AN IN-DEPTH ANALYSIS OF THREATS AND COUNTERMEASURES IN THE PERIOD OF DIGITAL TRANSFORMATION FOR CYBER SECURITY

Sujata Roychowdhury
Technology Expert, Pune, India
sujatadas24@yahoo.co.in

ABSTRACT
Cyber security refers to the policies and procedures used to prevent unwanted access to and data breaches on digital devices, networks, and information. In response to growing cyber dangers, it has experienced tremendous expansion. Techniques like firewalls, encryption, safe passwords, and threat detection systems are important aspects of cyber security. Employee training on these strategies is essential in the age of digital transformation. The article underlines the need for enterprises, organizations, and individuals to take precautions to protect their sensitive data from cybercrime and discusses the present difficulties facing the cyber security industry. It also emphasizes cyber security methods. In order to effectively protect digital environments against electronic dangers, it also emphasizes the significance of increasing public knowledge of cyber security hazards. In addition to the current threats and countermeasures in cybersecurity, there is also a future scope for research in this field.
Keywords*:* Cyber security, cyber threats, cyber ethics, countermeasures, digital transformation

Introduction

The rapid advancement of technology has led to significant societal changes but has also created challenges in protecting private information. Cybercrime has increased as a result, highlighting the need to enhance cybersecurity measures to safeguard critical information infrastructures. Securing cyberspace is crucial for national security and economic prosperity. However, combating cybercrime requires a comprehensive approach that goes beyond technical measures. Law enforcement agencies must possess the necessary capabilities to investigate and prosecute cybercrime effectively (Reddy, 2014).

Cyber Security

Global investment in computer security technologies has expanded as a result of the rise of cybercrime, digital money, and e-government. Cybersecurity involves protecting digital information through various approaches and procedures. The focus is on safeguarding data, as it is the primary target for criminals. Networks, servers, and computers are simply means through which data is accessed. Cyber security that is effective lowers the danger of cyber-attacks and protects people and businesses against illegal system, network, and technology use. It entails comprehending various cyber threats and creating defence measures that put the privacy, integrity, and accessibility of digital data first. A system's availability ensures that those who require it may access it, while confidentiality prevents unauthorized disclosure and integrity prevents unauthorized change or destruction. (Perwej et al. 2021; S. Lin et al., 2007). According to the Symantec cybercrime report from April 2012, cyber-attacks cost the economy 114 billion US dollars annually. Because they are more accessible, practical, and secure than physical assaults, cyber-attacks are becoming more and more common. Cybercriminals may easily carry out assaults because all they need is a computer and an internet connection. It is projected that the quantity and complexity of cyber-attacks will continue to increase due to the allure and efficacy of attacking information technology systems. (Figure 1&2) (Ilkina, 2013)

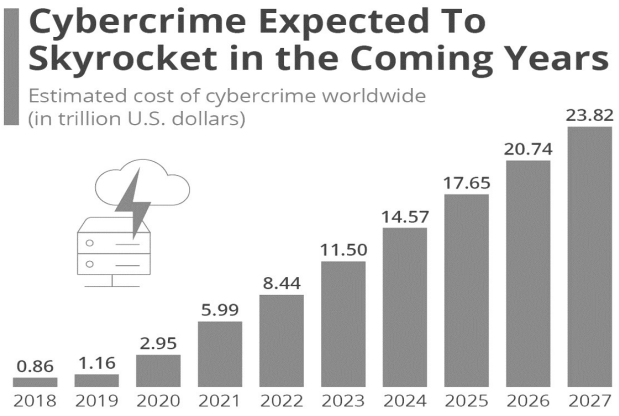

Figure 1: The Estimated costs of cybercrime from 2018 to 2027
(Source: https://www.statista.com)

Figure 2: Cybersecurity statistics for the period 2021-2022
(Source: https://stefanini.com)

Cybersecurity is of utmost importance due to the rapid growth and increasing sophistication of cyber-attacks worldwide. In the Asia-Pacific region, businesses face a high frequency of attacks, with an average of six per minute. These attacks not only threaten governments and corporations but also put individuals at risk of identity theft. Education is crucial in combating cybercrime, as awareness of risks associated with network and application usage is essential for everyone. Weak passwords and improper online practices make it easier for hackers to gain unauthorized access to personal accounts and exploit information. Businesses are now focusing on developing response plans to minimize damage from cyber-attacks. Ultimately, cybersecurity plays a critical role in protecting cherished lifestyles (Perwej, 2020).

The Era of Digital Transformation

The term "digital transformation" describes how businesses use more advanced technology to increase their operational effectiveness, business capabilities, and consumer experiences. When approached strategically, digital transformation can provide companies with a competitive advantage, including faster time-to-market for products and services and improved solution quality through incremental releases. Investing in digital transformation supports customers and employees, with a key component being the adoption of an Agile mindset to deliver continuous, high-value solutions and enhance operational efficiencies. The concept of digital transformation was defined in 2013, and it is expected that various industries, such as physical, financial, and healthcare, will undergo digitization. The adoption of digital technologies started with the proliferation of digital computers and storage in the second half of the 20th century, leading to the development of advanced computer systems capable of automating manual tasks. (Source: Laster, 2021)

Literature Review

Cybersecurity is a subset of IT security. Cyber security protects digital data stored on networks, computers, and other devices from unauthorized access, attack, and destruction. Cyber security, its history, and related activities will be discussed in this section.

The strategies, instruments, and practices used to stop unauthorized access to computer systems, software, networks, and data are referred to as cyber security. (Kruse et al., 2017). Cybersecurity is the activity of defending against malicious attacks on servers, computers, mobile devices, electronic systems and data networks (Chang and Coppel, 2020). It is also denoted as electronic information security or information technology security. Seventy years ago, the terms "viruses," "Trojan horses," "worms," "spyware," and "malware" were not even in the language of information technology. The development of cyber security was sparked by the discovery of viruses. In the 1970s, Robert Thomas developed the first computer "worm" while working as a researcher for BBN Technologies in Cambridge, Massachusetts. The Melissa virus was made widely known in late 1999. Infecting email accounts was the main goal when this macro-virus was developed. One of the worst cyberattacks in 2013 and 2014 targeted Yahoo. (Choucri and Goldsmith, 2012).

Brenner describes the initial approach for coming up with measures to rate online criminality. She suggests a straightforward taxonomy of damages that divides into three categories: individual, systemic, and social because she admits how difficult it is to develop measures and scales for cybercrime. (Kshetri ., 2006). Cybercrime is typically described using the crime triangle, which stipulates that three factors—a victim, a motive, and an opportunity—must all be present for it to happen. (Dhanjani et al., 2009). The 128-bit block cypher Camellia is described in this article. The Advanced Encryption Standard (AES) interface specifications, which call for 128-bit block sizes and 128-, 192-, and 256-bit keys, are followed by Camellia. Camellia is renowned for its outstanding level of security and effectiveness on both hardware and software platforms. (Fink, et al., 2011). In terms of hardware and software, Camellia's encryption speed is at least comparable to that of the AES finalists, particularly RC6, MARS, Rijndael, and Serpent, & Twofish. A framework for empirically evaluating harm that takes into account a number of processes is provided by Greenfield et al. (2013). The five main areas where harm may occur are functional integrity, freedom from humiliation, material support and amenity, reputation, and privacy. The phrase "cyberspace cartography" was created by Grant et al. (2014), who also applied the idea

of "cyber-geography" to military operations. Mathieu and Guy (2015) explore the present state of Internet jurisdiction law and the issue of selecting a specific venue when a case crosses state lines.

In order to harm web services in a specific circumstance, hacker-activist organizations have conducted online security attacks (Edwards, 2016). The author used tweets from Twitter users to demonstrate a sentiment analysis technique that was based on a daily collection of tweets from users who use the site to express their opinions on crucial subjects and to disseminate information about web security breaches. Slyke et al. (2016) focused on the victimization aspect of white-collar crimes in order to create taxonomy of harms for these crimes. They look at a number of white-collar offenses and the costs associated with them. They combine desk research with victim surveys and put a strong emphasis on how injuries to particular people will affect them in the long run. Punter (2016) advised that timely intelligence regarding cyber security threats and vulnerabilities are necessary in order to secure crucial personal and organizational systems. CERT warnings, blogs, social media, dark web services, and the National Vulnerability Database are a few of the overt and covert sources of information regarding these dangers.

Other attempts are concentrated on improving risk frameworks and modeling business system resilience (Kennedy, Mike, 2017). A threat-based model is developed with various destructible processes, particular vulnerabilities, and particular system resilience barriers for every threat. The author offers a simulation-based training scenario that allows student trainees to practice their response to a DDos attack in a virtual environment utilizing hacking tools and a simulator in order to better prepare them for actual attacks (TT., 2017). Fuzzy (2017) mean (FKM) is used to split the data into three clusters, manually label a small sample, and then train the neural network classifier Multi-Layer Perception (MLP) on the manually labeled data to classify cyber security logs into the three categories of attack, unsure, and no attack. The innovative methodology presented by Nguyen et al. (Lindsay, 2017) is based on the "top-down" methodology that is explored in the field of criminology. In order to secure their assets against cyber-incidents, some users would be prepared to pay "premiums,".

Cyberattacks may jeopardise patient safety by compromising data security or interfering with the functionality of medical devices. The WannaCry and NotPetya ransomware outbreaks, as well as programming problems in Medtronic implantable cardiac devices, are just a few examples of recent events that have adversely impacted the ability to provide healthcare (McGuire, 2018). According to Xingan (2018), social media is now a crucial component of people's everyday lives and, for some, even their source of income. Combating cybercrime requires a thorough understanding of who can be the target of an attack and why it might be challenging to identify the perpetrators. Teenagers and the elderly are said to be the most vulnerable victims because they are the ones who are least aware that these attackers exist (Foroughi, & Luksch, 2018). The use of analytical models, machine learning, and big data are common ways that may be improved by supplying applicable knowledge to control or reduce the effects of hazards.

Sayeed et al. (2019), presented a novel method for extracting opinions from a given data source. The suggested strategy was evaluated using business travel. TripAdvisor-related thoughts and attitudes posted on Twitter were analysed. There are also cyberattacks in the bitcoin industry. There, 51% of assaults aim to take over more than 50% of a Blockchain, enabling hackers to take over the system (Catherine et al., 2019). Contrarily, there can be various risk factors linked with both victimization and offense in cybercrime because it occurs in a different setting than typical crimes (Boussi, 2020). However, there is no actual physical connection in either place or time between cybercriminals and their victims. This is in contrast to traditional victimization and offending, which call for a direct physical link between victims and offenders. By keeping track of their activities on electronic devices, a framework is provided in combating cybercrime (Datta et al., 2020).

Cybersecurity safeguards the data and integrity of computing assets that are a part of or connected to an organization's network in order to defend against all threat actors during a cyber-attack. (Perwej et al., 2021). Cyberattacks on IT domain infrastructure have a direct impact on how securely corporate operations are run, and they may even result in system failure. Zahrani (2022), sought to identify the key cyber risks in the transportation sector. Cyber security is a difficult task that requires domain knowledge and rely on cognitive skills to recognize possible threats from enormous volumes of network data, as Eze et al. (2023) shown. This study investigates how a simple network's capacity to identify breaches is influenced by information security and network management skills. Security and risk management leaders must review how they equalize their investments across structural, technological and human-centric aspects. Restructuring approach points to solutions and broader attack coverage, rebalancing practices to concentrate on people, process, and technology, and pursuing sustainable, balanced cybersecurity programs are some of the steps organizations take to address four key priorities (Perri, 2023).
(Figure 3).

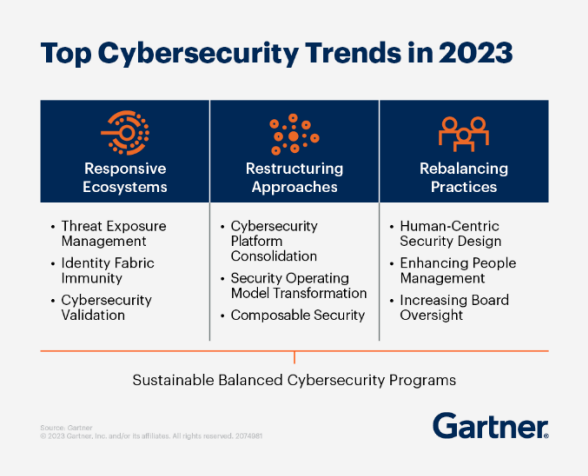

Figure 3: Top Cybersecurity Trends in 2023
(Source: https://www.gartner.com)

Research Gap:
Our existing understanding of cyber security mainly relies on information from news reports, past research, and commercial threat reporting. However, this information only provides a partial and skewed view of cyber threat activities since it is usually politicized and affected by the needs of powerful clients and the interests of knowledgeable suppliers (Furnell , 2017). In order to examine cybersecurity threats and countermeasures in the age of digital transformation comprehensively and methodically, the current study makes use of material that is already publicly available.

Objectives
The following are the objectives of study:
1. To describe the techniques used in cyber security
2. To examine the threats to cyber security
3. To research countermeasures for cyber threats in the context of digital transformation.

Research Methodology
An extensive analysis of threats and countermeasures on the cyber security in the periods of digital transformation is undertaken utilising already-existing sources in this study. In this research, secondary data and a descriptive methodology are used. The researcher's data was only acquired from reliable, published secondary sources because this methodology solely used secondary sources. Among them are books, periodicals, reports, websites, and other sources. Statistical information from a number of sources has been highlighted to emphasise the importance of the objectives studied.

Data Analysis
1. Description of the Cyber Security Techniques (Figure 4) (Reddy,2014)

Password Security and Access Control: A crucial component of protecting our information has been the concept of a user name and password. One of the first cyber security precautions might be this.

Data Authentication: It is usually vital to confirm, before to downloading, that the papers we receive have originated from a reliable source and have not been altered. Usually, these documents are verified using antivirus software that is installed on the machines. So, in order to protect the devices from infections, a reliable anti-virus tool is required.

Malware Scanners: Typically, this software scans all of the system's files and documents for harmful code or infections. Trojan horses, worms, and viruses are examples of malicious software, also referred to as malware.

Firewalls: A firewall is a piece of hardware or software that blocks Internet-based access to computers by hackers, viruses, and worms. Every message that enters or leaves the internet is examined by the installed firewall, and those that do not follow the set security standards are blocked.

Antivirus Software: It is a kind of computer program that searches for and gets rid of harmful software programs like viruses and worms by finding them and taking preventative action. Most antivirus programs have

an auto-update feature that enables them to obtain profiles of new viruses so that they can scan for them as soon as they are discovered.

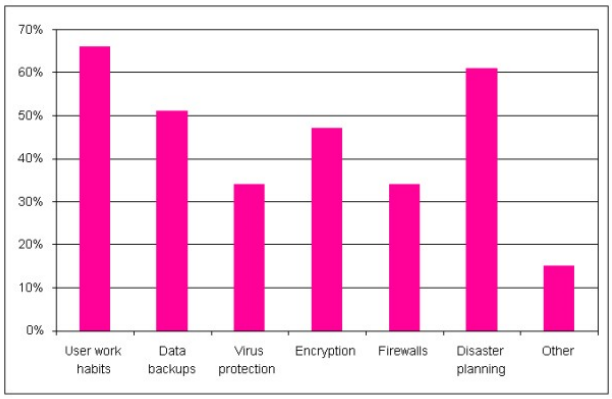

Figure 4: Cyber Security Techniques
(Source:https://www.researchgate.net)

2. Examination of the Threats to Cyber Security

The following are some of the most well-known threats in the era of digital transformation (Mijwil et al., 2022; Kim et al., 2021):

Ransomware Attack

Ransomware attacks are highly sophisticated and malicious cyber-attacks aimed at encrypting a victim's computer files or entire system. Attackers ask for a ransom in return for a code or decryption key. Phishing emails, social engineering, and exploit kits are just a few of the delivery methods for these attacks. The loss of data can have severe consequences, such as financial losses and damage to reputation, forcing victims to comply with the attacker's demands to avoid losing their data. To mitigate the risk of ransomware attacks, regular data backups, protective software implementation, and user education are crucial to avoiding falling for phishing scams. In recent times, With an increase in their frequency and continued progress in system penetration, data encryption, and even the theft of important information, ransom ware assaults have undergone substantial development. It is evident how urgent the situation is. (Figure 5), a representation of a hacker encrypting a victim's data, setting a deadline for compliance, and threatening to completely wipe all the victim's data if the demands are not satisfied.

Figure 5: Example of ransomware attack
(Source: https://www.thesagenext.com)

IoT Attacks

The IoT (Internet of Things) environment consists of various interconnected devices such as appliances like washing machines, televisions, and lights that can communicate via the internet and share data. In recent years, IoT devices have experienced a range of attacks, including physical attacks and social engineering attacks (Figure 6). These attacks grant attackers full control over users' devices, infiltrate their data, monitor their activities, and misuse the gathered information for malicious purposes. Attackers may make use of this information to harm users, destroy their reputations, or steal money. IoT attackers frequently utilize social engineering to take advantage of trust relationships between users and devices, giving them access to sensitive data without the users' knowledge. Figure 6 provides statistics on the types of attacks targeting IoT devices.

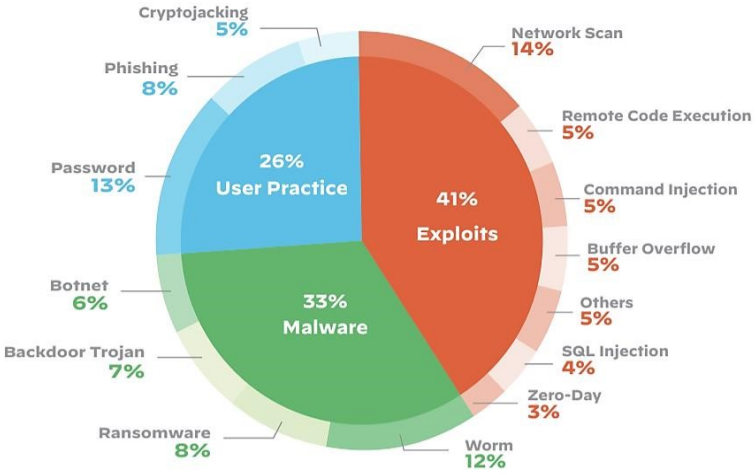

Figure 6: Statistics of attacks on IoT
(Source: https://threatpost.com)

Cloud Attacks

Cloud computing is a revolutionary technology that enables efficient storage and transfer of large amounts of data. It offers cost-effectiveness and convenience for businesses but also raises concerns about data security breaches. Factors such as lack of encryption, authentication, and improper configuration contribute to compromised data security. Attackers use vulnerabilities in cloud computing systems to access sensitive data without authorization, disrupt services and applications, and exploit security flaws. To address these risks, companies implement security measures like access controls, encryption, monitoring, and regular assessments to prevent cloud attacks and protect cloud environments.

Phishing Attacks

Phishing assaults are frequent online technological crimes where attackers try to steal people's sensitive information. This includes passwords, credit card numbers, and personal information. Attackers often use deceptive tactics, such as sending fake emails that appear to be from trustworthy sources like well-known websites, platforms, or banks (Figure 7). These emails contain fake links that mimic legitimate websites, aiming to deceive victims into providing their information unknowingly. In addition, sophisticated malware is used in these attacks to infect computer systems or apps, giving the attacker access to the victim's machine or the ability to steal important data. People should be cautious when opening unsolicited emails (spam) or questionable messages, use strong passwords, use antivirus software, and maintain all software and operating systems up to date in order to defend themselves from phishing attacks.

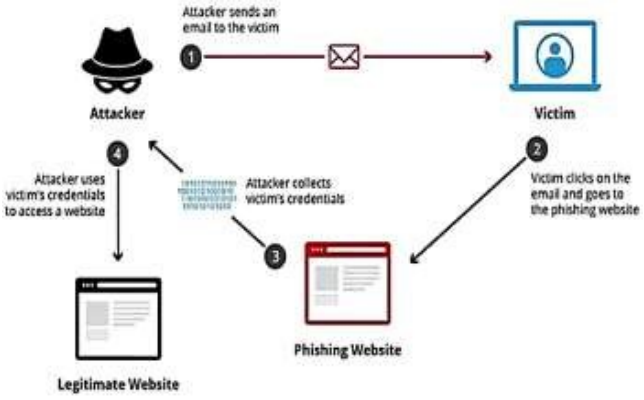

Figure 7: The Phishing Attack
(Source:https://www.researchgate.net)

Cryptocurrency and Blockchain Attacks

A variety of cyber-attacks that target crypto currency wallets, exchanges, and blockchain networks are referred to as crypto currency and block chain attacks (Gisbert, 2019; Ramos et al., 2021). Phishing attacks, in which con artists send false emails or messages to target crypto currency users and steal their login information or sensitive data, are frequent. Malware is also used to steal bit coin wallets and infect devices. Distributed denial-of-service

(DDoS) attacks can be used to target crypto currency exchanges and wallets in order to acquire unauthorized access. Attempts to seize control of a block chain network (51% attack) may occur. (Figure 8) or exploit vulnerabilities in the code. Users should enable two-factor authentication, use strong passwords, and keep their software updated to protect themselves against these attacks. Service providers must have strong security measures in place, such as intrusion detection systems, firewalls, and encryption.

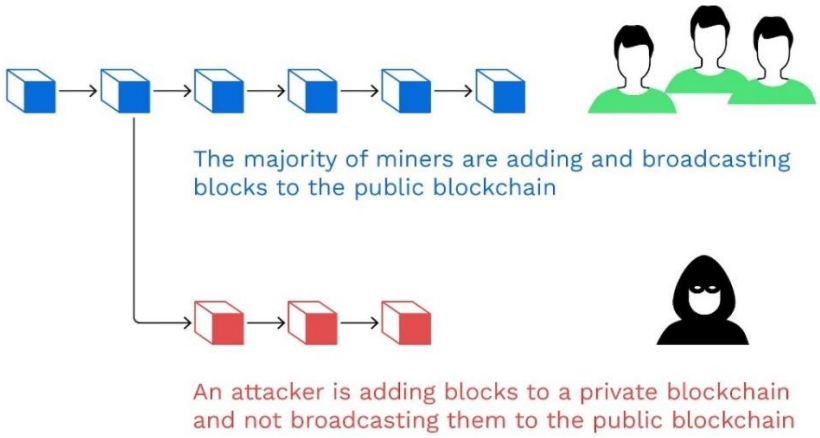

Figure 8: Blockchain Attack
(Source: https://threatpost.com)

SQL Injection (SQLi)
An attack known as SQL injection targets SQL databases explicitly. It takes advantage of holes in database permissions and employs HTML forms on websites to run SQL statements that change the database's data. Servers frequently interface with databases using SQL to speed up data retrieval and change. (Figure 9). Attackers use malicious SQL statements to trick computers into performing unauthorized actions. Through SQL injection, attackers can directly access and modify personally identifiable information (PII) stored in databases.

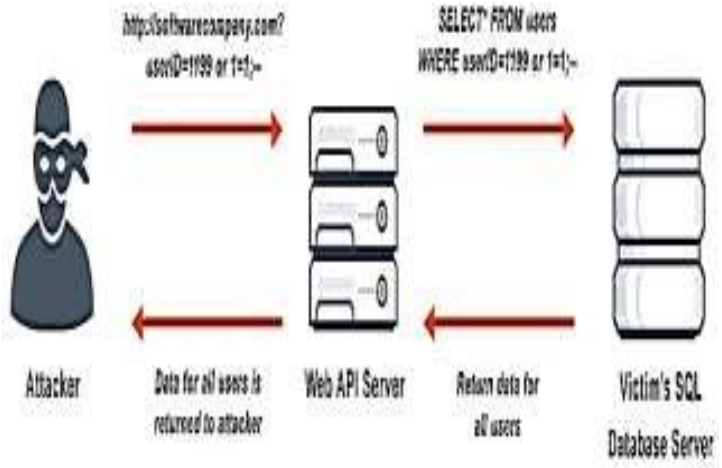

Figure 9: The SQL Injection
(Source: https://www.researchgate.net)

Findings
1. Strengthening Cyber-security Measures (National Police Agency, 2013)
In July 2012, the NPA created the position of Director-General of the Commissioner to supervise cyber-security policies and reinforce reactions to cyber threats. A cross-organizational structure was created to review and improve policies related to cybercrimes, cyber-attacks, international cooperation, technological advancements, and legal amendments.

2. Countermeasures against Cybercrimes
To address the abundance of information on the Internet, the NPA collaborates with private businesses and relies on their hotline services. Coordinated measures are taken to combat illegal and harmful information, utilizing a nationwide cooperative investigation approach to prevent duplication of efforts by prefectural police

forces. The NPA has taken steps to reinforce cyber-security measures by establishing leadership positions, implementing cross-organizational structures, enhancing policies, promoting international cooperation, and addressing illegal/harmful information through collaboration with private sector organizations and coordinated investigations (Figure 10).

- Since June 2006, the NPA operated Internet Hotline Centre (IHC), which accepts reports from regular Internet users regarding illegal or harmful information, handles police reports, and takes action by, for example, requesting website administrators to remove illegal or harmful contents. It also works to promote coordination between member organisations of "INHOPE," which was established as a liaison organisation.
- As per IHC reports, the police make an effort to gather illegal/harmful information and, using the nationwide cooperative investigation method, carry out effective enforcement against illegal/harmful information.

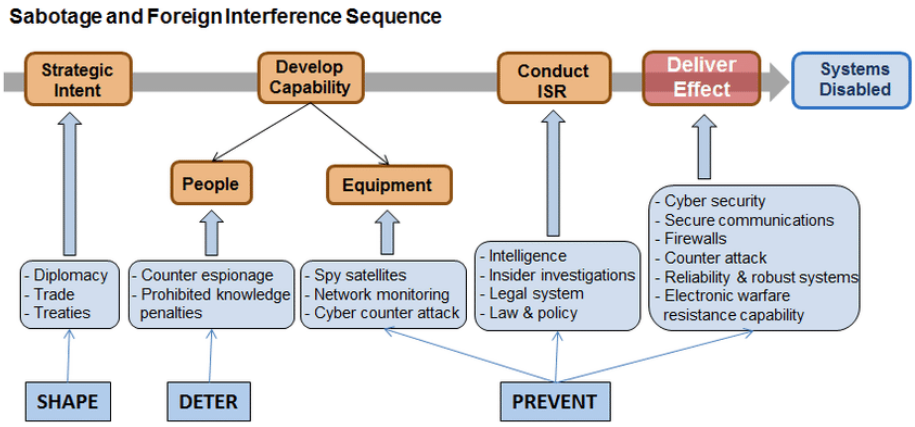

Figure 10: Cyber Countermeasures
(Source:https://www.researchgate.net)

3. Measures against Cyber-attacks

The NPA focuses on reinforcing structures, exposing actual conditions, and promoting cooperation with the private sector to effectively combat cyber-attacks.

- In May 2013, the NPA's Cyber Force Center established the position of Director for Counter Cyber-Attacks to guide investigations, promote public-private cooperation, and facilitate information exchange with international security intelligence agencies. The Anti-Cyber-Attack Units provide support to other police forces, gather information, and establish relationships with private sector businesses.
- The police analyze computers and malware involved in cyber-attacks to expose the techniques and conditions used by attackers. International cooperation is sought through organizations like International Criminal Police Organization (ICPO) to investigate overseas sources. Information exchange with overseas security intelligence agencies helps expose actual conditions related to cyber-attacks.
- Collaboration with private sector companies is crucial to prevent and respond to cyber-attacks. The police have established cooperative frameworks with private sector companies to leverage their expertise and knowledge in dealing with cyber threats.

4. Technological Assistance for Enforcement against Crime

The police have established High-Tech Crime Technology Divisions in the NPA and prefectural info-communications departments to provide technological support for criminal investigations. The NPA Info-Communications Bureau possesses specialist knowledge, technological expertise, and advanced analytical equipment to assist in high-level IT analyses such as data extraction from damaged storage devices and malware analysis.

5. Improvement of International Cooperation on Cybercrime Investigations

To combat transnational cybercrime, the NPA seeks international cooperation through frameworks like Mutual Legal Assistance Treaties and ICPO. Information exchanges, discussions, and cooperative relations with foreign investigation agencies are actively pursued through international conferences and engagements.

Conclusion and Limitations

Cybercrimes target sensitive information for the purpose of theft, manipulation, or deletion. Attackers use a variety of techniques to take advantage of people and institutions, including hacking, phishing, identity theft, cyber stalking, and online fraud. Significant harm is caused by these acts, including financial loss and the disclosure of personal information. Due to the Internet's global reach and elusiveness, it is difficult to verify and

address cybercrimes. Artificial intelligence techniques play a crucial role in analyzing the behavior of malicious software. Combating cybercrime requires a comprehensive approach encompassing technological solutions, legal frameworks, and international cooperation.

Restrictions on the study's time and resources were experienced during study. The amount of time that can be spent to analyze a research problem and track development through time is constrained by a number of practical reasons. The breadth and depth of the ideas presented in this study are constrained in a variety of ways when compared to the works of scholars with more expertise. The researcher had limited access to organizations or documents.

Future Directions

In this section, we go into greater depth about these speculative future study possibilities.

Research in the area of privacy focuses on various aspects such as selectively disclosing data, protecting shared data, and sanitizing data (Madden, 2012). Johnson et al. (2012) studied languages for specifying privacy policies and detecting and addressing violations of privacy. Future research will provide methods for data policy in areas including data gathering, data sharing, data transfer, and dealing with privacy infractions. It will also provide privacy assurances. Overall, the focus is on enhancing privacy protection and establishing effective mechanisms for managing and safeguarding sensitive information.

The next-generation secure internet's "clean-slate design" idea seeks to build a system from the ground up in order to acquire an objective viewpoint on the issue at hand (Paul & Jain, 2011). This comprises ideas and initiatives centered on privacy protection, anti-spam safeguards, trust structures, names and identities, and cryptography. The more recent paradigms recommend (Bellovin et al., 2006) placing content delivery first at the network architecture's core rather of concentrating only on host connectivity. The requirements of heterogeneous networking settings, such as wireless ad hoc networks, where constant end-to-end connectivity cannot be anticipated, are also especially addressed by research in challenging networks.

In the pursuit of trustworthy systems, several research threads have emerged. These involve investigating reliable separation, virtualization, and isolation approaches in both hardware and software (Hasselbring et al., 2006). In addition to self-testing, self-diagnosing, and self-reconfiguring capabilities, robust architectures that are resilient to compromise and provide automatic remediation are also being created. (Lim, 2012).

Global identity management and trace back methods are being investigated to improve management of user data on computers. Ingress filtering (Wang, et al., 2011), egress filtering, and marking (John, & Siva Kumar., 2009) are commonly used traceback techniques, but they have limitations and can be evaded by skilled attackers (Kukkala, 2022). The capacity to track modifications and alterations made to computer resources is provided by provenance approaches (Moreau et al., 2008). To aid in tracking and recognizing the flow and consumption of resources, tool advancements are suggested. Current version control systems for file compression and natural language translation may offer helpful insights for creating methods in this area. The objective is to improve the ability to manage identities and trace activities on a global scale, ensuring greater security and accountability.

Usable security focuses on improving the usability of security technologies, which often fall short in this aspect. Human-computer interaction (HCI) research is carried out to develop methods for interface design, assessment of useable security, and tool creation. Research on assessing usability in connection to security is claimed to be necessary, and HCI research approaches can significantly advance this field. (Furnell, 2007).

References

Altair. (2017). Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. *Procedia Computer Science*, *109*, 1086-1091.

Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). On the Effectiveness of Machine and Deep Learning for Cybersecurity. In *10th International Conference on Cyber Conflict (CyCon)* 371-390.

Al-Zahrani, A. (2022). Assessing and Proposing Countermeasures for Cyber-Security Attacks. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *13*(1).

Bergmann, M. C., Dreißigacker, A., von Skarczinski, B., & Wollinger, G. R. (2018). Cyber-Dependent Crime Victimization: The Same Risk for Everyone? *Cyberpsychology, Behavior, and Social Networking*, *21*(2), 84-90.

Boussi, G. O. (2020). A Proposed Framework for Controlling Cyber-Crime. In *8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*. IEEE,

IndiaBCS (March 3, 2023). *The Importance of Cybersecurity and Mentoring in Digital Transformation*. Retrieved from: https://www.bcs.org

Boussi, G. O. (2020). A Proposed Framework for Controlling Cyber-Crime. In *8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*. IEEE, India.

Bellovin, S. M., Clark, D. D., Perrig, A., & Song, D. (2006). *A Clean-Slate Design for the Next-Generation Secure Internet*.

Bhatt, N. (October 2022). What are the Top 10 Emerging Cybersecurity Challenges? *Sagenext*. Retrieved from https://www.thesagenext.com

Chang, L. Y., & Coppel, N. (2020). Building Cyber Security Awareness in a Developing Country: Lessons from Myanmar. *Computers & Security*, 97, 101959.

Choucri, N., & Goldsmith, D. (2012, March). Lost in Cyberspace: Harnessing the Internet International Relations and Global Security. *Bulletin of the Atomic Scientists*, *68*(2), 70-77.

Cross, M., & Shinder, D. L. (2008). *Scene of the Cybercrime*. Syngress.

Catherine, D., et al. (2019). Handbook on Crime and Deviance. *Handbooks of Sociology and Social Research*.

Datta, P., et al. (2020). A Technical Review Report on Cyber Crimes in India. In *International Conference on Emerging Smart Computing and Informatics (ESCI)*. IEEE, India.

Dhanjani, N., Rios, B., & Hardin, B. (2009). *Hacking: The Next Generation*. O'Reilly Media, Inc.

Eze, et al. (2023). A Study of Cyber Security Threats, Challenges in Different Fields and its Prospective Solutions: A Review. *INOSR Scientific Research*, *9*(1), 13-24.

Fossi, M., et al. (April 2011). *Symantec Internet Security Threat Report Trends for 2010*, 16. Retrieved from: http://book.itep.ru

Fink, E., Sharifi, M., & Carbonell, J. G. (2011). Application of Machine Learning and Crowdsourcing to Detection of Cybersecurity Threats. In *Proceedings of the US Department of Homeland Security Science Conference–Fifth Annual University Network Summit*, Washington, DC.

Foroughi, F., & Luksch, P. (2018). *Data Science Methodology for Cybersecurity Projects*. *arXiv preprint arXiv:1803.04219*.

Furnell, S., & Emm, D. (2017). The ABC of Ransomware Protection. *Computers & Fraud & Security*, *10*, 5-11.

Fleck, A. (2022). Cybercrime Expected to Skyrocket in Coming Years. *Statista*. Retrieved from https://www.statista.com

Greenfield, V. A., & Pa. L. (2013). A Framework to Assess the Harm of Crime. *British Journal of Criminology*, *53*, 864-885.

Grant, T., & Liles, S. (2014). On the Military Geography of Cyberspace. In *Proceedings of the International Conference on Information Warfare*, *66*.

Grpoup, D. (2011). Cyber Crime: New Challenge to Mankind Society. *Introduction to the Nature of Cyber Crime and Its Investigation Process*.

Hernandez-Suarez et al. (2018). Social Sentiment Sensor in Twitter for Predicting Cyber-Attacks Using ℓ1 Regularization. *Sensors*, *18*(5), 1380.

Hernández, A., Sanchez, V., Sánchez, G., Pérez, H., Olivares, J., Toscano, K., & Martinez, V. (2016). Security Attack Prediction Based on User Sentiment Analysis of Twitter Data. In *2016 IEEE International Conference on Industrial Technology (ICIT)*. 610-617.

Hasselbring, W., & Reussner, R. (2006). Toward Trustworthy Software Systems. *Computer*, *39*(4), 91-92.

History of Digital Transformation (March 24, 2023). *Capacity*. Retrieved from: https://capacity.com

Hasselbring, W., & Reussner, R. (2006). Toward Trustworthy Software Systems. *Computer*, *39*(4), 91-92.

Jang-Jaccard, J., & Nepal, S. (2014). A Survey of Emerging Threats in Cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973-993.

Johnson, M., Egelman, S., & Bellovin, S. M. (2012). Facebook and Privacy: It's Complicated. *SOUPS '12: Proceedings of the Eighth Symposium on Usable Privacy and Security*, Article No.: 9, 1–15.

Kowtha, S., Nolan, L. A., & Daley, R. A. (2012). Cyber Security Operations Center Characterization Model and Analysis. In *Proceedings of the IEEE Conference on Technologies for Homeland Security (HST)*, 470-475.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends. *Technology and Health Care*, *25*(1), 1-10.

Kshetri, N. (2006). The Simple Economics of Cybercrimes. *IEEE Security & Privacy*, 4, 33-39.

Lin, H. S., Spector, A. Z., Neumann, P. G., & Goodman, S. E. (October, 2007). *Toward a Safer and More Secure Cyberspace*. *Communications of the ACM*, *50*(10), 128. https://doi.org/10.1145/1290958.1290991

Kennedy, M. (2017). *Equifax hack shows we need more regulation.* Daily Herald. Infotrac Newsstand

Kranenbarg, M. W., Holt, T. J., & van Gelder, J. L. (2019). Offending and Victimization in the Digital Age:

Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap. *Deviant Behavior*, *40*(1), 40-55.

Levin, A., & Ilkina, D. (March 2013). *International Comparison of Cyber Crime*. Retrieved from: [link not accessible]

Li, X. (2018). Crucial Elements in Law Enforcement against Cybercrime. *International Journal of Information Security Science*, *7*(3), 140-158.

Lindsay, J. R. (2017). Restrained by Design: The Political Economy of Cybersecurity. Digital Policy, *Regulation and Governance*, *19*, 493-514.

Lim, H. S., Ghinita, G., Bertino, E., & Kantarcioglu, M. (2012). A Game-Theoretic Approach for High-Assurance of Data Trustworthiness in Sensor Networks. In *2012 IEEE 28th International Conference on Data Engineering.*

Laster, D. (2021, September 23). *Why The Era of Digital Transformation Is Important for Companies of All Sizes*. *Forbes*. Retrieved from: https://www.forbes.com

Maloof, M. A. (Ed.). (2006). *Machine Learning and Data Mining for Computer Security: Methods and Applications*. Springer Science Business Media

Mathieu, T., & Guy, P. (2015). A Framework for Guiding and Evaluating Literature Reviews. *Communications of the Association for Information Systems*, *37*(6), 6.

McGuire, M. (2018). *Understanding the Growth of the Cybercrime Economy*. Bromium.

Mijwil, M. M., Unogwu, O. J., Filali, Y., Bala, I., & Al-Shahwani, H. (2023). Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview. *Mesopotamian Journal of Cybersecurity*, Vol. 2023, 57–63.

Madden, M. (2012). Privacy Management on Social Media Sites. *Pew Internet Report*, *24*, 1-20. National Police Agency. (2013). White Paper on Police. Retrieved from https://www.npa.go.jp

Nguyen, K. D., Rosoff, H., & Richard, S. J. (2017). Valuing Information Security from a Phishing Attack. In *International Conference on Applied Human Factors and Ergonomics* (pp. 140-158). Springer.

O'Donnell, L. (March 2020). More Than Half of IoT Devices Vulnerable to Severe Attacks. *Threatpost*. Retrieved from https://threatpost.com

Ong, Y. J., Qiao, M., Routray, R., & Raphael, R. (2017). Context-Aware Data Loss Prevention for Cloud Storage Services. *IEEE 10th International Conference on Cloud Computing (CLOUD)*

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). *A Systematic Literature Review on the Cyber Security*. *International Journal of Scientific Research in Multidisciplinary Studies*, *9*(12). DOI: 10.18535/ijsrm/v9i12.ec04

Perwej, A. (2020). The Impact of Pandemic Covid-19 On The Indian Banking System. *International Journal of Recent Scientific Research*, *11*(10B), 39873-39883.

Perwej, Y., Hannan, S. A., Parwej, F., & Akhtar, N. (2014). *A Posteriori Perusal of Mobile Computing*. *International Journal of Computer Applications Technology and Research*, *3*(9), 569-578. DOI: 10.7753/IJCATR0309.1008

Perwej, Y., Haq, K., Parwej, F., & Mohamed Hassan, M. M. (2019). The Internet of Things (IoT) and Its Application Domains. *International Journal of Computer Applications*, *182*(49), 36-49. DOI: 10.5120/ijca2019918763

Parwej, F., Akhtar, N., & Perwej, Y. (2019). An Empirical Analysis of Web of Things (WoT). *International Journal of Advanced Research in Computer Science (IJARCS)*, *10*(3), 32-40. DOI: 10.26483/ijarcs.v10i3.6434

Perwej, Y. (2018). The Ambient Scrutinize of Scheduling Algorithms in Big Data Territory. *International Journal of Advanced Research (IJAR)*, *6*(3), 241-258. DOI: 10.21474/IJAR01/6672

Pasqualetti, F., Dorfler, F., & Bullo, F. (2013). Attack Detection and Identification in Cyber-Physical Systems. *IEEE Transactions on Automatic Control*, *58*(11), 2715-2729.

Perwej, A., Haq, K., & Perwej, Y. (2019). Blockchain and Its Influence on Market. *International Journal of Computer Science Trends and Technology (IJCST)*, *7*(5), 82-91. DOI: 10.33144/23478578/IJCST-V7I5P10

Perwej, Y., Haq, K., Jaleel, U., & Parwej, F. (2009). Block Ciphering in KSA, A Major Breakthrough in Cryptography Analysis in Wireless Networks. *International Transactions in Mathematical Sciences and Computer*, *2*(2), 369-385.

Punter, A., Coburn, A., & Ralph, D. (2016). *Evolving Risk Frameworks: Modelling Resilient Business Systems as Interconnected Networks*. *Centre for Risk Studies, University of Cambridge*.

Pan, J., Paul, S., & Jain, R. (2011). A Survey of the Research on Future Internet Architectures. *IEEE Communications Magazine*, *49*(7), 26-36.

Pan, J., Paul, S., & Jain, R. (2011). A Survey of the Research on Future Internet Architectures. *IEEE Communications Magazine*, *49*(7), 26-36.

Perri, L. (April 19, 2023). Top Strategic Cybersecurity Trends for 2023. *Gartner*. Retrieved from https://www.gartner.com

Reddy, G. N., & Reddy, G. J. U. (February, 2014). A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies. *ResearchGate*. Retrieved from https://www.researchgate.net

Sayeed, S., & Marco-Gisbert, H. (2019). Assessing Blockchain Consensus and Security Mechanisms Against the 51% Attack. *Applied Sciences*, *9*, 1788.

Stefanini Group. (2022). Cyber Security Statistics For 2022: List of Data and Trends. Retrieved from https://stefanini.com

Teoh, T. T., Zhang, Y., Nguwi, Y. Y., Elovici, Y., & Ng, W. L. (2017). Analyst Intuition Inspired High Velocity Big Data Analysis Using PCA Ranked Fuzzy K-means Clustering with Multi-Layer Perception (MLP) to Obviate Cybersecurity Risk. In *13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD).* 1790-1793.

Verizon Enterprise (2018). *Data Breach Investigations Report*.

Van Slyke, S. R., Van Slyke, S., & Benson, M. L. (2016). *The Oxford Handbook of White-Collar Crime*. Oxford University Press.

Vaz, R. A. N., Lord, S., & Bilusich, D. (December, 2014). From Strategic Security Risks to National Capability Priorities. *Security Challenges, 10*(3), 23-49. DOI: 10.2307/26241274

Wu, S., Chen, Y., Li, M., Luo, X., Liu, Z., & Liu, L. (2020). Survive and Thrive: A Stochastic Game for DDoS Attacks in Bitcoin Mining Pools. *IEEE/ACM Transactions on Networking*, *28*(2), 874-887.

