CYBERTERRORISM AS A NEW TYPE OF TERRORISM AND THE 2007 CYBER-ATTACKS ON ESTONIA AS AN EXAMPLE OF CYBERTERRORISM

Карделя О. В.
National Aviation University, Kyiv
Науковий керівник –Рижков М.М., д-р політ. наук, проф

Annotation –the article explores the role of cyberterrorism in modern international relations and analyzes how the 2007 cyber-attacks on Estonia have affected cyberterrorism development.

Cyberterrorism is the use of computer and telecommunication technologies, including the Internet, to achieve terrorist goals. Since the modern world develops quickly, technological progress is an integral part of people's lives, and terrorists use this phenomenon to commit terrorist acts. Cyberterrorismshould be perceived as attacks on computer systems, primarily via the Internet, that threaten people's property, lives, or health and can cause destruction of infrastructure facilities. In other words, cyberterrorism is a terrorist activity conducted incyberspace or with its use. Thus, cyberterrorism includesinformation technology use that allows terrorists or terrorist groupsto accomplish their objectives [1].

Importantly, cyber-attacks can be committed for financial or political reasons. Cyberterrorists can focus on different goals, such as the achievement of the unauthorized access to state and military secrets, theft or destruction of information by dealing with systems of protection and viruses use, influence on software and information, the threat of publication of classified information, the spread of fake news and disinformation, demonstration of a terrorist organization's power, conducting information and psychological operations, and others [4].Cyberterrorists aim to use thedata to affect politicians' and people's actions and show their power.

The September 11 attacks made countries throughout the world focus on their national security: states aimed to prevent not only ordinary terrorist attacks but also cyber-attacks. The media provided citizens with relevant information concerning cyberterrorism and made them aware of the possible consequences of that type of terrorism. People have realized that cyberterrorism can harm human lives and cause various disruptions, including a disruption of the national economy [5].

Nevertheless, numerous countries have suffered from cyberterrorism that has significantly affected their national security. For instance, the 2007 cyber-attacks on Estonia belong to the most famous examples of cyberterrorism. In 2007, Estonia faced cyber-attacks that aimed to hurt the vast majority of its citizens. The attacks, which began on 27 April 2007, had to harm the websitesof Estonia organizations, including parliament, ministries, banks, social media, and others [2].Importantly, the 2007 cyber-attacks on Estonia were caused by the deterioration of Estonia and Russiarelationships. The Estonian government's decision to move the Bronze Soldier to a military cemetery was the primary reason for the attacks [3]. Estonia's institutions and agencies could not work because their websites faced interventions. Moreover, the hackers used Estonia's social media to share fake news. The Estonian institutions faced massive spamwaves, destruction of cash machines and online banking services, a lack of ability to communicate on email, inability to deliver the news, and others [2]. As a result, the country could not continue the normal operation, and all the spheres of life were harmed by the hackers' activities, while the authorities could not control the processes that occurred in different fields.

Estonia believed that Russia was playing a crucial role in the attacks and blamed that country. However, the Estonian government suffered from a lack of evidence to explain their opinion. NATO and the European Commission could not prove that the Russian authorities had participated in the attacks on Estonia [3]. That situation made Estonia take all the essential measures to increase cybersecurity protections. In addition, the 2007 cyber-attacks on Estonia motivated NATO to assess their cybersecurity. That process led to creating the NATO Cooperative Cyber Defence Center of Excellence (CCDCOE) in May 2008 [2].

Under these circumstances, cyberterrorism tends to become a widespread phenomenon in the near future. Since all the vital information is stored on the Internet, hostile states can use it to destroy particular countries' institutions. Cyberterrorism allows people not to be presentedphysically in the places where terrorist attacks have to be committed. Nevertheless, cyber-attacks are dangerous as well, and modern countries should improve both national and cybersecurity. The 2007 cyber-attacks on Estonia demonstrated that all states could face cyberterrorism, and NATO membership could not protect them from devastating consequences. Governments throughout the world have to focus on the 2007 cyber-attacks on Estonia to prevent similar problems in their states. Thus, the creation of the departments responsible for cybersecurity, improvements in national security, protection of information stored on the Internet, the establishment of the organization that has to fight against cyberattacks are the most effective methods to overcome cyberterrorism.

References:

1.Akhgar B. Cyber crime and cyber terrorism investigator's handbook / BabakAkhgar., 2014.

2.McGuinness D. How a cyber attack transformed Estonia [Електроннийресурс] / Damien McGuinness // BBC News. – 2017. – Режимдоступудоресурсу: https://www.bbc.com/news/39655415

3.Ottis R. Analysis of the 2007 cyber-attacks against Estonia from the information warfare perspective [Електроннийресурс] / Rain Ottis // Cooperative Cyber Defence Centre of Excellence. – 2018. – Режимдоступудоресурсу: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

4.Terrorist use of cyberspace and cyber terrorism: New challenges and responses [Електроннийресурс] // North Atlantic Treaty Organization. – 2020. – Режимдоступудоресурсу: https://www.nato.int/cps/en/natohq/topics_140739.htm?

5.Weimann G. Cyberterrorism: The sum of all fears? / Gabriel Weimann. // Studies in Conflict & Terrorism. – 2004. – №28. – С. 124–149.