strengthening more secure information technology infrastructure, and updating regulations to accommodate changes in cyberattack trends.

The creation of global guidelines for online conduct is a crucial first step in solving this issue. Various nations must cooperate to develop frameworks that encourage responsible state conduct in cyberspace. Cyberwarfare will continue to develop into an uncontrolled entity in the absence of a coordinated worldwide reaction, raising geopolitical issues and reversing international peace. The United Nations, NATO, and regional alliances are among the international or peacekeeping organizations that must collaborate to create legally binding cybersecurity standards that specify what constitutes appropriate and inappropriate cyber behaviour. These frameworks require to include precise guidelines for resolving cyber conflicts, routes for exchanging intelligence, and penalties for nations that commit cyberattacks when proven with involvement.

Also, reducing cyber conflicts involves encouraging global trust. Increased diplomatic efforts can reduce the political tensions and insecurities which caused many cyberattacks. Discussions focused on cybersecurity agreements and regulations, or "cyber diplomacy," need to be a major component of international relations. Regular regional and global discussions can help countries work together to combat cyberthreats, clarify misconceptions, and stop disputes from getting worse because of cyberattacks. Above mentioned Conclusions on the situation, can light the way for future application of international law.

REFERENCES

1. https://www.thehindu.com/news/international/irans-cyber-attacks-against-israel-surged-since-gaza-war-report/article68759281.ece
2. https://www.bbc.com/news/articles/cgq18w507dko
3. https://www.jpost.com/israel-news/article-838245
4. https://www.bbc.com/news/world-us-canada-44825345
5. https://www.inss.org.il/publication/iran-israel-cyber-war/
6. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/
7. https://socradar.io/blog/india-pakistan-kashmir-escalation-on-cyber-world/
8. https://industrialcyber.co/reports/russian-hybrid-threats-likely-to-escalate-around-2025-nato-summit-putting-european-critical-infrastructure-at-high-risk/
9. https://sqmagazine.co.uk/cyber-warfare-statistics/
10. https://www.reuters.com/technology/norway-spy-chief-blames-russian-hackers-dam-sabotage-april-2025-08-13/
11. https://www.aha.org/news/headline/2025-09-03-advisory-warns-activity-chinese-state-sponsored-cyber-actors
12. https://www.researchgate.net/publication/276248097_Cyber_warfare_Issues_and_challenges
13. https://www.academia.edu/144745460/Cyber_Warfare_Exploring_New_Dimensions_in_the_History_of_Modern_Warfare_in_Indonesia
14. https://www.academia.edu/40629003/The_Perfect_Weapon_War_Sabotage_and_Fear_in_the_Cyber_Age
15. https://www.academia.edu/144738731/The_Law_of_Cyber_Warfare_in_Terms_of_Jus_Ad_Bellum_and_Jus_in_Bello_Application_of_International_Law_to_the_Unknown
16. https://www.academia.edu/145450024/An_introduction_to_cyber_peacekeeping
17. https://www.academia.edu/145501529/Deterritorializing_Cyber_Security_and_Warfare_in_Palestine_Hackers_Sovereignty_and_the_National_Cyberspace_as_Normative
18. https://www.orfonline.org/expert-speak/operation-sindoor-and-india-s-cyber-threat-landscape