IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 4, April 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304350 |

What is Digital Politics and Information Security Threat? How to Navigate Through International Politics in the Information Age?

Sunayna Adlakha

Student, Uttam School for Girls, India

ABSTRACT: A diverse strategy is needed to navigate the confluence of information security risks and digital politics. In order to promote responsible governance and global cybersecurity, this paper examines the importance of regulatory frameworks, ethical issues, and international cooperation. This research attempts to provide a nuanced view of the potential and problems in the Information Age by looking at important themes and ideas from academic literature. The results highlight the necessity of open and honest rules, moral data practices, and cooperative endeavors to guarantee a stable and safe global digital ecosystem.

KEYWORDS: Digital Politics, Information Security Threats, Global Governance

I. INTRODUCTION

The convergence of information security risks and digital politics has become a central focus of interest in international relations in the ever-changing landscape of the Information Age. Digital politics, which includes using technology for political purposes, has changed how countries interact with their citizens and with one another (Attatfa et al., 2020). This paradigm shift is changing the dynamics of political communication, mobilization, and strategy, as seen by the widespread use of social media platforms, online campaigns, and data analytics.

Social media platforms have completely changed the way people talk about politics by creating a virtual forum where people may freely exchange ideas, opinions, and facts. Politicians and political organizations use these channels to communicate with voters, spread messages, and sway public opinion (Barrinha and Renard, 2020). The quick dissemination of information can also amplify false information and polarize society, thus there are drawbacks to this increased connectedness.

Political actors can now effectively communicate with voters, raise money, and advance their objectives by using online campaigns. Digital platforms allow for more focused outreach, allowing marketers to tailor their messaging according to psychographic and demographic information (Beaunoyer et al., 2020). Political techniques become more effective as a result, but privacy, manipulation, and the moral use of personal data are also raised.

Political decisions are greatly influenced by data analytics, which enables campaigns to better allocate resources, anticipate voter behaviour, and customize messaging (Attatfa et al., 2020). However, there are issues with data privacy, security lapses, and the possibility of malevolent manipulation by outside parties because to the huge amounts of data that need to be collected and analysed.

Information security concerns have become a crucial worry for governments navigating the intricacies of international relations amidst this digital transition (Cavelty and Wenger, 2020). State-sponsored cyber-attacks, hacking incidents, and the weaponization of information pose substantial hazards to the stability and security of nations. Protecting sensitive data, election procedures, and vital infrastructure becomes essential as political contacts move more and more into cyberspace.

In this sophisticated dance between digital politics and information security, governments must adeptly manage the difficulties of international relations (Beaunoyer et al., 2020). To promote a stable and safe international political environment, it is imperative to strike a balance between the advantages of technical breakthroughs and the requirement

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304350 |

for strong cybersecurity measures. Comprehending and tackling these obstacles will be crucial for countries aiming to maximize the possibilities of digital politics while defending their interests globally as the Information Age progresses.

II. RATIONALE AND OBJECTIVE

Rationale: In a world where digital connectivity rules, digital politics and information security must work together in order for countries to compete, adapt, and protect their interests abroad. Recognizing the dangers introduced by digital technologies and their transformative effect on political processes is the motivation for tackling this convergence (Barrinha and Renard, 2020). The political scene has changed due to the popularity of social media, online campaigns, and data-driven tactics. This has created chances for improved engagement and communication. National security is seriously at stake due to the connectedness of the digital world, which has also created opportunities for information manipulation and cyberattacks (Cavelty and Wenger, 2020). For countries hoping to capitalize on the advantages of digital politics while reducing the risks involved, comprehending and managing this nexus properly is essential.

Objectives:

1. Enhance Cybersecurity Infrastructure: To reduce the risks brought on by information security threats, strengthening the country's cybersecurity infrastructure is essential. Investing in cutting-edge technologies, encouraging global cooperation on cyber defence, and putting in place strong safeguards to protect sensitive systems and data from cyberattacks are all necessary to achieve this goal (Gasser et al., 2020).

2. Promote Responsible Digital Politics: To promote ethical and transparent participation in political processes, it is crucial to encourage the appropriate use of digital tools. This goal includes creating and enforcing laws pertaining to social media use, online campaigning, and data protection. The objective is to achieve a harmonious equilibrium between using digital channels for political discourse and averting information misuse.

3. Build International Cooperation on Cybersecurity: Given the global nature of cyber risks, it is imperative to promote international cooperation (Ghelani et al., 2022). To achieve this goal, cooperative frameworks, information-sharing protocols, and diplomatic campaigns are set up in order to confront cyber threats as a group. Nations can strengthen their resilience to the changing challenges of the Information Age by forming alliances and putting up a united front against cyber threats.

III. METHODOLOGY

The study will mainly use a secondary research methodology to explore the complex connection between information security risks and digital politics in the Information Age. This approach includes reviewing and synthesizing previously published works as well as scholarly articles, official documents, and pertinent case studies (Pandey and Pandey, 2021).

Suitability*:* Secondary research is particularly suitable for this study due to several reasons:

Data Availability: There is an abundance of literature regarding information security threats and digital politics. Academic papers, government publications, and reports from international organizations offer a thorough basis for comprehending the subtleties and intricacies of these related subjects.

Time and Cost Efficiency: It saves money and time to conduct secondary research. Secondary research makes it possible to quickly assess the body of knowledge without having to gather a lot of data, which is advantageous in the fast-paced Information Age and when it comes to addressing new difficulties (Pandey and Pandey, 2021).

Broad Perspective: The examination of many viewpoints and insights from various sources is made possible by secondary research. This inclusivity is essential for gaining a thorough understanding of the subject from a variety of political, cultural, and geographic perspectives when analysing the global ramifications of digital politics and information security (Mishra and Alok, 2022).

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304350 |

Historical Context: Over time, risks to information security and digital politics have changed. By using secondary sources, one may monitor the evolution of these occurrences, identify significant turning points that have shaped the contemporary environment, and incorporate historical context.

This research endeavours to provide an extensive examination of past developments, present difficulties, and prospective patterns concerning the convergence of digital politics and information security risks, through the utilization of secondary sources (Nayak and Singh, 2021). A more nuanced understanding of how countries can manage the risks and opportunities associated with navigating the complexities of international politics in the Information Age will be possible due to the thoroughness of secondary research, which will make it possible to identify patterns, correlations, and gaps in current knowledge.

IV. LITERATURE REVIEW

Theme 1: Evolution of Digital Politics

As stated by Horowitz (2020), the way that political communication and engagement are shaped is being fundamentally altered by the development of digital politics. The effects of social media sites like Facebook and Twitter on political environments have been well-studied by academics. Political actors are now able to interact directly with voters and gather support on a never-before-seen scale due to these platforms, which have proven essential in facilitating real-time communication, political action, and the quick distribution of information.

Social media's instantaneous nature enables politicians to respond to popular moods, handle issues quickly, and engage with a wide range of people. Political processes are now more inclusive and participative as a result of this dynamic interaction, which has altered the conventional top-down communication paradigm.

But there are difficulties with this evolution. As mentioned by Kassen (2022), the analysis of disinformation in the digital era brings attention to a more sinister side of the change. A serious challenge to the integrity of democratic processes is the quick dissemination of inaccurate or misleading information on social media platforms. Election results can be affected by disinformation, which can also polarize society and shape public opinion. Social media is used by nearly 3.6 billion individuals worldwide as of 2022, demonstrating its widespread impact. Studies reveal that on social media platforms, false information spreads six times more quickly than true information, highlighting the difficulties caused by the fast spread of false information.

In addition, social polarization has become another obstacle in the political landscape of digital media. Ideological gaps already present widen due in part to the echo chambers that have developed on social media platforms, where users are mostly exposed to viewpoints that align with their own (Leese et al., 2022). This division can obstruct productive political dialogue and jeopardize efforts to reach consensus on crucial topics.

It is vital for nations aiming to leverage the advantages of digital politics while minimizing its drawbacks to comprehend the way it has developed. In order to counteract misinformation, increase transparency, and advance a more inclusive and knowledgeable democratic process, policymakers must address the complicated issues of social media's influence on political communication (Liebetrau and Christensen, 2021). As societies navigate this changing terrain, they can work to optimize its advantages while confronting the difficulties presented by the digital era of politics.

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304350 |

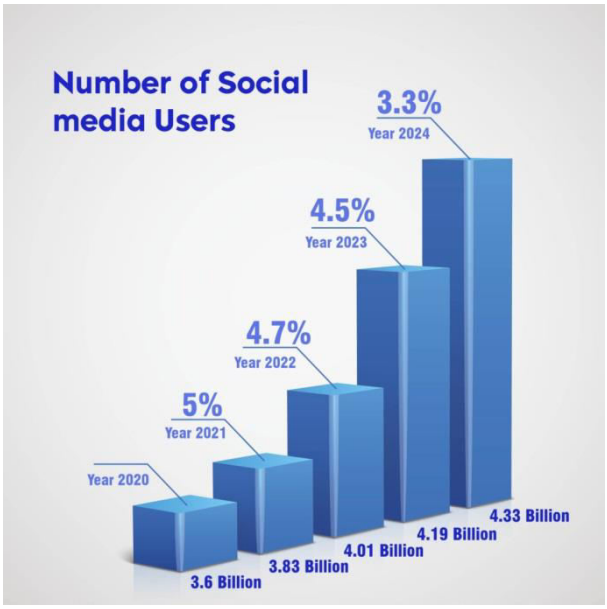

Figure: Number of social media users
Source: (Fleck, 2022)

Theme 2: Cybersecurity Challenges in the Information Age

As suggested by Liu (2021), national security is seriously threatened by the increase in cybersecurity difficulties brought about by the Information Age. Scholarly publications have examined the dynamic character of cyberthreats, encompassing state-sponsored assaults, cybercrime occurrences, and the information being weaponized. Globally interconnected digital systems increase danger and necessitate sophisticated cybersecurity solutions. Events like the Stuxnet attack and the suspected Russian meddling in the 2016 US presidential election highlight the necessity for countries to strengthen their cybersecurity defenses in order to safeguard vital infrastructure and democratic procedures.

Reading the works of different scholars offers important insights into the complexity of cyber threats. A particularly difficult problem is state-sponsored attacks, which are frequently planned by nation-states looking to further their own agendas (Ly, 2020). These assaults may target private information, vital infrastructure, or even democratic processes. The interdependence of worldwide digital networks increases the risks posed by cyberattacks. Because the internet has no borders and bad actors can operate across borders, countries must implement cutting-edge cybersecurity safeguards. The dynamic and sophisticated methods used by cyber adversaries render traditional approaches to security inadequate.

The Stuxnet event and the suspected Russian meddling in the 2016 U.S. elections serve as prime examples of how urgently countries must strengthen their cybersecurity infrastructure. While the purported meddling in political processes brought attention to the susceptibility of voting systems to outside manipulation, the Stuxnet catastrophe showed how malware might enter and impair vital industrial systems.

As commented by Miller and Vaccari (2020), Countries must strengthen their cybersecurity capabilities in response to these threats in order to protect vital systems and democratic procedures. In order to handle the transnational dimension of cyber threats, this calls for both technological breakthroughs and international cooperation. In the Information Age, when the digital sphere has turned into a major theater for geopolitical conflicts and clandestine operations, fortifying cybersecurity measures is essential to preserving the stability and security of countries.

Cybercrime is expected to cost the world economy more than $1 trillion a year by 2022, illustrating the financial implications of cybersecurity issues. With over 50 countries having developed offensive cyber capabilities, it is

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304350 |

noteworthy that state-sponsored cyber-attacks have increased (Polizzi, 2020). Cyber threats can affect essential infrastructure, as demonstrated by the 2010 discovery of the Stuxnet event, a sophisticated cyber weapon that targeted Iran's nuclear facilities. Studies also show that there were more than 8.4 billion malware attacks in 2021, highlighting the scope and regularity of cyberthreats. In order to combat the constantly changing panorama of cyber threats, these numbers emphasize how vital it is for countries to strengthen their cybersecurity infrastructure and participate in international cooperation.

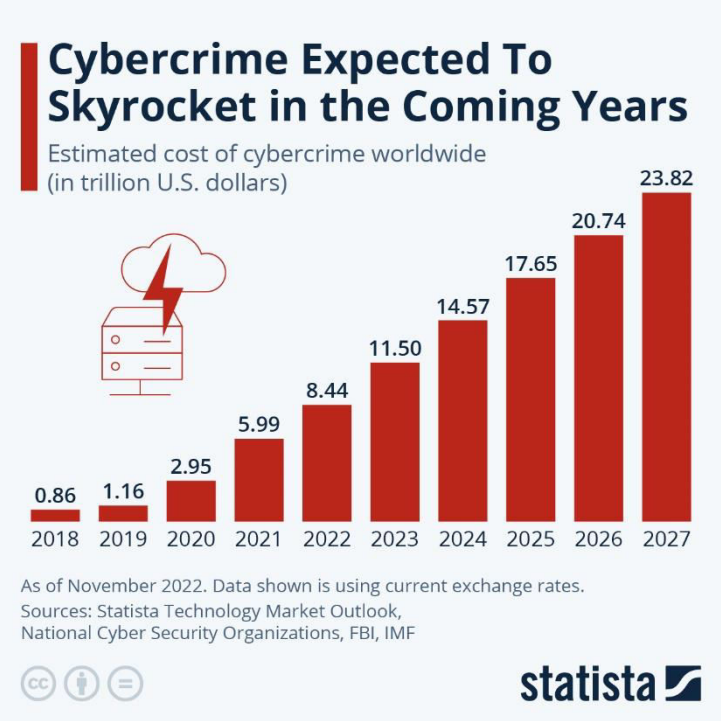

Figure: Cybercrime Expected to Skyrocket in Coming Years
Source: (Fleck, 2022)

Theme 3: Data Privacy and Ethical Concerns

As mentioned by Robinson et al. (2020), Data privacy and ethical considerations have become major concerns as a result of the introduction of data-driven methods into the field of digital politics. Early studies on this topic demonstrate the wide-ranging effects of intensive data collecting and analysis on personal privacy.
Political campaigns in the era of digital politics are depending more and more on data analytics to understand voter behaviour and customize messages. This strategy could lead to more focused and successful political campaigns, but it also raises moral concerns about how personal data should be used.

The broad notion of "big data" is essential to comprehending this dynamic since it allows for the precise customization of political messages, the identification of patterns, and the prediction of behavior based on the massive volumes of data generated by individuals in the digital sector. The fundamental right to privacy is directly threatened by this data-centric approach, which calls into question the morality of using personal information for political purposes.

Research on the topic of surveillance capitalism highlights larger moral issues related to the selling of personal information (Tsourapas, 2021). Critical problems of permission, autonomy, and manipulation are raised by the widespread profiling and targeting of people for political reasons in the context of digital politics.

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304350 |

Striking a careful balance between using data to further political agendas and protecting people's privacy requires effectively resolving these concerns. To ensure that people are aware of how their data is being utilized, data gathering procedures must be transparent in order to establish an ethical foundation for data-driven politics. People's right to privacy and autonomy must be respected, and this requires getting their informed consent. Strong cybersecurity measures are also necessary to prevent misuse and unauthorized access to sensitive personal data.

The moral questions raised by data-driven tactics in digital politics will always be relevant to discussion as technology develops (Roberts et al., 2020). Policymakers, technologists, and society at large must work together to find a way to cohabit peacefully between successful political campaigns and individual privacy protection. Maintaining the democratic norms that support political participation in the constantly changing digital era requires the responsible and ethical use of personal data.

Data breaches worldwide revealed more than 1.5 billion records in 2021, underscoring the increased hazards to private data. Research reveals that 70% of customers express concern about the usage of personal data, highlighting the pervasiveness of data privacy concerns. Strong cybersecurity measures are crucial in digital politics since the average cost of a data breach is more than $4 million (Whyte and Mazanec, 2023). The financial consequences of poor data protection are also significant.

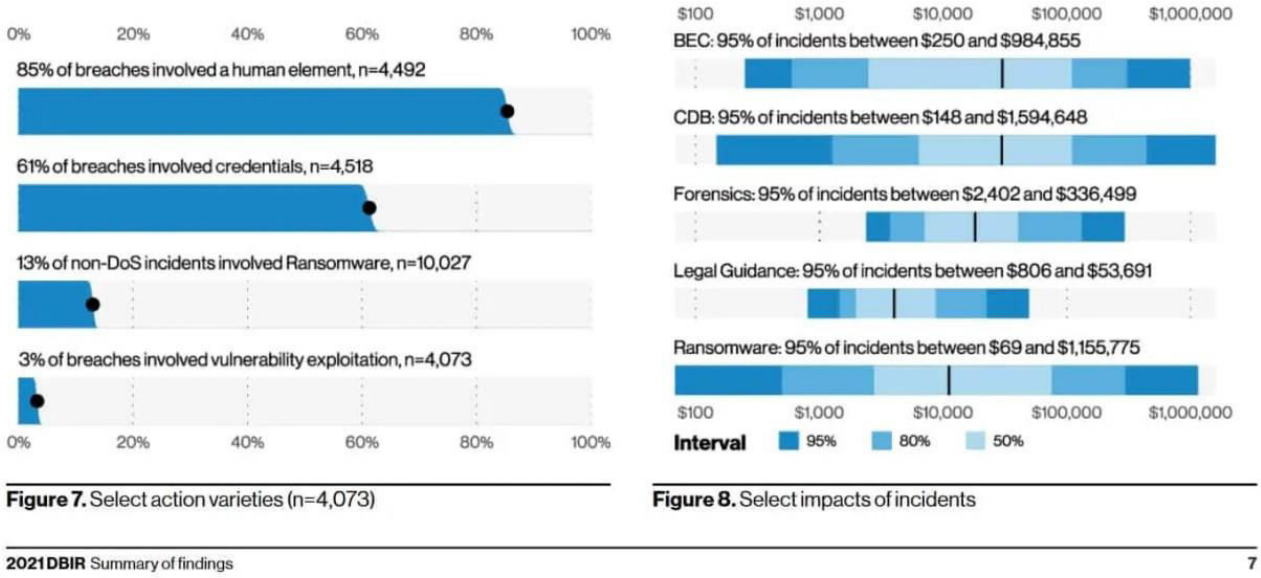

Figure: Data breach incidents impacted in large and small enterprises respectively
Source: (Pawar, 2022)

Theme 4: Regulatory Frameworks and Responsible Governance

Scholars have highlighted the need for regulatory frameworks in digital politics to promote responsible governance, given the possibility of digital tools being misused in the lack of comprehensive rules (Fleck, 2022). The dynamic field of digital politics, characterized by the swift growth of virtual spaces and growing dependence on digital instruments, demands a flexible and all-encompassing regulatory strategy.

In digital politics, the risks of manipulation and exploitation become evident in the lack of defined standards. Examples of the difficulties caused by the existing regulatory gaps are evident in the cases of data breaches and electoral meddling. The need for regulatory action is underlined even more, especially in regards to data privacy, social media usage, and online campaigning.

Explicit norms are necessary to maintain ethical behaviors and stop the spread of misinformation in online campaigning, a crucial aspect of contemporary political communication. A number of problems that compromise the integrity of democratic processes can arise from a lack of strong laws in this area. Another crucial issue that needs

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304350 |

regulatory attention is the use of social media in politics (Pawar, 2022). Significant risks to responsible governance come from the possibility of manipulation and the dissemination of false information on these platforms.

In the digital age, data protection is becoming increasingly important. In order to avoid privacy violations and protect the democratic ideals that guide political processes, it is essential to handle personal information responsibly. In order to prevent the misuse of digital platforms for political communication, countries must have a legislative framework that takes these issues into account.

To reduce the risks, present in the existing regulatory environment, clear standards for responsible governance in digital politics are needed. Regulatory frameworks should include essential components for protecting personal data, combating misinformation campaigns, and guaranteeing transparency (Attatfa et al., 2020). Nations may cultivate an atmosphere that maximizes the advantages of digital politics while mitigating the potential risks resulting from the improper use of digital tools by instituting and implementing all-encompassing rules.

Just 32% of nations had comprehensive data protection legislation in place as of 2022, underscoring the legal gaps that exist globally for the protection of personal data. 90% of users, according to studies, think that internet platforms should be subject to more regulation, highlighting the public's desire for better governance (Barrinha and Renard, 2020). The need for clear limits on online campaigning is increasing, as political ad spending on social media has topped $1.8 billion in the 2020 U.S. elections. These numbers highlight the need for strong regulatory frameworks in order to guarantee responsible governance and solve issues in digital politics.

Theme 5: International Cooperation and Diplomacy in Cyberspace

Given that information security threats pose issues that transcend state boundaries, the topic of international cooperation and diplomacy in cyberspace is crucial. Academics stress how crucial it is for groups to work together in order to confront cyberthreats. Creating a unified front against the complexity of cyber threats on a global scale requires forging alliances, exchanging information, and launching diplomatic initiatives.

As mentioned by Beaunoyer et al. (2020), segregated approaches to countering information security threats are inadequate in the globally interconnected world of cyberspace, where a country's actions can have far-reaching effects. Understanding that one country's security is inextricably tied to other countries' security calls for cooperation.

This requirement of shared accountability highlights even more how nations must work together to overcome their respective interests and address common cyberthreats. Collective defense becomes essential in a world where cyber threats are always changing and adapting. This entails not just exchanging information but also launching diplomatic campaigns to encourage candid dialogue and cooperation on cybersecurity-related issues.

For international collaboration in cyberspace to be effective, alliance building is essential. To bolster their combined cyber defences, nations can combine their resources, knowledge, and intelligence (Cavelty and Wenger, 2020). In addition to working with governments, this cooperative strategy also involves private companies, international organizations, and other players in the digital ecosystem.

Information sharing about cyberthreats improves situational awareness and makes it possible to react to new problems more quickly. A foundation for productive discussion and the creation of common standards and agreements is fostered by the establishment of diplomatic initiatives. In cyberspace, where attribution and response processes are intricate, these diplomatic initiatives play a critical role in averting and lessening disputes.

One of the most important factors in promoting a safe and stable global digital environment is the creation of international norms and agreements (Gasser et al., 2020). This entails establishing guidelines and standards for responsible state conduct in cyberspace in order to lessen the possibility of misinterpretations and incorrect calculations that can result in cyberwarfare.

A thorough international agreement on cybersecurity is absent from more than 60% of nations as of 2022, underscoring the continued difficulties in creating universal standards. Research projects that by 2025, the cost of cybercrime will be $10.5 trillion annually, highlighting the financial consequences of inadequate global cooperation

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304350 |

(Ghelani et al., 2022). In light of the growing complexity of cyber threats, the establishment of common standards and agreements is essential to promoting a safe worldwide digital environment.

V. CONCLUSION

To conclude, the dynamic terrain of digital politics and information security risks need a comprehensive strategy. The foundational elements of responsible governance and global cybersecurity are regulatory frameworks, ethical considerations, and international cooperation. To maintain a secure digital environment, nations must address these issues with a dedication to openness, moral data practices, and cooperative efforts. Together, nations can solve these complex concerns and reap the benefits of digital politics while mitigating potential hazards, therefore promoting a stable and resilient global information environment.

REFERENCES

1 Attatfa, A., Renaud, K. and De Paoli, S., 2020. Cyber diplomacy: A systematic literature review. Procedia computer science, 176, pp.60-69.
2 Barrinha, A. and Renard, T., 2020. Power and diplomacy in the post-liberal cyberspace. International Affairs, 96(3), pp.749-766.
3 Beaunoyer, E., Dupéré, S. and Guitton, M.J., 2020. COVID-19 and digital inequalities: Reciprocal impacts and mitigation strategies. Computers in human behavior, 111, p.106424.
4 Dunn Cavelty, M. and Wenger, A., 2020. Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Contemporary Security Policy, 41(1), pp.5-32.
5 Fleck, A. (2022). Infographic: Cybercrime Expected To Skyrocket in Coming Years. [online] Statista Infographics. Available at: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/.
6 Gasser, U., Ienca, M., Scheibner, J., Sleigh, J. and Vayena, E., 2020. Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid. The Lancet Digital Health, 2(8), pp.e425-e434.
7 Ghelani, D., Hua, T.K. and Koduru, S.K.R., 2022. Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. Authorea Preprints.
8 Horowitz, M.C., 2020. Do emerging military technologies matter for international politics? Annual Review of Political Science, 23(1), pp.385-400.
9 Kassen, M., 2022. Blockchain and e-government innovation: Automation of public information processes. Information Systems, 103, p.101862.
10 Leese, M., Noori, S. and Scheel, S., 2022. Data matters: The politics and practices of digital border and migration management. Geopolitics, 27(1), pp.5-25.
11 Liebetrau, T. and Christensen, K.K., 2021. The ontological politics of cyber security: Emerging agencies, actors, sites, and spaces. European journal of international security, 6(1), pp.25-43.
12 Liu, L., 2021. The rise of data politics: digital China and the world. Studies in Comparative International Development, 56, pp.45-67.
13 Ly, B., 2020. Challenge and perspective for digital Silk road. Cogent Business & Management, 7(1), p.1804180.
14 Miller, M.L. and Vaccari, C., 2020. Digital threats to democracy: Comparative lessons and possible remedies. The International Journal of Press/Politics, 25(3), pp.333-356.
15 Mishra, S.B. and Alok, S., 2022. Handbook of research methodology.
16 Nayak, J.K. and Singh, P., 2021. Fundamentals of research methodology problems and prospects. SSDN Publishers & Distributors.
17 Pandey, P. and Pandey, M.M., 2021. Research methodology tools and techniques. Bridge Center.
18 Pawar, P. (2022). 46+ Data Breach Statistics 2022 Trends, Facts and How To Prevent? [online] Enterprise Apps Today. Available at: https://www.enterpriseappstoday.com/stats/data-breach-statistics.html.
19 Polizzi, G., 2020. Information literacy in the digital age: Why critical digital literacy matters for democracy. Informed Societies: Why information literacy matters for citizenship, participation and democracy, pp.1-23.
20 Robinson, L., Schulz, J., Dunn, H.S., Casilli, A.A., Tubaro, P., Carvath, R., Chen, W., Wiest, J.B., Dodel, M., Stern, M.J. and Ball, C., 2020. Digital inequalities 3.0: Emergent inequalities in the information age. First Monday, 25(7).
21 Tsourapas, G., 2021. Global autocracies: Strategies of transnational repression, legitimation, and co-optation in world politics. International Studies Review, 23(3), pp.616-644.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304350 |

22 Walker-Roberts, S., Hammoudeh, M., Aldabbas, O., Aydin, M. and Dehghantanha, A., 2020. Threats on the horizon: Understanding security threats in the era of cyber-physical systems. The Journal of Supercomputing, 76, pp.2643-2664.

23 Whyte, C. and Mazanec, B., 2023. Understanding cyber-warfare: Politics, policy and strategy. Routledge.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details