IAP NEWS

IAP INTERNATIONAL ASSOCIATION OF PROSECUTORS

#91, November 2023

Specifics of the fight against cybercrime in the Republic of Armenia

By Anna K. Vardapetyan, Prosecutor General of the Republic of Armenia

The fight against cybercrime is a pressing concern that affects us all in this digital age. As our world becomes increasingly interconnected, the threat of cybercrime looms larger than ever, including individuals, the justice system, the business sector, and the entire national security.

To combat cybercrime effectively, we must first understand its root causes. Often, it stems from the exploitation of vulnerabilities in our digital infrastructure, as well as the lure of financial gain for those who engage in criminal activities online. Understanding criminals' motivation, prevention measures, effective investigation, stringent laws, capacity building, and comprehensive international cooperation are key elements of the fight against cybercrime.

Our analysis identified two types of crimes often committed using digital technologies in Armenia: cyber-theft and illegal drug trafficking.

Cyber-fraud is driven by a combination of financial incentives, technological opportunities, and various reasons, including:

> *The fight against cybercrime is a collective endeavour. It requires enhanced cooperation and support of communities, law enforcement agencies and policymakers.*

Anonymity: the internet provides a degree of anonymity, allowing cybercriminals to operate with reduced risk of identification and apprehension.

Low Barrier to Entry: Engaging in cyber-fraud requires little physical presence, minimal resources, and limited technical expertise, making it accessible to a wide range of individuals, including those with criminal intent.

Global Reach and Rapid Technological Advancements: Criminals adapt to new technologies and exploit emerging vulnerabilities.

Lack of Awareness: Many individuals and organisations are unaware of the various cyber threats and may not implement adequate security measures, making them vulnerable targets for cyber fraud.

Desire for Information: Some cybercriminals seek to steal sensitive information, such as personal data, intellectual property, or trade secrets, to gain a competitive advantage or sell the stolen information on the dark web.

In some cases, criminals use more complicated mechanisms, taking advantage of the software errors or gaps of the non-cash transaction systems, e.g., taking advantage of the devices which record the inflow and outflow with some delays.

Cyber-theft investigations also face certain difficulties. Usually, the necessary information is possessed by corporations operating in foreign jurisdictions (e.g. Facebook, Viber). It takes a long time for the investigator and the prosecutor to address the MLAR, which is time-sensitive due to the crime. The MLAR responses are also not prompt. As a result, belated responses negatively affect the investigations.

Studies regarding the illegal sale of narcotics by social websites and telecommunication applications show a significant increase in illegal drug trafficking in recent years. In many cases, the narcotics were sold over Telegram, which, known for its encryption and privacy features, has unfortunately become a favourable platform for these illicit activities.

The rise in drug trafficking over Telegram is a grave concern for several reasons:

Global Reach: Telegram's widespread use provides drug traffickers with a vast and anonymous network to conduct their illegal trade.

End-to-End Encryption and Anonymity: Users can join Telegram channels and groups without revealing their true identities. In this regard, it should be noted that some information on cryptocurrency transactions may not be encrypted. It could be possible to obtain relevant data on the chain of financial means, relevant accounts, payment instruments, and the actors.

Ease of Transactions: Telegram offers a convenient platform for buying and selling drugs, often using cryptocurrencies to hide financial transactions.

In this regard, the effective use of criminal procedural measures and operational tools, together with financial investigation, are indispensable factors in determining the success of cybercrime investigations. In order to detect cases of illegal drug trafficking through the internet and effectively address cybercrime, the mentioned measures should be conducted simultaneously. It is important to obtain complete information about the used Apps, subscriber data, IP addresses, payment methods, and other relevant information. Also, continuous capacity building, professional training for the investigators and prosecutors, and the introduction of effective investigative techniques should not be underestimated in effectively preventing and addressing this constantly evolving crime.

The role of prosecutors is also crucial in this context. Prosecution is responsible for gathering evidence, building cases, and ensuring that those involved in drug trafficking face the consequences of their actions. Prosecutors must navigate the intricate legal frameworks to bring these criminals to justice.

Prosecutors should also coordinate interagency cooperation and collaborate with involved stakeholders, which is vital in the successful prosecution of drug traffickers.

In conclusion, it should be noted that successful investigation and prosecution of cybercrimes depends on effective and timely communication mechanisms between foreign agencies and domestic inter-agency cooperation, effective legislation and investigation guidelines and technical skills of the involved professionals to face the challenges of new technologies and address them accordingly.

View Main
Newsletter
Online