

of the world that cover the entire scope of child sexual abuse investigations: conducting investigations in the online environment; the use of INTERPOL's International Child Sexual Exploitation database; victim identification methods; victim and offender interview techniques; categorization of child sexual abuse material.

While many countries have child protection and special victims units, few have specialized staff able to investigate online child sexual abuse cases or perform victim identification. Specialized officers can advise countries on how to set up victim identification units and can provide tailored support to national authorities.

The INTERPOL Specialists Group on Crimes Against Children meets annually to facilitate and enhance the investigation of sexual crimes against children. Gathering law enforcement, regional and international organizations, NGOs, the private sector and academia, the group identifies new trends and techniques and develops best practice. Private sector partners such as financial institutions, internet service providers and software developers also play a crucial role in tracking child sexual abuse material and shutting down illegal distribution channels. Their input is highly valued and a key part of our coordinated approach.

Список використаних джерел

1. URL: <https://www.interpol.int/Crimes/Crimes-against-children> (дата звернення 30.09.2020).
2. <https://www.interpol.int/Crimes/Crimes-against-children/Our-response-to-crimes-against-children> (дата звернення 30.09.2020).
3. <https://www.interpol.int/Crimes/Crimes-against-children/Victim-identification> (дата звернення 30.09.2020).

Шупик О., курсант Національної академії внутрішніх справ

Консультант з мови: Марченко І.

COVID-19 A BIOLOGICAL WEAPON?

As the economic and health risks of the COVID-19 pandemic are predicted to persist into next year, there are growing reservations about society returning to normal. The impacts of COVID-19, like the 2008 financial crisis and the 2001 September 11th attacks before, are changing global consciousness and reopening uncertainties about security, privacy and public health. Unfortunately, the current COVID-19 pandemic reveals systemic infrastructural and security deficiencies that rendered countries [3]. This could have been avoided with better preparedness. However, preparedness requires maximum co-operation and transparency between government, researchers and industry. As countries experience the ongoing economic and public health shocks caused by COVID-19, rogue actors seeking to take advantage of the pandemic may use bioweapons to similar effect.

Any biosecurity threat or epidemic could easily become a global concern. Pathogens do not recognize borders and will spread indiscriminately, ultimately disproportionately affecting poorer nations. Globalization – which is being analyzed as a contributor to the spread of COVID-19 – could also help thwart the spread of man-made or naturally occurring diseases, provided multilateral co-operation remains intact. The response has to be global because pandemics and terror attacks have persisting and grave effects, not tied specifically to a single state and its economy [2]. Governments must take a proactive stance against the growth and development of deadly pathogens (engineered or naturally occurring), which might require an overhaul of the socioeconomic and political relationships that govern health and our shared environments.

The most crucial response is intergovernmental collaboration and compliance with medical experts. This would involve the sharing of information and effective mitigation strategies against bioterrorism. The remarkable and unprecedented global unity today is demonstrated by scientists freely sharing information related to COVID-19 to speed up the development of a vaccine.

Governments and their collaborators must also stop the spread of disinformation to quell panic and alleviate the public's fears. This includes maintaining public trust in experts which must be differentiated from popular and political opinions that have led to chemical poisoning [2]. This has also been exacerbated with ongoing distrust for WHO officials as false claims and pandering to China has led to failures in the initial response to COVID-19 including indecision within the scientific community. Terrorist organizations will undoubtedly use the spread of bioweapons to create civil turmoil and instability, reinvigorating or inciting national contentions such as scarcity, ethnic tension or religious infighting. This applies to countries already destabilized by entrenched conflicts, which can rapidly metastasize through competition and inequality already present in developing countries. Overcoming pandemics and terrorism will inevitably rely on national infrastructure such as employing the military, which the Canadian government has done to supplement medical resources. Deploying a nation's armed forces has the potential to apply the vast resources, equipment and labour that an organized and skilled military maintains.

Preventing the bioengineering, emergence, release and spread of pathogens will require aggressive strategies. These include implementing regulations against the mistreatment and harvesting of wild and domestic animals to prevent their mixing and the unintentional mixing of viruses and infectious diseases [2]. Managing land reclamation and protecting habitats can prevent biodiversity loss and reduce human contact with pathogenic viruses.

Other technologies in the fight against bioterrorism or pandemics include heightened surveillance and tracking in the form of smartphones and drones. Deployable 3D isolation units repurposed as mobile laboratories could also quickly respond to bioweapons threat.

To guarantee safety, the public has to be willingly compliant with government policies. In Canada, closing the national border and enacting quarantine Laws mitigated the spread of COVID-19, but the public's co-operation was essential to the public good [2].

Recommendations from health-care professionals and epidemiologists must be implemented at every stage, and directed by governments. The consequences of neglecting to act expeditiously are apparent in the United States, which has been marred by bureaucratic red tape, equipment scarcity and vacillating in leadership responses. Lessons from previous pandemics can prepare us for both future inevitable global outbreaks and possible bioterrorist attacks.

Biological weapons have been and remain until today a very plausible threat, with numerous cases of use in history. Nowadays, with the spread of terrorist organizations in some regions of the world and in unstable countries which are suspected to have continued developing biological warfare programs, the threat posed by bioweapons is becoming more and more pressing. Furthermore, if biological weapons are Weapons of Mass Destruction, which means that they have the objective of causing public panic, leading to social disruption and eventually mass destruction, they are also known to be efficient for isolated assassination [1]. One of the most recent cases demonstrating this probability is the Anthrax letters in 2001 in the USA, when letters full of Anthrax bio-agent were specifically sent to US politicians and journalists. Nevertheless, one should not confuse these realistic threats with other darker theories about Covid-19. Thanks to the information about biological weapons, we can now find some arguments going against the unfounded concerns about the eventuality to weaponize recent viruses like Ebola or Covid-19. First, Covid-19 like Ebola, are not airborne viruses, which means that to be used as a Biological Weapon, it would rely on the transmission from person-to-person, and not on a delivery via an aerosol for instance, which is known to be the most efficient way to spread a biological agent [1]. Additionally, Covid-19 and Ebola are very unstable viruses and would be extremely difficult and dangerous to weaponize since no vaccines are yet available, and since it would require a BSL4 Lab (Biosafety level 4 is the highest level of biosafety precautions) to manipulate these viruses. And as previously mentioned, these laboratories are in limited numbers. Now yes, one could argue that the Wuhan Institute of Virology in China, originally a BSL3 Lab, was recently completed by a BSL4 facility in 2015, and therefore could have been able to manipulate this virus, and it did after the discovery of the new coronavirus. But the probability that this virus could have been created by biologists in the BSL4 Lab in Wuhan is very low, since SARS-CoV-2 does not look like any viruses already known by the scientific community, which could have served as a base to create this new virus. Indeed, until now, scientists have been able to create new viruses, only based from already existing viruses, and by changing a very small genome sequence of that virus [1]. For COVID-19, the origin of the virus is still unknown. A study published in

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,