Cybercrime, Cyber law and cyber security related to cyberspace: Bangladesh perspective.

-Jubayer Ibn Kamal

Cybercrime, Cyber law and cyber security related to cyberspace: Bangladesh perspective

What is Cyber Crime?

Cybercrime is a criminal activity that targets or uses computers, computer networks, or network devices. Most cybercrimes are committed by cyber criminals or hackers who want to make money. However, sometimes cybercrime aims to harm computers or networks for reasons other than profit. These can be political or personal.

Cybercrime can be carried out by individuals or organizations. Some cybercriminals are organized, use sophisticated tactics, and are highly technologically proficient. Others are new hackers.

Categories of Cyber Crime

Generally, there are three major categories of cybercrimes that you need to know about. These categories include:

Crimes Against People- While these crimes occur online, they affect the lives of actual people. Some of these crimes include cyber harassment and stalking, distribution of child pornography, various types of spoofing, credit card fraud, human trafficking, identity theft, and online-related libel or slander.

Crimes Against Property- Some online crimes happen against property, such as a computer or server. These crimes include DDOS attacks, hacking, virus transmission, cyber and typosquatting, computer vandalism, copyright infringement, and IPR violations.

Crimes Against Government- When cybercrime is committed against the government, it is considered an attack on that nation's sovereignty and an act of war. Cybercrimes against the government include hacking, accessing confidential information, cyber warfare, cyber terrorism, and pirated software.

Types of Cybercrime

Identity Theft
This cybercrime occurs when a criminal gains access to a user's personal information to steal funds, access confidential information, or participate in tax or health insurance fraud. They can also open a phone/internet account in your name, use your name to plan criminal activity and claim government benefits in your name. They may do this by finding out users' passwords through hacking, retrieving personal information from social media, or sending phishing emails.

Cyberstalking
This kind of cybercrime involves online harassment where the user is subjected to a plethora of online messages and emails. Typically, cyberstalks use social media, websites, and search engines to intimidate a user and instill fear. Usually, the cyberstalked knows their victim and makes the person feel afraid or concerned for their safety.

Social Engineering
Social engineering involves criminals making direct contact with you usually by phone or email. They want to gain your confidence and usually pose as a customer service agent so you'll give the necessary information needed. This is typically a password, the company you work for, or bank information. Cybercriminals will find out what they can about you on the internet and then attempt to add you as a friend on social accounts. Once they gain access to an account, they can sell your information or secure accounts in your name.

DDoS Attacks
DDoS attacks are used to make an online service unavailable and take the network down by overwhelming the site with traffic from a variety of sources. Large networks of infected devices known as Botnets are created by depositing malware on users' computers. The hacker then hacks into the system once the network is down.

Botnets
Botnets are networks from compromised computers that are controlled externally by remote hackers. The remote hackers then send spam or attack other computers through these botnets. Botnets can also be used to act as malware and perform malicious tasks.

PUPs
PUPS or Potentially Unwanted Programs are less threatening than other cybercrimes but are a type of malware. They uninstall necessary software in your system including search engines and pre-downloaded apps. They can include spyware or adware, so it's a good idea to install antivirus software to avoid the malicious download.

Phishing
This type of attack involves hackers sending malicious email attachments or URLs to users to gain access to their accounts or computer. Cybercriminals are becoming more established and many of these emails are not flagged as spam. Users are tricked into emails claiming they need to change their password or update their billing information, giving criminals access.

Prohibited/Illegal Content
This cybercrime involves criminals sharing and distributing inappropriate content that can be considered highly distressing and offensive. Offensive content can include but is not limited to, sexual activity between adults, videos with intense violence, and videos of criminal activity. Illegal content includes materials advocating terrorism-related acts and child exploitation material. This type of content exists both on the everyday internet and on the dark web, an anonymous network.

Online Scams
These are usually in the form of ads or spam emails that include promises of rewards or offers of unrealistic amounts of money. Online scams include enticing offers that are "too good to be true" and when clicked on can cause malware to interfere and compromise information.

Exploit Kits
Exploit kits need a vulnerability (bug in the code of software) to gain control of a user's computer. They are readymade tools criminals can buy online and use against anyone with a computer. The exploit kits are upgraded regularly similar to normal software and are available on dark web hacking forums.

What Is Cyber Law?
Cyber law is any law that applies to the internet and internet-related technologies. Cyber law is one of the newest areas of the legal system. This is

because internet technology develops at such a rapid pace. Cyberlaw provides legal protections to people using the internet. This includes both businesses and everyday citizens. Understanding cyber law is of the utmost importance to anyone who uses the internet. Cyber Law has also been referred to as the "law of the internet."

The DSA, while of recent vintage, is not the first law to curb online freedom of expression in Bangladesh. The DSA was preceded by the Information and Communication Technology (ICT) Act 2006 (later amended in 2013). Since 2014, the ICT Act has come under harsh criticism as it was widely used to arrest and persecute individuals for expressing their views online. According to Human Rights Watch, Bangladeshi police filed nearly 1,300 charges from 2013 to April 2018 under the ICT Act.

Legal Perspective in Bangladesh

The Digital Security Act 2018 (DSA) was passed in Bangladesh in September 2018, to provide legal protection for digital information and electronic

transactions. The act also aims to prevent cybercrime and ensure the security of digital communications and information.

The DSA covers a wide range of activities, including hacking, identity theft, online fraud, the distribution of malware, and cyberstalking. It also includes provisions for the protection of sensitive information, such as personal data and confidential business information. The act also includes provisions for the protection of critical infrastructure, such as power plants and transportation systems.

The DSA also includes provisions for the punishment of individuals and organizations found guilty of cybercrime. Penalties can include fines, imprisonment, and the confiscation of assets. The act also includes provisions for the compensation of victims of cybercrime.

However, the DSA has faced criticism from civil rights groups and the international community, who argue that the act is overly broad and may be used to restrict freedom of speech and the press. In particular, critics have pointed to the vague and overly broad language used in the act, as well as the broad discretion given to law enforcement officials to investigate and prosecute cases under the act. In addition, several journalists, activists, and human rights defenders have been arrested under the act for their online activities and expression, which raised concerns about the use of the act to silence dissenting voices.

The Digital Security Act 2018 (DSA) in Bangladesh has been criticized for its potential impact on freedom of expression and the press. The act has been used to target and arrest journalists, activists, and human rights defenders for their online activities and expression. This has led to concerns that the act is being used to silence dissenting voices and disrupt the activities of journalists.

One of the main concerns with the act is its vague and overly broad language, which allows for a wide range of activities to be criminalized. For example, the act criminalizes spreading propaganda against the liberation war of Bangladesh, defaming the national fathers, hurting religious sentiments, and spreading rumors. This broad language has led to concerns that the act may be used to target journalists for reporting on sensitive political and social issues.

The act also gives broad discretion to law enforcement officials to investigate and prosecute cases under the act. This has led to concerns that the act may be used to target journalists and activists who are critical of those in power. In particular, there are concerns that the act may be used by those in power to silence dissenting voices and suppress criticism.

The DSA also criminalizes hacking and identity theft, which is a positive aspect of the act. But the scope of the Act is broad and it may be used to target and punish legitimate activities. For example, the act's provisions against unauthorized access to computer systems could be used to punish journalists who use hacking techniques to uncover information in the public interest.

Furthermore, the act's provisions for the protection of sensitive information, such as personal data and confidential business information, may be used to justify the criminalization of legitimate activities by journalists. For example, the act's provisions against unauthorized access to sensitive information could be used to punish journalists who uncover information in the public interest.

In conclusion, The Digital Security Act 2018 in Bangladesh has raised concerns about its potential impact on freedom of expression and the press. The act's vague and overly broad language, as well as the discretion given to law enforcement officials, have raised concerns about its potential misuse. There are concerns that the act may be used to silence dissenting voices and disrupt the activities of journalists, particularly those who are critical of those in power. It's also feared that the act may be used to financially ruin journalists and activists who are critical of those in power.