February 2020 by the Wuhan Institute of Virology identifies the bat coronavirus RaTG13 as the closest parent of SARS-CoV-2, sharing 96,2% of their overall genome sequence identity. A second study from the Hong Kong University and Guangdong-Hongkong Joint Laboratory of Emerging Infectious Diseases shows that a group of beta-coronaviruses found in the pangolin species are even closer, with 97,4% similarities with the SARS-CoV-2 amino acid sequence. However, despite their apparent close parental ties, in genetic these differences are too big to assume that SARS-CoV-2 could have been elaborated in a lab, by human hand.

If questions still remain regarding the emergence of the virus, no valid proof can support the theory that the SARS-CoV-2 was weaponized and intentionally released by the Chinese. Nonetheless, this crisis makes us reflect on Biological threats in general and their consequences: biological hazards are a threat not only to our health but also to our economies, and our social and political models, and will need to be taken more seriously and better address in the future.

Список використаних джерел

1. Ophelie Guillouet-Lamy, Analyst, IB Consultancy URL: https://nct-magazine.com/nct-magazine-may-2020/covid-19-a-biological-weapon-a-guide-to-biological-weapons-to-answer-that-question/(дата звернення 26.10.2020).

2. Trushar R. Patel Assistant Professor and Canada Research Chair, Department of Chemistry and Biochemistry, University of Lethbridge URL: https://theconversation.com/the-covid-19-pandemic-can-prepare-us-for-future-outbreaks-and-bioterrorism-136685 (дата звернення 26.10.2020).

3. https://www.interpol.int/Crimes/Terrorism/Bioterrorism (дата звернення 26.10. 2020 р.).

Щур С., курсант Національної академії внутрішніх справ
Консультант з мови: ***Хоменко О.***

THE USA EXPERIENCE IN COMBATING CYBER-CRIME

Words and phrases that scarcely existed a decade ago are now part of our everyday language, as criminals use new technologies to commit cyberattacks against governments, businesses and individuals. These crimes know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide [1].

Cybercrime is any criminal activity that involves a computer, networked device or a network. Malicious cyber activity threatens the public's safety, national and economic security.

In the United States, at the federal level, there is the Federal Bureau of Investigation's (FBI) Cyber Division which is the agency that is charged with combating cybercrime [3]. The FBI's goal is to change the behavior of criminals and nation-states who believe they can compromise US networks,

steal financial and intellectual property, and put critical infrastructure at risk without facing risk themselves. To do this, they use their unique mix of authorities, capabilities, and partnerships to impose consequences against their cyber adversaries [2].

The FBI is the lead federal agency for investigating cyberattacks and intrusions. They collect and share intelligence, engage with victims while working to unmask those committing malicious cyber activities, wherever they are. So the FBI's cyber strategy is to impose risk and consequences on cyber adversaries through their unique authorities, their world-class capabilities, and their enduring partnerships [2].

Whether through developing innovative investigative techniques, using cutting-edge analytic tools, or forging new partnerships in the USA communities, the FBI continues to adapt to meet the challenges posed by the evolving cyber threat. The FBI has specially trained cyber squads in each of their 56 field offices, working hand-in-hand with interagency task force partners. What is more this rapid-response Cyber Action Team can deploy across the country within hours to respond to major incidents [2].

Internet fraud does not have traditional boundaries as seen in the traditional schemes. No one knows the full extent of the fraud being committed on the Internet. Not all victims report fraud, and those who do, do not report it to one central repository. For traditional fraud schemes the FBI has systems in place to identify and track fraud throughout the country. In addition to the basic investigative steps required in any investigation, cybercrime investigations require that new types of questions be asked, new clues looked for, and new rules be followed concerning the collection and preservation of evidence. In order to successfully conduct these investigations, investigators require significantly advanced skills. As a result, the development of a proactive strategy to investigate Internet fraud through the establishment of an Internet Fraud Complaint Center (IFCC) as a central repository for criminal complaints was essential. The IFCC is a joint operation with the FBI and the National White Collar Crime Center (NW3C).

The IFCC was necessary to adequately identify, track, and prosecute new fraudulent schemes on the Internet on a national and international level. It serves as a clearinghouse for the receipt, analysis, and dissemination of criminal complaints concerning frauds perpetrated over the Internet. IFCC personnel collect, analyze, evaluate, and disseminate Internet fraud complaints to the appropriate law enforcement agency. Also the IFCC provides a mechanism by which the most egregious schemes are identified and addressed through a criminal investigative effort.

The IFCC identifies current crime problems, and develops investigative techniques to address newly identified crime trends. The information obtained from the data collected is providing the foundation for the development of a national strategic plan to address Internet fraud.

Public awareness of the existence and purpose of the IFCC is paramount to the success of this effort. The IFCC provides a convenient and

easy way for the public to alert authorities of a suspected criminal activity or civil violation. Victims of Internet crime are able to go directly to the IFCC web site (www. IFCCFBI.gov) to submit their complaint information, relieving considerable frustration for the victim in trying to decide which law enforcement agency should receive the complaint.

The FBI web page also aids in this effort. A detailed explanation of the complaint center, its purpose and contact numbers, is provided so that consumers can report Internet fraud. The FBI web page provides victims with a hyperlink to the IFCC web page [4]. The Internet Crime Complaint Center (IC3) collects reports of Internet crime from the public. When CyWatch is the FBI's 24/7 operations center and watch floor, providing around-the-clock support to track incidents and communicate with field offices across the country [2].

The FBI has taken a number of other steps to address cybercrime. The National Infrastructure Protection Center (NIPC) was created in February, 1998, and was given a national critical infrastructure protection mission per Presidential Decision Directive (PDD) 63. The NIPC mission includes: detecting, assessing, warning of and investigating significant threats and incidents concerning our critical infrastructures. It is an interagency center physically located within the Counterterrorism Division at FBI headquarters.

In conjunction with the center, the FBI created the National Infrastructure Protection and Computer Intrusion Program (NIPCIP) as an investigative program within the Counterterrorism Division. The FBI has 56 field offices with NIPCIP squads with 16 regional NIPCIP squads, which are comprised of specially trained investigators and analysts. Initial investigations into computer intrusion matters have been primarily conducted by NIPCIP squads. During the course of such investigations, it is increasingly found that the intrusion was merely the first step in a more traditional criminal scheme involving fraud or other financial gain.

In addition, the FBI continues to develop and operate cybercrime task forces consisting of investigators and resources from other federal agencies as well as state and local agencies. The FBI considers such task forces an efficient and effective means to leverage resources and expertise in coordinating investigations into cybercrime. The complex nature of cybercrime investigations make cooperation and coordination among law enforcement agencies vital in this area. Cybercrime task forces provide an invaluable mechanism to cover investigative areas that cross jurisdictional and program lines. The FBI plans to aggressively pursue development of such task forces in all FBI field divisions[4].

Cybercrime is progressing at an incredibly fast pace, with new trends constantly emerging. Cybercriminals are becoming more agile, exploiting new technologies with lightning speed, tailoring their attacks using new methods, and cooperating with each other in ways we have not seen before. Complex criminal networks operate across the world, coordinating intricate attacks in a matter of minutes. Police must therefore keep pace with new

technologies, to understand the possibilities they create for criminals and how they can be used as tools for fighting cybercrime. The IFCC serves as an example of an innovative approach to an emerging crime problem. It provides the benefits of community policing, forging an effective partnership between law enforcement at all levels, ordinary citizens, consumer protection organizations. The FBI's IFCC serves to facilitate and coordinate this collaborative effort.

Список використаних джерел

1. Cyberattacks know no borders and evolve at a rapid pace. URL: https://www.interpol.int/Crimes/Cybercrime.
2. The Cyber Threat. URL: https://www.fbi.gov/investigate/cyber.
3. Rouse M. Cybercrime. URL: https://searchsecurity.techtarget.com/definition/cybercrime.
4. Kubic T.T. The FBI's Perspective on the Cybercrime Problem Rouse. Washington, 2001. URL: https://archives.fbi.gov/archives/news/testimony/the-fbis-perspective-on-the-cybercrime-problem.

Югас О., здобувач ступеня вищої освіти Національної академії внутрішніх справ
Консультант з мови: ***Романов І.***

ORGANIZED CRIME IN JAPAN

Organized crime in Japan is represented by organizations called the “Yakuza”. The Yakuza is a traditional form of organized crime in Japan, whose groups occupy a leading position in the country's criminal world. Yakuza members are also known as "gokudos". In literature and the press, the yakuza or its individual groups are often called the "Japanese mafia" or «boryokudan». Yakuza is based on the values of the patriarchal family, the principles of unquestioning submission to the boss and strict adherence to the rules (Mafia Code), for violation of which there is an inevitable punishment. Stability and longevity of the Yakuza clans provide both specific links between the boss and his subordinates, and the preservation of horizontal ("fraternal") relations between ordinary members of the group.

It is believed that the word yakuza comes from an insignificant hand in a Japanese card game similar to baccarat or blackjack: ja-ku-sa cards ("eight nine three"), when they are made, give the worst of possible results.

There are various theories about the emergence of such a phenomenon as the yakuza. The main one indicates that it all began in Japan in 1612, 12 years after the Great War. The army of the mighty Tokugawa Ieyasu, numbering 100,000 samurai, defeated the army of Ishida Mitsunari. Ishida himself was buried by the neck in the ground and executed with a blunt sword. Tokugawa Ieyasu became the de facto ruler of Japan. After this war, a large army was disbanded. Crowds of ryonins (samurai who were left