

DATE ___/___/___

ENGLISH - ESSAY

Name: Hadia Khalid

CYBERCRIME IS A BIGGER CHALLENGE FOR DEVELOPING COUNTRIES THAN FOR DEVELOPED NATIONS

Outline:

I. Introduction

Definition

Background

Thesis statement: Cybercrime poses a more significant threat to developing nations due to weaker infrastructure, limited resources, and higher vulnerability than developed nations.

II. Cybercrime Landscape: Developing vs Developed nations

A. Overview of cybercrime globally

B. Comparative analysis of Target profiles

III. Factors exacerbating cyber crime challenges in Developing nations

A. Weak cyber security infrastructure

- Lack of upto date technology
- Inadequate internet security protocols.

B. Limited financial and human resources

- Insufficient funding for defense and education.
- Shortage of trained cyber security professionals.

C. Legal and Regulatory Challenges.

- Gap in cyber laws.
- Ineffective enforcement mechanism

D. Low public awareness and digital literacy.

- uninformed users as easy targets
- weakness in social engineering defenses.

IV - Social and Economic Impacts on Developing Nations

A. Disruption of critical services

- health, finance & energy sector

as well as
A. Financial Issues and Reputational Damage

• Impact on Foreign Investment
• Loss of public trust

C. Adapting to Digital transformation
• Ability to technological progress

V Case Studies

A. Examples from developing nations

B. Examples from developed nations

C. Comparative insights

VI Addressing the Disparity

A. Strengthening International Cooperation

B. Capacity Building and Training initiatives

C. Policy Reforms and law Enforcement

D. Raising Public Awareness

VII Conclusion

• Restate Thesis and main argument

• emphasize urgent need for multifaceted responses

• Call to action

Globally, cyber crime attacks have increased sharply in frequency and sophistication over recent years. Incidents including ransomware phishing, and data breaches are regularly reported against governments, corporations and citizens world wide. However developing nations are often targeted more relentlessly because their defenses remain inadequate, leading attackers to view them as 'softer' target.

Developed countries, typically poses extensive cyber security infrastructure, including advanced encryption, multilayered defenses and incident response capabilities supported by highly skilled professionals. They maintain robust regulatory framework and enforcement ecosystem. In contrast, developing countries like Pakistan lag behind due to underfunded systems, a shortage of trained experts and fragmented legal and institutional mechanisms. This mismatch exposes critical infrastructure, financial systems and citizens to greater exploitation.

DATE: ___ / ___ / ___

Pakistan's cyber security landscape suffer from several foundational weaknesses. Digital infrastructure trails behind developed nations, with out dated systems, insufficient encryption, and lack of comprehensive security protocols. Many institutions including banks and public agencies struggle to keep pace with new cyber threats.

Investment in cyber security is often sidelined in favour of urgent developmental needs. Pakistan faces a shortage of trained professionals, cyber security divisions within government and private organisations are often underfunded and understaffed.

Although, Pakistan has cyber laws such as Prevention of electronic Crimes Act (PECA), the legal framework is still maturing. Enforcement is inconsistent, prosecution is difficult, and jurisdictional issues often hinder justice. Most cyber crimes go unreported or unsolved.

Pakistan's A large portion of population lacks awareness

DATE: ___/___/___

of digital security. Even if they are aware they lack security practices. According to case study conducted by Hadia Khalid in University of Azad Jammu and Kashmir, university students don't follow security protocols despite awareness. People often use weak passwords, fall for social engineering tricks and don't secure their devices, allowing attackers easy access. Low digital literacy and makes the public more vulnerable to scams and frauds.

Here are social and economic impacts on developing nations. Cyber attacks have targeted Pakistan's banking sector, utility companies, and even healthcare systems, threatening to disrupt essential services. Attacks on national data base compromise the delivery of govt services.

Pakistani businesses report substantial financial losses due to ransomware and data breaches. Such incidents weaken foreign investor confidence and damage the global perception of

developing nations' business environment.

Cyber insecurity acts as a barrier to digital innovation and e-governance. Domestic and foreign stakeholders hesitate to adopt new platforms or invest in digital services, slowing economic growth and technological progress.

Here are a few case studies. In 2018, hackers breached major Pakistani banks, accessing sensitive financial data and causing consumer panic. Several banks temporarily suspended international transactions, highlighting systematic vulnerabilities.

While banks in the developed nations like US also face cyber attacks, their investment in multifactor authentication, rapid incident response, and insurance minimize direct and indirect damages and customers often recover lost funds swiftly.

The difference lies in preparedness, mitigation and recovery.

DATE / /

Developed nations generally detect and respond to the threats faster, while developing states, owing to their hurdles, endure longer disruptions and more severe fall outs.

There are few suggestions to address the challenge of cyber crimes.

Pakistan and its peers benefit from global intelligence sharing, joint investigations, and partnerships with agencies like Interpol and cyber units in developed countries.

International donors and NGOs sponsor training workshops and technology transfers. Expanding domestic education in IT and cyber security is equally pivotal.

Continued updating of cyber laws, swift implementation and enhanced law enforcement capabilities are vital to address new and evolving threats.

Nationwide awareness campaigns and digital literacy programs help citizens recognize and prevent fraud, creating

ATE: _ / _ / _

a more resilient society

Cyber crime's threat is acute for developing nations like Pakistan, where weaker infrastructure, resource shortages, and limited digital literacy aggravate their vulnerability. Addressing these challenges demands not only national reforms and investment but also collaborative international efforts, capacity building and public education. Without swift and coordinated action, the digital divide between nations may become a chasm exploited by cyber criminals, making global cyber resilience an urgent shared responsibility.