Нерез В.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: Василенко О.

CYBERTERRORISM: CHALLENGE FOR SOCIETY AND LAW ENFORCEMENT

Before we start, we need to understand what is “cyberterrorism” and how it is used different terror groups? The term “cyberterrorism” is complex and combines two concepts: “cyber”, referring to cyberspace, and “terrorism”, whose meaning and scope will be analyzed later. On this basis, we can assume that cyberterrorism is a special type of terrorism, where the “place” or “medium” is carried out in cyberspace. Cyberspace is considered “a globally interconnected network of digital information and communications infrastructures”, normally understood to mean the internet and, more broadly, computer networks.

The concept of cyberterrorism usually refers to a range of very different actions, from the simple spread of propaganda online, to the alteration or destruction of information, and even to the planning and carrying out of terrorist attacks via the use of computer networks. As such, in order to better understand what cyberterrorism is, this article will begin by analyzing the concept of “terrorism” – including its structure, harm principle, and elements – as a broad category to which the species “cyberterrorism” belongs; later, it will delimit the idea of cyberterrorism and distinguish it from others with which it has a certain similarity; finally, it will raise some of the most important challenges that cyberterrorism implies in a global and technologically interconnected world.

That cyberterrorism is defined by its location or the medium through which it is executed can be criticized to some extent. To address such criticisms, a comparison can be made to aircraft hijacking terrorist acts, such as the 9/11 terrorist attacks on the World Trade Center; or vehicle-based terrorist attacks, such as when a truck deliberately drove into a crowd of people on the Nice promenade in 2016. In reality, the scope of cyberterrorism appears to follow the general tendency for many “real world” phenomena to be replicated online. Thus, it is common to talk about “cyber activism” as a type of activism carried out online; or “cyberbullying” being a type of bullying which also occurs online. Similarly, it’s not difficult to imagine that, with the rise of terrorism, there has also emerged it’s virtual strain: cyberterrorism.

However, it is possible to distinguish between two kinds of “cyberterrorist”: The first kind, likely to be more common, is the traditional “terrorist” that uses the internet as well as information and communication

technologies to perpetrate their attacks. In this case, those carrying out traditional terrorist attacks take advantage of the benefits offered by these technological tools, for example the ability to negatively impact a large number of people in a brief period of time without personally physically exposing oneself, but from the comfort of their own computer. This applies both in the preparation of crime (planning, conspiracy, etc.) and to their partial execution (attempted crime) or completion (successful crime.) In the case of attacks that make some use of technology, a terrorist can, amongst other things, attack the networks that allow for control and supervision of industrial processes, systems known as SCADA (Supervisory Control And Data Acquisition) or, damage "critical infrastructure", for example the water supply and potable water, means of transport and telecommunications, health services, etc., which in turn affect a considerable number of people.

Regarding the harm principle, cyberterrorism does not directly attack individual interests, that is, those that belong to or serve a specific person or a set group of people. On the contrary, cyberterrorism directly affects a collective interest, an interest that is owned by or serves the general public. As in terrorism, the collective interest directly attacked by cyberterrorism is the democratic constitutional order. Hence, it can be affirmed that cyberterrorism constitutes an attack against institutional, state, or national interests.

Said characteristics distinguish cyberterrorism from common crimes like homicide or assault, but also distinguish cyberterrorism from cybercrimes such as computer fraud, all of which directly affect individual rather than collective interests. In other words, even if cyberterrorism harms or threatens individual interests like the life or health of others, this indirect impact is not its ultimate goal, instead the goal is a direct attack on the democratic constitutional order.

As a result we can say that cyberterrorism must comply with the structure, harm principle and elements that define terrorism. Consequently, if these are not verified, we may be in the presence of a cybercrime and not cyberterrorism (for example a computer sabotage.) In terms of its structure, cyberterrorism requires the existence of an organization destined to perpetrate (cyber)terrorist attacks. Regarding its harm principle, cyberterrorism must directly violate a collective interest identified with the democratic constitutional order. In terms of its elements, cyberterrorism must be executed with the specific purpose of altering constitutional order or to topple the legitimately elected government; and must be carried out in a manner appropriate to instill terror in people's minds, establishing a belief that anyone anywhere could be a victim of an attack.

Finally, cyberterrorism creates several challenges in a global and technologically interconnected world. Committing cyberterrorism involves the use of the internet, which offers a series of advantages for those participating in the act. In addition, because the real dimensions and potential of cyberterrorism are not yet clear, reacting with preparation becomes difficult.

Список використаних джерел:

1. Ambos, K. (2015). Responsabilidad penal internacional en el ciberespacio. InDret. (2), 1-32. Recuperado de https://bit.ly/2QNF1D5 [Links].
2. Asúa Batarrita, A. (2012). Estudios jurídicos en memoria de José María Lidón. En Echano Basaldua, J (coord.); Concepto jurídico de terrorismo y elementos subjetivos de finalidad: Fines políticos últimos y fines de terror instrumental. Bilbao: Universidad de Deusto.
3. Conway, M. (2014). Cyberterrorism. En Chen, T., Jarvis, L., Macdonald, S (autor.); Reality Check: Assessing the (Un)Likelihood of Cyberterrorism.". (103-121). New York: Springer Recuperado de 10.1007/978-1-4939-0962-9_6
4. Gillespie, A. (2016). Cybercrime: Key Issues and Debates. London: Routledge
5. Goodman, S., Kirk, J., Kirk, M. (2007). Cyberspace as a medium for terrorists. Technological Forecasting and Social Change. 74(2), 193-210. Recuperado de 10.1016/j.techfore.2006.07.007
6. Favale, T.; Soro, F.; Trevisan, M.; Drago, I.; Mellia, M. Campus traffic and e-Learning during COVID-19 pandemic. Comput. Netw. 2020, 176, 107290. [Google Scholar] [CrossRef].
7. Guzmán Dalbora, J. (2017). Colectánea criminal: Estampas de la parte especial del derecho penal. En El terrorismo como delito común. (203-255). Montevideo: B de F.
8. Kochheim, D. (2015). Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik. Munich: Beck.