Journal of Contemporary Politics

RESEARCH ARTICLE

Cyber Security in Cyberspace: Changing Trends in the Security Aspects of Cyberspace

C Bhagyasree Menon[1,*]

[1] *Research Scholar, Department of Political Science, University of Kerala, Kerala, India*

ARTICLE INFO

Article history:
Received 24.12.2024
Accepted 28.12..2024
Published 31.12.2024

[*] *Corresponding author.*
C Bhagyasree Menon
sreemenonc9@gmail.com

https://doi.org/10.53989/jcp.v3i4.58

ABSTRACT

Cyberspace is increasingly vital in this new era of information and communication technology. With the advancement of the internet and related technologies, everything has been bought at a fingertip. In such a way, cyberspace has made progress. Even though there are so many factors that are making cyberspace the most valued innovation of the time, there are also so many issues related to this. The increasing number of cyber threats and attacks is the most important among them. Increasing cyber security concerns can be considered as the most important reason for these threats and issues. Related to the development of cyberspace, there are so many rules and regulations to cope with the threats, attacks, and other issues; all these laws seem to be insufficient to control the fundamental problem of cyber security, which is the root cause of all of the other concerns. These issues have been getting national or international importance when these aspects become a loophole for different kinds of attacks between countries by affecting the overall international peace. In such a way, in this new era, cyber security can influence global peace. In earlier days, the security was outside the cyber platform, which has been shifted to the cyber platform, creating adverse effects in society. In this aspect, the paper analyzes the changing dynamics of security in this new era and its impact. The paper primarily seeks help from secondary sources like articles, books, and journals. It tries to find solutions for the existing issues and suggests possible measures to tackle this concern.

Keywords: Cyberspace; Cybersecurity; Cyber Threat; Cyber-attacks; Cyber Laws

INTRODUCTION

The 21st-century digital era has revolutionized society, transforming it from offline to online platforms. Cyberspace, a networked space, facilitates communication without revealing one's own identity and makes communication easier, but it also poses a threat to international peace. The study aims to identify major concerns and their evolution and propose solutions to address these issues in this new technological era.

DEFINING CYBER SECURITY

Cybersecurity is an evolving concept that encompasses all cyber activities and internet-related activities. It aims to address complex security challenges and resolve various organizational, economic, and social issues of human beings in the online platform. Its meaning varies depending on the situation and context.[1] Fredrick Chang, former US National Security Agency director, views cybersecurity as a multi-disciplinary field that requires a multidisciplinary approach. It involves adversarial engagement, requiring insights from fields like computer science, electrical engineering, and mathematics. At its core, cybersecurity involves adversarial engagement, where humans defend machines against attacks from other humans using those same machines.[2] Various thinkers have explained the concept of cyber security in different ways. Certain definitions include, "Cybersecurity consists largely of defensive methods used to detect and thwart would-be intruders."[3]

"Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption."[4]

The practice of maintaining the information society of a nation, ensuring and safeguarding its information, assets,

and critical infrastructure in Cyberspace.[5]

"The condition of being safeguarded against criminal or unauthorized access to electronic data, along with the actions taken to ensure this protection."[6]

These definitions are just a few among the piles of definitions that are used to explain the concept of cyber security. The concept of cyber security can be used in a complete technical aspect, or it can be used in relation to social, political, and economic dimensions. In such a way this term is multidisciplinary in its nature.[7]

In a multidisciplinary aspect, the idea of cybersecurity can be explained as follows, Cybersecurity involves organizing and coordinating resources, processes, and structures to protect cyberspace and systems enabled by cyberspace from events that misalign legal and actual property rights.[8]

Cybersecurity is a multidisciplinary concept that focuses on threats, deterrence, and mitigation. It is used to protect systems and activities from hackers and malware attacks. The concept varies depending on the situation and can be used by individuals and government agencies to ensure the protection of property, lives, and privacy in a networked society.[9]

EXPLAINING CYBERSPACE

The concept of cybersecurity is closely linked to the concept of cyberspace, which has been widely circulated in recent years. This has led to the development of various terms such as cyber society, cyber-attack, cyber threat, cyber terrorism, cyber security, and cybercrime, all of which are related to cyberspace.[10] The term "cyber" was first introduced in 1948 by Norbert Weiner's work, 'Control and Communication in the Animal and Machine'. It was influenced by cybernetics, which suggests that human and machine interaction can create an alternative environment for interaction[11]. William Gibson's 1982 work, Burning Chrome, further developed the concept of cyberspace.[12] According to the US Department of Defence, Cyberspace is a global domain within the information environment, consisting of interconnected networks of information technology infrastructures like the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[13]

"Cyberspacetime encompasses all events that involve interactions among humans and computers, among humans communicating through computers, and among computers interacting with each other".[14] There are a vast number of explanations for the concept of cyberspace. It can be considered completely as a technical concept or can also be considered as an essential platform for individuals in order to communicate with others. The nature of cyberspace is really dynamic; it changes according to the conditions and over time. While analysing these features of cyberspace, it can be explained as "cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems."[10]. The US Department of Defence elaborates that cyberspace has a fixed procedure, its procedures are standard in nature, and it has specific stages in order to perform various tasks. While explaining the concept of cyberspace, an important idea was given by National Strategy secure Cyberspace in the year 2003 and it says that cyberspace is the "Nervous system is the control system of our country, composed of hundreds of thousands of interconnected computers, servers, routers, switches, and Fiber optic cables that enable our critical infrastructures to function effectively."[15]

CYBERSPACE AND CYBERSECURITY IN THE INTERNATIONAL CONTEXT: RECENT TRENDS

Cyberspace has expanded, and social media platforms have opened up new opportunities for individuals to share their lives. Social media has revolutionized communication by enabling people to connect with people with similar interests and create groups within a short time. With data from Digital 2020 reports showing a 3.8 billion user base in 2020 by January 2025, there were 5.24 billion social media users, which is 63.9% of the global population, according to Kepios data[16]. This growth reflects the increased engagement on these platforms (Figure 1).

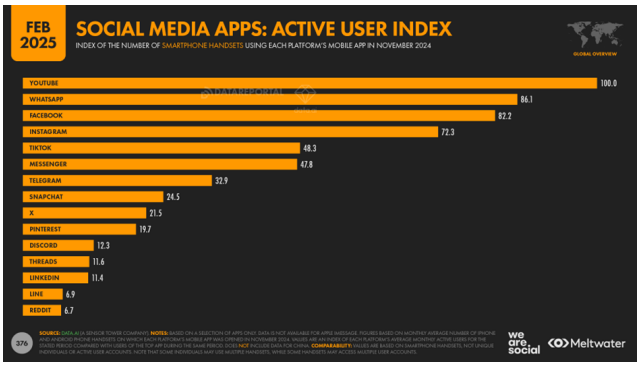

Fig. 1: Global Social Media Statistics- DataReportal - Global Digital Insights. [n.d.]. DataReportal – Global Digital Insights. https://datareportal.com/social-media-users

Not only social media platforms, e-banking, e-services, and e-governance have made activities easier worldwide, leading to increased engagement with online platforms. Global Internet Usage Statistics show that the number of internet users has increased from 5.35 billion in 2024 to 5.52 billion in 2025, with 97 million people starting to use the internet for the first time in the past 12 months.[17]

Cyberspace issues have increased due to increased engagement, leading to cyber threats, attacks, theft, espionage, and wars. These cybercrimes are primarily due to a lack of cybersecurity, which is essential for creating a safe environment. Initially, cybersecurity focused on machine-based threats, deterrence, mitigation, and recovery. However, human interference in online platforms, particularly

social media, has made it more human-centric. Humans contribute to numerous cyber dangers, such as harmful software development, social engineering, and a lack of defensive practices like antivirus or password encryption[18].

The information overload in cyber platforms has created an increase in cybercrimes because cybercrimes mainly happen due to the misuse of data that is already provided by individuals during their online activities.

According to data on cybercrimes, by the end of 2022, at least 422 million people had been affected by various forms of cybercrimes, with over 8 lakh complaints being filed during that same year. 33 billion accounts were compromised in 2023, resulting in losses of almost $8 trillion (Figure 2).[19]

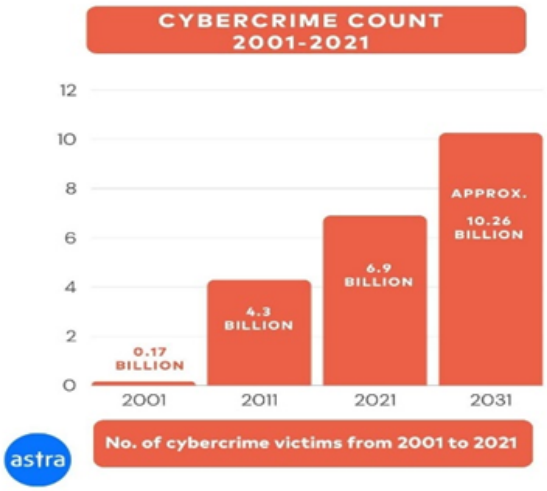

Fig. 2: [19], Palatty, N. J. (2025, February 6). 90+ Cyber Crime Statistics 2025: Cost, Industries & Trends. Astra Security . https: //www.getastra.com/blog/security-audit/cyber-crime-statistics/

Cybercriminals exploit data for various attacks, including identity theft, phishing, hacking, assaults, Denial of Service attacks, ransomware attacks, and malware attacks. Information overload increases cyber security threats. Identity theft involves stealing personal information and claiming identity on social media, while phishing involves sending trustworthy emails and collecting sensitive data, leading to financial fraud. Malware attacks steal data or take over devices, while social engineering attacks convince victims to click on harmful links or provide personal information.[20] The rise in social media attacks and threats, coupled with increased information accessibility, threatens individuals' basic rights. When there is easiness in the accessibility of information, it will lead to an increase in the number of cyber criminals. While cyberbullying and harassment embarrass individuals through messages, photos, and videos, it is another threat faced by individuals on online platforms. Cybercriminals target accounts to use private information and create hacking attacks. The rise of cybersecurity issues on social media platforms is linked to advancements in technology.[20]

CYBER ATTACKS AND THREATS; DATA ANALYSIS

An analysis of the number of threats and their constant upgradation is necessary to know more about the number of cyber security threats, types of threats and the reasons for their increase. The comparison of such data is necessary in order to understand the range of its escalation and to provide necessary ways to reduce the increasing threats to ensure the complete resolution of all the issues related to cyberspace. Cyber threats and the risks associated with them deeply affect the maintenance of peace on digital platforms. The statistics about cyber-attacks are alarming and have been rising exponentially each year. According to the Global Risk Report 2019 by the World Economic Forum, "data fraud or theft" and "cyber-attacks" ranked 4th and 5th, respectively, among the top ten global risks in the online platform in terms of the highest possibility of happening over decade. Furthermore, the severity of their impact placed them in the top ten global risks. As such, cyber risks are still very important and fall within the quadrant marked by high probability and high impact in the Global Risks Landscape. The report by the EU Agency for Cyber Security said that ransomware was responsible for about 39% of data breaches globally. The same malware was responsible for around 70% of all cybercrime incidents involving education institutions, and healthcare organizations saw 85% of all their malware infections were from ransomware.[20]

As the data were stolen, by considering the importance of the data and recovering stolen data, many countries opted to pay ransom. Among the total number of organizations that lost the data 48% chose to pay the ransom amount and the remaining ones lost their data. In such a way, people are losing their sensitive data from the online platform to those people who stole their data to gain money.[20] Recent trends indicate an increase in cyberattacks utilizing tactics such as crypto-jacking and encrypted communication.

The primary motivation behind many cyber-attacks is the gathering of intelligence. Attackers collect data from internet users with the intention of leveraging this information in subsequent attacks for financial gain.[20] In such a way it can be explained that profit is the major motive of almost all kinds of cyber security threats. When examining cybercrimes, statistics show that the number of malware attacks in 2020 grew by 358% over 2019. It is highlighted that phishing is the most frequent cyber threat that both individuals and businesses must deal with. More than 3 lakh internet users fell victim to phishing attempts in 2021, meaning that half of those who experienced data breaches did so. By the first half of 2022, there were over 236.1 million ransomware assaults worldwide, according to statistics. From a worldwide perspective, compared to 2020

data, the number of cyberattacks grew by 125% in 2021. An average of $4.88 million will be lost due to data breaches by 2024.[21]

Using examples from other nations, it is anticipated that approximately 736 million pounds were lost in the UK as a result of cybercrime in 2021. According to reports, over 24% of UK charities experience cyberattacks between 2022 and 2023. The UK is ranked second on the Global Cyber Security Index, eleventh on the E-development Index, and tenth on the Network Readiness Index. The research also indicates that phishing was the most prevalent danger in 2022.[21]

According to US cybercrime statistics, citizens are expected to have lost more than 6.9 billion USD as a result of cybercrimes by 2021. Only half of US firms have cyber insurance to deal with cyber threats, according to the report. The potential damages resulting from individual cybercrimes in 2022 were over $10 billion, which was a substantial amount more than the 6.9 billion lost in 2021[21]. Canada also has experienced rise in the number of cybercrimes year after year. In the 2017, the crimes reported were 27,829 but it has increased to 70,288 by 2021. A study on 2020 revealed that 48% of Canadians are extremely worried about their data being used in identity theft. In 2023, the largest data breach expense in the US was $5.09 million. 95% of enterprises were impacted by cybersecurity incidents, per IBM's 2023 study[19]. The number of financial fraud cases in Pakistan surged by 83% between 2018 and 2021, with Facebook accounting for 23% of the complaints received in 2021. India is also affected by the rise in cybercrimes; in the first two months of 2022 alone, over 2 lakh cybercrimes were reported in India, surpassing the total number of cybercrimes in 2018.[21]

From Asian to African nations, Nigeria was ranked 16th on the list of nations most affected by cybercrimes in 2020. Zambia, on the other hand, was ranked 58th out of 161 countries in the National Cyber Security Index and 73rd out of 194 countries in the Global Cyber Security Index that same year.

While listing out the percentage of cyber-attacks against the various organisations, Asian suffered most attacks worldwide in 2021. Asia with 26% of attacks, Europe 24%, North America 23%, Middle Est and Africa 14%, and Latin America 13%. In such a way, all nations have been facing higher amounts of cybercrimes and cyber security issues and its range has been increasing year by year.

Every year the National Cyber Security Index has been calculated and as of December 2023, 5 countries have scored highest in NCSI and it includes, Poland, Estonia, Ukraine, Latvia, and the United Kingdom.[21]

CYBER HYGIENE

Cybersecurity issues are increasing, necessitating increased caution in online platforms. Cyber hygiene is crucial to protect data from attackers and prevent cyberattacks. Digital cleanliness, defined by the Council on Cyber Security and the Center for Internet Security, involves protecting and maintaining IoT systems and devices[22,23]. The healthcare and finance sectors are facing major cyber threats, with the Australian Securities and Investments Commission recommending technological strengthening to reduce risks. With a study named cyber resilience and health check[24]. Ransomware and malware attacks, particularly crypto-ransomware, affect individual data security[25]. Cyber-attacks occur through various stages, starting with Recon, identifying weak links in the user's system, and progressing to intrusion, lateral movement, and privilege escalation[26].

Lack of cyber hygiene leads to a cyber mess, a digital hazard factor. This mess can be technical or non-technical, resulting from insufficient security monitoring, authentication, incident response plans, data control, risk assessment, and risk factor management. Non-technical aspects include organizational policies, employee training, security awareness, and social engineering awareness.[26]

Cybercriminals often focus on ransomware attacks for profit maximization, entering systems through weak ports and sometimes demanding ransoms for access to infected data. Malware can activate through malicious email links or attachments and can enter systems through compromised websites or specific pages. It encrypts user files, makes them inactive, and makes them inaccessible. It can also infect servers connected to the infected system and lead to network lockdowns.

Cyber-attacks have been targeting individuals and organizations worldwide, with WannaCry being a major example. The ransomware attacks targeted Microsoft Windows, affecting users of Windows 8, 2003, and XP. Unupdated Windows software was the major reason for this. Hospitals, banking institutions, and corporations were affected, and MRI scanners, CT scanners, computers, and databases were compromised. Cybercriminals often target billionaires, large industries, defence departments, corporations, and government agencies to maximize profits.[26] In this issue that affected these sectors across the globe about 150 countries and about 200,000 to 300,000 of their computer systems were also affected because of the cybersecurity threats.

Cyber espionage has been rampant, with Russian hackers' spear phishing Kazakh diplomatic entities and embedding malicious code in diplomatic documents. Russia's cyber-attacks on Ukraine increased to 70% in 2024, affecting infrastructure. In March 2024, American Express warned its customers that an unauthorized party accessed sensitive customer information as a result of a merchant processor breach. A point-of-sale attack had successfully been executed to cause the breach. American Express emphasized the fact that no breach occurred with its internal systems, though the breach at the merchant processor leaked the sensitive data of American Express customers: names, current and former account numbers, and card expiration

dates[27]. Indian government organizations experienced a 138% increase in cyberattacks between 2019-2023. China's National Cyber Security Agency reported a US intelligence agency conducting cyberattacks on Chinese tech firms. The UK's National Cyber Security Centre found a threefold increase in cyberattacks compared to 2023, with China, North Korea, Iran, and Russia listed as real threats. Iranian hackers are targeting defense, aerospace, and aviation industries in Israel, India, Turkey, Albania, and India.[28] In September 2023, a ransomware attack wiped out four months of data of the Sri Lankan government and the country's cloud system did not have backup services. During the same time, Indian cybersecurity firm uncovered plans from Pakistani and Indonesian hacking groups to disrupt the G20 summit. In August 2023 Unnamed hackers took X formerly known as Twitter, offline in several countries and demanded that owner Elon Musk open Starlink in Sudan. Attackers flooded the server with traffic to disable access for over 20,000 individuals in the U.S., UK, and other countries. In September 2023, Microsoft AI researchers accidentally exposed 38 terabytes of private data while publishing open-source training data on GitHub. The data contained sensitive corporate information from two employees' workstations, including secrets, private keys, passwords, and over 30,000 internal Microsoft Teams messages. The researchers misconfigured Azure's SAS tokens, granting access to the entire storage account rather than specific files.[27] In May 2023, two ex-employees stole and released Tesla's confidential data to German news outlet Handel blatt. The company's IT security and data protection policies were breached, allowing malicious actors to unlawfully obtain and disclose 23,000 internal documents, resulting in the exposure of 75,735 current and past employees. The company could lose up to $3.3 billion if their data protection is poor. In June 2022, Pegasus Airlines discovered an error in configuring a database, exposing 6.5 terabytes of valuable data. The error led to 23 million files with flight charts, navigation materials, and crew personnel information being accessible to the public.[27] In January 2022, the International Committee of the Red Cross [ICRC] experienced a significant data breach and cyber-attack, resulting in over 515,000 people being separated from their families.

In order to reduce these developing concerns digital hygiene can be considered as important remedy. It is because, Digital hygiene aims to disrupt the digital attack chain, preventing potential attacks. Basic security training programs alone are insufficient. Maintaining data security requires translating technical digital information into actionable insights. Digital cleanliness involves mitigating risks in applications, patching vulnerable systems, and strengthening server and network security. Individuals and organizations must adopt specific policies to address this issue and learn different practices to recognize weak connections in their systems.[29]

LEGAL FRAMEWORK IN THE FIELD OF CYBERSPACE

The evolution of cybersecurity laws has been influenced by technological advancements and escalating cyber threats. The Computer Fraud and Abuse Act (CFAA) was introduced in 1986 by the United States, and subsequent laws were developed in the late 1990s and early 2000s[30]. The Budapest Convention, signed in 2001, is the most relevant international agreement on cybercrime and electronic devices. As the world becomes more aware of cyber threats, human rights in cyberspace become a concern[31]. The General Data Protection Rule was implemented by the European Union in 2018, and the California Consumer Privacy Act (CCPA) was effective in 2020. The United States' Cybersecurity Information Sharing Act (CISA) encourages the sharing of cybersecurity threats and improves overall cybersecurity. The Health Insurance Portability and Accountability Act (HIPAA) focuses on the security and privacy of health-related data. China's cybersecurity law imposes strict restrictions on critical information infrastructure and network operations. Australia updated its privacy act in 2021, including the Notifiable Data Breaches (NDB) scheme[30].

Together with national laws of different countries, international organizations and their actions, and groups work together to protect cyber platforms and ensure cybersecurity. The United Nations has established an Open-ended Working Group on Information and Telecommunications to enhance international cybersecurity. The International Telecommunication Union focuses on developing ICT standards, capacity building, and international cooperation. The Organization of American States (OAS) has issued resolutions and agreements to develop cybersecurity in America and promote collaboration among member nations. The Inter-American Committee Against Terrorism (CICTE) under OAS addresses cybersecurity challenges and encourages member governments to fight cybercrime. NATO has established a cyber operations centre to strengthen its defence capabilities. The European Union Agency for Network and Information Security promotes cybersecurity among its member countries. Asia-Pacific Economic Cooperation (APEC) aims to improve digital infrastructure security and resilience for the countries in the Asia-Pacific region[30].

Cyberspace's dynamic nature across borders hinders data protection efforts, but the importance of cyber laws has increased due to the governance concept by various states in cyberspace.[32] Rather than the above-mentioned laws and regulations, while relating to the violations created by cyber threats on human rights, some other conventions and laws have been established to combat the issue of human rights violations. The United Nations Convention on Transnational Organized Crime, also known as the Palermo Convention, was established in 2000 to protect human rights from cyber threats. Its provisions are significant in

combating cybercrime. The Convention on the Rights of the Child (1989) mandates state parties to protect children from sexual exploitation and abuse, including prostitution and pornography. The Optional Protocol to the Convention on the Rights of the Child (2001) addresses issues related to the sale of children, child prostitution, and child pornography, explicitly prohibiting the production, distribution, dissemination, sale, and possession of child pornography. The Preamble recognizes the Internet as a medium for distributing such materials. The Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist or Xenophobic Nature Committed Through Computer Systems (2003) obligates state parties to enact laws to criminalize racist or xenophobic acts expressed or communicated online.[33] Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence (2022) – This protocol remains unimplemented as of December 2022. The Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007) explicitly prohibits the use of information and communication technology (ICT) for accessing child pornography (Article 21(1)(f)), distributing child pornography (Article 30(5)), or soliciting children for sexual purposes (Article 23).[33] Together with these, the UN General Assembly Resolution 70/237 sets out fundamental principles, such as respect for human rights in cyberspace and international cooperation to prevent and mitigate cyber incidents.

The concept of data security has to be given more significance, especially the security of personal data. The laws and regulations in this area have to be maintained well in order to solve these security issues and data breaches. In the international scenario, the idea of data protection starts with the privacy rights. The right to privacy attained legal recognition with the UN Declaration on Human Rights, which explicitly included privacy rights. Later, the European Convention of Human Rights of 1950 and OECD Guidelines of 1980 also included the importance of privacy and the right to privacy in their respective guidelines. During digital development, privacy concerns increased because a lack of security mainly means a lack of privacy.[34]

In the case of India, the IT Act of 2000 and its amendments in 2008, 2011, the national policy on IT in 2012, the National Cyber Security Policy in 2013, and the Digital Personal Data Protection Act of 2024 can be considered major laws to protect the rights of data citizens.[35]

Rather than the above-mentioned laws and regulations, there are so many other kinds of rules that exist in the cyber platform in order to protect the data of not only citizens, but also so the data of different institutions and government organizations.

The implementation and enforcement of cybersecurity standards are hindered by divergent interests between states, technical capabilities, and legal frameworks. when some Countries prioritize national security while some others give importance to online privacy, leading to concerns in creating rules and regulations for cyberspace. The rapid development of technology, such as Artificial Intelligence and the Internet of Things, poses challenges to existing laws and regulations. These new innovations create new threats that require proactive responses from regulators and legislators. To address international cybersecurity and data protection challenges, a multifaceted approach combining cooperation among states, fostering a global security culture, and strengthening technical and legal capabilities is required. Mutual Legal Assistance Treaties (MLATs) and international agreements facilitate cooperation in investigations and prosecutions of cybercrimes, but their effectiveness is limited by different legal barriers, diplomatic considerations, and bureaucratic systems among various countries.[36]

Rather than concentrating on laws and regulations the individuals, organizations and different institutions can also find and do different activities to reduce the cyber security threats and create a safe cyber environment.

INDIVIDUAL METHODS TO OVERCOME ISSUES

Proactive cybersecurity measures can help individuals protect themselves from cyber risks. Awareness about these risks and providing technical solutions should be prioritized. Techniques like multi-factor authentication and regular updates can help restrict unauthorized access to personal and sensitive data[37]. Multi-factor authentication involves creating an extra security password or layer of security for accounts, while regular updates resolve app vulnerabilities and provide more protection from cybercriminals. Other practices, such as avoiding dubious links and communications and changing passwords frequently, can also contribute to cybersecurity.[38]

SOCIAL MEDIA ORGANIZATIONS AND GOVERNMENTS

Social media organizations and government bodies can assist individuals using social media platforms by creating strict encryption to ensure data privacy and prevent misuse[38]. They must also develop strong cyber security rules to protect users. Organizations can create their own rules and regulations, while governments can provide public awareness about data security and threats. Collaboration can sometimes be used to secure online platform safety[37].

The data breach of International Committee of the Red Cross (ICRC) which was considered the largest and most sensitive in the organization's history, causing migration and other disasters. The attack was initially thought to have occurred on a subcontractors' server, but it was revealed that malicious actors had compromised privileged accounts and used lateral movement techniques to gain higher privileges. This incident highlights the increasing frequency

of cyberattacks on online platforms, both nationally and internationally. The breach affected vulnerable sections of society and highlighted the need for increased security measures.[27] Using weak or incorrect security configurations can also lead to data leaks. The exposure of data by Microsoft AI researchers can be cited as an example of this.[27]

To prevent incidents like the Pegasus case, proper education and practice should be provided to employees dealing with sensitive data. Regular security audits should be conducted to identify vulnerabilities in databases and systems. This can help resolve security gaps and prevent malicious actors from exploiting the system's infrastructure.[23] Incidents like the leakage of Tesla's confidential data are common and often motivated by financial gain or profit, with the rise in such incidents occurring on online platforms when security standards and laws are not strictly enforced.[27]

One of the major steps in order to secure an organization's important data is to limit access to the data. Implement the principle of least privilege to ensure robust management of access to your systems. Protect your critical systems and the valuable data in them by ensuring that they are not compromised. Monitoring and auditing user activity can help your cybersecurity team detect suspicious behaviour by employees, such as accessing data or services irrelevant to their position, using public cloud storage services and data transfer apps, or sending emails with attachments to private accounts. User activity monitoring can also help you track file uploads, downloads, and clipboard operations. With USB device management, you can control the use of external devices within your organization and ensure that employees do not use such external devices to steal confidential information.[27]

From these examples, it is evident that up to recent times, the threat and attacks towards cyber platforms have not been reduced. From smaller to bigger organizations, from underdeveloped to developed countries, from ordinary citizens to government agencies are not excluded from cyber-attacks, threats and various security breaches.

There are different ways in order reduce the increasing number of cyber threats and to reduce their impact on people and organisations. The intersection of legal tech and cybersecurity presents opportunities for innovation and collaboration, enhancing resilience and addressing emerging threats. Improving incident response capabilities, enhancing compliance, and streamlining legal processes can create new opportunities for reducing cyber threats. Blockchain-based smart contracts and automobile compliance monitoring tools can help organizations navigate the complex regulatory landscape more efficiently. Public-private partnerships can help develop cybersecurity law, enabling government agencies to leverage private sector partners' innovations to strengthen laws and regulations. Private companies can benefit from government support and guidance for addressing cyber risks. Joint research projects, cybersecurity awareness campaigns, and knowledge sharing initiatives can enhance cyber resilience and build a more secure digital ecosystem. Lawyers can provide guidance and expertise to policymakers in implementing and drafting cybersecurity laws that balance security with civil liberties, innovation, and privacy.[39]

CONCLUSION

The rapid growth of cyberspace and related technologies has led to a global engagement in various activities in cyberspace. Despite these advancements, they have also created issues and threats to those involved. The increasing number of cyber threats affects privacy, security, and freedom of citizens. As security issues and crime rates increase, it is crucial to focus on reducing these alarming rates at personal and high levels. Individuals should be given extra awareness of every security measure they need to take during different scenarios to reduce cybersecurity issues.[40] This can be achieved at personal and high levels, following the level of risk associated with the issues. Using strong passwords, updating the software, turning on multi-factor authentication, thinking before clicking suspicious links, as for organisations encrypting data and creating backups, conducting regular employee training, reducing attack surface, installing firewalls, can be considered as the basic things to do for improving online safety[41]. For both government and private entities, developing and implementing tailored cybersecurity plans and processes is key to protecting and maintaining business operations. As information technology becomes increasingly integrated with all aspects of our society, there is an increased risk of wide-scale or high-consequence events that could cause harm or disrupt services upon which the economy and the daily lives of millions of people depend.[40] Even though a sudden change is not possible, following different kinds of threats, reducing mechanisms can reduce the increasing cybersecurity issues and enable a strong and peaceful cyber platform full of merits.

REFERENCES

1. Goodall JR, Lutters WG, Komlodi A. Developing expertise for network intrusion detection. *Information Technology & People*. 2009;22(2):92–108. Available from: http://dx.doi.org/10.1108/09593840910962186.
2. Chang FR. Guest Editor's Column. *The Next Wave*. 2012;19(4):1–2. Available from: https://www.govinfo.gov/content/pkg/GPO-TNW-19-4-2012/pdf/GPO-TNW-19-4-2012-1.pdf.
3. Kemmerer RA. Cybersecurity. In: 25th International Conference on Software Engineering, 2003. Proceedings. IEEE. 2003. Available from: https://doi.org/10.1109/ICSE.2003.1201257.
4. Lewis JA. Cybersecurity and Critical Infrastructure Protection. Center for Strategic and International Studies, Washington, DC. 2006. Available from: http://csis.org/publication/cybersecurity-and-criticalinfrastructure-Protection.
5. Canongia C, Mandarino R. Cybersecurity: The New Challenge of the Information Society. In: Crisis Management: Concepts, Methodologies, Tools and Applications. Hershey, PA. IGI Global. 2024;p. 60–80. Available from: http://dx.doi.org/10.4018/978-1-4666-4707-7.ch003.

6. Oxford Online Dictionary. 2014. Available from: http://www.oxforddictionaries.com/definition/english/Cybersecurity.
7. Cavelty MD. Cyber-Security. In: Burgess JP, editor. The Routledge Handbook of New Security Studies. London. Routledge. 2010;p. 154–162. Available from: https://www.routledge.com/The-Routledge-Handbook-of-New-Security-Studies/Burgess/p/book/9780415539333?srsltid=AfmBOorJxoKO1zbSGsfzyQiSb3FYGsggPtAqv4tlWT660ax-aevZvVtG.
8. Craigen D, Diakun-Thibault N, Purse R. Defining Cybersecurity. *Technology Innovation Management Review*. 2014;4(10):13–21. Available from: http://timreview.ca/article/835.
9. Bay M. What Is Cybersecurity? In search of an encompassing definition for the post-Snowden era. *French Journal For Media Research* . 2016;6:1–28. Available from: https://www.researchgate.net/publication/308609163_WHAT_IS_CYBERSECURITY_In_search_of_an_encompassing_definition_for_the_post-Snowden_era.
10. Ottis R, Lorents P. Cyberspace: Definition and implications. 2011. Available from: https://www.researchgate.net/publication/287868009_Cyberspace_Definition_and_implications.
11. Wiener N. Cybernetics: Or Control and Communication in the Animal and the Machine. Cambridge, MA. MIT University Press. 1948.
12. Gibson W. Neuromancer. New York. Ace Books. 1982.
13. DOD Dictionary of Military and Associated Terms. 2017. Available from: http://www.dtic.mil/doctrine/dod_dictionary.
14. Strate L. The Varieties of Cyberspace: Problems in Definition and Delimitation. *Western Journal of Communication*. 1999;63(3):382–412. Available from: https://doi.org/10.1080/10570319909374648.
15. The National Strategy to Secure Cyberspace. The White House. 2003. Available from: https://georgewbush-whitehouse.archives.gov/pcipb/.
16. Kemp S. Digital 2020: Global Digital Overview. DataReportal. 2020. Available from: https://datareportal.com/reports/digital-2020-global-digital-overview.
17. Team SK. Dominating the Internet Landscape: Global Internet Usage Statistics by Country in 2025. SG Analytics. 2025. Available from: https://www.sganalytics.com/blog/global-internet-usage-statistics/.
18. King Z, Henshel D, Flora L, Cains MG, Hoffman B, Sample C. Characterizing and measuring maliciousness for cybersecurity risk assessment. *Frontiers in Psychology*. 2018;9:1–19. Available from: https://doi.org/10.3389/fpsyg.2018.00039.
19. Palatty NJ. 90+ Cyber Crime Statistics 2025: Cost, Industries & Trends. Astra Security . 2025. Available from: https://www.getastra.com/blog/security-audit/cyber-crime-statistics/.
20. Bahuri A, Isa Z. Social Media and Cyber Security: Protecting Against Online Threats and Attacks. 2023. Available from: https://www.researchgate.net/publication/373328868.
21. Griffiths C. The Latest Cyber Crime Statistics, AAG IT Support. AAG IT Services. 2025. Available from: https://aag-it.com/the-latest-cyber-crime-statistics/.
22. Weinberg D, et al. Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons*. 2015;58(6):615–624. Available from: https://doi.org/10.1016/j.bushor.2015.06.005.
23. Holm E. The role of the refrigerator in identity crime. *International Journal of Cyber-Security and Digital Forensics* . 2016;5(1):1–9. Available from: http://dx.doi.org/10.17781/P001974.
24. Arias O, Wrum J, Hoang K, Jin Y. Privacy and security in Internet of Things and wearable devices. *IEEE Transactions on Multi-Scale Computing Systems*. 2015;1(2):99–109. Available from: https://doi.org/10.1109/TMSCS.2015.2498605.
25. Billingsley L, McKee SA. Cybersecurity in the Clinical Setting: Nurses' Role in the Expanding "Internet of Things". *The Journal of Continuing Education in Nursing*. 2016;47(8):347–349. Available from: https://doi.org/10.3928/00220124-20160715-03.
26. Singh D, Mohanty NP, Swagatika S, Kumar S. Cyber-hygiene: The key Concept for Cyber Security in Cyberspace. *Test Engineering and Management*. 2020;83:8145–8152. Available from: https://www.researchgate.net/publication/342069141_Cyber-hygiene_The_key_Concept_for_Cyber_Security_in_Cyberspace.
27. Storchak Y. Top 10 Best-Known Cybersecurity Incidents and What to Learn from Them. 2024. Available from: https://www.syteca.com/en/blog/top-10-best-known-cybersecurity-incidents-and-what-to-learn-from-them.
28. Significant Cyber Incidents | CSIS. 2023. Available from: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
29. Ehrenfeld JM. WannaCry, Cybersecurity and Health Information Technology: A Time to Act. *Journal of Medical Systems*. 2017;41(7):104. Available from: https://doi.org/10.1007/s10916-017-0752-1.
30. Joshi A. Study of Cybersecurity Laws and Regulations. *Indian Journal of Law*. 2024;2(3):7–14. Available from: https://doi.org/10.36676/ijl.v2.i3.27.
31. 27 Jan A new look at the Budapest Convention on Cybercrime. ICTLC Australia. . Available from: https://www.ictlc.com/a-new-look-at-the-budapest-convention-on-cybercrime/?lang=en.
32. Hollis DB. A brief primer on international Laws and Cyberspace, Carnegie Endowment For International Peace. 2021. Available from: https://carnegieendowment.org/posts/2021/06/a-brief-primer-on-international-law-and-cyberspace?lang=en.
33. 33.Georgetown law library, Guides: International and Foreign Cyberspace Law Research Guide: Treaties & International Agreements. 2024. Available from: https://guides.ll.georgetown.edu/cyberspace/cyber-crime-treaties.
34. Mishova A. Data protection Laws around the world: A Global perspective. *GDPR Local*. 2024. Available from: https://gdprlocal.com/data-protection-laws-around-the-world-a-global-perspective.
35. Cyber Laws, legislations, and regulations of 2024. June 21, 2024. Available from: https://www.knowledgehut.com/blog/security/cyber-security-laws.
36. Cybersecurity and International Law: Addressing Global Challenges in Cyberspace. 2024. Available from: https://theimpactlawyers.com/articles/cybersecurity-and-international-law-addressing-global-challenges-in-cyberspace.
37. Primary technology, when and why to use Multi-Factor Authentication. 2023. Available from: https://primaryt.co.uk/when-to-use-multi-factor-authentication.
38. Al-Janabi S, Al-Shourbaji I. A Study of Cyber Security Awareness in Educational Environment in the Middle East. *Journal of Information & Knowledge Management*. 2016;15(01). Available from: https://dx.doi.org/10.1142/s0219649216500076.
39. Academike, Recent developments in Cybersecurity Law: Challenges and opportunities. 2024. Available from: https://www.lawctopus.com/academike/recent-developments-in-cybersecurity-law-challenges-and-opportunities/.
40. Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA. . Available from: https://www.cisa.gov/topics/cybersecurity-best-practices#top.
41. Sukianto A. 10 ways to reduce cybersecurity risk for your organization. Up Guard. Jan 02, 2025. Available from: https://www.upguard.com/blog/reduce-cybersecurity-risk.