Cybercrime: Modern Criminal Law Challenges

By: Mustafa Riaz
Reviewed By: Ritaj Habib

Introduction

What good is social media when we cannot combat its main consequence, cybercrime. Social media is useful in various aspects like education and socialization, but when criminals exploit technology to commit various crimes, including theft, fraud, and even terrorism, Social media then turns out to become a place where we can be threatened for almost anything, leaving cybersecurity as a necessity to combat it. Despite efforts to combat cybercrime, law enforcement agencies often struggle to keep pace with the rapidly evolving tactics employed by cybercriminals. Traditional methods of investigation and prosecution are frequently inadequate when applied to the complexities of cyber offences. As a result, there is a pressing need to evaluate and enhance existing legal frameworks and enforcement strategies. Research shows that an average of 97 victims worldwide are affected by cybercrime per hour, this means there is a victim of cybercrime every 37 seconds! If we simplify this, thousands, if not millions worldwide get affected by a simple act which people either may think is funny to do instead or take it as a hobby. This article will present the ongoing commitments made by digital forensics as well as the international community to deter the rate of cybercriminal activities and what is holding them back, so we can combat it.

Ongoing Commitments:

Cybersecurity, being a major criminal activity has been observed by major global organizations with the urge to end it. The United nations serves as a global institution where solutions for major problems like this are being found. *The United Nations Convention on Cybercrime*, which was proposed in 2017 by Russia, has been adopted through *Resolution 79/243* on the 24th of December 2024. *Resolution 79/243* calls for the awareness of cybercriminal activities and to prevent it as mentioned in preamble 12, *"Decides that, in order to raise awareness of cybercrime and of the role of the Convention in combating and preventing it, 24 December should be designated International Anti-Cybercrime Day".* The UN convention on cybercrime article 7, 8 and 9 states such punishments of these activities are recognized as criminal offences, showing how keen the UN is on combating cybercrimes on a global level.

Moving on, other nations that have growing cybercriminal activities such as the state of Qatar have embedded cybercrime laws into their constitutions such as Law no.11 of the constitution of the state of Qatar. *"Law No. 11 introduces a new provision, Article 8 (bis), into Qatar's 2014 Cybercrime Law, directly targeting the unauthorized use of personal images and videos online and penalizes such acts up to USD $27,500 and 5 years of imprisonment"* – these steps encourage other nations to follow the same and thus collectively combat cybercrime. Another example followed by Qatar is to educate the youth on the consequences of social media and the cybercriminal activities (perhaps through the Ministry of Education and Higher Education (MoEHE) project, "My Values Shape My Identity – 2026").

The main issue in cybersecurity is identity theft. Countries who have acted in securing online identity like Australia who have implemented the *"Online Safety Amendment (Social Media Minimum Age) Act 2024"* which bans the usage of social medias for people under 16, lowering identity theft and allowing opportunities for young teens to be aware of cyberattacks.

Current issues on combating cybercrime:

Despite global and domestic efforts, cybercrime is still shown as a major issue as third world countries lack the technology and expertise to combat this issue, making them prone and vulnerable to cyberattacks. Furthermore, cybercrimes are difficult to prevent due to the lack of security systems. "*In 2023, data breaches cost businesses an average of $4.88 million"*

Many people have no knowledge on how social media works and what are their negative outcomes, making them easy to attack. The lack of understanding and awareness of digital security practices can lead individuals or organizations to overlook basic security issues, such as updating passwords. Many individuals or organizations would press a link curiously, not knowing it may well be a worm or a trojan horse that can allow hackers to steal their personal information. "*In 2021, 323,972 internet users reported falling victim to phishing attacks. This means half of the users who suffered a data breach fell for a phishing attack"*. During the height of the pandemic, phishing incidents rose by 220%.

Social engineering is the act of exploiting a user's emotions into making them give their personal information. What makes it dangerous that it is conducted in the form of emails(phishing) that look like legitimate companies or calls that claim they are from their insurance company, requesting for the user's personal information. The lack of knowledge of social engineering make a person vulnerable to such attacks. *"In 2016, the US department of justice was hacked from a social engineering attack that leaked the information of 20000 FBI and 9000 DHS employees. The hacker claimed that he downloaded 200 GB of sensitive government files out of a terabyte of the data to which he had access".*

Conclusion

To sum it up, the globe has made considerate effort to reduce cybercrimes by limiting social media, educating students on the internet and its negative as well as positive effects, penalizing cybercrimes as well as countries embedding cybercrime acts into their constitutions. The United Nations have also played a role by adopting the UN convention on cybercrime that was proposed in 2017 by Russia. But problems like the lack of awareness which has cost hundreds of thousands of user's personal information, the lack of security strategies and systems which has costed companies millions of dollars and social engineering, which has taken hits on large intelligence organizations like the FBI.

SOURCES:

- https://aag-it.com/the-latest-cyber-crimestatistics/#:~:text=With%20an%20average%20of%2097,their%20data%20leaked%20eve ry%20second.
- https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870057820240001000023
- https://www.unodc.org/unodc/en/cybercrime/convention/home.html
- https://www.researchgate.net/publication/396417537_Cybercrime_Challenges_and_Solutions_in_Law_Enforcement_in_The_Digital_Era
- https://docs.un.org/en/A/RES/79/243
- https://aag-it.com/the-latest-cyber-crimestatistics/#:~:text=What%20was%20WannaCry?,service%20around%20%C2%A392%20 million
- https://indonet.id/factors-causing-cyber-crimes-to-easilyoccur/#:~:text=Cybercrimes%20often%20occur%20due%20to,facilitate%20the%20actio ns%20of%20cybercriminals.
- https://www.infosecinstitute.com/resources/security-awareness/the-top-ten-most-famoussocial-engineeringattacks/#:~:text=The%20social%20engineering%20attack%20against,name%20in%20the %20signature%20line.
- https://www.legislation.gov.au/C2024A00127/asmade/text