CYBERTERRORISM

Tamashevich D.V.

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Sinkevich L.E. – Senior Lecturer

Information about cyberterrorism, severity of this problem, ways to deal with it as well as examples of cyberterrorism are presented in the article.

Nowadays digital technologies control almost every aspect of the life. Of course, such automation has a lot of advantages: computers work much faster than humans; they never tire and make less mistakes. On the other hand, heavy dependence on the machines also has one massive downside: they have vulnerabilities that can be exploited by malefactors. According to the statistics, 86,2% of organizations were compromised by at least one successful attack [1]. But these attacks can actually be aimed at the state instead of private businesses, thus affecting countless human lives and their wellbeing.

Such thoughts bring us to the concept of cyberterrorism. According to Dorothy Denning, cyberterrorism is “unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives” [2]. She also highlights that, in order to qualify as cyberterrorism, an attack must have an impact in the “real world” that goes well beyond damage to data or information technologies.

Actually, cyberterrorism in this violent sense has never occurred. Because of the expensiveness and the lack of skills for successful cyber-attacks it is very hard for terrorist groups to launch these attacks. But while probability of massive cyber-attack is indeed low, the consequences of it will be catastrophic, so we shouldn’t discard possibility of it.

The only person to get prosecuted because of cyberterrorism was 20-year old Ardit Ferizi, a citizen of Kosovo. In 2015 he gained sys admin level access to a US company server and gained information on 1300 military and government individuals [3]. However, this act can’t be classified as a pure cyberterrorism because of the lack of impact on the real world.

There was also an attack that did bodily harm and targeted crucial infrastructure but can’t be called a terrorist act. In 2007, a fourteen-year-old Polish teenager decided to break into the tram depot in the city of Lodz. After four months of studying he was able to construct a device capable of capturing the track switching signal from an old TV remote. The consequences of such act were quite grim: twelve people were injured and four vehicles were derailed [4]. This act could be classified as an example of cyberterrorism if there was a motivation of attacker, his connection to any terrorist cell. Of course, in that case consequences would have been even worse.

As it has been said previously, cyberterrorism in its purest form doesn’t exist. Instead of it, cyberspace became a supportive tool for terrorists. They use the Internet for communication, recruitment, planning, fundraising, etc. Also cyber-attacks can have purely symbolic impact, while causing minimal economical or physical damage. As an example we can take defacement of many websites after the terrorist attacks in France in the beginning of 2015, when around twenty thousand sites have been targeted [5].

These attacks can target both government entities and businesses. So, in order to protect themselves from cyberterrorism, businesses should use methods similar to defending against regular cybercrimes: organizations should use firewalls, antivirus software, do regular backups, and implement continuous monitoring techniques.

To give a conclusion, cyberterrorism threat indeed exists, but it's not as serious as some people may think. Despite that fact, we should always prepare to the worst outcome and improve security of important objects and state structures.

References:

1. 300+ Terrifying Cybercrime and Cybersecurity Statistics (2022 EDITION) – [Electronic resource]. – Access mode: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends – Date of access: 22.02.2022.

2. Dorothy E. Denning "Cyberterrorism Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives" Georgetown University May 23, 2000.

3. ISIL-Linked Kosovo Hacker Sentenced to 20 Years in Prison – [Electronic resource]. – Access mode: https://www.theregister.com/2008/01/11/tram_hack – Date of access: 11.02.2008.

4. Polish Teen Derails Tram after Hacking Train Network – [Electronic resource]. – Access mode: https://www.justice.gov/opa/pr/isil-linked-kosovo-hacker-sentenced-20-years-prison – Date of access: 23.09.2016.

5. Charlie Hebdo: 'Islamist Cyber Attacks' hit France – [Electronic resource]. – Access mode: https://www.bbc.com/news/technology-30850702 – Date of access: 16.01.2015.