PLURALISTIC CYBER GOVERNANCE

Shraddha, Gujarat National Law University, Gandhinagar

ABSTRACT

"Cyberspace is the ultimate global commons, where nations, corporations, and individuals interact and interconnect."

- William Gibson

Cyber world is a borderless world which knows no boundaries, no scope. The impact of cyber activities is far reaching i.e. on individuals, organizations, nations or even universal- both positively and negatively. It's a double edged sword. It is not only the tool for freedom but also of oppression. However, there are inadequate regimes of governance internally and externally to respond to the consequences. Therefore, to ensure security, stability, privacy and growth at the same time, a proper mechanism of governance at these levels is essentially required.

This paper addresses this deficiency by providing a unique pluralistic approach of cyber governance by looking into challenges and benefits of establishing a global legal and policy framework for cyber activity.

"Cybercrime is a global problem that requires a global response."

- Ban Ki-moon, former UN Secretary-General

The principles of global constitutionalism in this new framework of global rule generation would emerge as a common democratic instrument of people to meet common challenges in addition and complementary to action for cybersecurity at the local, regional, national and supranational levels and shall promote inclusive decision making. This approach acknowledges that cyberspace is a global, decentralized, and dynamic environment, requiring a collaborative and inclusive governance framework. By making a comparative analysis we shall study the perspective of some countries with respect to this approach as these perspectives shape countries' approaches to global pluralism in cyberspace governance, influencing their policies, regulations, and international engagement.

Concluding, ultimately cyberspace is where the future is being written and we as a state need to write it together keeping in view and respecting each other's sovereignty and integrity and thereby addressing this frontier by maintaining the equilibrium between state laws and international law.

Keywords: cybersecurity, pluralistic, global cyber governance

INTRODUCTION

Cyberspace represents a living reality that influences all the aspects of human behavior today. The influence is multifaceted, nearly touching every element of our lives, from the way we connect and interact with each other, democratizing our access to knowledge, revolutionizing learning processes, to reshaping social, political, economical, cultural, and global relationships. Not just that, it facilitated global connectivity and conflicts. The 2016 US Presidential Election showed, among other things, the way in which technologies can interfere with or even compromise political processes. Digital innovation entails cybersecurity concerns that may have major negative impacts on the whole of society. Therefore, as the technology keeps on developing, so does the burden on our shoulders increase for addressing this issue of cyber governance. The cyber world has developed into a borderless environment in the connected world of today, where conventional geographic borders are mostly irrelevant. By definition, cyberspace crosses national boundaries and has an international impact on people, organizations, and countries. It exhibits a dual nature, acting as an instrument for exploitation, domination, and criminal activity in addition to being a force for freedom and creativity. The wide-ranging effects of cyber activity, whether in the form of beneficial advancements like digital progress or detrimental consequences like cybercrimes and data breaches, highlight the complexity of this field. Because of this double-edged effect, it is essential that global stakeholders address the governance issues that cyberspace presents.

Nonetheless, both within national borders and across international frameworks, the tools to regulate cyberspace continue to be insufficient and dispersed. Cyberwarfare, privacy violations, security flaws, and a lack of accountability have all been brought on by weak governance frameworks. At the national, regional, and international levels, a clearly defined governance system is necessary to strike a balance between the objectives of security, stability, privacy, and economic progress. This paper proposes a pluralistic approach to cyber governance, focusing on the need for a collaborative global legal and policy framework. Such a framework, rooted in the principles of global constitutionalism, aims to foster inclusive and democratic decision-making. It advocates for complementing national cybersecurity strategies with transnational policies that reflect shared responsibilities and mutual respect for sovereignty. Recognizing cyberspace as a decentralized and dynamic environment, the paper emphasizes the importance of cooperation between states to achieve sustainable governance. Through a comparative analysis of various national approaches, the study will explore how different perspectives influence countries' policies and international engagement in cyber governance. This examination will shed light on the challenges and benefits of establishing a global pluralistic framework that promotes inclusive decision-making while safeguarding state integrity and sovereignty.

Ultimately, the future is being shaped in cyberspace, and it is imperative for states to collaboratively craft rules that reflect mutual respect and common interests. Balancing national laws with international frameworks will be essential to addressing the challenges posed by cyberspace governance while ensuring long-term security, stability, and equitable growth.

The following research questions are formulated in the light of the preceding discussion-

1. What are the key challenges and opportunities associated with cyber governance in a borderless and interconnected world?

2. How can global legal and policy frameworks address the dual nature of cyberspace as both a tool for freedom and innovation and a platform for exploitation, crime, and conflict?

3. In what ways do national and regional approaches to cyber governance differ, and how these differences shape international collaboration?

4. How can global cyber governance ensure a balance between individual privacy, national security, and economic growth?

PLURALISTIC CYBER GOVERNANCE

Pluralistic global cyber governance is a system in which cyberspace is managed and regulated through the active participation of various stakeholders at different levels, including states, international organizations, private sector entities, civil society, and technical communities.

Key Features

1. This pluralistic mode of governance brings **varied actors** into the making of a policy. Besides governments, it would also involve non-governmental organizations, industry leaders, technical experts, and civil society groups. Each one of these brings along different expertise and priorities, thus contributing to a more holistic and balanced approach toward cyber governance.

2. Whereas in most cases, decisions are taken within the model by an agent or a few, pluralistic governance supports **decentralizing decision-making**. That is, instead of resting with one agent or a small number of agents, decisions can be distributed amongst several stakeholders, and hence, be more inclusive and representative.

3. It recognizes the fact that cyber issues cut across **multiple layers of governance**, from international treaties and agreements to national regulations and local policies. For global cyber challenges, coordination and harmonization are supported in such multi-layers in pluralistic governance.

4. Given not only the rapid pace of technological change but also that cyber threats continue to evolve, pluralistic governance frameworks are designed to be **flexible and adaptive**. This facilitates their response in light of new developments and emerging issues in cyberspace.

5. Pluralistic forms of governance often see the establishment of **collaborative frameworks** and platforms for different stakeholders to converse and share their information toward common goals. This may be through formal institutions, informal networks, or ad hoc working groups.

STAKEHOLDERS

Global stakeholders can promote digital inclusion and reduce the digital divide by working together to develop accessible infrastructure, affordable services, digital literacy programs, and inclusive policy frameworks. This requires a coordinated effort among governments, international organizations, private sector companies, civil society groups, and academia to address both the technological and socioeconomic barriers that contribute to the digital divide.

These are the four major stakeholders in cyberspace recognized by the United Nation General Assembly.

1. **Government** - With cyberspace becoming an arena for geopolitical tensions, diplomatic efforts to establish cyber non-aggression pacts can reduce conflicts and ensure mutual respect for privacy and economic interests. It bears the principal responsibility for policies pertaining to cyberspace, including cyber-security, and for the implementation of cyber technologies in pursuit of national governance goals. For instance, in Ukraine, since the start of the armed invasion of Ukraine in February 2022, cyberattacks account for 89% of all incidents. The most targeted sectors were the public administration, media, ICT, financial, and trade. Five incidents, targeting Ukrainian entities, were attributed to state-sponsored actors. For instance, incidents have been attributed to APT282, a Russian state-sponsored actor. It was reported by CERT-UA that in a phishing campaign, to obtain authentication data for Ukrainian public mail services. The Ukrainian team discovered HTML files imitating the interface of mail services used to exfiltrate authentication data entered by the target using HTTP POST requests, transferring the stolen data by using previously compromised Ubiquiti devices. It was also reported on a cyberattack targeting a critical energy infrastructure facility in Ukraine. The IT Army of Ukraine reported over 25 strikes during the first examination of hostile cyber activities related to the current war in Ukraine. Apart from this, based on studies conducted by the Cyber Peace Institute, the three nations that were most attacked in August 2023 were Italy, the Netherlands, and Poland. Poland had 26 cyber incidents that were reported, with the Netherlands and Italy following closely after with 24 and 20, respectively.[1] It therefore falls upon the governments to ensure that international co- operation in cyber- space is effective to achieve these goals of protecting the cyberspace and ensure the cybersecurity of the nations. For instance, in India, coordinating efforts across several government departments and agencies, the National Security Council Secretariat (NSCS) is in charge of overseeing the execution of national cybersecurity policies and plans and the Ministry of Electronics and Information Technology (MeitY) is in charge of developing and carrying out cybersecurity and information technology policy. Apart from that the National Cyber Security Coordinator (NCSC) works with many stakeholders to improve cyber

[1] Cyber-Dimensions_Ukraine-Q3-2023.pdf (cyberpeaceinstitute.org)

resilience while coordinating and supervising the national execution of cybersecurity projects.

2. **Business**- Governments' national cyber policy and worldwide collaboration approaches on cyber challenges are greatly influenced by businesses. Owing to their emphasis on innovation and the utilization of cyber technologies that they have either copyrighted or patented, corporations perceive cyberspace as a new avenue for expansion and revenue. A stable and efficient international framework for cyberspace is becoming more and more important to businesses as a result of the development of a global trade framework for e-commerce regulation. For instance, in India through working groups and industry forums, groups like the Confederation of Indian Industry (CII) and the National Association of Software and Service Companies (NASSCOM) significantly influence cybersecurity standards and policy. In Public-Private Partnerships the Indian government encourages collaboration between the government and private business enterprises with a view to enhance capability and resilience, not just in terms of building capability and resilience but also in countering new threats like cybercrimes. These include initiatives such as the **Cyber Surakshit Bharat program** is a project the Indian government started to improve the nation's cybersecurity framework. The Ministry of Electronics and Information Technology (MeitY) launched the initiative in January 2018 with the intention of enhancing the cybersecurity ecosystem and raising awareness of cyberthreats, particularly in government institutions and vital industries. Also, governments can work with tech companies and internet service providers to share information on emerging threats while maintaining privacy. Initiatives like the **Global Forum on Cyber Expertise (GFCE)** allow for capacity-building and knowledge sharing across sectors, fostering innovation and improving responses to security incidents. Apart from this, Governments could provide tax incentives for companies investing in cybersecurity infrastructure or privacy-enhancing technologies. This would encourage businesses to prioritize data protection and resilience while boosting economic growth. Insurance requirements that mandate stringent cybersecurity practices and data protection can help companies mitigate risks while supporting overall economic stability.

3. **Academia**- Cyber governance is a multidisciplinary discipline that incorporates elements of economics, psychology, and law. To give a comprehensive strategy to

addressing cyber concerns, academic institutions incorporate various disciplines within cybersecurity curricula. Digital literacy is critical for individuals to access opportunities online meaningfully. Stakeholders can develop training programs to build digital skills and competencies across age groups and regions. Academia contributes to research and development, invention, and framing of theories about cyberspace in order to give it a global outlook. Most of these ideologies have been spread all over the globe either by corporations or governments. Academics have also become increasingly important in developing the basic building blocks of understanding of cyberspace; for example, the imparting of cyber skills and values through education as global cyber activities increase. Universities and research centers provide policy analysis, new technology creation, and cybersecurity research. Organizations such as the IITs and IISc introduce vast knowledge and innovation in the cybersecurity field. The Interdisciplinary Centre for Cyber Security and Cyber Defence of Critical Infrastructure, for instance, is housed at IIT Kanpur and focuses on cybersecurity research, especially as it relates to safeguarding critical infrastructure. A Center of Excellence in Cybersecurity is located at IIT Kharagpur, providing cutting-edge cybersecurity teaching and research. Also innovation centers and incubators have been established by several academic institutions to assist cybersecurity firms. These businesses frequently offer cutting-edge products to the market, improving cybersecurity as a whole.

4. **Civil society** - It is concerned with the impacts of government, corporate, and academic activities in cyberspace on civil society. The urgent problems faced by the global civil societies are the issues of bridging the digital gaps, enablement of man and society through new cyber platforms and technology usage among other concerns, and in defense of basic human rights and freedoms in cyberspace. Individual groups and organizations in civil society advocate open internet policy, digital rights and privacy interests through different groups such as the **Internet Freedom Foundation** organize campaigns against laws that potentially violate people's digital rights, such as those requiring data localization or involving widespread surveillance. All these civil society groups are also engaged in making the general public aware about **digital literacy** to inform the public about cybersecurity risks, safe online conduct, and their digital rights. People are now more equipped to safeguard themselves online and choose wisely about their digital imprint.

Therefore, these 4 pillars play a critical role in identifying the strengths and vulnerabilities of cyberspace. In varying degrees around the world, all four have expressed interest in creating the building blocks for a multi-stakeholder inter-national framework for cyberspace.

In contrast to centralized or monolithic governance, perhaps driven by one dominant actor or narrow set of rules, pluralistic governance recognizes that cyberspace is complex and multifaceted and attempts to bring various perspectives and interests into decision-making processes. However, the concept of pluralistic approach of cyber governance is not just limited to these stakeholders. These stakeholders justify the approach when we talk about any particular countries' mechanism to govern its cyberspace. Whereas when we look at the global governance of the the same various other factors comes into play. Cyberspace knows no borders. So it becomes essential for us to consider it as a global challenge instead of just making the domestic arrangements. The 2030 Agenda for Sustainable Development emphasizes the significance of global interconnection and information and communication technology (ICT) as potent drivers of growth, accelerating human progress, closing the digital gap, and fostering the development of knowledge societies. Digital transformation is bringing about significant changes in industries including healthcare, banking, and education and along with it comes the threats to be countered. Their susceptibility to operational disruptions due to cyberattacks and the utilization of monitoring technology is obvious. For example, if a cyber-attack hits a healthcare facility, the attack would have accessed sensitive data on patients, which includes personal information, medical history, and even financial information. In extreme cases, cyber-attacks have resulted in shutting down an entire healthcare facility, putting all the lives of all patients at risk. Cancelled outpatient appointments and elective surgical procedures have frequently been disrupted by certain ransomware attacks that block access to vital healthcare IT systems. In the most severe cases, hospital emergency rooms had to turn away ambulances and cancer clinics had to put patient treatment on hold. Recent cyberattacks have resulted in the theft of personal mental health information, which the attackers then posted publicly as a last option. This illustrates how an attack may affect a victim's physical and mental health.[2] This demonstrates that the impact of a cyber-attack, if there, would know no boundaries and can cause unimaginable consequences. This is how serious it is- beyond imaginations. Today, cyberspace controls everything. And to control such a magnanimous power, a global control

[2] Cyber-attacks on critical health infrastructure (who.int)

has to be established. The approach of Global Constitutionalism with respect to the governance of cyberspace has to be adopted. A unified set of rules which all the nations can abide by keeping in view their sovereign sanctity. In addition to and in support of cybersecurity action at the local, regional, national, and supranational levels, this common democratic tool of people, that is, global constitutionalism will encourage inclusive decision-making and help address shared concerns.

CONSEQUENCES OF LACK OF GLOBAL CYBER GOVERNANCE

Bad governance in the cyber world would lead to severe consequences, such as a more vulnerable state of those critical infrastructures that are very important and vital for national security towards cyberattacks, raising the chances towards a cyber-conflict, geopolitical tensions, and instability around the world. There is considerable insecurity in cyberspace because the barriers to entry are low and offence is cheaper than defense. This lack of a global governance framework for cyberspace creates huge challenges. Today, cybersecurity is no longer a matter concerning any nation individually or organization; it has grown to be an international issue affecting various areas such as international relations, economic stability, and personal privacy. The status of the current state of global cyber governance remains disjointed and incoherent-a reflection of a patchwork of national regulations along with a multitude of bilateral agreements instead of a coordinated strategy at the international level.

A few characteristics typify this lack of global cyber governance.

- First, there is **no standardization of regulations**, meaning that countries apply various rules and policies concerning cybersecurity, data protection, and cybercrime. This inconsistency raises complexities in compliance for large, multinational organizations and further hampers efforts to combat such threats effectively.

- It allows the cyber-criminal to **exploit the jurisdictional difference** in case of the absence of a coordinated global approach to the problem and hence making its pursuit and prosecution across borders challenging. This may result in more frequent incidents of cyberattacks and other malicious activities transcending national boundaries.

- This is further exacerbated because some nations have **more cybersecurity resources** and capabilities than others. For every advanced cyber defense system that has matching regulatory foundations, there is another without the necessary infrastructure or expertise to protect themselves well. It is this imbalance that creates vulnerabilities that could be leveraged by adversaries.

While there are no globally laid-down governance frameworks, many challenges are hard to deal with, including disinformation, misinformation, and cyber espionage, which are seriously impinging on international stability and public trust. They still go on, though different international organizations and forums are trying to lay down guidelines and agreements in place. Comprehensive and effective global governance, however, is far more complex and dynamic to achieve in cyberspace, which calls for the cooperation and commitment of nations, businesses, and other stakeholders across the world.

Through a well-thought-out, multi-layered strategy that harmonizes international standards, global cyber governance can strike a balance between economic growth, national security, and individual privacy. National security vulnerabilities are reduced and countries are encouraged to construct secure infrastructure by establishing consistent security procedures and interoperability standards, such as those set forth by the International Organization for Standardization (ISO).

Differences in national and regional approaches to cyber governance

National and regional cyber governance approaches vary widely, shaped by cultural values, security priorities, and political systems. These differences impact international collaboration by creating legal and operational barriers. One of the starkest differences in cyber governance is seen in how regions approach **data privacy and security laws**. For instance The EU's GDPR is among the most comprehensive data protection laws globally, enforcing strict standards on how personal data is collected, stored, and shared. The GDPR's extraterritorial scope also requires any organization handling EU citizens' data to comply, even if it operates outside the EU. In contrast, the U.S. follows a more fragmented approach, with sector-specific privacy laws like the Health Insurance Portability and Accountability Act (HIPAA) for healthcare data and the California Consumer Privacy Act (CCPA) for consumer data protection. The U.S. model places more emphasis on self-regulation within the private sector, allowing companies flexibility but resulting in weaker unified protections compared to the GDPR. It complicate collaboration as multinational companies must navigate varying standards, while governments face challenges in aligning cross-border data regulations.

Nations also vary widely in their approach to online freedom of expression, often influenced by cultural and political factors. **China's cyber governance** is marked by strict censorship and state control under the Cybersecurity Law of 2017, often referred to as the "Great Firewall of China." The Chinese government requires that all digital content aligns with national security interests, using extensive filtering and surveillance mechanisms to block foreign platforms and censor online discourse. This state-controlled model reflects **China's focus on sovereignty, stability, ideological control and cultural preservation.** The law mandates that all internet and technology-related activities align with state interests, ensuring the government can censor content, monitor communications, and restrict foreign influence. This approach is deeply rooted in China's political philosophy, prioritizing collective security and national unity over individual freedoms. The law enforces data localization for "critical information infrastructure," compelling companies to store Chinese users' data within China. The government utilizes the "Great Firewall" to **control internet access**, blocking foreign websites and censoring content that is deemed harmful to Chinese values or government policies. Whereas India's cybersecurity model, while also prioritizing national security, takes a **more balanced approach** between regulatory control and democratic values such as privacy and free speech. Although India has introduced some **data localization requirements** under its proposed data protection law, these are more limited compared to China's. For instance, data localization mandates in India are generally restricted to certain categories of data, and the government allows cross-border data transfers, unlike the more stringent requirements in China. India allows greater freedom of expression compared to China. The **Section 69 of IT Act** allows the government to order the removal of certain types of content, such as hate speech, misinformation, and illegal activities, but it must justify such actions within legal and democratic norms.

CHALLENGES AND SOLUTIONS

In attaining this pluralistic form of cyber governance, there are many challenges to overcome in between some of which are discussed below-

- Firstly, approaches toward plural cyber governance differs because each country has a different set of national interests, priorities, and policymaking capacities, as well as regulatory processes that involve cyberspace. Coordination or coming to a consensus among so many stakeholders is cumbersome. The conflict of priorities and perceptions results in disagreements on the best common issue, which again delays decision-making. This consensus is very important to be achieved among countries and different stakeholders otherwise the cybercriminals will always remain untraceable due to the borderless nature of the crime. A decentralized approach of decision making needs to be followed like a decentralized autonomous organization.

- It is also to be ensured that all voices are heard and that no interest or group takes over the governance process. This is to say that the Global Constitution with respect to Cyber Governance should not just be the creation of superpowers of the world. It should be by the cooperation and consensus of all the signatories. Also the rules must be such so as to ensure and respect the national sovereignty of all member nations. Even in case any sought of interference is required to tackle any situation, a harmonious and ethical way must be construed. Principles of Natural Justice have to be duly upheld. A number of competing interests-security, privacy, innovation, and so on-can be balanced only with great care through negotiation and compromise.

- Furthermore, the adoption and implementation of such a pluralistic framework can be challenging in the case of a multiplicity of jurisdictions and varying sectors. Because data is dispersed across several services, providers, locations, and even jurisdictions in the setting of cloud computing, securing electronic evidence for the criminal justice system can be very difficult. The Budapest Convention on Cybercrimes is now addressing these issues. Enabling criminal justice to access evidence stored in cloud computing environments is a top concern for the convention.

- Appropriate mechanisms for ensuring compliance and addressing violations will be essential. This must be in cooperation with other relevant stakeholder actors. Also in this regard, one fundamental underlying factor that may impact pluralistic governance is that of inequalities among stakeholders in resources and capabilities when speaking, for example, of developed and developing countries. It also seems that governments find it hard to place cybercrime above different forms of crimes-especially those that seem to carry with them the potential for more seriousness. When the latter occurs, the consequences are loss of life and a more destabilizing effect on their countries. This may be particularly true in terrorism cases. For example, the United Kingdom has been able to implement a cyber-budget of 1.3 billion pounds over five years for the comparative budget in counterterrorism work, more than 2 billion pounds per year 41 within the same budget period.[3] Attention must be paid to ensure that any poorly resourced entities receive fairness and are supported.

- There are obstacles in place at the strategic level as well, such as creating a mechanism for interagency collaboration and clearly defining the duties of various government entities working on cyber-related matters. This is frequently made worse when there is no central body in charge of managing this kind of coordination. For example, there is no one organization or individual in charge of coordination among the many government organizations and law enforcement institutions involved in cybercrime enforcement in the United States. These groups sometimes have overlapping and redundant duties. This has resulted in inefficiencies, duplications, and challenges in guaranteeing that US congressional oversight initiatives are linked to a comprehensive agency-wide strategy approach to cybercrime[4]. Even though many countries have strong national cyber strategies with anti-cybercrime components, this problem is exacerbated by the fact that these strategies are not always supported by a legal framework that allows official interagency cooperation in cybercrime cases at the strategic and operational levels. Despite the possibility that establishing a single body with the authority to supervise this sort of coordination would be considered a "good practice," many governments currently lack this kind of division. However, there has been some progress made in this field. For instance, the Singaporean government unveiled a cybersecurity strategy in 2016 along with a National Action Plan on Cybercrime that outlines the many steps each entity would take to meet the goals of the plan. A Minister-in-Charge of Cyber Security was

[3] Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime Strengthening Global Capacity on Cybercrime on JSTOR (refread.com)

[4] To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors, THIRD WAY (2018), https://thirdway.imgix.net/pdfs/override/To_Catch_A_Hacker_Report.pdf

named to help coordinate implementation of the Strategy.[5]

- Additionally, at the strategic level, countries have failed to institute sufficient mechanisms to track metrics on both the rates of cybercrime and the law enforcement actions taken against cybercriminals. Cybercrime data typically relies on victim reporting, which the USA FBI acknowledges usually only represents a "fraction" of the crimes that occur.[6] In addition to challenges in getting victims to report cybercrimes, few countries have any mechanisms in place to track metrics for law enforcement actions taken against cybercriminals. This inhibits law enforcement and policymakers from understanding the impact of anti-cybercrime efforts and determine needed changes to make progress in defending against the cybercrime threat.[7]

- Investigations into cybercrime sometimes span international borders, necessitating coordinated efforts by several law enforcement agencies to apprehend offenders. Even if there are still many problems, there have been a number of advancements in the past few years that, when combined with efficient execution, have the potential to improve collaboration. For instance, **Mutual Legal Assistance Treaties (MLATs)** facilitate cooperation between countries in investigating cybercrime while respecting privacy laws.

- Global economic integration requires a balanced approach to data sovereignty and cross-border data flows since data localization regulations may clash with privacy requirements and international corporate operations. Agreements such as the U.S. CLOUD Act, for example, balance privacy rights and national security by offering legal foundations for cross-border data access with stringent restrictions.

CONCLUSION

Regarding India, the country's adoption of a plural cyber governance policy says a lot about its belief that the governance and management of cyberspace should involve the public and private sectors, technology communities, and civil society. However, it is confronted with the same

[5] releases/ncap-document.pdf Singapore's Cybersecurity Strategy, CYBER SECURITY AGENCY OF SINGAPORE (2016), https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf

[6] E.U. final report on prevention and combating cybercrime

[7] U.N. Study on Cybercrime

challenges, it has not yet subscribed to the International regime of Budapest Convention keeping in view its national security and sovereignty. Despite amending the IT Act in 2007 and 2008 to bring it more closely aligned with the Budapest Convention, India has not yet ratified this convention. Nonetheless, India's entrance to the Budapest convention may have been hampered thus far by foreign policy considerations. It is past time for the Indian government to reevaluate this in light of the rise in cybercrime and India's ambition of Digital India. An essential component of the network of solutions required to handle cyberspace security and the rule of law is international agreements. Here the role of international law and agencies comes into picture. I agree to the fact that national sovereignty is a concept that no country would compromise with. However, when it comes to the global agenda like cybersecurity, the harmonious construction in the ideologies should be built up. As is rightly said, precaution is better than cure. Therefore, all the countries must come to a consensus on a particular law to govern the cyberspace because to secure this idea of plural cyber governance, a legal framework that accommodates diverse national and international laws, foster global cooperation to address transnational cyber issues and also ensures transparency and accountability has to be created in order to have a more inclusive, diverse and effective cyber governance ecosystem.