The Evolution of Crime: From Traditional to Cybercrime

Bikash Chandra Das

Apr 16, 2026

Abstract

This article traces the transformation of crime in Bangladesh from primarily physical offences to increasingly complex forms of cybercrime. Traditional crimes such as theft, robbery, murder, and corruption are described as having been shaped by economic hardship, political instability, and social inequality, while the expansion of internet access, mobile technology, social media, and digital finance created new opportunities for remote offending. The post discusses hacking, identity theft, phishing, online fraud, cyberbullying, misinformation, and mobile-banking scams as major examples of this shift. It also explains how cybercrime challenges conventional policing because offenders can operate anonymously and across geographic boundaries. Government responses include stronger digital-security laws, specialized cybercrime units, cybersecurity investment, digital forensics, and increasing collaboration with international partners. The article identifies low digital literacy as a major vulnerability, particularly for inexperienced users. It concludes that Bangladesh must continuously improve cybersecurity infrastructure, public awareness, legal frameworks, professional training, and digital resilience as criminal methods evolve alongside technology.



Over the years, the face of crime has been radically changed with the criminal activities becoming more complex and sophisticated into cybercrimes. In Bangladesh, the process of change of traditional crime into cybercrime also indicates the tendencies of the global scene, which is influenced by the rapid use of technologies, the popularization of the internet, and the development of a digital economy. Crime in Bangladesh was traditionally fueled mainly by choices to struggle economically, political instability and social inequalities. Nonetheless, due to the emergence of the internet, mobile technology, and social media, new types of criminal actions have appeared, transforming the world of crime in a previously unseen manner.

Previously, most of the crimes in Bangladesh were physical in nature. Some of the most prevalent crimes that were a menace in the country include theft, robbery, murder, and corruption. These types of crimes were mostly localized and the communities struggled with the economy and social consequences of these activities. The criminal justice system was also tense but was basically meant to process the traditional crime and the law enforcement agencies were interested in physical evidence, eye-witness accounts and direct investigations. Although this method was successful in several aspects, it started having serious problems with the advent of the digital era.

With the changing technology, crime also changed in nature. The term cybercrime, which not so long ago could be called a foreign term in Bangladesh, has become one of the most topical problems of the contemporary criminal environment. The development of the internet and the growth of the mobile phone use was a completely different setting whereby crimes could be perpetrated remotely, on a far greater scale. Contrary to the old types of crime, the cyber ones are not limited to a particular geographical area and that

is why they are more difficult to track and law enforcement activities are more difficult to cope with.

The initial phases of cybercrime in Bangladesh were fairly easy and the main actions included hacking, online fraud and identity theft. The perpetrators of these crimes used to be individuals or small groups of people that had the technical expertise to abuse vulnerabilities in the digital infrastructure. These crimes were mainly driven by financial gains since hackers were interested in robbing individuals and organizations of money, data or precious information. Cybercrime was perceived as a niche issue at this point at large, with its targets being large corporations or high-value targets.

Cybercrime started to target wider audience when internet penetration and e-business flourished in Bangladesh. Phishing attacks, in which fraudsters will attempt to steal valuable data such as credit card numbers or passwords, became even more common. The emergence of the social media created a new dimension of cybercrime, as an online harassment, cyberbullying, and the delivery of fake news became a common problem. Also, there was an improved sophistication in online frauds against individuals as scammers would employ social engineering tricks to lure people into revealing their personal and financial details. This introduced a different form of weakness since people were now more reliant on digital platforms to carry out their daily tasks like shopping, banking, and communication.

Cyber criminals especially targeted the banking industry. Cyberattacks on financial institutions increased in Bangladesh by a significant margin with the emergence of mobile banking and online payment systems. Unauthorized transactions, phishing attacks, and fake job offers were more widespread fraud attempts on mobile banking apps. Cybercriminals were given new avenues of exploiting the loopholes in the system as mobile money services were easily and quickly embraced by millions of people in Bangladesh and were convenient and easily accessible. There were frauds, identity thefts and mobile payment scams which were rampant causing big losses among people.

To counter the increasing menace of cybercrime, the Bangladesh government made a number of measures to reinforce the legal framework of digital security. One of the key steps in the fight against cybercrime was the creation of the Digital Security Act in 2018 that criminalizes such actions as hacking, data breaches, and dissemination of false information over the Internet. Although the law was perceived as a move towards the right direction, it has also been criticized because it may be abused and used in political motives. Opponents believe that the legislation can be taken to the extremes of censorship of freedom of expression and political opposition and bring up the question of how far is security and privacy in the digital realm.

A lack of digital literacy is one of the greatest issues in addressing cybercrime in Bangladesh. There are still a lot of citizens, particularly the rural population, who cannot even guess the fundamentals of online security and how to safeguard themselves against cyber threats. This information gap exposes them to online frauds, phishing, among other cybercrimes. Lack of a proper understanding on how to protect

personal information and detect frauds make possible most people to fall prey to cybercriminals. To solve this problem, the necessity to conduct the campaign of public awareness aimed at educating the population about the danger of cybercrime and the ways to remain safe on the Internet is increasing.

Even with these challenges, some steps have been made to deal with cybercrime in Bangladesh. Over the last few years, the number of cybersecurity specialists, digital forensics specialists, and special law enforcement units that focus on combating cybercrime has been rising in the country. The business sector has also increased its activities and a great number of corporations are making investments in the cybersecurity measures to safeguard their online resources and consumer information. This increased vigilance and the desire to invest in cyber security plays a vital role in combating cybercrime because business and individuals are becoming more involved in protecting their presence on the internet.

Cybersecurity industry has also emerged in Bangladesh due to the emergence of cyber-crime. With the expected growth in the digital presence of businesses, both local and international, the need of cybersecurity professionals, and services, has been increasing. This has brought fresh employment opportunities in the technology industry and has opened the frontier to the emergence of special cybersecurity training courses. Additionally, it has been emphasized more on working closely with international organizations and law enforcement agencies to share information, resources and best practices in combating cybercrime.

Although cybercrime is dynamic in Bangladesh, it is no doubt that in future the nature of crime in the country will be determined by the current digital revolution. Cybercriminals will develop the tools that they use as technology advances. Bangladesh will have to keep its digital security infrastructure, culture of digital literacy, and the legal framework on cybercrime up to date to successfully deal with the challenge of cybercrime. The government, the private and civil society should collaborate to create a safer digital world to everyone so that the positive side of the digital era is not seen to be overshadowed by the dangers of cybercrime.

To sum up, it is essential to note that the transformation of the traditional crime to the cybercrime in Bangladesh is a global trend that is triggered by the technological progress. Although cybercrime is a big challenge it provides opportunities in the cybersecurity industry, creation of jobs and online education. Through sound investment in cybersecurity, improved civil awareness, and improved legal regulations, Bangladesh will be able to overcome the challenges of the digital era and create a more secure digital future of its people.