M T W T F S ①

DATE:

"Cyber-crime is a bigger challenge for developing countries than developed countries"

Overall your arguments are okay
Structure is fine:
Improve introduction
Start with strong attention grabber
Improve your paper presentation

Outline:

1) Introduction
2) Decode the "cybercrime" and its types
3) Why Cybercrime is a bigger challenge for developing countries than developed countries?
   (i) Weak cyber security infrastructure to secure digital space (Case study of Sub Saharan countries)
   (ii) Inefficient legal system to reduce the threats of cyber-crimes (Case study of Pakistan)

(iii) Lack of skilled cyber-security personnel (Cyber-Security Index Report - 2021)

(iv) Less public awareness and digital literacy to avoid cybercrimes (Case study of India)

(v) Severe economic impacts of cybercrimes in developing countries (Bangladesh Money Heist)

(vi) Threathen public service delivery in developing countries (Ransomware attack on health system in Kenya).

(vii) Breach of data can threathen the national security of less developed countries (Indian cyber attack on Pak).

(viii) Damage to key infrastructure of developing countries
(Cyber attack of Russia on Ethiopia online infrastructure)

(ix) Exclusion of women from digital space due to online harassement
(Human Rights Commission Report)

4) How to reduce the threats of cybercrimes in developing countries?

(i) International collaboration to reduce cybercrimes in developing countries
(Case study of INTERPOL Organization)

(ii) Strengthening of legal infrastructure to reduce cybercrimes.
(Case study of EU)

(iii) Increasing digital literacy to decrease cybercrimes

M T W T F S

(4)

DATE:

(case study of Finland)

5- Conclusion

M T W T F S (5) DATE:

ESSAY

Just as technology has empowered people around the globe, it has threathen the security of people and states through cyber crimes. However, developing countries are more vulnerable to cybercrimes than developed countries. There are several reason to justify it. Firstly, cybercrimes act as a bigger challange for developing countries due to weak cybersecurity infrastructure and inefficient legal system. In addition, cybercrimes in developing countries increase economic crisis and jeopardise public service delivery. Moreover, breach of sensitive data can threathen the national security and key infrastructure of developing countries. In order to reduce the threats of cybercrimes, developing countries have to take certain corrective

measures. It includes increasing international collaboration, strengthening a legal infrastructure and increasing digital literacy. Thus, Cybercrime is a bigger challenge for developing countries due to weak cyber security infrastructure and less digital literacy. However, the cyber threats can be minimized by taking corrective measures.

Cybercrime is a crime which is committed with the help of technology. It has various types including ransomware attacks, data hacking and money frauds.

Firstly, cybercrime is a bigger challenge for developing countries due to weak cyber security infrastructure. There is unavailability of sophisticated technology to protect their digital space from cyber attacks. As a result, their

digital system are more vulnerable to cyber attacks. In contrast to developing countries, developed countries have invested in their digital infrastructure and adopted new technologies which reduce the threats of cybercrimes. For example, the Sub-Saharan countries are more vulnerable to cybercrimes due to lack of cybersecurity infrastructure to insulate their digital space from cybercrimes. Hence, developing countries are more vulnerable to cybercrimes due to less sophisticated cybersecurity infrastructure.

Secondly, developing countries are more vulnerable to cybercrime due to inefficient legal system to reduce the threats of cybercrimes. They do not have robust laws and institutions to reduce the incidents of cybercrimes. In contrast, developed countries have robust laws and institutions which prevent

cybercrimes. For instance, the Financial Investigation Agency (FIA) of Pakistan has less financial and human capacity to reduce cybercrimes. Hence proved, the inefficient legal system is the reason of increase cybercrimes in developing countries.

In addition, the lack of skilled cybersecurity personnel also increase the prospects of cybercrimes in developing countries. People are less skilled and efficient to find out ways to reduce cybercrimes. In developed countries, there are cybersecurity professionals who bring about new technology to secure their digital space. According to the Cybersecurity Index 2025 report, "Pakistan and Nigeria are more vulnerable to cybercrimes due to the presence of less experts to device measures to reduce cybercrimes." In short, less human

capital to secure digital space increases the threats of cybercrimes in developing countries.

Similarly, cybercrime is a bigger challenge for developing countries owing to less public awareness and digital literacy to avoid cybercrimes. People in developing countries have digital technologies but with less knowledge of using it. As a result, they fall prey to digital financial frauds. However, people in developed countries have more digital literacy and are techno-savvy. They are less prone to cybercrimes than people in developing countries. To illustrate, people in India have access to technology. However, they are more vulnerable to be a victim of digital money fraud due to less literacy [The Hindustan Times Report]. Thus, less digital literacy is also the reason

g developing countries vulnerability to cybercrimes.

Besides, there are severe economic impacts g cybercrimes in developing countries. They produce less GDP and the financial crimes through digital technology further increase their economic crisis. On contrast, developed countries generate more GDP and are generally prosperous, the cybercrimes do not threathen their economy like that g developing countries. To illustrate Bangladesh Money Heist is the best example g economic vulnerability g developing countries due to cyberattacks. It led to the loss g $81M from the Banks g Bangladesh and in turn increased their economic crisis. In short, cybercrimes act as a bigger threat to developing countries due to increase economic crunch.

In addition, it threathen the public servce delivery in developing countries. As developing countries are suffering from gavernance crisis, cybercrimes further reduce public servce. However, the developed countries are less vulnerable due to sophisticated technology which cannot be intercepted by malware attacks. For example, In Kenya, the health system was hindered due to ransomware attack it jeopardised the health of several patients. Hence, developing countries are more vulnerable to cybercrimes as it threathen their basic public servce delivery system.

Furthermore, the breach of sensitive data can threathen the national security of less developed countries. The data can be used by the enemy countries to threathen the survival of other countries. In contrast to developing

countries, the developed countries are adopting new technologies to increase their national security against cybercrimes. For instance, In 2019, India launched cyberattacks on the Defense Sector of Pakistan to extract sensitive information. However, its attempt failed. Thus, cybercrime is a bigger challenge for developing countries as it can threathens their national security.

Moreover, cybercrimes damage the infrastructure of developing countries. Their digital systems are less secured to malware attacks. Unlike developing countries, the developed countries have secured their infrastructure against cyber attacks. To illustrate, the cyber attacks of Russia on Kenya has damaged its digital infrastructure including online shopping and digital transaction system. Hence,

the infrastructure damage is another manifestation of developing countries vulnerability to cybercrimes.

Lastly, cybercrimes lead to the exclusion of women from digital space due to increase instances of online harassement. Cyber criminals breach the privacy of social media users especially women. This increases gender inequality in developing countries. In contrast to developing countries, women in developed countries, are more empowered to report the cases of cybercrimes. This increase the convection rate to cybercriminals and the digital space becomes more secure for women. According to the Human Right Commission Report, "There is a widening digital technology gap between man and woman." Women in developing countries, due to conservative

society, are forced to reduce their presence on digital platforms." Thus, cybercrimes threathen the digital presence of women in developing countries.

In the above paragraphs, the reasons of cybercrimes as a bigger threat to developing countries has been discussed. In the following paragraphs, the corrective measures for cybercrimes will be discussed.

Firstly, the international collaboration will be highly effective to reduce cybercrimes in developing countries. This will curtail their vulnerability to cybercrimes. For example, the International Police Organization (INTERPOL) provides an opportunity to developing countries to collaborate with developed countries to prevent cybercrimes. Thus, international collaboration provide opportunity

to developing countries to reduce the threats of cybercrimes.

In addition, the strengthening of legal infrastructure also reduces the chances of cyber attacks. The strict penalties and laws of each country would detter cyber criminals from their malpractices. To illustrate, European Union (EU) has devised effective laws and Intelligence Units to reduce cybercrimes. Hence, strengthening of legal system is indispensable for reducing cybercrimes.

Moreover, there is a need of increasing digital literacy to reduce the chances of cybercrimes in developing countries. As a result, people would differentiate between real information and fake information. For example, Finland inculcates digital literacy in its youth from early years of their

education. It reduces their vulnerability to cybercrimes. Hence proved, digital literacy is mandatory for reducing cybercrimes in developing countries.

In a nutshell, cybercrime is a bigger challenge for developing countries due to their less developed cyber infrastructure and public awareness. Moreover, it threathens their national security and public service delivery system. However, these vulnerabilities to cybercrimes can be reduced by taking corrective measures. These include increase international collaboration with developed countries and digital literacy. Thus, by all these measures, the digital technology will be used to benefit humankinds rather than threathen their survival in the 21st century.