Scientific and Practical Cyber Security Journal (SPCSJ) 8(4): 78 – 81 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

CYBERTERRORISM: RISING THREATS AND STRATEGIC RESPONSES

Andro Gotsiridze

Cybersecurity Education and Research Centre

ABSTRACT. Cyberspace, as one of the domains of conflict, often gives a weak actor with few resources an asymmetric advantage over a strong opponent, as it provides the development and use of offensive capabilities with limited financial, human or organizational resources. With this, cyberoperations increase area of disinformation penetration and distribution, the ability to influence the audience, which is why they are widely used in information campaign production.
Nowadays, the most of cyber-attacks that cause immense damage, disruptions of financial loss are carried out by criminal organizations or state actors, not terrorist organizations. Nevertheless, cyber capabilities are developing all over the world, and proliferation control tools, financial and technical barriers are scarce and ineffective, which is why new technologies and intelligence vital to conduct cyber operations are becoming more and more accessible for terrorist organizations.
This article overviews those technical and organizational factors that increase the threat of cyber terrorism; it also provides a list of countermeasures to be implemented by the state and critical infrastructure.

KEYWORDS: Cyber attacks, cyber terrorism, RaaS, MaaS, DDoS- for-hire

INTRODUCTION

Non-state actors, financially motivated organized crime groups, hacktivists, and ideologically motivated cyber groups are spending increasingly more time developing their cyber capabilities and integrate cyber operations into their strategic agendas and means of achieving their goals.
The trend also applies to terrorist organizations. They have significant motivation to conduct offensive cyber operations, thus analyzing their cyber capabilities and the threats they pose is of great importance for both state and individual security.
Today, the cyber capabilities of even major terrorist organization, such as Daesh and Al-Qaeda, are rudimentary. There is no evidence that these groups are competent to conduct large scale cyber-attack that could cause casualties, significant damage, or destruction, however, there is evidence of the development of cyber capabilities and the increasing integration of cyber operations into terrorist operations.
Based on the analysis of the attacks described so far, the cyber potential of terrorist organizations can be characterized as Low Skill/Low Value Target (LS/LT) capabilities. Strategic planning of cyber operations is weak, vulnerability detection of target networks - ineffective, and the attacks themselves have little effect and are limited to defacement and low-tech DoS techniques. None of the known cyber-attacks to this day has caused any operational disfunctions, nor has resulted in damage of long-term strategic or tactical significance.[1] The attacks of cyber groups rarely have shown economic nature, their goal is propaganda, information retrieval, and publishing jihadist calls (including threats) on websites with large number of visitors, as well as recruiting followers through social media.
Given the significant conventional successes of anti-terrorist coalition in recent years, the necessary base of human or material resource for traditional terrorist attacks shrunk drastically, and the territories controlled by these organizations' state-like entities became almost nonexistent, which pushed them to use asymmetric methods to achieve their goals. Moreover, certain areas of cybercrimes developed

[1] A notable exception is Hamas' cyber capabilities, which actively use malware and sophisticated, high-tech cyberespionage techniques. This is likely due to cooperation with Iranian state actors.

significantly over the past decade, giving terrorist organizations access to previously inaccessible cyber capabilities with an even higher level of conspiracy.
Based on the above, the threat of cyberterrorism is growing and significant, and in order to develop effective countermeasures, it is important to consider the factors that are driving the significant growth of cyber capabilities of terrorist organizations.

Organizational and technical factors leading to the growth of cyber capabilities of terrorist organizations

ORGANIZATIONAL FACTORS

Due to the loss of controlled territories, a large part of terrorist organizations has transformed into a network coalition with a horizontal vector of expansion. The fragmentation of the territory led to the shift of focus from military and territorial goals to traditional terrorist acts. At the same time, the market for hacking tools has become more diverse, and the opportunity to use hacking services has emerged on the dark web, which has led to terrorist organizations' increased interest in cyberspace.
The following organizational factors should be considered as contributors in the significant growth of terrorist organizations' cyber capabilities:

- Radicalization or recruitment of Western resident lone wolves with relevant skills who can carry out cyberattacks against the targets of interest with minimal communication with the organization.
- Expanding the scope of recruitment: Intentions to develop cyber capabilities are detected in Southeast Asia, where compromise of websites are means to raise funds for terrorist activities or to support incarcerated extremists.
- Cooperation with states with highly developed destructive potential, which increases the threat of high-tech terrorist cyber-attacks.

TECHNICAL ENABLERS

While organizational factors like recruitment and collaboration have expanded the reach of terrorist groups, their growing access to advanced cyber tools and technologies further amplifies their potential for disruptive cyber operations.
RaaS[2]**, MaaS,**[3] and **DDoS- for-hire**[4] services, as well as other tools accessible on illegal forums, give terrorist organizations a chance to expand their capabilities in an easy, cheap way. The ability to coordinate actions remotely from a secure environment makes such attacks much more attractive to a new, technology-savvy generation of terrorist organizations, increasing the intensity of cyber operations.

[2] Ransomware-as-a-Service is a criminal business model wherein an interested party or organization can commission a cybercriminal group to carry out ransomware attacks on a chosen target. Over the past five years, several significant cyberattacks on critical U.S. infrastructure, such as the Colonial Pipeline incident, have been executed via Russian-based criminal operators like ReVil and DarkSide.
[3]. Malware-as-a-Service refers to a cyberattack model in which cybercriminals offer malicious software and its deployment on a target's digital infrastructure through illegal online marketplaces. This model is particularly appealing to resource-constrained, less capable actors as it eliminates the need for them to invest financial, human, and time resources in developing their own cyber capabilities, allowing them instead to leverage the offered service.

4. An illegal service that involves renting out infrastructure required for conducting DDoS attacks. The proliferation of such services creates additional risks by enabling individuals or organizations without the necessary technical or intellectual capabilities to carry out such attacks.

The usage of DDoS- for-hire enables terrorist organizations to conduct these types of attacks more effectively. There is data on attempts to purchase such a tool on illegal forums.

RaaS technology, widely spread on illegal forums, could become a source of additional income for terrorist organizations, as well as a tool to disrupt the functioning of an adversary's critical infrastructure or sow fear.
Another common illegal service, MaaS, allows terrorist organizations to penetrate industrial control systems or other critical infrastructure networks. However, it should be noted that using such a service is quite expensive and requires technological skills from the user's part, in this case the terrorist organization, and a high degree of coordination with the provider.
Aside from aforementioned areas, the growth of cyber capabilities can be achieved by acquiring high-level **zero-day exploits**,[5] hiring information security specialists, or recruiting them with the prospect of further education.
In order to obtain the information needed to cause cyber incidents with significant damage, terrorist organizations are likely to become more active in terms of collaborating with insiders of the critical infrastructure of target countries. Radicalization of the insider or recruitment with financial motives and obtaining sensitive information from them significantly increases the likelihood of a successful cyberattack.

PROPOSED COUNTERMEASURES

The potential targets of high-impact terrorist cyberattack are critical infrastructure facilities, which require robust defenses to mitigate risks.
To address the growing threat of cyberterrorism, the following measures are recommended:

- **Strengthen International Cooperation**: Enhance information-sharing between nations and agencies to improve incident detection and response.
- **Develop Public-Private Partnerships**: Foster collaboration between governments and private sector stakeholders to strengthen critical infrastructure defenses.
- **Implement Insider Threat Mitigation**: Introduce programs to monitor and counteract insider threats at critical infrastructure facilities.
- **Leverage Social Media Analysis**: Integrate social media content analysis into signals intelligence (SIGINT) to detect and disrupt planning for terrorist cyberattacks.

CONCLUSION

The evolving cyber capabilities of terrorist organizations pose a growing threat to global security. Although their current capabilities are limited, their access to advanced tools and the growing availability of cybercrime services signal an urgent need for proactive countermeasures. Strengthening collaboration, improving defenses, and addressing insider threats are critical steps to mitigate the risks of cyberterrorism effectively.

ACKNOWLEDGEMENTS

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220.

[5] . A zero-day exploit refers to a cyberattack that leverages an undisclosed software vulnerability, giving developers no time to patch it. These exploits are highly dangerous and often used in targeted attacks by cybercriminals or nation-state actors.

BIBLIOGRRAPHY

1. Cyber Terrorism: Assessment of the Threat to Insurance, Cambridge: Centre for Risk Studies, November 2017.
2. ICCT Press Publication. Handbook of Terrorism Prevention and Preparedness. July 2021. Chapter 29. Shashi Jayakumar. Cyber Attacks by Terrorists and other Malevolent Actors: Prevention and Preparedness. DOI: 10.19165/2020.6.01 ISSN: 2468-0486 ISBN: 9789090339771
3. G. Weimann; 2005. 'Cyberterrorism: The Sum of All Fears?', Studies in Conflict & Terrorism. 28:129-149, 2005
4. Simon P. Handler. THE CYBER STRATEGY AND OPERATIONS OF HAMAS: Green Flags and Green Hats. Atlantic Council Cyber Statecraft Initiative. 2022.
5. Michael Schmitt, "Normative Voids and Asymmetry in Cyberspace," Just Security, December 29, 2014