The Issue of Cyber Crime

Cyber Crime is a fast-growing problem. Many criminals exploit the speed, convenience, and anonymity of the internet to commit crimes that cross borders and jurisdictions. They can cause serious harm and pose real threats to victims worldwide.

There is no single definition of cybercrime. However, there are two main types of internet-based crime:

- Advanced cybercrime – sophisticated attacks that are conducted against hardware and software. Examples include hacking into databases to steal information.
- Cyber-enabled crime – "traditional" crimes that have taken a new and advanced turn because of the internet-such as financial crimes, fraud, etc.

New trends in cybercrime are emerging all the time and estimates for the damage they cause the global economy run into billions or even trillions of pounds a year. Two of the latest trends in cybercrime are:

- Social engineering scams: This refers to a non-technical kind of intrusion, in the form of e-mails or social networking chats, that rely heavily on human interaction and often involves fooling victims into downloading malware or leaking personal data. Social engineering is highly effective for attacking well-protected computer systems with the exploitation of trust. Social networking becomes an increasingly important tool for cybercriminals to recruit money mules to assist their money laundering operations around the globe. Spammers are not only spoofing social networking messages to persuade targets to click on links in emails; they are taking advantage of users' trust of their social networking connections to attract new victims.

- Use of malware: malware generally takes the form of a virus, a worm, a Trojan horse, or spyware. In 2009, the majority of malware connected to Web sites registered was in the USA (51.4%), with China second (17.2%), and Spain third (15.7%). The primary way malware is distributed via email. It is truly international in scope.

In the past, cybercrime was mainly committed by individuals and small groups however now there are highly complex cybercriminal networks that bring together people from across the globe in real time to commit crimes on an unpreceded scale. Criminal organisations are increasingly turning to the internet to commit their activities and maximize their gains in the shortest possible amount of time. The crimes are not always new, and examples include theft, fraud, the sale of fake pharmaceuticals and illegal gambling. They are evolving with time, and they are able to become more widespread and damaging because of the internet.

Another form of cybercrime is state-sponsored cyber-crimes. This is when a country deliberately attacks a particular country, agency or company. An example of this is when North Korean Hackers allegedly attempted to steal $1,000,000,000 ($1 billion) from the Bangladesh Central Bank's account in the New York Federal Reserve by hacking their systems via malware on an email and sending false payment orders to hundreds of accounts across the world. This entire crime was made possible because of the internet and people being unaware of how to recognise and deal with spam emails.

Points to Consider:

- Is there a way to stop cybercrime on an international scale?
- Should there be a UN body that deals with Cybercrime or is it the member state's job?
- How will state-sponsored cybercrime be handled?
- What should the punishment for cybercrime be and who should enforce these punishments?

Useful Links:

- North Korean heist: https://www.youtube.com/watch?v=Usu9z0feHug&vl=en
- Interpol Cyber Crime website: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
- Hashed out Cybercrime statistics: https://www.thesslstore.com/blog/2018-cybercrime-statistics/