Паламарчук В.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: Могилевська В.

CRIME AND TECHNOLOGY

New technological innovations have been developed to prevent crime and to improve the performance of the police, but we know remarkably little about how and why certain innovations are adopted, and the consequences –both intended and unintended - of technology-driven solutions to the problem of crime [1].

While many technological advances play an important role in a wide range of criminal activities, none has likely had greater impact or influence than the internet. Just as internet can be used to enhance and augment the daily lives of everyday citizens, and the functioning of businesses and services, it has not only given rise to a completely new form of crime, but can facilitate or assist criminality across almost all other crime areas. The internet is of course fundamentally a source of information, and an environment where communities of like-minded individuals can meet. The list of information that could be used to assist criminals is essentially endless, but key examples include access to detailed map data, including satellite and street-views for reconnaissance, shipping routes and schedules, tutorials, guides and recipes for drugs or explosives, and tips on operational security.

Cybercrime is a global phenomenon, and is as borderless as the internet itself. The attack surface continues to grow as society becomes increasingly digitised, with more citizens, businesses, public services and devices connecting to the internet. Moreover, the potential for one attacker to affect many victims is scaling exponentially. The term ‘cybercrime’ encompasses a broad range of different criminal threats however. The most threatening aspects of cybercrime involve crimes such as the distribution of ransomware and other malware, fraud involving non-cash payments and the online trade in child sexual exploitation material.

It is clear that that any developments in the use of technology by criminals must be matched and countered by an appropriate and effective law enforcement response. There is an obvious challenge here for law enforcement to not only keep pace with new technological developments, but with emerging crimes and a continually changing threat landscape. Cybercrime, as a relatively new crime area, is a good example of this, and poses many challenges peculiar to that crime area. Attribution – determining who is behind an attack, and where they globally are located, is especially challenging, particularly in an environment where cybercriminals

share tactics and tools with malicious actors with other motivations, such as hacktivist or nation state actors [2]. Furthermore, many aspects of cybercrime are developing rapidly, requiring specific expert knowledge and the use of cutting-edge investigative techniques and advanced digital forensic tools.

In order for law enforcement to effectively fight technology-enabled crime, it must of course embrace technology itself. Technology can also be a significant aid to law enforcement authorities in the fight against serious and organised crime, often using the very same technology abused by criminals. For example, mapping and geo-location tools have proved to be invaluable for planning and co-ordination during large events such as public protests, especially if combined with other technologies such as drones and social media monitoring on the Internet.

Developments in artificial intelligence and machine learning could have significant benefits when considering predictive policing software, or the processing of the increasing volumes of (big) data that potentially arise from modern police investigations. Naturally, the use of such technology by law enforcement has considerable resource implications, not just in gaining access to or ownership of the technology in question, but in ensuring that adequate training is available to capitalise on the technology. A harmonised and co-ordinated approach towards training and capacity building across the EU is therefore essential. Many aspects of the criminal abuse of technology are out with the implicit remit of law enforcement, and instead lie with regulators and policy makers. This applies to issues such as encryption, or the commercial availability and use of drones. Emerging technology fields such the Internet of Things (IoT) for example, have resulted in the creation of new legal, policy and regulatory challenges, and demand cooperation between different sectors as well as different stakeholders. In such discussions, it is essential for law enforcement to have a voice, and to provide guidance and recommendations regarding the needs and requirements of law enforcement in order to be able to continue effectively combatting crime where these technologies are involved.

Combatting crime however is not something law enforcement can or should shoulder alone. A critical factor for success is therefore to develop working relationships with private industry and academia. Industry and academia often have access to data, resources, technology and expertise that is simply unavailable to law enforcement. Moreover, they are often willing partners, particularly when a threat affects their industry. An excellent example of this are Europol's Global Airport Action Days that target fraudsters travelling on tickets bought using compromised payment cards. Such events bring together law enforcement, airline companies, travel

agents, banks, and payment card companies from over 60 countries round the world, and have had a significant impact on this threat area.

Prevention is a key non-investigative measure that must also be considered. Lack of knowledge or information about potential threats from various technologies often leaves potential victims vulnerable to more tech-savvy criminals. Simply raising awareness of these threats, and educating potential victims, can have significant impact on the success of malicious actors.This is again, particularly pertinent in cyberspace where a little knowledge can protect victims from attacks such as phishing, malware or sexual extortion.

Technology will continue to adapt and develop, often at a pace greater than either law enforcement or potential victims can maintain their knowledge or perhaps even awareness of it. New and developing technology will also continue to create new attack vectors, and further expand existing ones. While criminals continue to abuse and exploit new and existing technologies - in order to enhance their criminal activities, or perhaps as a key component of their criminality - it is essential that law enforcement continues to use all the resources, tools, and opportunities at its disposal. Public-private partnerships, the development of innovative technical solutions, prevention measures, and training and capacity building are all required in order for law enforcement to remain an effective countermeasure to crime in the age of technology.

Список використаних джерел:

1. BYRNE, J., MARX, G. (2011). “Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact”, Cahiers Politiestudies, Jaargang 2011-3, nr. 20, p. 17-40. [Online]. URL: https://www.ojp.gov/pdffiles1/nij/238011.pdf. [Accessed: 10-Dec-2021]

2. Crime in the age of technology. [Online]: URL: https://www.cepol.europa.eu/sites/default/files/924156-v7-Crime_in_the_age_of_technology_.pdf [Accessed: 10-Dec-2021].

Папуніцька К.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: Скриник Л.

FIGHT AGAINST CYBERCRIME

The article deals with the features of fighting against cybercrime through the creation of appropriate cyber units in Ukraine and in the world.