3D-printed gun. So legal systems should be getting ahead to ensure gun control regulations are not circumvented.

In this year Europol announced that an international network of 3D printed firearms experts will be created to keep law enforcement abreast of developments in 3D printed firearms. Having faced a similar threat in the United States, the US Department of Justice (DOJ) already proposed a regulation to update firearm definitions last year, closing a loophole with guns made by 3D printing technologies.

Public safety threats related to 3D printed guns are a sensitive topic in countries with stricter or non-existent public ownership of firearms. Growth in 3D printing technology provides a new and accessible tool that can be used by those with ill intentions to bypass gun laws and manufacture illegal weapons that would otherwise be difficult to acquire.

Список використаних джерел

1. Europol Concerned About Growing Number of 3D Printed Weapons. URL: https://www.google.com/amp/s/www.3dnatives.com/en/europol-concerned-3d-printed-weapons-08062022/amp/.

2. Europol keeps wary eye on threat from 3D-printed guns. URL: https://www.euractiv.com/section/justice-home-affairs/news/europol-keeps-wary-eye-on-threat-from-3d-printed-guns/.

3. Dangers and Benefits of 3D Printing by John Hornick, J.D. URL: https://leb.fbi.gov/articles/featured-articles/dangers-and-benefits-of-3d-printing.

Дорошенко В.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: **Гіпська Т.**

GLOBAL TRENDS IN COMBATING CYBERCRIME

Cybercrime is crime committed via the Internet and computer systems. One category of those affecting the confidentiality, integrity and availability of data and computer systems; they include: unauthorised access to computer systems, illegal interception of data transmissions, data interference (damaging, deletion, deterioration, alteration of suppression of data), system interference, identity theft.

There are types of cybercrimes are online child sexual abuse material, material advocating a terrorist-related act, extremist material (material encouraging hate, violence or acts of terrorism), cyber-bullying (engaging in offensive, menacing or harassing behaviour through the use of technology).

Cybercrime is part of a broader cybersecurity approach, and is aimed at ensuring Internet safety and security [1].

Nothing remains static within the world of technology, and cybersecurity is no different. All around the world, developers and engineers at tech companies – or in IT and information security departments

of other businesses – continually work on methods to safeguard valuable personal, financial and professional data. Methods such as encryption, multi-step verification and others have been implemented to protect vulnerable systems [2].

But that doesn't stop the attackers, they actors on the web closely monitor cybersecurity trends and react to them by reshaping viruses, exploits and other attack methods to subvert safety nets. Thus, there always arise instances in which attackers seize the advantage and their opponents appear to have brought a knife to a gunfight, figuratively speaking [2].

Cybercrime has a complex nature, because it takes place in the boundless cyberspace, is compounded by the increasing involvement of organized crime groups. Perpetrators of cybercrime, and their victims, are often located in different regions, and its effects ripple through societies around the world. This highlights the need to mount an urgent, dynamic and international response [3].

The Global Programme on Cybercrime is mandated to assist Member States in their struggle against cyber-related crimes through capacity building and technical assistance.

Prior to the commencement of the Global Programme, UNODC's open-ended intergovernmental expert group was established to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector. This work includes the exchange of information on national legislation, best practice, technical assistance and international cooperation.

The Global Programme is designed to respond flexibly to identified needs in developing countries by supporting Member States to prevent and combat cybercrime in a holistic manner.

The Global Programme on Cybercrime funded entirely through the kind support of the Governments of Australia, Canada, Japan, Norway, UK and USA [3].

Goals of global trends in the fight against cybercrime:

- increased efficiency and effectiveness in the investigation, prosecution and adjudication of cybercrime, especially online child sexual exploitation and abuse, within a strong human-rights framework;
- efficient and effective long-term whole-of-government response to cybercrime, including national coordination, data collection and effective legal frameworks, leading to a sustainable response and greater deterrence;
- strengthened national and international communication between government, law enforcement and the private sector with increased public knowledge of cybercrime risks.

Список використаних джерел

1. Cybercrime. URL: https://dig.watch/topics/cybercrime.
2. Emerging trends in global cyber crime. URL: https://online.maryville.edu/blog/emerging-trends-in-global-cyber-crime/.
3. Global Programme on Cybercrime. URL: https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.