**Dark cyber world**

BY M A R I A T A I M U R 2021-12-28

THE last two decades, and especially the last two years that have been marked by the Covid-19 pandemic, have made all of us more dependent on technology including the internet, to carry out bank transactions, shop, pay utility bills, etc. But the more we use technology, the more we are exposed to cybercrime or digital crime.

Cybercrime can take the shape of hacking, online financial fraud, identity theft, cyberbullying, cyber harassment, child pornography, data theft, cyberstalking, cyber extortion, crypto jacking and cyberespionage. It falls into two main areas: criminal activity that targets computers and criminal activity that uses computers to commit crimes.

Given its quantum all over the world, it is becoming more and more dif ficult to tackle cybercrime. As opposed to traditional crime where material objects are stolen or people are physically hurt, cybercrime operates in the shadows. For this reason, the community and law-enforcement agencies give more attention to the more obvious non-cybercrime.

The ease with which cybercrime is committed, without risking the perpetrator`s identity, liberty or life, makes it a lucrative exercise that does not require much skill.

Any person with access to technology can breach the privacy of another individual, with or without their knowledge.

Online financialfrauds,identity theft and phishing of information are rampant and most ordinary computer users are unable to detect foul play. It is also not known to most users whether or not the company whose product they are using has good cybersecurity. In our daily lives, we share our personal data on too many online spaces.

On the detection side, what makes cybercrime equally, if not more, challenging, is the fact that there are very few complaint channels to report to or to investigate the crime. Most police resources are diverted towards maintenance of law and order and the prevention of crime. Special laws are enacted for digital crimes, and law-enforcement agencies given the specialised task of investigating such crimes mostly remain understaffed and resource-deficient.

There are three crucial areas to look into in order to curb digital crime. One is awareness of the crime itself, the second is prevention and the third is curbing such crime.

Awareness is very low and victims of cybercrime usually don`t know about complaint mechanisms. An additional challenge is the time consumed in first getting the complaint verified and then routing it through different data corporations in order to receive legitimate responses.

Awareness of cybercrime is the collectiveresponsibility of the community and police.

In most cases of digital crimes against girls or women, the victims are hesitant to go through the process of reporting the crime for fear of stigma and lack of support from their families. Just as in other crimes, they are required to approach law enforcement for recording their statement and following up. This proves too cumbersome and many women opt out of even reporting the crime.

In the case of children, community stakeholders mainly comprise of parents, teachers, schools and police. If suf ficient information is available to the community about how they can avoid such crimes and what to do in case a crime is committed, prevention and detection become easier. Cybercrime against children mostly occurs through friend requests on social media, where the child faces indecent exposure, image violence, blackmailing and bullying.

For controlling cybercrime, linkages are identified between crimes in virtual and real space. Identifying websites, the dark web and internet centres used for cybercrime andmapping cybercrime helps prevent and control crime. Effective prevention is helped by prior identification of targeted groups, including the latter`s gender and age bracket.Lessons can be learnt from the way the US has countered cybercrime. A training and technical assistance programme provides task forces and their affiliates the training and technical assistance needed to conduct effective investigations and prosecutions.

The programme helps identify social networking sites, peer-to-peer file sharing, wireless networks and mobile phone technology that is used to exploit victims.

It also incorporates training for law enforcement, prosecutors and other stakeholders to improve their investigative, prosecutorial and forensic capabilities; create and distribute information on guidelines, best practices and investigative methodologies; and coordinate meetings with practitioners. For victim support, the programme has a comprehensive mental health and wellness programme to address the trauma that cybercrime victims experience.

In order to enhance cybersecurity to protect our lives and communities, we must invest collectively in awareness campaigns.

Police must be trained ef ficaciously to build an active response plan and implement it.  The writer is a police officer.