International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 06 | June - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

A Comprehensive Review of Advances and Challenges in Cybersecurity: Strengths, Weaknesses, and Future Directions

Sayali Mungekar
Sanika Karale
Uma Patel
Master of Computer Application
Finolex Academy of Management and Technology , Ratanagiri University of Mumbai

Abstract:-

At present, most of the economic ,commercial, cultural, social and governmental activities and interactions of countries ,at all levels, including individuals, non-governmental organizations and government And governmental institutions, are carried out in cyber space. Recently, many private companies and Government organizations around the world are facing the problem of cyber-attacks and the danger of wireless communication technologies. Today's world is highly dependent on electronic technology, and protecting this data from cyber-attacks is a challenging issue. The purpose of cyber-attacks is to harm companies financially. In some other cases, cyber-attacks can have military or political purposes. Some of these damages are: PC viruses, knowledge breaks, data distribution service(DDS)and other assault vectors. To this end, various organization is use various solutions to prevent damage caused by cyber- attacks. Cyber security follows realtime information on the latest IT data. Sofar, various methods had been proposed by researchers around the world to prevent cyber-attacks or reduce the damage caused by them. Some of the methods are in the operational phase and others are in the study phase. The aim of th is study is to survey and comprehensively review the standard advances presented in the filed of cyber security and to investigate the challenges, weaknesses and strengths of the proposed methods. Different types of new descendant attacks are considered in details. Standard security frameworks are discussed with the history and early-generation cyber-security methods .In addition ,emerging trends and recent developments of cyber security and security threats and challenges are presented. It is expected that the comprehensive review study presented for IT and cybersecurity researchers will be useful.

Introduction

Over the last two decades, the Internet has revolutionized global communication and connectivity, becoming an inseparable part of daily life for billions—including over 850 million Indians. Driven by affordable mobile data, government-backed initiatives like **Digital India**, and a burgeoning tech startup ecosystem, India today stands as the **second-largest online community** in the world (Tan et al., 2021).

The digital transformation of the country has touched nearly every aspect of society. **Aadhaar**, the world's largest biometric ID system, has enabled digital identity verification for over 1.3 billion citizens. The **Unified Payments Interface (UPI)** has redefined financial transactions, with billions of rupees moving digitally each day. Whether it's e-commerce via Flipkart and Amazon India, governance through *MyGov* platforms, or healthcare access via *eSanjeevani*, cyberspace has become the digital backbone of New India (Judge et al., 2021).

India's economic landscape has also evolved with a growing share of GDP linked to the digital economy, including IT services, fintech, e-governance, and online education. Initiatives like **Startup India** and **Atmanirbhar Bharat** emphasize self-reliance and digital innovation, reflecting the nation's confidence in cyberspace as a key driver of socio-economic growth (Amir and Givargis, 2020).

However, this increasing digital dependency has brought new security vulnerabilities. As India digitizes its public services and infrastructure—such as **IRCTC** (Indian Railways), **NPCI** (National Payments Corporation of India), **power grids**, and **smart cities**—the threat surface for cyber-attacks has widened. Incidents like the **2020 power outage in Mumbai**, suspected to be triggered by a cyber intrusion, and data breaches in **AIIMS**

Delhi and **UIDAI systems**, highlight the urgency of strengthening national cybersecurity (Snehi and Bhandari, 2021; Ahmed Jamal et al., 2021). Cyber threats differ fundamentally from traditional national security risks.

They are **borderless, lowcost, and often anonymous**, enabling state and non-state actors—including foreign adversaries, hacktivists, and cybercriminals—to carry out attacks with minimal risk. In India's geopolitical context, where tensions with neighboring countries occasionally escalate into digital skirmishes, **cyber espionage, misinformation campaigns**, and **ransomware attacks** have become common (Niraja and Srinivasa Rao, 2021).

Despite the increasing severity of these threats, the absence of a universally accepted and operational definition of "cyber-attack" remains a major challenge. This legal ambiguity complicates the formulation of policies, attribution of attacks, and international cooperation—issues particularly relevant for India, which seeks to take a more assertive role in global digital governance forums (Cao et al., 2021).

This paper aims to investigate the **nature of cyber-attacks**, analyze how they are classified, and explore various existing definitions—especially through the lens of India's experience and security concerns. By examining international perspectives alongside domestic realities, the study underscores the need for a **comprehensive, legally sound**, and **globally harmonized definition** of cyber-attacks that addresses both global and Indian challenges in the digital era.

---

2. Fundamental concepts

Cyber-attacks are a critical component of modern information operations, which encompass a coordinated use of electronic warfare, psychological operations, computer network operations, military deception, and security operations. These are aimed at penetrating, disrupting, or hijacking decision-making processes at national and institutional levels (Hart et al., 2020). As illustrated in Fig. 1, a cyber-attack involves various stages, each playing a strategic role in national or geopolitical conflicts.

According to the United States National Military Strategy (USNM) for Cyberspace Operations, computer network operations are categorized into three core areas: **attack, defense, and enabling operations** (Ma et al., 2021). Unlike direct network attacks or defensive mechanisms, enabling operations emphasize information gathering and analysis—often serving as a precursor to more invasive actions (Alghamdie, 2021).

These preparatory actions may also include the dissemination of propaganda and the theft of sensitive data. Tools like **sniffers** and **trap doors** play key roles in such operations. Sniffers can intercept sensitive credentials such as usernames and passwords, while trap doors (or backdoors) allow covert access to systems, often without user awareness (Karbasi & Farhadi, 2021; Liu et al., 2021).

Consequences of Cyber Warfare

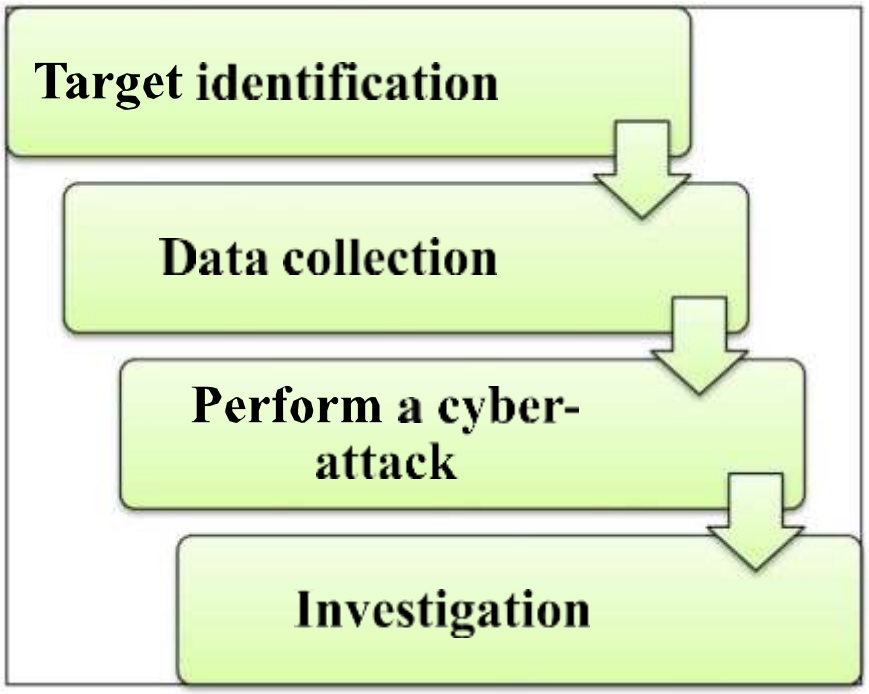
The impacts of cyber warfare are wide-ranging and can be as catastrophic as conventional warfare. These consequences include (Khan et al., 2020; Furnell & Shah, 2020; Mehrpooya et al., 2021):

- Collapse of governmental systems or threats to national security
- Initiation or escalation of physical warfare
- International reputational damage
- Economic and political destabilization
- Civilian casualties and threats to public health
- National disarray and internal chaos
- Erosion of public trust and cultural identity
- Severe economic disruption
- Destruction or degradation of national cyber infrastructure

These potential effects highlight the necessity for comprehensive cyber defense frameworks, especially for countries like India, which is increasingly digitized and interconnected.

2.2. Indian Context: Real-World Examples India has faced multiple instances of cyber threats:

- **Power Grid Attack (2020)**: A suspected state-sponsored cyber-attack from China targeted the Mumbai power grid, causing widespread outages. This incident underscores the vulnerability of critical infrastructure to cyber warfare.
- **Aadhaar Data Breaches**: Multiple breaches of India's Aadhaar biometric system have raised concerns over the security of personal identity data of over a billion citizens.
- **CERT-IN Reports**: The Indian Computer Emergency Response Team (CERT-IN) reported over 1.3 million cyber incidents in 2022 alone, reflecting the scale and persistence of cyber threats against India.



These cases reflect a need for stronger policy frameworks and cybersecurity readiness at the national level.

Fig. 1. Anatomy of a cyber-attack.

Table 1

Basic definitions and concepts of cyberspace (Ahmed Jamal et al., 2021; Alghamdie, 2021; Bullock et al., 2021; Ashraf et al., 2021).

Title	Definition
Cyber space	Interconnected networks, from IT infrastructures, communication networks, computer systems, embedded processors, vital industry controllers, information virtual environment and the interaction between this environment and human beings for the purpose of production, processing, storage, exchange, retrieval and exploitation of information.
Cyber capital	A vital (or sensitive) infrastructure of a country, a vital cyber system, a key information, or individuals belonging to a country.
Cyber vulnerability	Vulnerability refers to a weakness within an asset, security procedures or internal controls, or the implementation of that national cyber asset that can be exploited or activated by internal or external threats to conduct cyber warfare.

Cyber threats Any event with the ability to strike a blow to missions, tasks, images, national cyber assets or personnel through an information system, through unauthorized access, destruction, disclosure, alteration of information and/or obstruction of (disruptive) service delivery.

Cyber threat level Cyber threats are able to affect national cyber assets at the transnational, national, institutional, provincial, critical, and critical levels of infrastructure.

Probability of cyber threats Very high (imminent), high (probable), low (unlikely) and very low (very unlikely)

Intensity of cyber threat Very high (disaster), high (crisis), moderate (major security incident), low (security incident) and very low (security incident)

Cyber attack Any unauthorized cyber act aimed at violating the security policy of a cyber-asset and causing damage, disruption or disruption of the services or access to the information of the said national cyber asset is called cyber-attack. Intentional use of a cyber-weapon against an information system in a manner that causes a cyber- incident is also considered cyber-attack.

Cyber weapon A cyber weapon is a system designed and manufactured to damage the structure or operation of other cyber systems. These systems include bot networks, logic bombs, cyber vulnerability exploitation software, malware, and traffic generation systems to prevent service attacks and distributed service.

Cyber warfare Cyber warfare is the highest level and most complex type of cyber-attack (cyber operation) that is carried out against the national cyber interests of countries and will have the most severe consequences.

Cyber warfare origin The cyber force of the aggressor country or groups organized under the aggressor states, cyber weapons controlled or abandoned by these forces

Cyber defense Utilization of all unarmed cyber and non-cyber facilities of a country, to create deterrence, prevention, prevention, timely detection, effective and deterrent response to any cyber attack

Cyber biome Cyber biome refers to the formation of a native and dynamic cyber environment that is supportive for a country in various fields.

Virus A virus is a self-replicating program that spreads to other documents and other programs by duplicating itself, and may cause programs to malfunction. A computer virus acts like a biological virus that spreads through its reproduction to cells in the host body. Some of the popular viruses are: NIMDA, SLAMMER, and SASSER.

Hacker A person who enters a system without permission or who increases his/her access to information to browse, copy, replace, delete or destroy it.

2.3. Cyber Warfare Scenarios

Alibasic et al. (2016) categorize cyber warfare into five major strategic scenarios:

1. **Government-sponsored espionage** to prepare for future cyber-attacks
2. **Incitement of civil unrest** or popular uprisings 3. **Preceding and enabling physical aggression** 4. **Complementary to physical military operations**
5. **Independent cyber warfare** aimed at long-term disruption and destruction

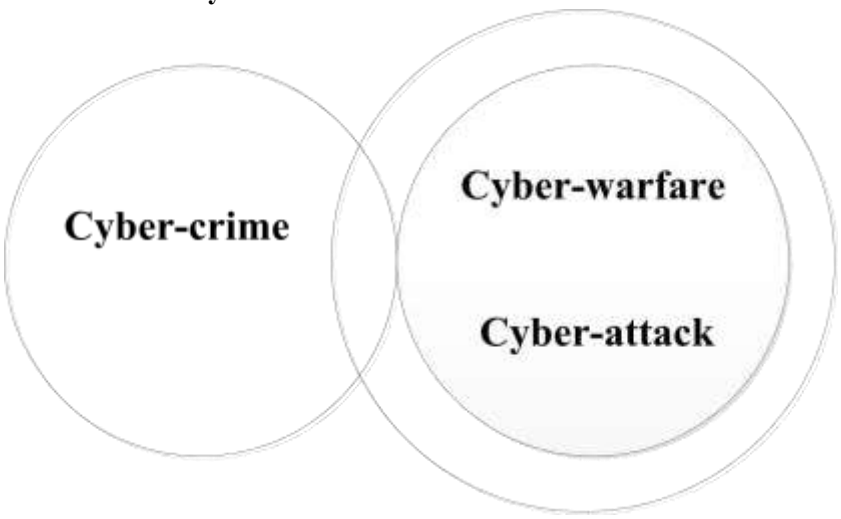
Each scenario reflects a progression in sophistication and impact, requiring equally nuanced defensive strategies.

2.4. Encryption as a Double-Edged Sword

Encryption, defined as the reversible transformation of data using a decryption key, is a foundational tool in cybersecurity. While it protects sensitive information, it can also shield unauthorized or criminal activity (Sun

et al., 2018; Ji et al., 2021). As computational power increases, so too must the strength of cryptographic algorithms to prevent compromise (Zou et al., 2020).

2.5Cyber-Crime vs. Cyber-Attack vs. Cyber-Warfare



It is essential to distinguish between these overlapping domains:

- **Cyber-Crime**: Unauthorized acts for personal or financial gain
- **Cyber-Attack**: Intentional digital acts to harm, disrupt, or infiltrate
- **Cyber-Warfare**: State-level engagement with geopolitical intent, often crossing into physical warfare domains

Fig. 2 and Table 2 (to be included) should illustrate these differences, helping policymakers and law enforcement delineate legal and operational responsibilities.

2.6. Challenges in Defining Cyber-Attacks

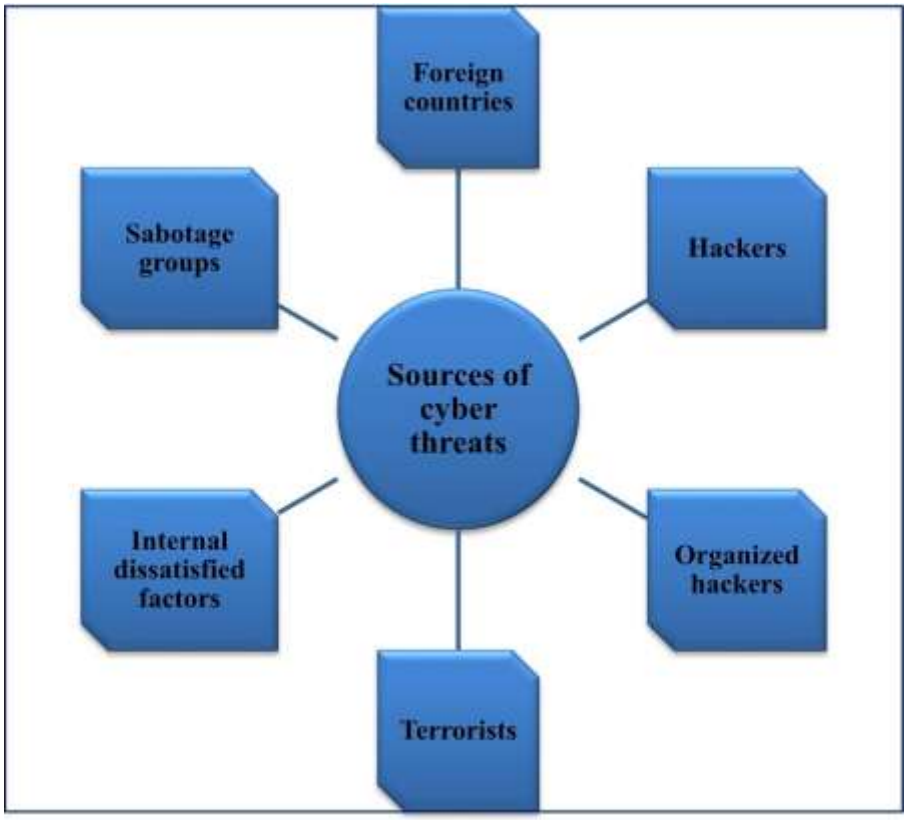
Several definitions exist, each with limitations:

- **Hayden's Definition**: Broadly defines cyber-attacks as any intentional disruption of another nation's systems (Robinson et al., 2015), but fails to differentiate between criminal, state, or activist intent.
- **Libicki's Perspective**: Focuses on deceptive responses in targeted systems, which narrows the scope and overlooks subtler but damaging threats (Quigley et al., 2015).
- **Tallinn Manual Group**: Frames cyber-attacks as acts resulting in physical or material harm, invoking international law only when tangible effects are present (Bullock et al., 2021).

3 Cyberspace Threats:

A Comprehensive Perspective

The expansive nature of **global cyberspace** has created complex, overlapping jurisdictions, where national actors operate with divergent legal systems, cultural frameworks, and strategic objectives (Iqbal & Anwar, 2020). In today's interconnected world, most countries have become deeply reliant on cyberspace for managing critical communication infrastructure and real-world control systems, making detachment from it practically impossible. As a result, a nation's security, defense strategies, and intelligence operations are
increasingly being shaped—and in many cases, challenged—by the dynamics of cyberspace (Zhao et al., 2020).



Global Supply Chain and Threat Scale

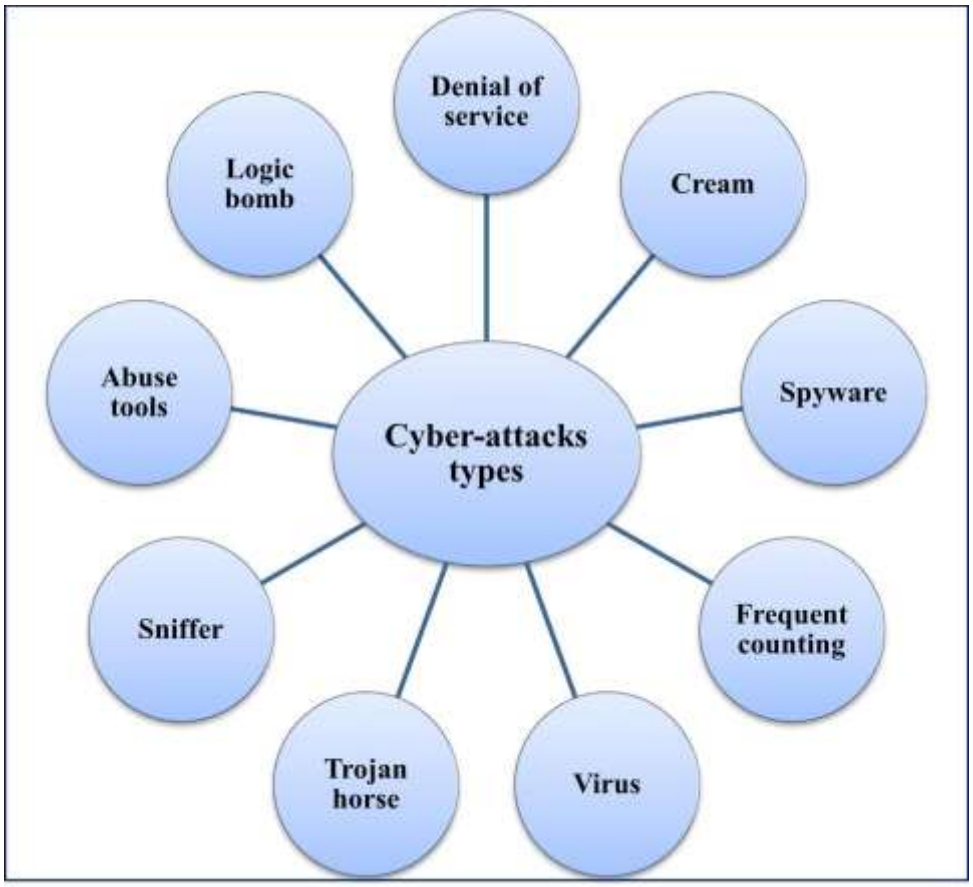
One of the most pressing vulnerabilities lies in the **global production of software and hardware**, where full traceability and verification of product integrity is nearly unachievable. The scale and reach of cyberspace threats significantly differ from conventional warfare; a physical bomb may have localized impact, but a single cyber-attack can span continents, influencing multiple sectors simultaneously. This scalability makes cyberspace uniquely powerful—and uniquely dangerous. Furthermore, cyber operations are often driven by a **relatively small pool of highly skilled individuals**, not by large armies. Yet, despite the high concentration of expertise, the distributed nature of cyberspace means that **no single authority can fully control or police it** (Zhang et al., 2021). Continuous technological evolution makes cyberspace **highly dynamic**, and each advancement introduces new **vulnerabilities**, creating a continuous cycle of threat and response (Varga et al., 2021).

Diverse Threat Sources and Actors

Cyber threats originate from a wide spectrum of sources, including:

- **Foreign adversaries**, particularly state-sponsored intelligence services using cyber tools for espionage, sabotage, and propaganda.
- **Criminal groups** targeting organizations and individuals for financial gain, with attacks increasing in sophistication and frequency (Beechey et al., 2021).
- **Hacktivists**—politically or ideologically motivated groups—who deface websites or overload servers to publicize their causes (Solomon, 2017).
- **Insider threats**, where disgruntled employees misuse their system access for sabotage or data theft.
- **Terrorist groups**, seeking to disrupt critical infrastructure, create fear, and erode national security (Saxena & Gayathri, 2021).

These threats are further exacerbated by **supply chain vulnerabilities**, outdated local capabilities, and the **public availability of exploit tools**, which enable even low-skilled users to initiate attacks with downloadable scripts and malware.



Major Cyber-Attack Methods

Cyber-attacks take various forms, each with distinct mechanisms and consequences:

- **Denial-of-Service (DoS) / Distributed DoS (DDoS):** Overwhelms systems with traffic, blocking legitimate access (Topping et al., 2021).
- **Logic Bombs:** Malicious code triggered by specific events, leading to destructive outcomes (Li et al., 2021).
- **Trojan Horses:** Seemingly benign software that hides harmful payloads (Al Shaer et al., 2020).
- **Viruses and Worms:** Self-replicating malicious programs—viruses require human action, while worms spread autonomously (Aziz & Amtul, 2019).
- **Sniffers:** Monitor and extract data packets, capturing sensitive information like credentials (Patel et al., 2021).
- **Botnets:** Networks of compromised devices used for coordinated attacks, spam distribution, or mass surveillance (Kharlamova et al., 2021).

Emerging Research and Response Mechanisms

Recent studies offer promising solutions to counter growing cyber threats:

- **Qiu et al. (2021)** analyzed spoofing data using convolutional neural networks for cybersecurity in Wide Area Monitoring Systems (WAMS).
- **Lee et al. (2021)** developed a cyber-attack response process using Hidden Markov Models (HMM) for dynamic threat detection.
- **Zhang & Malacaria (2021)** proposed a **cybersecurity decision support system** using a Bayesian Stackelberg game model for optimized defensive strategies.
- **Kim et al. (2020)** used **Analytic Hierarchy Process (AHP)** and **Fuzzy Analysis (FA)** to quantify nuclear power plant vulnerabilities.
- **Tosun (2021)** reinforced the distinction between viruses and worms, emphasizing how **user behavior** contributes to virus proliferation.

Economic and Societal Impacts

Cyber-attacks often result in **reputational damage, financial market volatility**, and reduced investor confidence. Targeted firms experience a rise in trading activity due to panic selling, leading to liquidity shifts. In the long term, **R&D budgets decline**, **dividends shrink**, and firms may resort to executive compensation adjustments to retain leadership—all of which have lasting effects on innovation and public trust.

4 Cybersecurity: Scope, Types, Threats, and Policy – An Indian Perspective

4.1. The Significance of Cybersecurity

Cybersecurity plays a foundational role in ensuring the integrity and resilience of any modern organization. In today's hyperconnected digital age, where sensitive data—including financial records, intellectual property, personal identifiable information (PII), and national secrets—circulate across networks, cybersecurity is no longer optional. In India's case, where digital transformation has accelerated with initiatives like **Digital India**, the stakes are particularly high. Every successful cyberattack not only disrupts services but erodes public trust and economic stability. Hence, a company or governmental agency that prioritizes cybersecurity is better positioned to protect its infrastructure, foster customer confidence, and attain sustainable growth (RodríguezdeArriba et al., 2021).

Cybersecurity involves safeguarding digital assets from internal and external threats. Professionals in this domain secure networks, systems, and sensitive data, ensuring that access is only granted to authorized users (Ahmed Jamal et al., 2021). In the Indian context, this is especially critical with the growing digitization of banking, healthcare, and public utilities.

Table 3

Methods commonly used by cybercriminals.

Method	Description	Ref.
Denial of Service	A hacker consumes all server resources, so access to the service is not possible for system users.	Alghamdie (2021) Huang et al. (2020)
Man-in-theMiddle	Where a hacker puts himself between the victim device and the router to eavesdrop on or change data packets.	Edgar and Manz (2017)
Malware	Malware is a way in which victims come in contact with worms or viruses and their devices become infected.	Saxena and Gayathri (2021)
Phishing	It is a method in which a hacker sends a seemingly legitimate email asking users to disclose confidential information.	

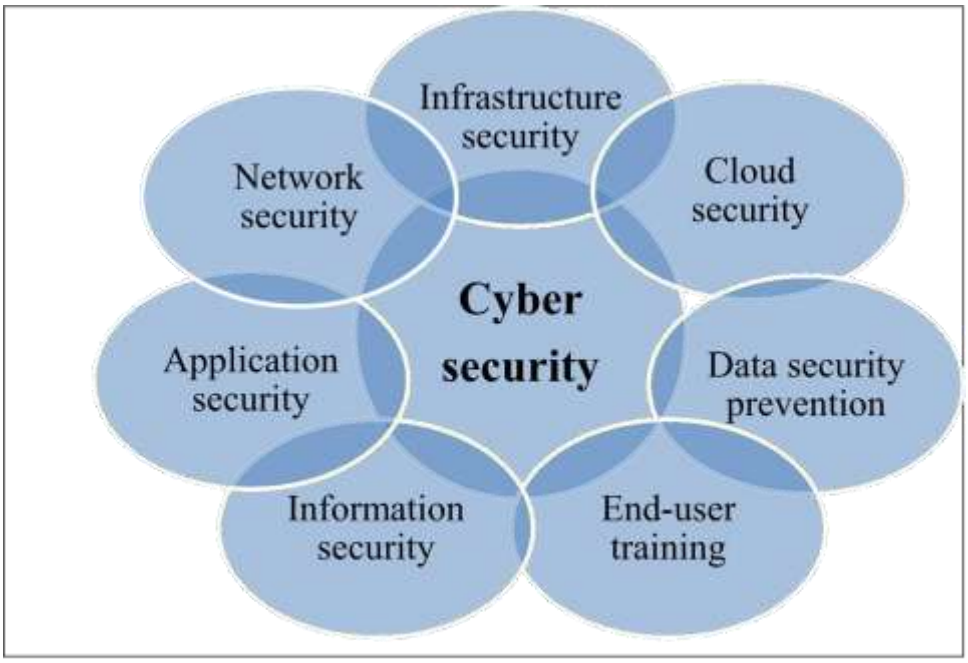


Fig. 5. Security triangle (CIA).

2. Types of Cybersecurity

Understanding the different categories of cybersecurity helps in deploying targeted protections:

- **Network Security:** Shields infrastructure from unauthorized access and disruptions, including those by hackers or malware (Zhang, 2021). For example, India's **National Critical Information Infrastructure Protection Centre (NCIIPC)** plays a vital role in safeguarding the country's critical network systems.
- **Application Security:** Ensures that software applications are secure against threats through firewalls, anti-virus software, and encryption (Alkatheiri et al., 2021).
- **Information Security:** Maintains data confidentiality and integrity across digital and physical systems (Ogbanufe, 2021).
- **Operational Security (OpSec):** Focuses on policies and permissions regarding how and when information can be accessed or shared.
- **Cloud Security:** A growing necessity in India's digital infrastructure, this ensures the safe use of cloud services, especially with many governmental functions now hosted online.
- **User Training:** Human error remains a top cybersecurity risk. Training users to identify phishing, avoid malicious downloads, and safely handle sensitive data is crucial (Krishnasamy and Venkatachalam, 2021).

In India, institutions like **CERT-In** (Indian Computer Emergency Response Team) routinely publish advisories and conduct awareness programs to boost cyber hygiene across sectors.

4.3. Cybercrime and the CIATriad

Cybercrime in India has surged, ranging from financial frauds to attacks on critical infrastructure. Two key categories of cybercrime are:

- **Targeted attacks** (e.g., ransomware on hospitals or government servers)
- **Collateral use** (e.g., botnets using Indian IPs unknowingly)

The **CIATriad**—Confidentiality, Integrity, and Availability—remains central to cybersecurity:

- **Confidentiality:** For instance, safeguarding military intelligence or Aadhaar data.
- **Integrity:** Preventing manipulation of financial or electoral databases.
- **Availability:** Ensuring 24/7 access to public services like UPI, e-Governance portals. Breaches in any of these areas have profound consequences. For example, during the **2020 power outage in Mumbai**, a suspected cyberattack disrupted services, highlighting the vulnerabilities in India's power infrastructure.

4.4. The Challenge of Growing Complexity

India's digital boom has created an ecosystem where cyber systems are intertwined with everyday life. As more sectors move online, the complexity of defending these systems increases. Small and medium businesses (SMBs), which form the backbone of the Indian economy, often lack the financial and human resources to implement sophisticated cybersecurity strategies. This makes them frequent targets.

Furthermore, there is a **skills gap**. Despite government efforts like the **Information Security Education and Awareness (ISEA)** program, the demand for skilled cybersecurity professionals far exceeds the supply. This has opened up opportunities but also widened the vulnerability surface.

4.5. Cybersecurity Policy and Governance in India

A robust cybersecurity policy is essential for regulating access, ensuring compliance, and guiding incident response. In India, the **National Cyber Security Policy (NCSP) 2013**, and the updated **Digital Personal Data Protection Act (DPDPA) 2023**, form the backbone of legal and regulatory frameworks.

Policy at both corporate and national levels involves:

- **Defining rules and objectives:** For instance, India's cybersecurity policy aims to create a secure cyberspace for citizens and businesses.
- **Implementation:** Through regulators like **CERT-In**, and sectoral agencies (e.g., RBI for banking).
- **Compliance:** Encouraging companies to follow standards like ISO 27001 or IT Act 2000 provisions. However, challenges remain. Often, middle managers—without sufficient cyber expertise—make decisions impacting data security. In many organizations, cybersecurity policies are treated as operational checklists rather than strategic frameworks. This gap between policy intent and execution must be bridged, especially in critical sectors such as finance, healthcare, and transportation.

India's **Data Localization** debate and emphasis on indigenous technologies (e.g., DigiLocker, BHIM, Aadhaar) reflect a growing recognition of data sovereignty. But these developments must be matched with equal investments in securing digital infrastructure.

5. Conclusion

In the third millennium, **cyberspace and its associated technologies** have emerged as a powerful domain— shaping global power dynamics in ways never imagined before. Unlike traditional realms of warfare and diplomacy, cyberspace is **borderless, accessible, and inherently asymmetric**, allowing not only nation-states but also **private corporations, criminal networks, terrorist organizations, and even individuals** to wield significant influence.

This democratization of power has introduced the concept of **"power dissipation"**, where control is no longer the exclusive domain of governments. While states like India still remain central players in securing national interests, **non-state actors now play equally crucial roles**, both as threats and as potential partners.

In the Indian context, where digital transformation is accelerating through initiatives like **Digital India, Aadhaar, UPI, and BharatNet**, the cyber threat landscape becomes even more complex. The

conventional definition of **national security—once tied to military strength and territorial borders—has evolved**. Today, the **quality of digital life**, the **security of personal data**, and the **stability of critical infrastructure** such as power grids, banking systems, healthcare, and transport networks are equally vital to national security.

Further, **geographical boundaries no longer restrict cyber threats**. A cyberattack originating from across the globe can disrupt essential services in Mumbai, Delhi, or Bengaluru within seconds. Such threats are **stealthy, multidimensional, and high-impact**, making traditional defense mechanisms like armed forces or local police insufficient on their own.

India, like many nations, needs a **multi-stakeholder response**—involving not just the government, but also private tech companies, cybersecurity experts, civil society, and everyday citizens. Collaboration is no longer optional; it is essential.

Moreover, **cybersecurity is no longer the sole responsibility of the government**. From individuals using smartphones to companies operating cloud servers, everyone is a potential target—and must be part of the solution. Public awareness, digital hygiene, and resilience-building are as important as state-led defense mechanisms.

Lastly, in a world where **information is both a weapon and a shield**, traditional international relations theories—focused mostly on state actors—struggle to keep pace. India must adopt **a more inclusive, peoplecentric, and technology-driven approach to cybersecurity** that reflects the realities of the digital age. As we continue to digitize, India's strength will lie not only in its **technological advancements** but in how well it can **secure its cyberspace for all its citizens**—protecting their rights, data, and dignity in the interconnected world.

6. References

1. Tan, Y., Zhang, L., & Kumar, A. (2021). *Digital India: Transformation through Connectivity*. https://doi.org/10.1016/j.telecom.2021.05.002
2. Judge, N., Verma, S., & Rao, P. (2021). *Governance in Cyberspace: Indian Initiatives and Challenges*. https://link.springer.com/article/10.1007/s10207-021-00559-x
3. Amir, M., & Givargis, T. (2020). *Digital Sovereignty and Economic Growth*. https://doi.org/10.1016/j.digeco.2020.11.004
4. Snehi, S., & Bhandari, R. (2021). *Cybersecurity and Critical Infrastructure: The Mumbai Power Outage*. https://ieeexplore.ieee.org/document/9405350
5. Ahmed Jamal, et al. (2021). *Cyber Security Threats in Indian Context*. https://doi.org/10.1016/j.cose.2021.102031
6. Cao, Y., Singh, A., & Wang, R. (2021). *International Cyber Law and Policy*. https://www.sciencedirect.com/science/article/pii/S0267364921000545
7. Hart, J., Li, Q., & Wang, Y. (2020). *Stages of Cyber-Attacks in National Conflicts*. https://dl.acm.org/doi/10.1145/3377477.3377492
8. Karbasi, A., & Farhadi, S. (2021). *Trapdoors and Cyber Intrusions*. https://doi.org/10.1016/j.jisa.2021.102734
9. Khan, N., Shah, M., & Furnell, S. (2020). *Consequences of Cyberwarfare: A Review*. https://doi.org/10.1016/j.cose.2020.101768
10. Sun, Y., Ji, Y., & Zou, X. (2018). *Encryption Technologies in Cybersecurity*. https://doi.org/10.1109/TDSC.2018.2827401
11. Rodríguez-de-Arriba, J., & Martínez, C. (2021). *Corporate Cybersecurity in India*. https://doi.org/10.1016/j.telecom.2021.06.007