Scientific and Practical Cyber Security Journal (SPCSJ) 2(1):11-14
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

TERRORIST'S CYBER ACTIVITIES – A GROWING THREAT

A.Gotsiridze
Cyber Security Advisor at the Georgia Innovation and Technology Agency, Tbilisi, Georgia

ABSTRACT. The 21st century is characterized by migration of political, social or criminal processes to cyberspace. Similar tendencies are also observed in terms of terrorism. Terrorist groups do not possess cyber-attacks sufficient to cause significant harm and therefore prefer conventional attacks. However, if at least one year ago, conventional attacks were the only mechanism available to them to cause real damage and fear, nowadays the likelihood of cyber-attacks is likely to increase, due to better aware extremist generation and the failure of the conventional forces of terrorist organizations in Afghanistan and Syria-Iraq

KEYWORDS: Cybersecurity, Cyberterrorism, CyberCaliphate, Cybercapabilities, Cyberthreat, Terrorist's Cyberatack

The 21st century is characterized by migration of political, social or criminal processes to cyberspace. Similar tendencies are also observed in terms of terrorism. Instead of stealing wallets and documents, stealing personal data from online databases, fraud with bank cards, breaking of company networks, and spreading child pornography by cyber channels are trends in modern crime. The separation of criminal and terrorist activities in cyberspace seems to be a difficult task at first glance and there may be a perception that cybercriminals and cyberterrorism merge with each other, but there is a substantial difference between these two directions - these are motives and goals. Cybercrime is a "digital version" of the traditional crime, focusing on stealing money or information that can be sold from information systems and is determined by financial motivation. While cyberterrorism like other demonstrations of terrorism has the ideological or political motivation and aims at instilling the atmosphere of public harm and fear.

An attempt to influence confidentiality, integrity and availability of computer networks and electronic-services, implemented by terrorist groups or extremists or with their help, is called a terrorist cyber-attack. It may serve to damage, disrupt the service, and attempt to use the computer network or the information gained from the network for terrorist purposes.

Despite the serious damage or the intention of having victims using cyberspace, the terrorists have no real possibilities to do this. Today, the most frequently implemented form of cyberterrorist attack in the world is Defacement against relatively vulnerable, weakly protected websites and social media, which can only cause minor disruptions.

The cyber capabilities of terrorist organizations are often exaggerated by experts for several reasons:

- The simplicity of damage to websites that are weakly protected is misunderstood by the media and unaware community;

- Cyber-attack implemented by some groups is incorrectly attributed to cyber-terrorist attacks and they have nothing in common with such ideology. For example, in January 2015, the Malaysian Airlines website was damaged by LizardSquard's hacker group and this attack was totally deprived of ideological grounds.
- This tendency is boosted by extremist hackers who exaggerate their own cyber capabilities in order to increase the reputation or have a psychological impact.
- The "false flag" cyber-attacks under the cover of a terrorist organization have also created an impression that groups of cyber terrorists have much more technical capabilities than in reality. The most resonant attack by cyberterrorists was a Russian-backed cyber-attack on the French Broadcasting Company under the legend of Cyber Caliphate. The handwriting of the cyber-attack and the Cyrillic elements found in the malicious codes are identical to the APT28's handwriting - the hacker grouping under the control of the Russian government, and the timing of the attack coincides with the deterioration of French-Russian relations.

Terrorist groups do not possess cyber-attacks sufficient to cause significant harm and therefore prefer conventional attacks. However, if at least one year ago, conventional attacks were the only mechanism available to them to cause real damage and fear, nowadays the likelihood of cyber-attacks is likely to increase, which is due to several factors:

- The attacks that have already been carried out, regardless of who was actually behind these attacks, was perceived as successful, creating a sense of the effectiveness of such attacks;
- There is an extremist generation with better awareness of computer systems, and some organizations will try to use their knowledge to achieve terrorist objectives;
- The failure of the conventional forces of terrorist organizations in Afghanistan and Syria-Iraq, as well as increased security measures against terrorist acts, is likely to push these organizations to carry out cyber-attacks.

Successful use of cyberspace is important for terrorist organizations: Hizballah, Hamas, al Qa'ida, ISIL continue to use the Internet to gain intelligence information, search for funds, recruitment, propaganda and other actions. The Taliban also uses Internet technologies for similar purposes. Hizballah and Hamas spread their cyber activities to the Middle East region, ISIL cyber divisions in order to further carry out terrorist attacks are constantly trying to obtain sensitive information about the citizens of the states who are members of anti-terrorism coalition, especially military personnel, so that the anxiety and fear after their attack could force the government leave the coalition or stop the military operations against the terrorist organizations. Cyberspace is actively used by the terrorist group in Nigeria, Boko Haram, which works in social networks and other contemporary communications systems aiming at recruitment, propaganda and obtaining financial resources.

In recent times, growing interest and discussions about cyberspace usage have been observed in terrorist forums, the number of extremists interested in studying the skills needed for cyber-attack is also increasing.

Despite the fact that, according to the current data, instead of organizing cyber-attacks the terrorist groups currently use their technically skillful members to implement such issues as the safety of communications and gaining electronic intelligence information for conventional attacks, the threat of cyberterrorism is rising.

The cyber capabilities of terrorist organizations and consequently the threat will be substantially increased if they cooperate with a state having strong cyber potential, with elite criminal hackers or recruit highly qualified specialists. Important facts of cooperation of hackers with terrorist organizations have not yet been observed, and the involvement of highly qualified specialists in extremist activities is rare. Only a small number of states have significant cyber capabilities for cooperation, and cooperation with terrorist groups is a big political risk and states are cautious about this. In this regard, it is more alarming the cyber-attack implemented by Russia under the cover of cyber terrorism on the French broadcasting Company that was discussed above. It is also dangerous trend the fact that experts estimate this attack as a political act, and link this fact to the refusal of French officials to sell Mistral to Russia and deny participation in the ceremonial events of May 9. Based on the above, we cannot exclude that some of the terrorist groups have highly developed opportunities due to their relationship with state patrons.

Distinguishing the Internet-based terrorists, their supporters and sympathizing persons is a difficult task. It is also difficult to create the evidence database on the transfer of funds over the Internet to terrorist organizations. Social networks are good for finding connections, but they do not provide the opportunity for collecting evidence. In addition to the classic anti-terrorism measures, in order to use the cyberspace against terrorist objectives, it is crucial sharing information at intergovernmental and international levels, as well as taking measures aimed at raising awareness. Educational activities should be actively used with the population, the access to communication channels should be limited for established terrorists, but in this regard communication with the holders of social networks is relatively difficult due to the policy of availability of these channels. It is important that during the fight against cyberterrorism, the state should carry out a balanced policy between national security interests and human rights**.**

REFERENCES

1. Defining cyber terrorism. Ruben Tuitel. Per concordiam - journal of european security and defense issues, vol. 7, issue 2, 2016. ISSN 2166-322x (print) ISSN 2166-3238 (online)

2. Statement for the record. worldwide threat assessment of the US intelligence community february 9, 2016

3. Defence Intelligence Agency. Russia Military Power - building a military to support great power aspirations. dia-11-1704-161. www.dia.mil/military-power-publications

4. **კიბერ თავდაცვა, კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების. პოლიტიკა, სტრატეგია და გამოწვევები. (ნაშრომების და სტატიების კრებული**).კიბერუსაფრთხოების ბიურო, თბილისი 2015 - ანდრია გოცირიძე და ვლადიმერ სვანაძე, კიბერთავდაცვა.

5. Joint statement for the record to the Senate Armed Forces Comitee. Foreign cyber threat to the United States of America. January 5, 2017