Int. J. Advanced Networking and Applications
Volume: 15 Issue: 04 Pages:100-200 (2023) ISSN: 0975-0290 (Special Issue – ASCIS 2023)

A Cyber Diplomacy Framework for Promoting Global Cybersecurity Norms and Cooperation

Niraj Kumar Singh
Research Scholar, Faculty of Computer Applications, Marwadi University, Rajkot, India
Email: nirajsingh98456@outlook.com
Sunil Bajeja
Associate Professor-FCA, Marwadi University
Email: sunilbajeja@yahoo.com
Salmiati
M.A in International Relations and Diaspora, Gujarat University, Ahmedabad, India
Email: ammysalmiatialam@gmail.com

----------**ABSTRACT**----------

In recent years, the escalating threat landscape in cyberspace and the imperative of maintaining a secure digital environment have garnered significant attention, necessitating the exploration of innovative approaches. This research introduces a novel "Cyber Diplomacy Framework for Promoting Global Cybersecurity Norms and Cooperation" to address the pressing challenges in the realm of cybersecurity. The primary goal of this study is to propose a comprehensive framework that emphasizes diplomatic efforts to mitigate cyber threats and foster cooperation among nations in establishing responsible cybersecurity norms at the global level. This research draws upon the constructivist theory of international relations to understand how norms are established and evolve through diplomatic interactions between nation-states. The constructivist perspective posits that the shared beliefs, values, and norms of actors in the international system play a vital role in shaping their behavior and interactions. Applying this theory to the realm of cybersecurity, the study explores how the Cyber Diplomacy Framework can contribute to the emergence of shared norms and responsible behavior in cyberspace through diplomatic engagement. By proposing a pioneering Cyber Diplomacy Framework and employing the constructivist theory as the underlying concept, this research aims to advance the field of cybersecurity and international relations. Through a comprehensive analysis of diplomatic strategies, international cooperation, and governance mechanisms, this study endeavors to provide valuable insights for policymakers, researchers, and practitioners in promoting global cybersecurity norms and cooperation. It is anticipated that the Cyber Diplomacy Framework will contribute significantly to the enhancement of cybersecurity practices and resilience in an increasingly interconnected digital world.

Keywords - **A Cybersecurity Cooperation, Cyber Diplomacy, Cybersecurity Norms, Framework.**

Date of Submission: 30 September 2023 Date of Acceptance: 15 November 2023

Int. J. Advanced Networking and Applications
Volume: 15 Issue: 04 Pages:100-200 (2023) ISSN: 0975-0290 (Special Issue – ASCIS 2023)

I. INTRODUCTION

In the modern era characterized by the digital revolution, the notion of national security has evolved from the conventional model, which primarily focused on protecting the nation from military and non-military dangers, such as armed assaults and acts of terrorism. Nevertheless, over the last decade, global dynamics have transformed due to the rise of information and communication technologies, resulting in a substantial change in the landscape of national security. National security is no longer solely related to physical aspects, but also extends to the complex dimension of cyberspace, known as cybersecurity (Ciuriak, 2020). The shift of national security to the cyber domain carries profound implications within the context of International Relations Cyber threats defy geographical boundaries, and cybersecurity has evolved beyond being a mere technical consideration to an issue that surpasses national limits and extends into geopolitical, economic, and social dimensions. Increasingly intricate and advanced cyberattacks have placed critical infrastructure, national security, personal privacy, and global economic stability in jeopardy. Hacking incidents, data theft, cyber espionage, and other forms of cyber threats have become evident and imminent realities (Maness & Valeriano, 2016).

In a time when information and communication technology has deeply penetrated various facets of human existence, cybersecurity has risen as a highly complex and urgent concern in the contemporary global community. The digital revolution has ushered in substantial changes in the way we communicate, conduct work, and participate in various endeavors. However, amidst the countless benefits and impacts, we also face increasingly serious and pervasive threats stemming from the virtual world (Abd-Rabo & Hashaikeh, 2021). Cyber challenges have introduced substantial complexity into the dynamics among states and non-state actors in the cyberspace. Various facets of cyber issues, such as national security, espionage, economic repercussions, conflicts, international norms, international cooperation, involvement of non-state actors, privacy, human rights, and uncertainty, are all interrelated and influence the dynamics of inter-state relations (Cavelty & Egloff, 2019).

Facing the challenges of cyber issues, international cooperation becomes highly essential. Countries must unite to formulate norms governing behavior in the cyber realm and develop collective responses to cyber attacks. Addressing cyber issues should also consider human rights and privacy aspects, while acknowledging potential economic impacts resulting from cyber attacks. Creating an environment where clear international norms and close international collaboration can flourish is crucial (Lewis, 2022). These collaborative efforts will aid in tackling the uncertainties often prevalent in the cyber world and reduce the potential for conflicts arising from cyber attacks. Moreover, as cyber attacks have evolved from individual or group hacking incidents to more complex and organized threats, states, non-state entities, and criminal groups have all exploited the cyber space to achieve their objectives, including espionage, sabotage, data theft, or disruption of critical infrastructure (Samantha Bradshaw & Global Commission on Internet Governance Paper Series, 2017).

In an era characterized by the swift expansion of digital technology, the virtual realm has become an integral component of contemporary human existence. The rapid advancements in technology and the internet have unlocked remarkable prospects across economic, societal, and cultural domains. However, alongside the benefits of this transformation, the global community is faced with various cybersecurity challenges that transcend national boundaries and require collective action. Cyber threats, such as data breaches, software piracy, and state-supported cyber espionage, continue to evolve in intelligence and scale, posing significant risks to individuals, businesses, and governments worldwide (Chen, et al., 2023). In this interconnected cyber landscape, traditional paradigms of diplomacy and governance must adapt to effectively address these threats and protect the digital domain. The pressing necessity to address cybersecurity challenges through a thorough and cooperative strategy has led to the emergence of the notion of Cyber Diplomacy. Cyber Diplomacy involves applying the principles and practices of traditional diplomacy in the context of the online world with the primary goal of promoting global cybersecurity norms and facilitating international cooperation (Boussi & Gupta, 2020).

In this research, an innovative Cyber Diplomacy Framework will be presented, aimed at shaping the future of cybersecurity through a holistic and inclusive approach. Based on the principles of mutual respect, trust, transparency, and shared interests, this framework aims to facilitate strong cyber governance and resilient digital infrastructure worldwide. Fundamentally, the Cyber Diplomacy Framework recognizes that cybersecurity challenges cannot be addressed through isolated efforts. Instead, its primary emphasis lies in forging partnerships and coalitions among countries, private enterprises, non-governmental organizations, and international bodies. Through collaborative dialogue and knowledge-sharing, the framework seeks to unite various stakeholders in facing threats and vulnerabilities together (Kumar, Pandey, Varshney, Kumar, & Kumar, 2023). Therefore, the research problem statement for this study is “What are the key components of the Cyber Diplomacy Framework that can effectively promote global cybersecurity norms?”

This research employs Constructivist Theory, which asserts that stakeholders in the realm of cybersecurity, including sovereign states, private sector actors, civil society organizations, and individuals as users of the cyberspace, collectively shape the landscape of cybersecurity (Eriksson & Giacomello, 2014).

In the realm of international relations, the constructivist theory has received considerable recognition, giving great importance to the influence of ideology, norms, and identity in molding the actions of nations and the dynamics among players in the global system.When applied in the context of cyber diplomacy, constructivism helps us understand the perspectives and responses of states, non-state

actors, and international organizations to threats, norms, and collaborative efforts in the cyber domain (Barnett, 2018).

Perceptions of cyber threats can be influenced by the norms that develop within the international community, governing what is considered a threat and what behaviors are acceptable in the cyber realm. Furthermore, the evaluation of threats is significantly influenced by the identity of a state or non-state actor. The interactions among international actors also affect how they perceive these threats. Therefore, diplomatic and negotiation efforts can have an impact on changing perceptions of cyber threats. Through dialogue and cooperation, international actors can influence how they view and respond to cyber threats. Furthermore, international agreements and the establishment of new norms can also influence how these threats are understood (Kolodziej, 2009).

II. RELATED WORK

As per paper [13] This research explores the dimensions of cyber diplomacy through a systematic literature review. This research focuses on the cross-disciplinary nature of cyber diplomacy, which emerged as a global security priority following the significant cyber attack on Estonia in 2007. This study fills a gap in the literature by differentiating cyber diplomacy from traditional diplomacy and aims to reveal its current dimensions in research cyber diplomacy. This study recognizes the cross-disciplinary nature of cyber diplomacy, combining aspects from policy, politics, sociology, digital/cyber science, multilateralism, and world history. However the discussions of cyber diplomacy primarily emphasize state-led diplomacy, potentially ignoring other important aspects of cyber interactions involving non-governmental entities. As the paper [14] The article analyzes the institutionalization of cyber-diplomacy in foreign ministries, highlighting the challenges and approaches adopted by different countries. Although this article provides a comprehensive theoretical discussion, it lacks empirical examples or specific case studies to illustrate the practical implementation of cyber-diplomacy by different countries.

As the paper [15] The authors propose a Cyber-Diplomacy and Cybersecurity Awareness Framework (CDAF) to address the gap in cyber-diplomacy and cybersecurity awareness levels among diplomats in developing nations. The CDAF comprises two components: cyber-diplomacy and cybersecurity awareness. The paper emphasizes the need for diplomats to undergo orientation and training in cyber-diplomacy to effectively address potential cyber threats. The framework is developed through a design science research approach and aims to enhance the role of diplomats in the international cyber-diplomacy domain. However the paper focuses on developing countries, it might benefit from comparative analyses with developed nations to provide a broader perspective on the challenges and solutions in cyber-diplomacy. As the paper [16] focus on the policy challenges and global inequalities in cyber capacity building, particularly in countries of the Global South. The article successfully highlights the existing cybersecurity divide between developed and developing countries. The descriptive data and regression models effectively demonstrate the significant gap in cyber capacity, emphasizing the need for transnational cooperation and support for capacity-building initiatives. The article briefly touches upon realist-based arguments linking increased security threats to cyber capacity building but fails to provide an in-depth exploration. The limited support for these arguments and the inconsistency in the findings necessitate a more comprehensive analysis of the relationship between security threats and cyber capacity.

As the paper [17] The main objective of this research is to amalgamate and standardize prevailing cyber risk frameworks and models, introducing a novel architecture for seamless integration. It proposes innovative design principles to assess and enhance IoT cybersecurity, with a specific focus on the importance of recovery planning—a aspect often overlooked in prominent Industry 4.0 initiatives. However the emphasis on recovery planning is considered innovative, but this research could provide more depth on the specific challenges and strategies associated with recovery planning in the context of Industry 4.0 initiatives.

As per paper [18] focuses on the role of states in ensuring cybersecurity through defense, deterrence, and diplomacy, and the challenges faced by some countries in effectively participating in cyber diplomacy due to limited resources. The main actors in cyber diplomacy involve diplomatic and non-state entities engaging in discussions through bilateral and multilateral forums. The author also successfully maps various training programs and provides a comprehensive overview of resources in the field of cyber security but The study acknowledges the lack of information on the private sector's contributions to cyber diplomacy, which may limit a holistic understanding of available resources.

Figure 1 : Top ten best and worst prepare countries for cyber incident [19]

III. THE CHALLENGE OF INTERNATIONAL CYBER SECURITY

The increasing cybersecurity challenges posed by cybercrime in our progressively globalized and technologically sophisticated world cannot be disregarded. In

a context of rapid economic and technological advancement, a diverse array of actors, encompassing governments, businesses, and individuals, find themselves susceptible to cyber threats. Unbounded cybercrime, facilitated by information and communication technology, has yielded substantial repercussions on the global economy. Projections indicate that the expenses associated with cybercrime will persist in their upward trajectory, possibly reaching a staggering USD 10.5 trillion annually by the year 2025 (Tan, Xian, Parsons, & Radiett, 2021).

One of the global cybersecurity challenges is cyber conflicts conducted by both state and non-state actors to disrupt critical infrastructure or dismantle military logistics. Conflicts that occur between countries and non-state entities in the virtual world, each with different capabilities and interests, highlight the necessity for the development of an international cyber code of ethics to foster mutual trust (US Department of Defence, 2023). The need for international cyber cooperation is seen as an urgent collaboration to prevent cybercrime, infrastructure attacks, and mass data interception. However, the issue is that cyber threats can come from anyone and anywhere, including cases where the actor behind them is the state itself (Relations, 2018).

The necessity for diplomacy and global collaboration within the realm of cyberspace is essential due to the worldwide scope of cyber risks, underscoring the significance of steadfast dedication and continual prioritization of international diplomacy for safeguarding cyber security (Commite on Armed Services United States Senate, 2017). The elements connected to diplomacy in cyber security have indeed been set in place by nations across the globe through foreign policies. These encompass forging alliances and participating in international cooperation, elevating collective initiatives, addressing incidents, and enhancing capabilities. Although policy initiatives aimed at establishing a consensus for global stability in the cyber domain have been initiated, their effectiveness remains limited and demands further endeavors to establish robust cybersecurity in the digital world (Painter, 2018).

Security in the cyber realm necessitates strong collaboration between the public and private sectors to address the escalating threats posed by cybercrime. Organizations need to invest in fortifying their digital environment to safeguard themselves and their customers (Maurer & Nelson, 2021). The interconnected nature of the digital economy calls for joint efforts to ensure trust, resilience, and the full utilization of its potential. Emphasizing the enhancement of cybercrime intelligence, bolstering cooperation for collective anti-cybercrime operations, developing regional capacities and capabilities to counter cyber threats, and promoting cyber hygiene for a safer cyberspace are imperative (Tan, Xian, Parsons, & Radiett, 2021).

Cybersecurity presents a critical challenge for the global community due to the interplay among civil society, commerce, governance, critical infrastructure, intelligence, and law enforcement, each having diverse interests in cybersecurity practices and policies. This diversity gives rise to conflicting agendas and expectations, often leading to mismatches and discord in cybersecurity goals. Compounding this, states, as stakeholders with national security responsibilities, are entrenched in the traditional paradigm of national security (Li & Liu, 2022).

The paradox emerges from the dilemma faced by nations in reconciling the fading concept of sovereignty with the imperative of cyber cooperation. While nations cling to the principles of traditional national security, they also emphasize military and law enforcement for upholding security. However, the challenge lies in the inadequacy of these traditional institutions to effectively tackle national security threats in the cyber domain (Carr, 2016).

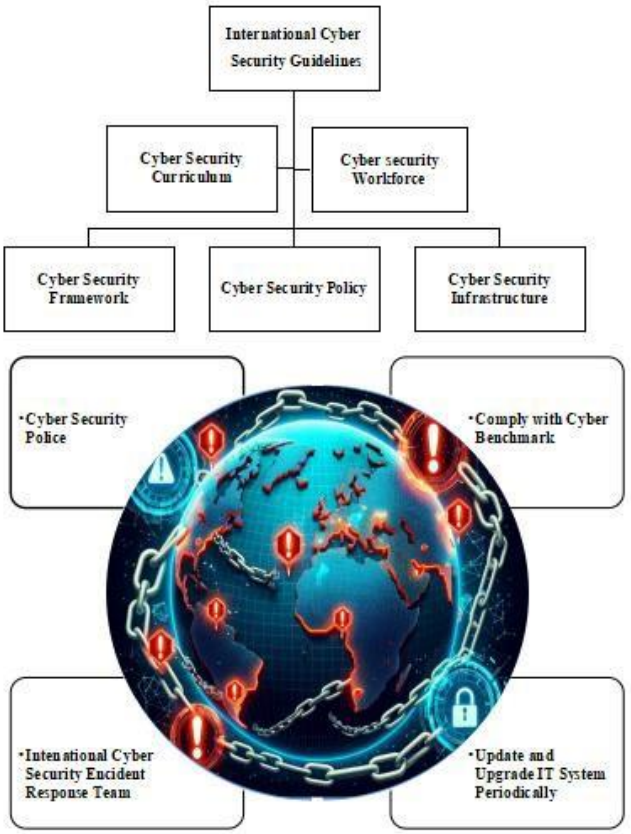

Figure 2: Tactics to safeguard digital world

IV. SOLUTIONS

In facing the complex challenges in the increasingly interconnected cyber world, a comprehensive approach and collaborative effort involving various stakeholders are necessary to maintain global cyber security. Efforts to address this issue involve the participation of various elements such as countries, international organizations, the private sector, academics, and civil society. The goal of these efforts is to create a secure digital environment capable of withstanding cyber attacks and safeguarding the privacy and data integrity of both individuals and institutions. The following are key

approaches in formulating solutions to uphold cyber security worldwide:

1.1 Cyber Security awareness and education Program

Many individuals do not fully comprehend the potential risks posed by cyber threats, making it difficult to motivate them to adopt and adhere to cybersecurity best practices. Therefore, all nations are required to implement a comprehensive Global Cyber Education and Awareness Initiative (GCEAI) under the guidance of the United Nations (UN). This initiative aims to promote global cyber education and awareness, empowering people with the knowledge and skills needed to navigate the digital landscape securely.

The Global Cyber Education and Awareness Initiative (GCEAI) should have a universal goal, ensuring that all international communities from diverse geographical backgrounds have access to cyber education resources. A standardized cyber education curriculum should cover fundamental cyber hygiene, digital literacy, data privacy, online etiquette, threat recognition, and safe online practices. Multi-stakeholder collaboration is essential in the Global Cyber Education and Awareness Initiative (GCEAI), involving governments, educational institutions, non-governmental organizations (NGOs), the private sector, and technology industry leaders to collectively contribute to the initiative's success.

To achieve success in cyber hygiene policy, the implementation of international policies that countries around the world must undertake under the auspices of the United Nations (UN) includes the following:

a. Global Awareness Campaigns

- Launch global awareness campaigns highlighting the significance of cyber education and its role in reducing cyber risks.
- Utilize social media, workshops, seminars, and conferences to engage diverse audiences.

b. Curriculum Development

- Collaborate with cybersecurity experts, educators, and industry professionals to create a comprehensive and adaptable curriculum.
- Include topics such as online security, phishing awareness, secure password practices, malware prevention, digital footprint management, and social engineering.
- Incorporate practical examples, real-world case studies, and interactive learning experiences.

c. Global Partnerships

- Collaborate with governments to integrate the curriculum into formal education systems.
- Partner with NGOs and community organizations to extend the program's reach to remote and underserved areas.
- Engage tech companies to provide expertise, resources, and funding for the initiative.

d. UN Oversight

- The United Nations can establish a dedicated body to monitor the progress and impact of the initiative.
- This body can collaborate with member states, international organizations, and experts to ensure the effectiveness and continuous improvement of the initiative.

1.2 Challenges of limited resources

One of the challenges faced by world cyber security is the challenge of human resources because not all countries have the same capabilities in the cyber field, therefore the solutions that can be taken for joint cyber security are:

a. Training and development

The cybersecurity industry is always changing quickly, and it can be challenging for human resources professionals to stay current with emerging risks and technology advancements while maintaining their knowledge and skill set. Organizations that lack the necessary expertise may be more susceptible to cyberattacks. As a result, businesses must invest in educating and developing their workforce's cyber security skills. Internal training, certification programme participation, and cooperation with relevant educational and training establishments are some ways to do this.

b. Security awareness

There is a greater need than there is supply of cybersecurity-trained workers. This results in a lack of qualified personnel in this industry. To overcome these obstacles, organizations must discover strategies to both attract and maintain a skilled workforce in addition to investing in the training and development of their current human resources. Thus, through frequent training programmers and security awareness initiatives, organizations should raise employee understanding of security issues. It is imperative to equip employees with enough knowledge about security risks and best practices.

c. Recruitment and retention

Due to a lack of knowledge about best practices in cybersecurity, human resources are frequently a weak point in the field. Workers who are not aware of security threats may unintentionally allow cyberattacks to occur. As a result, regular training and education are crucial to raising security awareness. Businesses must figure out how to draw in and keep skilled workers in the cybersecurity industry. This can be achieved by providing alluring incentives, defining career development, and establishing an environment at work that fosters learning and development.

Challenges with limited resources remain the largest obstacle for developing countries to take cybersecurity measures. Therefore, the solutions that the UN should implement to address resource limitations in cybersecurity are as follows:

a. Cybersecurity Aid Program for Developing Nations

The UN should facilitate member states and international partners in providing technical and financial assistance programs for developing countries to enhance their cybersecurity capabilities. This includes training, technology transfer, consultations, and funding to help them build cybersecurity skills and infrastructure.

b. Regional Training Centers

The UN should establish specialized regional training centers for cybersecurity across different regions of the world. These centers can provide intensive training in cybersecurity, including technical training, cybersecurity risk management, incident handling, and threat analysis.

c. Resource Sharing

The UN can facilitate resource sharing among member states, where more advanced cybersecurity countries can share their knowledge, experience, and best practices with those in need.

d. Alternative Funding

The UN can assist developing countries in seeking alternative funding for cybersecurity projects, such as funding from international financial institutions, donor organizations, or development assistance programs.

1.3. Geopolitical Trust Building

In contrast, due to strong geopolitical considerations, collaboration and information sharing between nations become difficult. Consequently, some countries are hesitant to adopt cybersecurity due to concerns about cyber surveillance, individual privacy, and national security. Therefore, the implementation that should be carried out by countries worldwide through UN forums is as follows:

a. International Cyber Diplomacy

The UN should facilitate specific diplomatic dialogues in cyber cooperation between nations to address and ease geopolitical differences. Such diplomacy can build the trust and understanding required for cybersecurity cooperation.

b. Neutral Forums

The UN can establish neutral forums that provide a space for countries to discuss cybersecurity without concerns about wider geopolitical consequences. These forums can separate cybersecurity issues from broader geopolitical conflicts.

c. Principles of Equality

The UN can advocate for principles of equality in cybersecurity, where countries are recognized to have equal rights and obligations to respect privacy and sovereignty. This can reduce concerns of using cybersecurity for political purposes.

d. Transparency and Limited Information Sharing

The UN can encourage countries to practice limited transparency in cybersecurity, where crucial information can be shared without revealing all sensitive details. This can address concerns about surveillance and privacy.

e. Integrated Security Principles

The UN can promote integrated security principles where cybersecurity is viewed as an integral part of broader national security. This can help countries perceive cybersecurity not as a threat but as an effort to protect the nation and its citizens.

f. Regional Cooperation

The UN can encourage countries to initiate cybersecurity cooperation at a regional level, which is more manageable and shares similar geopolitical contexts. This regional collaboration can serve as a stepping stone towards broader global cooperation.

g. Human Rights and Privacy

The UN can prioritize human rights and privacy principles in cybersecurity. This can help alleviate concerns about individual privacy violations and the misuse of cybersecurity for political purposes. By adopting diplomatic approaches, limited transparency, and principles of equality, the UN can facilitate inter-country cybersecurity cooperation and help overcome potential geopolitical barriers.

1.4 Solutions for International Cyber Law

Lastly, the variation in regulations and laws concerning cybersecurity across different countries is a significant challenge. The solutions to address this issue globally are as follows:

a. Establishment of International Principles

The UN should facilitate negotiations to develop international principles on cybersecurity that are acceptable to all countries. These principles can serve as guidelines for countries in developing their domestic regulations and laws.

b. Harmonization Framework

The UN can design a framework that harmonizes various cybersecurity regulations and laws worldwide. This framework can assist countries in adopting similar approaches to tackle cybersecurity challenges.

c. Development of Model Regulations

The UN can assist in creating model regulations and laws that can be adopted or customized by countries based on their needs and conditions. These regulations can serve as a starting point for countries looking to strengthen their regulatory frameworks.

d. Inter-Institutional Collaboration

The UN can encourage collaboration among international institutions like Interpol, UNESCO, and others to develop shared guidelines and cybersecurity frameworks. This collaboration can help avoid overlap and support global coordination.

e. Inter-Country Collaboration

The UN can incentivize countries to share experiences in developing cybersecurity regulations and laws. This collaboration can help countries learn from best practices and challenges faced by their peers. Through these approaches, the UN can help address differences in cybersecurity regulations and laws globally, ultimately leading to more coherent and effective global cooperation in tackling cybersecurity challenges.

1.5 Zero Trust Policy

The Zero Trust security model is a comprehensive approach that assumes no one, whether inside or outside an organization, should be trusted by default. Here's how to implement the zero trust policy for cybersecurity worldwide:

a. Awareness and Education

Promote awareness and education about the Zero Trust model among governments, businesses, and individuals worldwide. Encourage understanding of the principles and benefits of Zero Trust to foster a global cybersecurity culture.

b. International Standards

Collaborate with international cybersecurity organizations and standard-setting bodies to develop globally recognized standards for implementing Zero Trust policies. Create a framework that ensures consistency and interoperability across different industries and countries.

c. Collaboration Among Governments

Governments can lead by example, implementing the Zero Trust principles in their own digital systems and infrastructure. Establish international agreements or initiatives that promote the adoption of Zero Trust practices by both public and private sectors.

c. Protecting Cross-Border Data

Create secure cross-border data sharing guidelines that align with the principles of Zero Trust. Promote data protection regulations prioritizing user privacy and security, in line with the data-focused approach of Zero Trust.

e. Industry Cooperation

Encourage industries to collaborate in sharing threat intelligence, vulnerabilities, and best practices. Develop sector-specific Zero Trust guidelines tailored to address distinctive challenges.

f. Incentives for Cyber Insurance

Governments and organizations can offer rewards, like reduced cyber insurance premiums, to entities that implement and exhibit effective Zero Trust security measures.

g. Continuous Monitoring and Validation

Promote using ongoing monitoring tools and technologies that help organizations verify users, devices, and network activities in real-time.

h. Supplier and Supply Chain Accountability

Create guidelines for evaluating the cybersecurity practices of suppliers and providers according to Zero Trust principles. Encourage businesses to prioritize secure partnerships with entities following Zero Trust standards.

i. Collaboration between Public and Private Sectors

Facilitate public-private partnerships for sharing knowledge, resources, and expertise in implementing Zero Trust policies. Governments and organizations can cooperate to tackle emerging global cyber threats.

j. Global Incident Response Framework

Establish a global incident response framework aligned with Zero Trust principles, enabling coordinated responses to cross-border cyber threats. Enforcing the Zero Trust policy worldwide demands cooperation, collective responsibility, and a dedication to upholding security and privacy. Through nurturing a global culture of cybersecurity and collaborative efforts, countries and organizations can bolster their resistance against cyber threats in an interconnected global landscape.

1.6 Say No to Hacker

a. Technological Complexity

Hackers are always creating new ways to attack targets, and technology is developing at a rapid pace. Managing progressively intricate attacks necessitates a profound comprehension of technology and cybersecurity. Thus, the necessity for technological complexity through the use of intrusion detection systems, firewalls, and other robust security measures on networks and systems. Use data security solutions, such as antivirus and antispyware, to protect the system from malware attacks, perform routine software updates, and perform regular data backups and encryption to identify and address potential security gaps.

b. Collaboration among nations

Nations must work together to exchange intelligence and information about cyberattacks. This entails sharing information about threats that have been identified, attack strategies, and hacker tactics. Countries can alert one another and take the required precautions to safeguard their infrastructure by exchanging this information.

c. Establishment of International Treaties

International treaties can be drafted by nations to control cyber activity and impose sanctions on cyberattacks. These agreements might cover things like exchanging electronic evidence, helping with investigations, and extraditing of offenders. This may improve law enforcement's ability to combat hackers.

d. Increased awareness and Education

International awareness of cyber threats and best practises in security needs to be raised. Governments, corporations, and the general public can all benefit from the training and educational resources provided by international Organizations. Both individuals and Organizations can lower their chance of becoming hackers by learning more about cyberattacks and self-defense techniques.

e. Development of Security Standards

International Organizations are able to contribute to the creation of globally applicable security standards. Minimum security requirements for information technology products and services, security testing frameworks, and suggested security practises are a few examples of these standards. It is anticipated that systems and networks will be more resistant to cyberattacks with the adoption of uniform security standards.

f. Collaboration with The Private Sector

To counter cyber threats, international Organizations can work with the private sector. This entails exchanging intelligence regarding identified risks, working together to create security fixes, and encouraging businesses and private groups to adopt sound security procedures.

1.7 Separate the IT Ministry and The Cyber Security Ministry

For the following reasons, it may be crucial for cybersecurity globally to have a distinct ministry devoted to cybersecurity rather than integrating it into other ministries like IT and communications:

a. The field of cybersecurity is dynamic and complex, requiring specialised knowledge and experience. It is possible to address cybersecurity issues, create policies, and put policies into action to safeguard vital infrastructure, public systems, and citizens' digital assets with the help of a dedicated ministry.

b. Coordinated Efforts: Better coordination and collaboration between different stakeholders, such as governmental agencies, law enforcement, private sector companies, and international partners, could be facilitated by the establishment of a separate ministry for cybersecurity. In order to exchange information, respond to cyber threats, carry out investigations, and put in place reliable cybersecurity measures, coordination is essential.

c. Policy Development: Policies for cyber security must be all-encompassing, flexible, and up to date with changes in the threats that are currently in existence. A committed ministry can concentrate on creating and revising guidelines that tackle new cyber threats, encourage best practises, and guarantee adherence to global standards. This could contribute to the development of a robust national cybersecurity framework.

d. Incident Response and Recovery: Cybersecurity events can have far-reaching effects on the national security, the economy, and society. Ministries operating independently could create specialised incident response groups and create procedures to react to cybersecurity events in a timely and efficient manner. This entails carrying out investigations, liaising with pertinent agencies, and assisting with the healing process.

e. International cooperation is necessary to effectively combat cyber threats because they are transnational in nature. To support international cybersecurity efforts, committed ministries can take part in information-sharing programmes, cooperate with other nations, and participate in international forums.

f. Public Education and Awareness to Creating a resilient digital society requires a strong public education and awareness programme for cyber security. Increasing public awareness, supporting cybersecurity education initiatives, and enabling people and Organizations to adopt safe practises could be the areas of concentration for distinct ministries.

V. REFERENCE

[1] Ciuriak, D. (2020, January). Cybersecurity, National Security and Trade in The Digital era. *SSRN Electronic Journal*. doi:10.2139/ssrn.3374886

[2] Maness, R. C., & Valeriano, B. (2016, April). The Impact of Cyber Conflict on International Interactions. *Armed Forces & Society*, *42*(2), 301-323. Retrieved August 24, 2023, from https://www.jstor.org/stable/48670248

[3] Abd-Rabo, A., & Hashaikeh, S. A. (2021, August 01). The Digital Transformation Revolution. *International Journal of Humanities and Educational Research Journal* , *3*(4, August 2021), 124-128. doi:101.47832/2757-5403.4-3.11

[4] Cavelty, M. D., & Egloff, F. J. (2019). The Politics of Cybersecurity: Balancing Different Roles of The State. *St Antony's International Review*, *15*(1). Retrieved August 24, 2023, from https://www.jstor.org/stable/27027753

[5] Lewis, J. A. (2022). *Creating Accountability for Global Cyber Norms.* CSIS. Retrieved August 09, 2023, from https://www.csis.org/analysis/creating-accountability-global-cyber-norms

[6] Samantha Bradshaw & Global Commission on Internet Governance Paper Series. (2017). Combating Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity. pp. 105-120. Retrieved August 24, 2023, from http://www.jstor.org/stable/resrep05239.13

[7] Chen, S., Hao, M., Ding, D., Jiping, D., Zhang, S., Quo, Q., & Chundong, G. (2023, February 23). Exploring the Global Geography of Cybercrime and Its Driving Forces. *Humanities and Social Sciences Communications*, 1-10. doi:https://doi.org/10.1057/s41599-023-01560-x

[8] Boussi, g. O., & Gupta, H. (2020). A Proposed Framework for Controlling Cyber - Crime. *2020 8th International Conference on Reliability* (pp. 1060 - 1063). India: Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). doi:10.1109/ICRITO48877.2020.9197975

[9] Kumar, G., Pandey, S. K., Varshney, N., Kumar, A., & Kumar, M. (2023). Cybersecurity Education: Understanding the knowledge gaps based on cyber security policy, challenge, and knowledge. *2023 IEEE 12th International Conference on Communication Systems and Network Technologies (CSNT)* (pp. 735-741). Bhopal, India: IEEE. doi:10.1109/CSNT57126.2023.10134610

[10] Eriksson, J., & Giacomello, G. (2014, January 01). International Relations, Cybersecurity, and Content Analysis: A Constructivist Approach. *The Global politics*

of Science and Technology, 2, 205-219. Retrieved August 21, 2023, from https://link.springer.com/chapter/10.1007/978-3-642-55010-2_12

[11] Barnett, M. L. (2018). *The Oxford Handbook of International Security.* London, United States: Oxford Handbooks. doi:https://doi.org/10.1093/oxfordhb/9780198777854.013.7

[12] Kolodziej, E. A. (2009). *Security and International Relations.* London: Cambridge University Press. doi:https://doi.org/10.1017/CBO9780511614903.008

[13] Attatfa A., Renaud K., & Paoli S. D. (2020). Cyber Diplomacy: *A Systematic Literature Review.* International Conference on Knowledge-Based and Intellligent Information & Engineering Systems. Procedia Computer Science 176(2020) 60-69. DOI: 10.1016/j.procs.2020.08.007.

[14] Andre Barrinha & Thomas Renard (2017). *Cyber Diplomacy: The Making of an International Society in the digital age, Global Affairs,* DOI: https://doi.org/10.1080

[15] Zwarts H., Toit J. D., & solms B. V. (2022, June 08). *A Cyber - Diplomacy an Cybersecurity Awarness Framework (CDAF) for Developing Countries.* University of Johannesburg, South Africa: European Conference on Cyber Walfare and Security. DOI: 10.34190/eccws.21.1.226

[16] Andrea Calderaro & Anthony J. S. Craig (2020). Transnational governanceof cybersecurity: policy challenges and global inequalities in cyber capacity building, Third World Quarterly, 41:6, 917-938, DOI: 10.1080/01436597.2020.1729729

[17] Radanliev, P.; Mantilla Montalvo, R.; Cannady, S.; Nicolescu, R.; De Roure, D.; Nurse, J.R.; Huth, M. *Cyber Security Framework for the Internet-of-Things in Industry 4.0.* Preprints 2019, 2019030111. https://doi.org/10.20944/preprints201903.0111.v1

[18] Tan, J., Xian, T. W., Parsons, A., & Radiett, A. (2021). *ASEAN cyber threat Assessment 2021 Key cyber threat Trends Outlook From The ASEAN Cybercrime Operations Desk.* ASEAN. Singapore: INTERPOL Global Complex for Innovation . Retrieved August 25, 2023

[19] Marvin R. (2019, 12 27). " Which Countries Are Best Prepared for Cybercrime Response?". Retrieved 20 November 2023 from https://www.pcmag.com/news/which-countries-are-best-prepared-for-cybercrime-response.

[20] US Department of Defence. (2023). 2023 Cyber Strategy of the Department of Defence. Retrieved Oktober 01, 2023

[21] Relations, C. o. (2018, February 23). Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms. Retrieved August 25, 2023, from https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms

[22] Commite on Armed Services United States Senate. (2017). Foreign Cyber Threats to The United States. *U. S. Government Publishing office* (pp. 115-418). Washington: U. S. Government Publishing. Retrieved october 05, 2023, from http://www.Govinfo.gov/

[23] Painter, C. (2018, June). Diplomacy in Cyberspace The Rise of The Internet and Cyber Technologies Constitites One of The Central Foreign Policy Issues of The 21at Century. *The Foreign Service Journal*. Retrieved August 24, 2023, from https://afsa.org/diplomacy-cyberspace

[24] Maurer, T., & Nelson, A. (2021, March). The global Cyber treat. *Cyber Treat to The Financil Systm are Growing and The Global Community must Cooperate protect it*, pp. 1-4. Retrieved October 09, 2023

[25] Li, Y., & Liu, Q. (2022, October 05). A Comperensive Review Study of Cyber- Attacks and Cyber Security; Emerging trends and Recent Developments. Retrieved September 15, 2023, from https://doi.org/10.1016/j.egyr.2021.08.126

[26] Carr, M. (2016, January). Crossed Wires: International Cooperation on Cyber Security. Retrieved August 25, 2023, from https://www.researchgate.net/publication/327764208_Crossed_Wires_International_Cooperation_on_Cyber_Security.

Int. J. Advanced Networking and Applications
Volume: Issue: Pages: (2017) ISSN: 0975-0290

Niraj, is currently pursuing PhD an experienced and accomplished Cyber-Offensive Security Engineer with a proven track record of 4 years+ in the field of fin-tech, tel-co and Insurance sectors with 100+ Penetration testing (Including Web, Network, Cloud, Mobile & Database) and Red Teaming activities conducted globally. He is currently working as Cyber Security Consultant at Ernst & Young, India. He is Highly motivated, hardworking, technical minded, strong leader with excellent communication skills and a committed to teamwork, identifying and improving substandard processes, while solving critical issues. He has keen interest in Cyber Diplomacy as he believes in making the digital world a safer place stopping cyber warfare with strict global policy and controls for Global cyberspace. He believes cyber issues is to be placed in critical international agenda and he has been researching for international cyber law, rules and regulation to govern the digital space. He has been taking participate in public speaking, cyber security innovation and research projects.

Dr. Sunil Bajeja is an Associate Professor in Faculty of Computer Applications – Marwadi University (NAAC – A+) , Rajkot. He is having an experience of 26 years in the academics field. His research interest areas are Cyber Security, Blockchain Technology. He has published various research papers in reputed journals and presented in International conferences. Currently he is guiding 6 research scholars who are mainly focusing in Cyber Security domain. Academically he likes to teach various subjects like Operating Systems, Computer Architecture, Object

Oriented Concepts. Salmiati is International Relations Student from Indonesia. She is very interested in discussions, public speaking, research and learning new things. She actively participates in national and international studies related to politics, economics, conflict, women and environment issues. She has held responsibilities as head of the women's division and secretary of the Indonesian National Student Movement Organization. She also interesting about cyber security issues and her interest in cyber issues led her to research: China's Foreign Policy on Internet Censorship in the India - Galwan Valley Conflict in 2022, and this enabled her to successfully complete his undergraduate thesis. Currently, she is pursuing her master's degree at Gujarat University, India.