UDC 343.3+004

**SAZANOVA Larysa Serhiivna,**
*senior lecturer of the department of foreign languages of faculty No. 4*
*Kharkiv National University of Internal Affairs*
*https://orcid.org/0000-0002-3722-2593;*

**STUKOLOV Maksym Ihorovych,**
*a fourth-year cadet of faculty No. 4*
*Kharkiv National University of Internal Affairs*
*https://orcid.org/0009-0003-2534-5638*

## THE USE OF SOFTWARE APPLICATIONS TO COUNTE TERRORIST ATTACKS AND HUMAN TRAFFICKING

Democratic countries in the world have a belief in human freedom, which is sometimes exploited by terrorists using science and technology to conduct attacks across national boundaries. There is great hope that careful use of science and technology will make it difficult for terrorists to conduct further acts of violence.

Terrorism can be addressed more effectively if there are cooperative and multilateral efforts by the states, rather than a series of uncoordinated activities by individual states. Bringing together experts with common scientific and technical backgrounds from different cultures provide a unique opportunity to explore possible ways to prevent future terrorist attacks and human trafficking.

To better understand the nature of the terrorist threat faced in the world, and how it became a global phenomenon specialists will be better prepared to work together to counter the networks responsible for a variety of terrorist attacks, to see how science and technology could help in the fight against terrorism [1].

The Israel company's flagship spyware, Pegasus, is considered to be one of the most powerful cyber-surveillance tools available on the market, giving operators the ability to effectively take full control of a target's phone, download all data from the device, or activate its camera or microphone without the user knowing.

For years Israel police have used the Pegasus spying tool, developed by Israel's NSO Group (NSO stands for the names of the company's founders – Niv, Shalev and Omri,). According to the Israeli publication Calcalist, the surveillance, which was the responsibility of a special branch of the police cyber-intelligence SIGINT (Signals Intelligence) department was conducted without court authorization and control over what data was collected from the devices [2].

The Israel Police purchased the Pegasus from NSO in December 2013 and began using it in December 2015. According to Israeli law, only Israel's Shin Bet counterintelligence has the right to hack phones without a court warrant (with the approval of senior intelligence or the attorney general's office) and only to prevent terrorist attacks. NSO insists its product is meant only to assist countries in fighting crime and terrorism.

Fifteen years after the launch of the iPhone people got navigation anywhere in the world, the web and email on the go and their location, preferences and habits were transmitted to some faceless corporation. NSO Group, an Israeli firm, is probably the best known.

It sells Pegasus, a piece of spyware that allows the program's operators – typically spies and secret police – to see everything a mobile phone's owner does. By reading messages directly off the phone's screen, it can bypass the encryption built into apps such as WhatsApp or Signal. Pegasus can even activate a phone's camera and microphone, uploading whatever it hears or sees to its controllers [3].

Meta is a founding member of GIFCT (The Global Internet Forum to Counter Terrorism), which is a non-governmental organization that was created by tech companies in 2017 to combat extremist content online, including terrorism. Meta, formerly named Facebook, is opening a piece of its technology to combat terrorism and human trafficking across the internet.

It will allow other companies to share data and prevent the spread of violent images on the internet. Meta's Hasher Matcher Actioner will be a free, open-source content moderation software tool "that will help platforms identify copies of images or videos and take action against them" [4].

The Hasher Matcher Actioner allows companies to find duplicated images by looking at hashes, or digital fingerprints. Those fingerprints or hashes are created after images or videos are run through an algorithm developing a series of numbers or letters specific to that image. Meta spent $5 billion on safety and security in 2021 and had over 40,000 employees dedicated to the company's efforts on online safety.

When a terrorist attack happens, the GIFCT works collaboratively to create a hash based on the online video created by a perpetrator or accomplice during a terrorist attack. That hash allows companies to remove the images offline quickly. Companies in the GIFCT, including Microsoft, Airbnb, Amazon, and current chair YouTube, often use a hash-sharing database that works to block videos and images that violate their terms of service from their platforms. Companies work with law enforcement agencies to prosecute what they believe to be criminal behavior.

## References

**1.** Science and technology to counter terrorism Proceedings of an Indo-U.S. Workshop (2007) URL: htpps://nap.nationalacademicies.org/resource/11848/pga_054736.pdf.

**2.** Israel Police accused of using NSO spyware on civilians for years without oversight. URL: https://timesofisrael.com/israel-police-accused-of-using-nso-spyware-on-civilians-for-years-without-oversight/.

**3.** "Pegasus" lifts the lid on a sophisticated piece of spyware. URL: https://economist.com/culture/2023/01/19/pegasus-lifts-the-lid-on-a-sophisticated-piece-of-spyware.

**4.** Meta says it will share software in attempt to combat terrorism, human trafficking. URL: https://abcnews.go.com/Technology/meta-share-software-attempt-combat-terrorism-human-trafficking/story?id=94882414.

*Received 15.04.2023*