HAS Terrorism become more challenging in the Cyber Age?

1. INTRODUCTION

- Terrorism has become challenging to deal with in the new cyber age.
- With the advent of fifth generation warfare, it poses an even bigger threat.

Thesis Statement:

while the modern age of technology has made people's lives easier, it has also increased the threat of terrorism by providing safe access to financing, recruiting and communicating networks for orchestrating attacks.

2. CONTEXTUALIZING THE DYNAMICS OF THE NEW CYBER AGE

3. TERRORISM A GREATER CHALLENGE IN CYBER AGE

3.1. New financing mechanisms used by terrorists that are harder to trace

→ Funding through bitcoin and crypto currency accounts

3.2. Control of state systems by hacking and malware installation

→ Access to grid systems causing

region wide outages

3.3 Breach of privacy and surveillance made easier

→ Access to camera and microphone of any device possible.

3.4 Financial terrorism by increased phishing and cyber attacks on banking institutions

→ Cyber attack on american bank in New York leading to loss of millions

3.5 Rise in mobility and ease of carrying attacks

→ remote Use of drone technology

3.6 Narrative building and manipulation of population by online platforms

→ Use of bots to promote a narrative against state

3.7 Access to undetectable recruiting applications for terrorist organizations

→ Telegram and Discord used to reach out to potential individuals

3.8 Communication channels of terrorists harder to trace

→ PUBG used by members of TTP for exchanging information

3.9 Increased vulnerability of state systems holding sensitive data to hacking

→ Cyber attacks on Indian government entities entities rose by 138%.

between 2019 and 2023.

RECOMMENDATIONS TO MANAGE THE CHALLENGES

4.1 Cooperation internationally through bilateral and multilateral organizations

→ Cyber security agreement pact signed at SCO Summit in 2025

4.2 Integration of blockchain technology and encryption.

4.3 Banning use of platforms with vulnerable security systems

4.4 Updating cyber security laws and legislations

CONCLUSION

- Terrorism has evolved with the advent of the cyber age
- International cooperation and security measures are integral to tackle the threats of terrorism.

The modern era is defined by major leaps in technology and innovation. The advancements have improved the lives of individuals across the globe. However, such rise has also proved to be harmful. One example is of terrorism which has adapted to the modern methods. Terrorists have amplified their activities over time, digital spaces posing a greater challenge in dealing with the menace. The cyber space has allowed new modes of financing terrorist organizations. Transactions are harder to trace, giving more power to terror groups world wide. Similarly, the introduction of hacking softwares has increased vulnerability of state systems to attacks. Such hacking also results in the loss of confidential information, posing great risks to the soverignty of nations. Additionally, electronic devices are vee vulnerable to data and privacy breaches. The information is leveraged by terrorists to further their agenda. The cyber age has also changed the dynamics of warfare, increasing mobility and ease of attacks. Damage can be done remotely from a distance, instead of traditional face to face attacks. The attacks are not limited to just physical damage but

also financial. Institutions like banks and reserves are the regular targets of terrorists as they create more instability and chaos chaos. State systems are more exposed today than ever before. Furthermore, the cyber space has opened opportunities to recruit and hire individuals. The spaces are harder to surveil and keep a check over. Terrorist narratives are easily shared and propagated through cyber channels, creating a wider impact on society. Communication between terrorist cells have also evolved. There has been a shift from radio & and cell phones to using game rooms of gaming applications. In order to deal with the threats, international cooperation between governments is imperative, as terrorism is a transnational threat threat. Encryption technology and firewalls need to be enhanced while cyber security laws need to be updated to address the issues head on. While the modern age of technology has made people's lives easier, it has also increased the threat of terrorism by providing safe access to financing, recruiting and communicating networks for orchestrating attacks against a state.

The new cyber age is characterized a change in the uptake and use of technology. Electronic devices have become increasingly common while softwares have become advanced and complicated. The features have improved while the security of sq systems have lagged over time. Devices today contain a plethora of personal information. Similarly, governments perform key tasks and keep confidential information on operating systems. This has thus been complemented by a rising interest of criminal and terrorist enterprises to breach sensitive data, and make governments vulnerable.

The cyber age whe threats and to society the terrorism front. Information systems are increasingly vulnerable in the current age. The following section will highlight some of the challenges posed by terrorism in the present day.

One of the foremost challenges is the use of new financing mechanisms by terror organizations. The use of technology and internet spaces to

[margin annotation in red: "sentence structure?"]

send Send and recieve transactions is on the rise. Payments are increasingly being made through Bitcoin and crypto currency wallets and mechanisms. The transactions that are hard to trace because instead of currency value, amounts flow in the form of coins. Such coins are later converted into currency. The new medium of financing provided by the new cyber age makes terrorism a greater great challenge.

Furthermore, the digital infrastructure rise has increased the risk of hacking and malware attacks. Terror cells use trojans and malware to hack and control state systems or infiltrate certain industries. One example is of the grid system, which is automated and online. Hacking into the system leads to the possibility of a a blackout in the electron region covered by the electricity grid. This is a vulnerability exposed to non state actors and terror cells around the world. Thus, the ability to hack state owned systems & to spread fear and chaos is yet another challenge to counter terrorism.

Additionally, the wide use of digital tools and devices connected to the internet exposes one to risk of privacy breach and surveillance. The camera and microphone of a device, for example, can be accessed anytime, while connected to the internet. Such vulnerability gives an opportunity to terrorists to monitore and surveil their a targets, making their goals easier to achieve. Therefore, the wide access and use of internet devices exposes one to privacy breaches, making targets easier to tackle for terrorist organizations.

Moreover, the cyber age poses great threats in the form of financial terrorism as well. The rise in phishing schemes in an evidence for the argument, wherein, people lose thousands of dollars every year to such scams. Cyber attacks on financial institutions like banks have also increased in frequency. Such attacks more damage the trust of society on the state, and induces great economic losses. An american bank in New York was the target of a cyber crime, which resulted

in the loss of millions of dollars. The rise of financial terrorism aided by the new cyber age, thus, makes tackling terrorism more challenging.

To add on, the digital age has made carrying out attacks easier and more mobile. Certain devices are used as form of modern warfare instead of the traditional methods of combat and fighting. One example is the prevalence of drone technology in warfare. Drones are mannuvered off site and can easily carry out attacks in remote regions, without physical presence. The prevalence of such tools in the cyber age has made warfare easy and deadly, making terrorism even harder to curb.

In conclusion, the digital and cyber age has brought many opportunities for society. It has created ease and enhanced connectivity. However, such facilities have now been adopted by non state actors like terrorist organizations. The cyber age has allowed easy communication, ready financing and mobile infrastructure for carrying out attacks. It has enhanced the vulnerabilities of state systems and institutions to malicious attacks and control by foreign actors. It has also amplified the security risks and threat to soverignty of a nation. To tackle the challenges on this front, strong cyber security laws and mechanisms are required. Similarly, international cooperation through bilateral and multilateral organizations is imperative. Only by adapting and improving enhancing current measures of cyber security, the new challenges of terrorism due to the cyber age can be effectively tackled.

Understanding of the topic is fine but focus on your sentence structure