ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

CYBER SECURITY AS A NATIONAL SECURITY IMPERATIVE: ANALYSIS OF EMERGING NON-TRADITIONAL SECURITY THREAT TO INDIA

Dr. Mohammad Saqib

Department of Defence Studies, Hindu College Moradabad, U.P., India

Email: saqibdefence@gmail.com

ABSTRACT

Cyber security has become a key part of India's national security framework as the country quickly goes digital. As industries including defence, banking, government, and infrastructure become more reliant on information and communication technologies, they also become more vulnerable than ever before. Cyber threats, such as state-sponsored hacking and spying, financial fraud, ransomware, and disinformation operations, are a complicated and ever-changing problem for India's internal stability and strategic independence. This article looks at the many different types of cyber dangers that India faces and how cyberspace is a unique area of non-traditional security. It looks at the most important deficiencies in areas like energy, banking, healthcare, and defence, and it looks into how enemies use these weaknesses to hurt national interests. The report also looks at India's institutional and policy responses, like the roles of CERT-In, NCIIPC, and forthcoming cyber laws, and compares them to the best practices throughout the world. The paper says that cyber security is no longer just a technical issue; it's a strategic necessity that needs a broad, multi-stakeholder approach. It does this by looking at real-world events and strategic assessments. It suggests a full plan that includes changes to the law, improvements to technology, working together with other countries, and making people more aware of the issue in order to establish strong cyber infrastructure. In the end, the study shows that India's national security policy needs to include cyber security at its core in order to protect its sovereignty, economy, and democratic fabric in the digital age.

Keywords: *Non-Traditional Security, National Interest, Security Measures, Economic Threat, Cyber warfare*

1. INTRODUCTION

In the 21st century, the meaning of national security has changed. Non-traditional security threats that work in borderless, virtual, and often anonymous contexts have been progressively challenging traditional ideas about security, which are based on physical boundaries, military troops, and visible enemies. Cyber security has become one of the most important issues, affecting not only military readiness but also political processes, economic stability, and social cohesion. Land, sea, air, and space are the four domains of battle. Cyberspace is now the fifth. As countries grow more connected online, cyber threats put national infrastructure, intelligence networks, financial systems, healthcare, and even democratic institutions at considerable risk. Cyber attacks can be quiet and last a long time, or they might happen all at once and cause a lot of problems. They can include denial-of-service attacks on important systems, stealing intellectual property, ransomware blackmail, and spreading false information to change how people think about something.

India is at the front of this new problem since it is quickly becoming more digital. India is more reliant on technology than ever before, with over 1.2 billion mobile connections, 800 million internet users, and an ambitious Digital India program that aims to provide services and government online (MeitY, 2022). Now, government organisations, the military, banks, hospitals, electricity grids, railways, and regular people are all part of a highly efficient but also very fragile cyber ecosystem. Digitisation has given people more power and helped the economy thrive, but it has also made it easier for bad actors to attack. The rise of hostile state-sponsored cyber operations, especially from countries that are enemies of the US, like China and Pakistan, along with the actions of non-state actors like cybercriminal groups, terrorist groups, and hacktivists, shows how big and complicated the threat landscape is. Reports show that Indian military networks, electrical utilities, and health databases have been hacked several times. For example, the 2020 Mumbai power outage, which happened during the COVID-19 crisis and affected important services, is thought to have been caused by cyber sabotage (NYT, 2021).

The fact that cyber dangers let people have unequal amounts of power is what makes them so deadly. A tiny group of hackers may cause a lot of trouble, hurt a country's reputation, or even bring down its economy with just a few tools and anonymous channels. Cyber operations are a useful instrument for hybrid warfare, psychological manipulation, and covert coercion since they are cheap to carry out, have a big effect, and are hard to trace back to the person who did them. Also, India's current cyber defence is not well-organised and only reacts to threats. The lack of a complete Cyber security Law, the delay in finishing the National Cyber Security Strategy, and the fact that many government ministries still depend too much on old digital infrastructure all show that there are problems with the system. India still doesn't have a cohesive, strategic-level command structure for cyber defence, like those set up by other major cyber powers. CERT-In, NCIIPC, and the National Cyber Coordination Centre (NCCC) do provide useful technical reaction and monitoring, though.

The challenge to India's democratic integrity is just as serious. Fake news, deep fakes, and politically driven lies are spreading quickly, sometimes with the help of bot networks and troll farms. This has made people less trusting of public institutions, caused conflict between different groups, and hurt the fairness of elections. In a digital democracy, protecting the social compact between the state and the citizen is equally as important as protecting networks and systems. This research paper looks at how important cyber security is for India's national security from a strategic point of view, with an emphasis on the new, non-traditional threats that have changed the way India protects itself from both inside and outside. The study looks at the existing threat landscape in India, finds weaknesses in important infrastructure, evaluates the legal and institutional response frameworks, and suggests a multi-layered approach to making the country more cyber resilient. In this way, it wants to show that cybersecurity is not only a technical need, but also a basic need for sovereignty, economic growth, and democratic stability in the digital age.

2. UNDERSTANDING CYBER SECURITY IN THE NATIONAL SECURITY CONTEXT

In the modern age of digitisation, cyber security has emerged as a fundamental component of national security policy. It surpasses traditional notions of information security, encompassing the protection of national interests, key infrastructure, economic stability, and public confidence in digital systems. In India, where more than 800 million individuals utilise the internet and government services are progressively provided online, protecting cyber security has become essential for preserving sovereignty, strategic autonomy, and democratic integrity. Cyber security fundamentally entails safeguarding data, digital infrastructure, communication systems, and cyber-physical environments from unauthorized access, disruption, damage, or exploitation. Nevertheless, inside the national security framework, it acquires a more expansive and intricate significance.

India's defence forces now have computerised command systems, battlefield monitoring, encrypted communications, and satellite operations. These have given them both strategic benefits and new weaknesses. Military networks, including those used by the Strategic Forces Command, need strong cyber security to keep command and control systems safe from hacking, sabotage, or spying. Any weakness in this area could make India's military less ready and less able to repel enemies in times of war. India's economy is currently very dependent on information and communication technologies (ICTs) because it is a rapidly rising digital economy. Cybercrime and data theft can happen in banking, insurance, the stock market, digital payment systems, and e-commerce systems. Also, essential infrastructure like energy grids, air traffic control, healthcare systems, and smart city platforms depend on interconnected digital systems. Many of these systems are vulnerable to ransomware, malware, and denial-of-service (DoS) assaults. A well-planned cyberattack on any of these areas may bring the economy to a standstill, cause widespread chaos, and make people worry and lose faith in the government.

In a democracy such as India, e-governance tools, electoral infrastructure, and public communication platforms are crucial for facilitating participatory governance and transparency. Cyberattacks that alter electoral data, disseminate misinformation, or obstruct access to e-governance platforms can undermine the integrity of democratic institutions. Moreover, cyber-psychological operations (cyber-psyops) and social media manipulation have arisen as formidable instruments for engendering political instability, inciting communal discord, and shaping public opinion—each representing nuanced yet significant dangers to domestic security. Consequently, cybersecurity has transformed from a technological concern to a multifaceted national priority. It currently necessitates the participation of diverse stakeholders: governmental entities, military organisations, business enterprises, academic institutions, and civil society. India's cyber defence plan must encompass technological readiness, policy development, legal protections, public awareness, and international collaborations to safeguard its national interests in this competitive and ever evolving arena.

3. THE EMERGING CYBER THREAT LANDSCAPE IN INDIA

India is always under threat from state-sponsored actors, especially from China and Pakistan, who are said to have hacked into government websites, spied on India online, and attacked important sectors. After the Galwan Valley battle in 2020, India was the target of cyber attacks by Chinese groups including APT41 and RedEcho, which were directed targeting India's power sector (Recorded Future, 2021). Hacktivist groups, cybercriminal gangs, and terrorist groups are using the internet more and more to steal money, steal identities, spread propaganda, and attract new members. The 2016 Union Bank of India cyber robbery, in which Rs 940 crore was stolen using SWIFT manipulation, shows how weak Indian banks are (Raman, 2017). Insider threats, which happen when staff or trusted users purposefully or inadvertently harm systems, are still a big problem in both the public and private sectors in India. Also, the fact that many people, especially those who work for small firms or live in rural areas, don't know much about cybersecurity or how to keep their computers clean makes it easier for hackers to get in (NASSCOM-DSCI, 2019).

4. STRATEGIC IMPLICATIONS OF CYBER THREATS FOR INDIA

Cyber risks have strategic effects that go far beyond one-time cases of data theft or financial fraud. India is a country with more geopolitical power, a huge digital footprint, and plans to be more independent strategically. Cyber dangers are very closely linked to the country's stability, sovereignty, and status in the world. Cybersecurity is no longer just a technological problem; it is now a key part of national defence, economic stability, internal cohesion, and diplomatic policy. One of the most strategic worries about cyber-attacks is that they could weaken a country's sovereignty. Cyber espionage, especially when done by foreign enemies, targets government departments, the military, and research institutes. The purpose is frequently to obtain secret information, mess up the way strategic decisions are made, or even subtly change state policy.

For example, Advanced Persistent Threat (APT) groups have attacked Indian government ministries like the Ministries of Defence, External Affairs, and Home Affairs many times. These attacks are often linked to individuals in China, Russia, or Pakistan who are connected to the state. After the 2020 border standoff, the RedEcho organisation, which is connected to China, was said to have gone after India's electricity infrastructure (Recorded Future, 2021). These kinds of campaigns can put critical information at risk, break up decision-making chains, and give enemies an advantage in diplomatic or military talks. Also, cyber espionage is hard to find and much harder to prove, which lets countries deny responsibility and escape diplomatic penalties. This makes it harder for India to respond according to established international law, leaving a grey area in both conflict prevention and escalation control.

Cyber attacks against economic institutions including stock exchanges, central banks, payment gateways, and trade databases can shake up a country's financial system and make investors less confident. The Indian economy is becoming more dependent on digital financial networks, which makes it more likely to be attacked on a large scale. India wants to have a $5 trillion economy, but these kinds of weaknesses make it harder for the country to be economically independent. This is especially true if enemies try to use cyber disruptions as weapons during trade fights or geopolitical crises (NASSCOM-DSCI, 2019). Manipulating public opinion and democratic processes is a less obvious but just as harmful effect of cyber vulnerability. Cyber psychological warfare (cyber-psyops) today uses misinformation campaigns, political trolling, deepfakes, and bot-led propaganda to split populations, undermine democratic institutions, and make governments look bad.

Cyber attacks are often used to scare people or get back at them as tensions between countries rise. They can be used to show off capabilities, force changes in policy, or get back at someone without starting a fight. After India and China fought at the border and India and Pakistan had diplomatic problems, there has been more cyber activity in India. Also, countries with inadequate cyber defences are more likely to be influenced by other countries, especially now that we rely so much on technology. India is becoming more like Western democracies through groups like the Quad and the Indo-Pacific alliances. This means that strong cyber interoperability is needed, which can only be developed on safe, sovereign digital infrastructure. If India doesn't create strong cyber capabilities, it might also hurt its reputation as a trustworthy digital partner around the world, which would limit its ability to shape international cyber norms and rules.

5. CONCLUSION

India's weak cyber defences are a strategically important national security issue. As the country moves towards a digital economy and a knowledge society, it needs to understand that cybersecurity is not only a tech issue; it is a matter of national security. With hostile state and non-state actors taking advantage of every hole in India's cyber defences, it's time for a full strategy that includes strong institutional structures, skilled workers, legal changes, and public awareness. To make sure the country can handle an unpredictable and quickly changing digital battlefield, cybersecurity needs to be built into every level of national government, including defence, diplomacy, finance, infrastructure, and education.

REFERENCES

- *CERT-In. (2022). Annual Report 2021. Ministry of Electronics and IT.*
- *Chhibber, P., & Nooruddin, I. (2019). Democracy without Associations. University of Michigan Press.*
- *Khera, R. (2018). "The Aadhaar Project: Cybersecurity and Civil Liberties." Economic and Political Weekly, 53(4), 34–38.*
- *Lewis, J. A. (2011). Cybersecurity and Cyberwarfare: Preliminary Assessment. CSIS.*
- *Mehta, R. (2015). "India's Cyber Security Policy: A Critical Evaluation." IDSA Occasional Paper.*
- *Ministry of Electronics & IT. (2013). National Cyber Security Policy. Government of India.*
- *NASSCOM-DSCI. (2019). Cyber Security Sectoral Analysis Report.*
- *New York Times. (2021). "China Appears to Warn India: Push Too Hard and the Lights Could Go Out."*

- *Ottis, R. (2008). "Analysis of the 2007 Cyber Attacks Against Estonia." International Journal of Information Security.*
- *Raman, B. (2017). "Banking Cyber Heist and Cybersecurity Gaps." Indian Journal of Security Studies, 6(2), 45–52.*
- *Recorded Future. (2021). RedEcho Targets Indian Critical Infrastructure. Threat Intelligence Report.*
- *Singh, G. (2020). "Non-Traditional Security Challenges in India." Strategic Analysis, 44(1), 15–30.*