Cybersecurity, International Relations and India’s Foreign Policy- Historical Perspective and Prospects

Wajahat Mazahar Khan (M.A)

Department of Public Policy,
Research Fellow at International Institute of SDG’s and Public Policy Research, Delhi

Deepali Padhy (BBA LLB Hons)

Student at Department of Law, Amity University, Kolkata

ABSTRACT
India is trying to create an impactful strategy to handle the cybersecurity concerns as well as an international relation with countries in the context of cybercrimes. There have been many statutes which is made specifically to deal with cybercrimes. As of now, there has been an impact of terrorism as well where it creates an ample of challenges for the nation to overcome. The research is conducted for this paper to showcase the historical perspectives and even the prospects for the issues. The paper has showcased India’s role in international relations and law and order impact on cybersecurity. Internet governance has a major role when it comes to the cybersecurity concerns. Furthermore, this paper will study the performance of India in the area of cybersecurity. The bilateral engagement between India and US created a new relationship. Moreover, the study will try to focus and suggest ways forward regarding the issues and interventions through proper methodology and research by taking help from secondary sources. Owing to the research undertaken, in contrast to nations like China, India is actively considering the problem of cybersecurity and is supporting a multi-stakeholder approach. This stands out as an important element for India's overall transformation as a dynamic player as well as for protecting its digital infrastructure. The importance of developing both offensive and defensive cyber capabilities will increase due to the growth of cyber activities and the drive connect millions of Indians to the internet.
Key words: Cybersecurity; historical views; prospects; internet governance; India’s Foreign Policies; National Cyber Security Strategies

1. INTRODUCTION

India's positions in global Internet governance debates have been constantly noted and criticized for their strong preference for multinational models of engagement, as opposed to the multistakeholder approaches that are so well- established in the field. This was maybe most apparent when it proposed in 2011 to establish a Committee for Internet- related Policies (CIRP) within the United Nations (UN) as a new institutional medium to deal with big, global public policy questions in Internet governance. Grounded on indifferent geographic representation, the CIRP would have 50 member countries. Although the Internet Governance Forum (IGF) would give input, and the offer mentioned multistakeholder representation for good measure, this was a classic multinational approach[i]. As a result, critics ate the advertisement in June 2015 by Union Minister for Dispatches and Information Technology. Mr. Ravi Shankar Prasad, of a change in India's sanctioned policy to support a multistakeholder approach[ii]. This was reflected in a subsequent domestic contestation in September 2015, when the government released the draft public Encryption Policy. The policy included vittles taking over-the-top applications similar as WhatsApp to keep all communication logs for further than 90 days and make them available by simple text format if requested by the government.[iii] A significant public roar forced the government to withdraw the policy, but it was clear that India would continue to endorse unilateral programs on Internet- related security issues. When India surfaced from its social history in 1947, it sought to sculpt out a place for itself in the arising global order, despite a severe lack of resources and a shattered economy. This paper will demonstrate how this fundamental conception has shaped India's positions on Internet governance and cybersecurity over the last decade or so. This paper will collude the economic crisis, political, and historical antecedents of India's evolving positions on Internet governance as they're shaped by its cybersecurity enterprises, domestic environment, and the overall influence of global events as they unfold in order to more understand events and how these play out to shape this specific field.

2. RESEARCH METHODOLOGY

2.1 Objective(s) and Scope

The purpose of this paper is to showcase how cybersecurity affects international relations. Also discussed are the increased bilateral engagement between India and the United States, as well as India's various concerns regarding law and order, terrorism, and technology. The scope of the paper is broader, and it covers national cybersecurity policy, statutes, and critical information structure. Suggestions and future directions for national cybersecurity strategies are discussed.

2.2 Methodology

For the purpose of this paper, secondary sources of information, such as articles and other online publications, were consulted. The authors of these sources have been properly acknowledged in footnotes wherever their texts were relevant.

2.3 Research Questions

1. How cybersecurity is affecting international relations?
2. What are the contributions of India so far regarding its cybersecurity?
3. What is India's tryst with the new National Cyber Security Policy?
4. What is the need for a National Cyber Security Strategy and the steps that has to be followed as per the Report?

2.4 Hypothesis

The internet has grown dramatically in the last ten years. More than 3 billion people now have internet access worldwide. During the next ten years, growth will most likely come from developing countries. Cybersecurity has emerged as a critical component of foreign policy due to its importance for overall national security, public safety, and economic development. It will also become increasingly important for India to develop international agreements on how nations should behave in cyberspace and how to achieve a stable and open Internet. The government's responsibility is to ensure that the new Internet infrastructure is dependable and secure. As a result, in addition to the national security issue, the government will need to be sensitive to the demands and sensibilities of the industry. India has begun discussions on cybersecurity with the United States, the United Kingdom, Germany, the European Union, France, South Korea, Russia, Japan, and Australia. Opinions have been exchanged on national cybersecurity policies, the sharing of critical information, capacity development, and a variety of other topics during these discussions.

3. CYBERSECRITY AND INTERNATIONAL RELATIONS- INDIA'S ROLE

When discussing issues of war and peace, it is impossible to ignore the pervasive impact of technological change on issues, which has an impact on us as individuals, and on societies, and countries. These technologies, particularly information and communication technologies (ICTs), are an essential component of cyberspace's new man-made environment. Data is at the heart of this environment. Data collection, transmission, and use has become the new norm for countries, with varying degrees of visibility. Every day, we become more aware of the activity's interdependence.

Countries have recognized that international cooperation in cyberspace is required to accelerate socioeconomic development while ensuring cyberspace's integrity, predictability, and security. Because of the transnational nature of cyberspace and the contributions made to its evolution by various segments of society, a multi-stakeholder approach is the most sustainable approach for effective international cooperation. In addition to drawing on traditional principles of international law, international cooperation in cyberspace must address cyberspace's strengths and vulnerabilities. This necessitates a focus on the technologies and applications that underpin what is colloquially known as the internet. Wireless and fixed broadband, smartphones, mobile Internet, cloud computing, open data, big data, and social media, as well as linked "critical national infrastructures," are all staples of global cyberspace discussions. Because of their national economic and security interests, some countries have positioned themselves at the forefront of global discussions on the need for effective international cooperation in cyberspace.[iv] The United States, the Russian Federation, China, the European Union, Japan, the Republic of Korea, Brazil, and India are among them.

3.1 India and Cyber space

To establish a continual growth of information technology which has resulted software development and application exports were the first driver for greater international cooperation in cyberspace. India has entered into the zero- tariff import regime for computers and applications as a part of Information Technology Agreement. A second driver for India is the prioritization of ICTs for accelerated socioeconomic development through the Digital India platform, which has the dual impact of bridging digital divides and empowering citizens.

With the increased use of Aadhar, the world's largest national biometric database, the impact of the Digital India platform has been significantly multiplied. A third driver is a new dimension of electronic commerce, or E-Commerce, particularly in terms of the development of international trade rules in the digital domain. India's major trading partners, including the United States, the European Union, and Japan, have stated their intention to establish such a rules-based framework, requiring India to engage on this issue with its ambitious digital economy platforms for goods and services. There are multi-stakeholder approaches to cyberspace that are comprised of four major components: government, academia, business, and civil society.

- Governments have primary responsibility for cyberspace policies and the use of cyber technologies for public services within their respective national jurisdictions.
- Businesses have a significant impact on how governments formulate cyber policies at the national and international situations due to their focus on invention and the operation of cyber technologies that they've patented or copyrighted.
- Academia, which plays an important role in cyberspace research and development, innovating, and conceptualizing theories, frequently collaborates with businesses to bring the results of its activities to the wider world.
- Civil society focuses on the impact of government, business, and academic activities in cyberspace, with a particular emphasis on the human dimension, both individually and collectively. All four stakeholders are involved in raising awareness of cyber issues from their respective perspectives, highlighting cyberspace's strengths and vulnerabilities.

3.2 Global Cybersecurity Scenario

This strategy identified nine components that could help to support such a global culture. Risk assessment, security design and implementation, management, and reassessment were among the components, as were awareness, responsibility, reaction, ethics, and democracy. Following that, governments directed the UN Secretary General to seek the assistance of a Group of Governmental Experts (GGE) in order to advance this idea through an UNGA resolution in 2003. The GGE was given the authority to draw recommendations on "disarmament, global issues and risks to peace that affect the international community, and challenges to the international security regime."

The first issue addressed in the paper is how cybersecurity affects international relations. Some of the consequences are as follows:

- **Government hackers**- A recent example of a government attack can be found in 2022. According to a state government report, the Conti strain of ransomware was the most expensive in terms of victim payments as of January, and it has been blamed for infecting hundreds of servers with malware in order to gain corporate data or digital damage systems. And to spread misery throughout the world, which includes businesses, hospitals, government agencies, and so on.
- **Digital wars-** As the world has shifted to digital technology, there has been an increase in intrusions into private data. If Russia joins this digital war, it will almost certainly spread false information all over the world via the internet. It would have mastered the art of hacking political data, endangering the rest of the world. The day will soon come when hackers will use computer code to breach an adversary's security architecture. Cyberwarfare is becoming an increasingly lethal tool in international conflicts.
- **Individual attacks-** The main reason for these attacks is internet interaction with foreign nationals. Nigerians are very popular among cybercriminals who use online schemes to target individuals.

4. CHANGING THE DIRECTION OF FOREIGN POLICY

In the 1990s, India was on the verge of an economic meltdown, prompting a major overhaul of its profitable programs and the establishment of a further liberalised governance. As the Indian economy grew, the Internet began to take root slowly but steadily, giving rise to new enterprises about cybersecurity. This also played a significant part in strengthening India's foreign policy's ‘sovereignty' philosophy, while also leading to India reaching out to the world, seeking new alliances. [v]

Talking about the political changes, the Narasimha Rao government was already enforcing numerous far- reaching changes, and this adaption would pave the way for a deeper engagement a decade latterly, which would have a significant impact on India's cybersecurity posture. In the Muslim- maturity state of Jammu and Kashmir, there was also a major uprising against Indian rule. The uprising urged Pakistan to give active politic and material support to the bellicosity movement, having a significant impact on India's traditional foreign policy. While India was dealing with the rising insurrection in Kashmir, India and Pakistan began exchanging allegations of mortal rights violations. In numerous ways, this single event has had a long- continuing impact on India's foreign policy. This shift has been down from the' internationalism' that has been rehearsed since 1947, towards a new language of sovereignty.

4.1 A Bilateral engagement between India & the United States

Despite the sanctions assessed by the US on India following its nuclear tests in 1998, there were back- channel bilateral addresses that explored the possibility of the two countries forming a new relationship. The outgrowth of these secret bilateral addresses was made public in February 2000, when the United States and India agreed to a slew of measures to strengthen their ties. This agreement would lead to the establishment of a major bilateral security dialogue a time latterly, when Prime Minister Atal Bihari Vajpayee visited the US. During the trip both governments made a significant addition to the Joint Working Group on Counter Terrorism by creating a sub-group for cybersecurity. [vi]

The new forum was easily “born out of” the bilateral" counterterrorism dialogue," and it was" dedicated to guarding the critical structure of the knowledge- grounded economy." The forum included “government agencies and private sector participants from India and the United States,” with the thing of relating “pitfalls and common enterprises in cybersecurity” and developing “a work plan for securing networked information systems”[vii]. India's strongest cybersecurity relationship had now surfaced from a bilateral approach with the US, which would impact its positions in colourful multinational forums and administrations. The groundbreaking bilateral dialogue of 2000- 2001 would therefore review India's relations with the US and support India's belief in using bilateral connections to achieve issues that could change the paradigm in multinational settings.

4.2 Is there any impact of terrorism in context with cybersecurity?

The addition of a bilateral cybersecurity discussion between India and the US as a subset of the Joint Working Group on Terrorism is an important suggestion of how New Delhi linked technology and terrorism, making the ultimate the dominant paradigm. likewise, it reinforced New Delhi's preference for using government- to- government forums to advance its stated foreign policy objects. Although the impact of terrorism on India's cybersecurity and Internet governance stations is considerably discussed in section four of this paper, it's critical to understand the fundamentals of how it came such a top precedence then. Ironically, Pakistan's foreign policy seeks to involve India in the maturity of its positions on global forums similar as the United Nations or the OIC, an association of Islamic nations, a demand to discuss Kashmir, and/ or attempts to work India's successes, similar as the nuclear agreement with the US, to gain similar bilateral agreements. Renewing their relationship, India and the United States were also motivated in part by the notions that Washington and New Delhi discussed the AI9/11 Qaeda attack. Since 1990, when New Delhi fought off terrorist attacks in Jammu, it has asked for Washington's aggressive involvement in Kashmir to limit Pakistan's part in backing terrorism.[viii] Still, after9/11, this relationship would undergo significant change as terrorism became a combined concern, performing in lesser cooperation on issues similar as intelligence- sharing and further harmonious views on terrorism.

Away from bilateral connections, India has used multinational bodies that it helped establish to impact issues related to technology and security. This is reflected in India's appetite to use IBSA(a confederation of India, Brazil, and South Africa- a gauged - down interpretation of BRICS without China and Russia) to issue common statements on' enhanced cooperation' that will put' governments on an equal footing' [ix] Indeed, New Delhi emphasizes the "need for global cooperation to ensure that [the] Internet remains a free and secure medium for the entire world."[x] India's strongest cybersecurity relationship had now emerged from a bilateral approach with the US, which would impact its positions in colorful multinational forums and administrations. The groundbreaking bilateral dialogue of 2000- 2001 would therefore review India's relations with the US and support India's belief in using bilateral connections to achieve issues that could change the paradigm in multinational settings. The fact that India has tried and failed in colorful ways to gain class has not dampened its determination to gain a seat at the multinational forums that are important to its security enterprises and intentions. As a result, New Delhi has always responded appreciatively to statements like those made by Mr. Froman or President Obama, as mentioned over, and has constantly welcomed them. [xi]

5. LAW, ORDER AND THE TERRORISM

The proliferation of communication tools used by terrorists on Internet- based platforms has heightened India's enterprises about the intersection of technology and terrorism. The Lashkar-e-Taiba (stop) attack on Mumbai on November 26, 2008 demonstrated how terrorist handlers based in Karachi, Pakistan, used Voice over Internet Protocol (VoIP) to direct the attack on crucial targets in Mumbai.

The advent of the Internet, particularly social media, has been repeatedly cited by India's Law Enforcement Agencies (LEAs) as one of the crucial challenges for dealing with law- and- order issues. When collaborative screams erupted in the quarter of Muzaffarnagar in India's most vibrant state, Uttar Pradesh (UP), in September 2013, state police immediately criticized social media for" inflaming hatred between the warring communities." At a press conference shortly after the screams began, a elderly state police officer referred to" Facebook, WhatsApp, and Twitter."' Fear and mistrust between communities,' he claimed, was spreading' via' social media.

He also stated that -

“One specific video (being used to promote violence) that is widely circulated on social media is unrelated to any incident in western Uttar Pradesh and was uploaded to YouTube. [We believe] it is from an incident that occurred outside of India.”

The first significant use of Internet- based communication tools by terrorists was discovered by Indian security agencies in 2006, after a little-given outfit called the Indian Mujahideen (IM) carried out a series of bomb attacks in several major Indian cities, including Delhi and Mumbai. The IM terror attacks were planned over secure online communication channels, according to the examinations. When investigators began to track the dispatches transferred by the IM, they discovered that this case was unique. Tracing the IP addresses led them to an open Wi- Fi network, which the terrorists had used to shoot their dispatches and avoid being tracked. When the IM discovered that their MS Word documents could be traced, they extemporized.

rather, they began transferring their documents as PDFs, indicating that the group was learning to conceal its tracks between attacks.[xii] The document also goes on to explain how the group used secure and translated online converse operations to avoid discovery by security and intelligence agencies both before and after terrorist attacks. The26/11 attack would last three days before Indian battalions cleared the attackers from three different locales, carried out by members of the Pakistan- grounded terrorist group stop. Over the course of three days, Indian security agencies would block dispatches between terrorists and their instructors, who were allowed to be grounded in Karachi, Pakistan. The original detention in determining where the terrorists were calling from would be significant reversal encounter-terrorism operations, but the VoIP logs would be an important part of the substantiation. The alternate issue raised is what India has done so far or contributed to the issues at hand. Two intriguing developments in the last week of June stressed the significance of fastening attention on India's cyber security. On 28th June,[xiii] The International Institute of Strategic Studies (IISS), a London-based think tank, released a report on 'Cyber Capabilities and National Power,' which evaluated the cyber capabilities of 15 countries, including India. Unrelated to the report's release but related to its theme, India's Foreign Secretary (FS) Harsh Vardhan Shringla addressed the United Nations Security Council (UNSC) Open Debate on 'Maintenance of International Peace and Security: CyberSecurity on June 29th. Taken together, these two developments offer an excellent opportunity to shed light on India's overall approach to cybersecurity and the development of its cyber capabilities.

In recent times, cybersecurity has grown in significance in all public security debates. Cyber capabilities are now regarded as a critical element of public power. States use these capabilities for a variety of purposes, including furnishing essential services to their citizens, launching attacks on adversaries' digital structure, gathering intelligence, and stealing trade secrets and technologies for profitable gain.[xiv] Sophisticated cyber-attacks are carried out with the possible involvement and/ or support of state actors in order to put costs and shoot a communication to the adversaries. The eventuality for denial and lower costs of launching cyber-attacks make it an especially charming tool for security agencies.

The emergence of the Covid- 19 epidemics, as well as the performing increase in the number of people working from home digitally, has resulted in an increase in cyber-attacks and criminal activity in cyberspace. There are multitudinous exemplifications of businesses being routinely targeted and held for rescue, as well as attacks on public structure similar as power grids and channels. Security agencies around the world are scuffling with enterprises about terrorist groups' implicit use of cyber capabilities. preliminarily, the Islamic State of Iraq and Syria (ISIS) used cyberspace to spread its communication and retain new members. To be sure, the military operation of cyber capabilities, as well as the rise of a complex strategic terrain with a focus on obnoxious capabilities to maximize impact by dismembering digital systems, has emerged as a serious concern for public security planners. The significance of cyberspace is anticipated to grow indeed more in the coming times, challenging issues of internet governance, responsibility, norm setting, and the development of a broad frame to insure safe and secure cyberspace. The Indian Foreign Secretary's (FS) address to the UN Security Council is significant in this regard because it outlines India's broad approach to cyber security.

5.1 UNSC open debate about Maintenance of cybersecurity

The address began by acknowledging that the ‘nature of conflict and its underlying tools have transformed tremendously over the decades.’[xv] The world is now ‘witnessing growing security threats to Member States emanating from cyberspace’ and therefore, ‘this open debate is timely.’[xvi] FS noted that, the ‘borderless nature of cyberspace, and more importantly anonymity of actors involved, has challenged the traditionally accepted concepts of sovereignty, jurisdiction and privacy’ and that ‘open societies have been particularly vulnerable to cyber-attacks and disinformation campaigns.’[xvii] Russia’s alleged intervention in the American elections is a good example of such attacks and disinformation campaigns.[xviii]It gives rise to a new set of issues and an enterprise in the expression of public security policy, particularly in open societies where striking the right balance between privacy, openness, and security is a delicate task. The speech refers to" some countries" that" are using their moxie in cyberspace to achieve their political and security- related objects, as well as engage in contemporary forms of cross-border terrorism." likewise, terrorists" each over the world" use cyberspace to" extend their appeal, spread malign propaganda, incite abomination and violence, novitiate youth, and raise finances." Terror networks have also used" social media to plan and execute terror attacks and inflict havoc." In this environment, consider the 2019 Christchurch terror attack, which was livestreamed on Facebook by the bushwhacker. For a country like India, which has been at the entering end of terrorism, FS observed that it's important ‘ to address and attack the implications of terrorist exploitation of the cyber sphere more strategically.’[xix] According to FS, it's" in the international community's interest to insure that all actors abide by their international scores and commitments and don't engage in practice that could potentially disrupt global force chains and trade in ICT(Information and Communication Technology) products." The Covid- 19 pandemic, as well as the need to shift a large portion of work and other necessary conditioning online, has brought to light the critical issue of digital peak. The speech emphasized that countries widening" Digital gaps" and" Digital knowledge gaps" produce an unsustainable terrain in the cyber sphere. There's no other option but to concentrate on capacity structure and cooperative sweats. India has successfully abused the tremendous eventuality of cyber technologies in enforcing the SDG agenda and perfecting governance in recent times. FS concluded his speech by emphasizing India's station on cyber security. According to the speech," our overarching thing is to harness cyberspace for the growth and commission of people, not just of our own country, but of all humanity." To achieve this thing, India is committed to an open, secure, free, accessible, and stable cyberspace terrain that will serve as a catalyst for invention, profitable growth, and sustainable development, while also ensuring the free inflow of information and esteeming artistic and verbal diversity. The IISS report evaluates 15 countries across seven verticals. Some of these include strategy and doctrine, governance, command and control, core cyber-intelligence capability, cyber commission and dependence, cybersecurity and adaptability, transnational leadership in cyberspace affairs, and offensive cyber capability. Based on these criteria, countries are divided into three categories Tier 1 countries have" world- leading strengths" in all sectors. The United States is the only country in Tier One (US). league two countries have" world- leading strengths" in a variety of fields, including Australia, Canada, China, France, Israel, Russia, and the United Kingdom (UK). Eventually, league three countries have significant sins in some areas but significant strengths in others. Vietnam, India, Indonesia, Iran, Japan, Malaysia, North Korea, and Malaysia comprise Tier Three.

Now the question arises that's multilateralism the way forward? While India had therefore been pushing for a more multinational approach to governing the Internet through new covenants and fabrics on a global scale, on a domestic position, it remained sorrowfully inadequate in terms of cybersecurity. This, in turn, would shape India's foreign policy posture as it sought to balance its internal failings with a fleetly changing international terrain profoundly told by arising Internet- grounded technologies.

6. NATIONAL POLICY STATUTES ON CYBERSECURITY

6.1 The IT Act

The IT Act While the Information Technology Act, 2000, [xx]included basic data protection provisions, but none of them were comprehensive or took a legislative approach to cybersecurity. This is due to the fact that India was only beginning its adoption of the Internet and that the computerization of extensive government networks and operations had only begun. The original purpose of the IT Act was to safeguard the commercial interests of the IT-enabled services (ITES) sector. It is evident that the original IT Act did not completely grasp the potential of technology and its future effects. The original IT Act's omission of any reference to cybersecurity is evidence that Indian legislators are unable to adequately address the industry's fast rise of the IT and ITES industries. The statutory framework was revised with significant amendments to the Act in 2008 with the goal of building a national cybersecurity policy framework. This was done in consideration of the increase in cyber vulnerabilities, threats, and assaults as well as the emergence of new threats. The development of specific agencies with clearly defined roles for executing cybersecurity measures was also contemplated by sections 70A and 70B. While section 70B established the existing CERT-IN, section 70A outlined the requirement for the establishment of a new organization to safeguard the CII-designated sectors. The Government of India would issue an official gazette notification to create the new organization, which would be known as the National Critical Information Infrastructure Protection Centre (NCIIPC)[xxi]

6.2 National Cyber Security Policy, 2013

A cybersecurity framework that extends beyond CII was created by the National Cyber Security Policy, which was published in June 2013. Its claimed goals included the creation of a workforce of "500,000 professionals competent in cybersecurity in the next five years" and the goal of "generating appropriate trust and confidence in IT systems." Understanding the nature of next-generation threats, which are complex and mirror "Black Swan" occurrences in that they are disconnected at some levels yet sufficiently. The introduction of NGNs of (Next Generation Networks) and related technologies has also sparked the emergence of "Next Generation Security Threats," which are either organized or occasionally driven by flawed algorithms. For instance, security officials at first thought that the 2008 attack on the Baku-Tbilsi-Ceyhan pipeline in Eastern Turkey[xxii] was a conventional, physical terror attack. However, later investigations determined that it was a "cyberwar" act.

The third issue of the paper is about India’s tryst with the new National Cyber Security Policy. According to the current situation, data breaches occur in the country on a monthly basis. Hundreds of Indian residents' COVID-19 lab test results were leaked on several government websites beginning in 2021. A cyberattack on systems at an airline data service provider exposed the personal information of 4.5 million airline passengers on May 21[xxiii]. In the same month, 2020 Common Admission Test Candidates’ Personally Identifiable Information and test scores were leaked and put up for sale. In April of this year, a million credit card numbers and information about 180 million pizza orders, including customer names, phone numbers, and email addresses, were leaked. Despite the fact that these are some of the reported cases, the true number is most likely much higher. Despite the fact that cyberspace threats are well understood, our country lacks a policy that outlines how to combat them. There is no formal required framework that specifies a response strategy in the event that either of the two is attacked by an enemy in order to protect critical infrastructure for information and other national assets.

The Indian government published the National Cyber Security Policy (NCSP) in 2013, which outlined a number of tactics for fending off security threats via the internet. Despite the passage of eight years, there has been little implementation, and our nation continues to be one of those that is most frequently targeted. The fourth topic was on the requirement for a National Cyber Security Strategy and the actions that must be taken in accordance with the Report. The following are the requirements for this tactic: -

a. **An increase in cyberattacks**:

According to a 2021 report by American cybersecurity company Palo Alto Networks, Maharashtra was the most targeted state in India, receiving 42% of all ransomware attacks. According to the report, India is one of the more economically lucrative countries for hacker groups. As a result, these hackers demand ransom payments from Indian companies, which are typically made with cryptocurrency. In 2021, one in four Indian businesses experienced a ransomware assault, which is higher than the global average of 21%.

b. **Cyber Warfare Offensives:**

The US is one of many nations that has made considerable financial investments in creating not only defences against attack, but also the capacity to launch destructive cyber warfare offensives. The US, China, Russia, Israel, and the United Kingdom are thought to have the most advanced cyberwarfare capabilities.

c. **Post-Covid:**

There will be an increase in digital usage across the board. This includes financial services, banking, manufacturing, power, and nuclear power plants, among other critical infrastructure.

d. To Protect Critical Sectors:

Given the growth of entry points into the internet and the growing interconnection of sectors, which could grow even more with the deployment of 5G, it is especially significant. According to data submitted to and maintained by the Indian Computer Emergency Response Team, there were 6.97 lakh cybersecurity incidents reported in the first eight months of 2020, almost equal to the preceding four years combined (CERT-In).

e. Recent Cyber Attacks:

A Chinese gang by the name of Red Echo has dramatically increased the use of tools like malware to target "a big swathe" of India's power sector. Shadow Pad, a piece of malware that uses a backdoor to access servers, was utilized by Red Echo.[xxiv] "Identified holes and vulnerabilities in the IT architecture and supply chain software of Bharat Biotech and the Serum Institute of India," according to the Chinese hacker collective Stone Panda.

f. **For Government:**

A municipal, state, or federal government keeps a ton of secret information on the nation (geographic, military-strategic assets, etc.) and its people.

g. For Individuals and Businesses

Photos, videos, and other personal information given by a person on social networking sites may be misused by others, creating significant and even fatal situations. On their systems, businesses store a lot of data and information. A cyber-attack may result in the loss of proprietary information (such as patents or original work) and the private data of employees and customers, destroying all public confidence in the organization's integrity.

6.3 What steps is to be followed as per the report?

a. Financial Provisions or Budgetary

Cybersecurity has been advised to receive a minimum budgetary commitment **of 0.25 percent,** with a potential increase to **1 percent**. **15-20% of the IT/technology budget** for individual ministries and agencies should be set aside for cybersecurity. Additionally, it recommends creating a **Fund of Funds for cybersecurity** and giving central funds to states so they can develop their expertise in the area.

b. Technology development, innovation, skill-building, and research

In addition to putting up a short- and long-term agenda for cybersecurity through outcome-based programmes and giving investments in deep-tech cybersecurity innovation, the paper recommends spending money on **ICT modernization** and digitalization. Additionally, DSCI advises developing a **"cyber security services**" with personnel drawn from the Indian Engineering Services.

c. **Crisis Management**

DSCI advises conducting **cybersecurity simulations** that involve realistic situations and their effects in order to adequately prepare for handling a disaster.

d**. Cyber Insurance and Diplomacy Scenario**

Because it is a new area of study, **cyber insurance** needs actuarial science to address **cybersecurity risks in technological and business contexts** and to determine threat exposures. India's international relations are greatly influenced by cyber diplomacy. Therefore, initiatives, exchanges, and industrial support are required to maintain the cybersecurity preparation of important regional blocks like the **Shanghai Cooperation Organization (SCO)** and the **Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC)**. The government should promote India's reputation as a trustworthy participant in cybersecurity and appoint **"Cyber envoys**" to the important nations and regions in order to advance better diplomacy.

f. Investigation of cybercrime

The report suggests passing rules to deal **with spamming and fake news** in order to relieve the court system of the strain brought on by the rise in cybercrime worldwide. It also advises developing a five-year strategy that accounts for potential technological change, establishing special courts to **handle cybercrimes, and clearing the backlog of cybercrime**. In addition, DSCI advises agencies to undergo advanced forensic training to stay current in the era of AI/ML, Blockchain, IoT, Cloud, and Automation.

7. SUGGESTIONS

The following are the suggestions for the stability, maintainability and security for the cybersecurity in the nation-

- **Legal framework**- The Information Technology (IT) Act, 2000 addresses cybersecurity and related cybercrimes, despite the absence of a specific cybersecurity law in India. The Indian Penal Code, 1860(which punishes offences, including those committed in cyberspace), as well as the Companies (Management and Administration) Rules 2014 created under the Companies Act 2013[xxv], both contain some cybersecurity- related laws. The RBI, the IRDA 1999, the DOT, and the SEBI, among other regulators, have espoused sector-specific laws that demand that their regulated entities — banks, insurance firms, telecom service providers, and listed entities — maintain cybersecurity requirements. However, there have been significant changes to how businesses run and how crimes are started online. It's likely necessary to update the IT Act 2000, which was modified in 2008, and establish cybersecurity criteria consistent with the nature of the information assets managed by particular types of companies.
- **Data protection-** Data is a valuable resource for the country, and the majority of data interchange occurs online. Most countries with governments and citizens who use the internet for varied everyday tasks have data sequestration laws. In the USA, there's the California Consumer Privacy Act, and there's GDPR in the European Union. There has been little rush to adopt the Data Protection Bill despite the fact that many Indians have lost data on numerous times (which has been well-covered in the media)
- **Cyber Response Entity-** Any organisation charged with overseeing national cyberspace management should have a clear chain of command to ensure that all available resources are used to their fullest potential. Unfortunately, there is not such a framework. In India, there are numerous government organisations that deal with various facets of cybersecurity. Even the State Police have their own cyber investigators. Each of our defence services has its own cyber experts. Experts working for different government ministries and departments must urgently coordinate their efforts to achieve a common objective. A National Cyber Command- style organisation could be created by the government.

8. CONCLUSION

Currently, India is about to seize a significant opportunity. As this article has shown, India has long believed that technology can help it not just keep pace with political and economic development but also establish itself as a major participant on the international stage. India hasn't been able to reach its full potential, though, because of the discrepancy between its ideals and its actual capabilities—technological or otherwise. This might significantly alter, though, once India realises its potential as an Internet creator rather than just a consumer. In India, e-commerce and e-government are growing, enhancing connection, and luring more people online every day.

First, India is actively considering the issue of cybersecurity and is proposing a multi-stakeholder approach in contrast to nations like China, which want stronger state control over the cybersphere. These are the two broad themes that can be seen in the context of the FS address and IISS study. *Second*, as demonstrated by the creation and deployment of the Co-Win application for Covid-19 immunisation, cybersecurity is important for both protecting India's digital infrastructure and the country's broader transformation. However, the answer in this aspect still lies in bridging the digital gap by offering simple, affordable, and trustworthy access. *Third*, India has been making efforts to ensure that gaps in the cybersecurity sphere may be filled, as seen by the establishment of numerous agencies and the pursuit of diplomatic alliances with critical allies. However, far more work must be done to protect its cyber infrastructure. National security will increasingly depend on cybersecurity as we move into a new era. Consequently, there is no choice but to develop offensive and defensive cyber capabilities while promoting the development of regulating norms and frameworks for the use of cyberspace.

9. THE WAY FORWARD

Still, as the main actor and the trusted arbitrator, acknowledges the part of numerous stakeholders who may aid India in realizing its full eventuality, If the government. First out, a number of government stakeholders bear much near collaboration than is now possible under their current protocol. The Prime Minister's Office, the National Security Council and its Secretariat, the Ministry of Dispatches and Information Technology, the Ministries of Law and Home Affairs, the security agencies, etc. are just many examples of the stakeholders within the government who must produce institutional mechanisms to cooperate rather than contend. Although it appears that some of this has been handled, there's still important room for enhancement.

REFERENCE

1. [i] [i] India's Proposal for a United Nations Committee for Internet-Related Policies (CIRP). Statement by Mr. Dushyant Singh, Hon'ble Member of Parliament, India, on Agenda Item No. 16, Information and Communications Technology for Development. New York, Sixty Sixth Session of the UN General Assembly, https://internetdemocracy.in/wp-content/uploads/2014/07/India-UN-CIRP-Proposal-at-UNGA-2011.pdf
2. (Last visited 6 July, 2022)
3. [ii] Samanta, Pranab Dhal (2015). FM Arun Jaitley-led GoM Decides to Back US Model on Internet Governance via Concessions. Economic Times, http://articles.economictimes.indiatimes.com/2015-06-23/news/63746235_1_icann-gom-special-arrangement (last visited July 10, 2022)
4. [iii] Datta, Saikat (2015). The Government Won't Give Up Listening in on Private Communications. Newslaundry, http://www.newslaundry.com/2015/09/29/why-the-draft-national-encryption-policy-is-likely-to-return/ (last visited July 9, 2022)
5. [iv] The Diplomat, https://thediplomat.com/2019/12/indias-national-cybersecurity-policy-must-acknowledge-modern-realities/ (last visited July 12, 2022)
6. [v] Dutta, Cybersecurity, Internet governance, IFP- Historical antecedents, https://internetdemocracy.in/reports/cybersecurity-ig-ifp-saikat-datta
7. [vi] India-US Cyber Security Forum: Fact Sheet. New Delhi, Ministry of Foreign Affairs and Press and Information Agency, Government of India, http: //pib.nic.in/newsite/erelease.aspx? relid = 16132 (Last access date is July 9, 2022)
8. [vii] ibid
9. [viii] Rhode, David (2002). India Renews Call for US to Declare Pakistan a Terrorist State. New York Times, http://www.nytimes.com/2002/07/17/world/india-renews-call-for-us-to-declare-pakistan-a-terrorist-state.html (last visited Jul 7, 2022)
10. [ix] Statement by India, Delivered by Ambassador Dilip Sinha, Permanent Representative of India to UN in Geneva, at the UNCSTD Open Meeting on Enhanced Cooperation Pertaining to the Internet. Geneva, Permanent Mission of India to the UN, http://www.pmindiaun.org/pages.php?id=839, (July 10, 2022)
11. [x] ibid
12. [xi] Joint Statement 2012 US-India Strategic Dialogue. Washington DC, Embassy of India, https://www.indianembassy.org/archives_details.php?nid=1830 (last visited Jul 9, 2022)
13. [xii] Jaleel, Muzamil (2014). NIA Probe Shows IM Men Tech-Savvy; Used Proxy Servers, Complex Code to Chat. Indian Express, http://indianexpress.com/article/india/india-others/nia-probe-shows-im-men-tech-savvy-used-proxy-servers-complex-code-to-chat/ (last visited Jul 8, 22)
14. [xiii] India's Cyber Security: A look at the Approach and the Preparedness - Indian Council of World Affairs (Government of India) (icwa.in)
15. [xiv] International Institute of Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment", June 28, 2021. Available at: https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power (Accessed on July 10, 2022).
16. [xv] Ministry of External Affairs, "Foreign Secretary's Statement at the UN Security Council Open Debate on "Maintenance of International Peace and Security: Cyber Security", June 29, 2021. Available at: https://www.mea.gov.in/Speeches-Statements.htm?dtl/33963/Foreign_Secretarys_Statement_at_the_UN_Security_Council_Open_Debate_on_Maintenance_of_International_Peace_and_Security_Cyber_Security_June_29_2021 Accessed on July 10, 2022
17. [xvi] ibid
18. [xvii] ibid
19. [xviii] Patrick Howell O'Neill, "The Russian hackers who interfered in 2016 were spotted targeting the 2020 US election", *MIT Technology Review*, September, 10, 2020. Available at: https://www.technologyreview.com/2020/09/10/1008297/the-russian-hackers-who-interfered-in-2016-were-spotted-targeting-the-2020-us-election/(Accessed on July 10, 2022)
20. [xix] Ministry of External Affairs, No. 3
21. [xx] The Information Technology Act, 2000. New Delhi, Gazette of India, 9 June, 2000, http://www.dot.gov.in/sites/default/files/itbill2000_0.pdf
22. [xxi] The NCIIPC and evolving work accessed at https://www.orfonline.org/expert-speak/nciipc-its-evolving-framework/
23. [xxii] https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar
24. [xxiii] https://www.financialexpress.com/defence/indias-tryst-with-a-new-national-cyber-security-policy-heres-what-we-need/2304053/
25. [xxiv] https://www.drishtiias.com/daily-updates/daily-news-analysis/national-cyber-security-strategy-1/print_manually#:~:text=Red%20Echo%20used%20malware%20called,the%20Serum%20Institute%20of%20India.
26. [xxv] Companies and Management rules,2014 http://www.bareactslive.com/ACA/act2533.htm