

"Outline"

Cybercrime is a bigger challenge for developing countries than for developed countries;

(01)

Introduction;

1.1: Hooke

On one hand, Internet has revolutionized the modern world but on the other hand, it has brought threats in areas of privacy, security and misinformation.

1.2: Thesis Statement

Developing countries are often more susceptible and vulnerable to cybercrime than developed countries due to many reasons such as Infrastructure and resources, vulnerability and exposure, Economic Impact, Human capital and awareness, Legal and regulatory frameworks.

(02)

Main Body;

2.1 Infrastructure and Resources

2.1.1 Developed countries

Developed nations typically have advance technological infrastructure, law agencies, financial resources to invest in cybersecurity measure.

2.1.2 Developing countries

Developing nations often lack the necessary infrastructure, including reliable internet access, secure data storage facilities and advanced cybersecurity tools.

2.2 Vulnerability and Exposure;

2.2.1 Developed Countries;

While still vulnerable, they are better equipped to detect, prevent and respond to cyber-attacks and have more established cybersecurity protocols.

2.2.2 Developing Countries;

Their reliance on digital technologies for various sectors including finance, communication, and preservation make them attractive for cybercriminals, who exploit their vulnerabilities for financial gain, espionage or disruption.

2.3 Economic Impact:

2.3.1 Developed countries;

Through insurance, robust financial systems and well established recovery plans they can better absorb economic consequences of cyberattacks.

2.3.2 Developing Countries;

The cyber-attacks can lead to financial losses, disrupting essential services and damage to national infrastructure further hindering the development efforts and exacerbate existing inequalities.

2.4 Human Capital and Awareness;

2.4.1; Developed countries.

Developed nations have a higher level of digital literacy and cybersecurity awareness among populations making them less susceptible.

2.4.2 Developing countries;

Limited access to education and training in cybersecurity can leave individuals more vulnerable to cyberattacks, including scams, malware or identity theft.

2.5 Legal and Regulatory framework

2.5.1 Developed countries;

They often have more comprehensive frameworks and international cooperation mechanisms to address cybercrime, facilitating investigations and prosecution.

2.5.2 Developing countries;

They lack legal capacity and resources to address, investigate and prosecute cybercrimes, leading to sense of impunity among preparators.

(3) EPILOGUE

Addressing the disparity caused by cybercrimes, require International cooperation, targeted assistance to strengthen cybersecurity capabilities and increased efforts to promote digital literacy and awareness.

"ESSAY"

American businessman and former CEO of Google, Eric Schmidt once stated; The Internet is the first thing that humanity has built but humanity doesn't understand, the largest experiment in anarchy that we have ever had. The internet that has created or we can say revolutionized the modern life, transforming how we communicate, access information and conduct businesses. Its global reach and interconnected nature have created unprecedented opportunities for connection, learning and economic growth, while also presenting challenges in the areas of privacy, security and misinformation. Cybercrimes refer to criminal activities conducted through computers and internet. It encompasses a wide range of offenses, from financial aid fraud and identity theft to attacks on critical infrastructure and national security. The rise of internet and digital technologies has created new avenues for criminals, making cyber crime a significant and growing threat globally. Cybercrime poses larger threats on developing countries than for developed countries due to a combination of factors like poor cybersecurity infrastructure, limited resources for combating crimes and a greater reliance on digital technologies for economic development. While developed countries have more robust

defenses, developing countries often struggle to protect themselves from sophisticated attacks, making them more vulnerable and susceptible to the negative consequences of cybercrime. 215

In developed countries, governments establish agencies like the National Cyber Security Centre (NCSC) in United Kingdom UK or the Cybersecurity and Infrastructure Security Agencies (CISA) in United States of America USA, to coordinate and national security efforts against cybercrime, share threat intelligence and provide guidance to critical infrastructure providers. Many developed countries invest in Public Key Infrastructure PKI to secure online communications and transactions. These countries have specific laws addressing cybercrimes, including hacking, data breaches and online fraud. These laws often provide outline penalties for offenders and provide responsibilities of various stakeholders. Developed countries often actively participate in international collaborations like INTERPOL's cybercrime initiative, to address cyber threats. Specialized law enforcement agencies such as the FBI's cyber division in US or the NCSC National Cyber security centre in UK, focus on investigating and prosecuting cyber criminals. In addition to all these, organizations like Cyble utilize AI-powered platforms to monitor darkweb, analyze threat data and

provide real-time insights to organizations and governments. Automation tools help manage the complexity of cybersecurity and improve response time. These efforts aim to prevent, detect and respond to cyber threats effectively, protecting critical infrastructure and sensitive data.

185

On the other hand, developing countries face significant challenges in combating cybercrime due to limited infrastructures and resources. Lack of cybersecurity can lead to confidential information being accessed by unauthorized persons and compromise the computer networks. According to Kaspersky Lab, in 2009 seven of the top 10 countries for creating Trojans, designed to steal passwords, were developing countries which accounted for 92 percent of such Trojans globally. Cyber-crimes footprints across the developing countries are getting bigger. To be able to reduce the threats and disruption caused by cyberattacks, the developing countries rely on the products made by western world and what is more important, they use the technology developed by the same country to protect their information rather than investing in their own resources. and advanced technologies like AI-based threat detection systems, encryption technologies and intrusion detection systems is

crucial. Developing nations do not give much importance to implementation of comprehensive cybercrime laws that can address various forms of cybercrime, including online harassment and have no investments in training programs for law enforcement, judiciary and other relevant personnel to enhance their skills in cybercrime investigation and prosecution.