Volume XXI 2018
ISSUE no.1
MBNA Publishing House Constanta 2018

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

About modern terrorist activities in cyber space

To cite this article: Radu Moinescu, Dragoș GLĂVAN, Scientific Bulletin of Naval Academy, Vol. XXI 2018, pg. 90-96.

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-18-I1-013

About modern terrorist activities in cyber space

Radu MOINESCU[1], Dragoș GLĂVAN[2]

[1] Ph.D. Student, Military Technical Academy – Systems Engineering for Defense and Security Doctoral School
E-mail: radu.moinescu@gmail.com

[2] Ph.D. Student, Military Technical Academy – Systems Engineering for Defense and Security Doctoral School
E-mail: dragos.glavan@gmail.com

Abstract. Cyber space has become a vital element for terrorist entities because of the multitude of opportunities that it offers. The article presents an evolution of the use of cyber space for terrorist purposes, from advertising and propaganda platform, to recruiting, influencing or intimidation platform, and even to the development of specialized software for encrypted communications and the possibility in development of cyber threats.

1. Status

Cyber space has become as important as physical space for terrorist entities, which should be an alarm signal for international organizations involved in the fight against terrorism.

Advertising continues to be the main target of terrorist organizations, the means of communication evolving from the stage of narrative reporting to written press, radio, television and the Internet, the latter reinforcing the propaganda power of terrorists as they are the ideal tools for propagating ideas included in the sphere of terrorism. It is well known that terrorists and supporters of Jihad use cyberspace as a platform for transferring operational messages.

It can be noticed that after the attacks of September 11, 2001, a new side of terrorism, namely cyberspace-oriented terrorism emerges. This side of terrorism has the most significant rise and diversification since the Arab Spring (2011).

The main uses of the cyberspace by the terrorist entities are, at present, the following:

- collecting information;
- dissemination of terrorist propaganda;
- proselytism and radicalization;
- collecting and transferring funds;
- disseminating materials on preparing for attacks;
- coordination of activities and exchange of secret messages;
- support during the preparation and execution of the attacks.

However, the ultimate strategic goal of terrorist entities is to manipulate public opinion by any means, so that it can pressure / compel decision-makers to surrender to the claims of terrorists. Thus, the population becomes a tool in the hands of terrorist entities to form a political and religious agenda that justifies the execution of terrorist acts.

2. Collecting information

The development of WEB technologies has caused, besides the indisputable benefits provided by the explosion of mass communication (the trafficking of an enormous amount of information and the increase of social cohesion), negative effects such as the upward trend of terrorist activities undertaken online.

Sites such as Facebook, LinkedIn, Twitter, GoogleMaps, or Wigle.net are important and inexhaustible sources for terrorist organizations to get information about someone or a target and have become an important step in preparing and launching an attack.

Live streaming webcams are also an important tool in checking field conditions without requiring physical presence on the ground. Various time variations can be studied such as congestion, traffic conditions and the deployment of law enforcement.

Another opportunity by which terrorist organizations (and not only) can obtain valuable information is the use of the Shodan search engine. It can provide information on industrial control systems, air conditioning systems, servers, routers, web cameras, printers and other devices connected to the Internet, belonging to industrial entities, hospitals, schools, etc. Furthermore, they can be sorted by country, brand, model, version, etc. due to a specific query set provided by the site.

3. Using cryptography, steganography and anonymization techniques

One of the most fascinating aspects of cyber-terrorism operations is the use of cryptography, steganography and anonymization techniques, and this despite the initial refusal to use Internet technology. Terrorist organizations and groups have realized, however, that it is almost impossible to keep in touch with their members over long distances without the use of modern technologies.

After the attacks of September 11, 2001, US security agencies sought to intercept information to help them counter other potential terrorist plots of al Qaeda and others. This has made terrorist organizations rethink the way they communicate.

Fig. 1. Mujahedeen Secrets v2.0 Graphical User Interface

At the beginning of 2007, Al-Qaeda launched an encryption tool called "Mujahedeen Secrets" (Asrar al-Mujahideen) through the Global Islamic Media Front (GIMF). Its main features were:

- symmetric key encryption using one of the final algorithms designated by the National Institute of Standards and Technology (NIST) in 1998 (Rijandel, Serpent, Twofish, RC6 and MARS);
- symmetric encryption key size of up to 256 bits;
- 2048-bit asymmetric key encryption using the RSA algorithm;
- automatic identification algorithm encryption during decoding;
- secure file deletion.

A year later, in 2008, the second version of the Mujahedeen Secrets was released (Fig. 1). It contains some improvements such as:

- multicast encryption via text messages on forums;
- transferring different forms of text files encoded into forums;
- producing digital signature files and ensuring that they are accurate. [1]

The second version of the toolkit demonstrates the existence of a software development life cycle with a certain level of sophistication and planning by launching patches and new features.

Another encrypted communication method was developed by Rajib Karim, a former British Airways employee convicted of plotting terrorist attacks against British and American aviation and raising funds for terrorist organizations.

The method used several steps in message encryption and was used to communicate with his brother in Yemen, who was in contact with Anwar al-Awlaki. In the first stage the messages were copied to an Microsoft Excel table, and using a macro was made a substitution encryption. In the second stage, the result of substitution encryption was copied and inserted into Microsoft Word documents, which were then saved using the password protection function. Using this document protection feature is considered safe as long as a long and complex password is used. In the third stage, the Microsoft Word documents were password-protected using the RAR archiver program. Finally, the archived files were uploaded to hosting sites by using Shortener URLs in an attempt to anonymize the metadata. Avoiding the use of public e-mail services is a common feature for terrorist organizations and groups in their attempts to circumvent automatic alert systems. Although the method of communication used by Rajib Karim is apparently secure, he made a few mistakes that led to his capture and incrimination: he did not use complex and long enough passwords to protect documents, and the worst was to keep his passwords and encryption methods in Microsoft Excel files saved on his computer. [2]

After the release of NSA documents on mass surveillance by Edward Snowden in June 2013, there is an increased pace of innovation by launching new Jihadist platforms and three new encryption tools from three different organizations: Global Islamic Media Front (GIMF), the Al-Fajr Technical Committee (FTC), and the Islamic State of Iraq and al-Sham (ISIS).

On September 4, 2013, GIMF launches "Tashfeer al-Jawwal," the first Islamic mobile application to transmit encrypted SMS along with the ability to send encrypted emails. The application uses the TwoFish algorithm in CBC (Cipher Block Caining) and Elliptical Curve Encryption to exchange 192-bit encrypted keys. [3]

"Asrar Al-Ghurabaa" is another alternative encryption software launched by ISIS in November 2013, period coinciding with the breaking of this group from Al-Qaeda after a power struggle. ISIS says it is the only Islamic encryption program that uses proprietary algorithms. However, it is difficult to conclude this as this software apparently no longer exists.

On June 7, 2014, FTC, Al-Qaeda's exclusive online propaganda distributor, launches the Android version of the "Amn al-Mujahid" encryption program that uses 4096-bit public key encryption.

Steganography is another technique used by terrorist organizations to conceal messages and, implicitly, to communicate.

Among the first reported cases of using this technique were the radical group Front of the Revolutionary People's Liberation Party (DHKP-C), which used this technique to hide messages into JPEG and GIF files in order to communicate safely through public e-mail systems. [4]

On May 16, 2011, Austrian citizen Maqsood Lodin was detained and interrogated by the Bundeskriminalamt (BKA) after traveling from Pakistan to Berlin via Hungary. An external memory card containing multiple files, including an adult video, was found on it. After a thorough analysis, the German investigators have determined that over 100 files were hidden in the video using steganographic techniques with password protection features. After the password was broken, it was determined that the hidden files included training for terrorists and future plans for seizure of cruise ships and attacks on Europe. [5]

Becoming as important as encryption of data and communications, online anonymization is another tool used by terrorist entities.

The Onion Router (TOR) is one of the most popular, popular and handy online anonymity tools thanks to an almost-in-near routing algorithm. However, this anonymization method is not perfect since trafficking from both ends can lead to user's location.

On April 26, 2016, ISIS publishes in the online Dar al-Islam, written in French, an article titled "Sécurité Informatique", demonstrating the importance of using secret communication. The article is a guide to: installing and setting up The Amnesic Incognito Live System (TAILS), connecting to the TOR network, creating PGP keys, encrypting emails, and using XMPP / Jabber-based communication tools.

Mentioned more and more on jihadist forums, "TAILS" is a free operating system, based on one of the most popular Linux distributions, Debian. Designed to run from a live medium such as DVD or USB memory, it was chosen by terrorist entities for leaving no traces of use, thereby reducing mistakes made by users. Moreover, "Tails" includes a TOR that allows access to the hidden part of the Internet, the so-called "Dark Web," in which a lot of illegal activities take place and it is possible to find any resources in complete anonymity. [7] [8]

4. Social Engineering Techniques

Terrorist entities have realized that their operations may be successful by using social engineering techniques. Their use seems to get people out of sight.

The induction of panic among "Allah's enemies" is one of the main social engineering techniques used. The smallest rumor about an imminent terrorist operation is spread immediately in the online environment, especially through social networks platforms, spreading terror among the civilian population, uncertain and unknowing of what it has to do to deal with such a situation. The approach is supported by a well-coordinated history of al-Qaeda's threats, with the onset of the attacks, so that as soon as they begin to appear as a warning on the terrorist sites, they are taken over and transmitted as a first step a renewed series of attacks. The fact that many such messages were made public on the Internet - without any attempt to materialize - seems to have been ignored.

Probably the most conclusive example of civilian panic incitement was the enormous power surge in the Northeast of the United States and Canada on August 14, 2003. The incident raised the question whether or not it was a cyber terrorist attack because at August 18, 2003, the Egyptian daily Al-Hayat published extracts from a press release from Al-Qaeda, apparently obtained from the International Islamic Media Center website. The content of the communiqué said the Abu Hafs al-Masri Brigade group, al-Qaeda associated, had claimed up to the power outage, and the operation was done on the orders of Osama bin Laden. The communiqué does not specify how the alleged sabotage has been made, but it has produced a claim for the damage to the US economy in the fields of finance, transport, energy and telecommunications. To counter this information, the Federal Bureau of Investigation and the United States Department of Security presented in April 2004 a report stating that power shortages arose from natural causes and not as a result of acts of terrorism. [9]

Fear, the tactical objective of traditional terrorism, is another intense weakness speculated by terrorist entities in the cyberspace to support the achievement of the strategic goal, namely, the

attainment of the political goals motivating the action. Therefore, the immediate target of terrorists is to create panic rather than destroy the target. From this perspective, violence is used both to scare the population, to remove the opponents, but also to maintain control over a mass of people. Basically, when terrorist entities post photos or videos that show bombings, hostage-taking, or executions in the online environment, it turns into a weapon to induce fear and insecurity.

Another technique of social engineering used by terrorist entities is sympathy. Its use is through social network platforms, characterized by the worldwide launching of campaigns and requests from their supporters around the world. An example is the June 20, 2014 campaign when ISIS has asked supporters to post their messages, photos and videos waving their flags or a hashtag in English, #TheFridayofsupportingISIS as proof of their loyalty to the organization. [10] ISIS's strategy for using the hashtag symbol is also part of violent posts, such as the executions threats of American journalist Steven Sotloff, #StevensHeadInObamasHand.

Although we do not think that this weakness can be used by terrorist entities, compassion is often exploited by them. By using it, terrorist organizations have the opportunity to obtain various benefits, but also the proximity of other individuals to support and promote the terrorist cause. It is usually done by posting images and videos elaborated and edited with great attention in which victims of the anti-terrorist coalition bombings are presented, sometimes dramatized by the addition of slow-moving sequences.

Last but not least, the recruitment of fighters is also done through social engineering techniques. As part of the recruitment strategy, social networking videos are short videos about the life of mujahedin, how they help the civilian population, how they are offering candy to small children etc. Members' testimonies are also highlighted, which explains why they have left their family to join the cause, and that they do not lack anything, thus becoming an attractive opportunity for every recruiting potential.

5. Cyber threats

Although at present there is a wide variety of offensive cybernetic capabilities available to anyone, terrorist entities have not shown an advanced use of them. The types of cyber-attacks used by these entities were Distributed Denial of Service (DDoS) attacks using a tool called "Caliphate cannon", website defacement and phishing, with victims being "soft", such as small businesses with poor data security and the impact of which is negligible. An example of this is the cyber-attack launched on July 8, 2015 by the Cyber Army of the Khilafah (ISIS affiliated hacker group) on the Syrian Observatory for Human Rights (SOHR) site. The hackers managed to compromise the data stored on the servers and replaced the first page of the site with a fake image depicting SOHR director Rami Abdel Rahman, dressed in an orange jumpsuit and kneeling beside an ISIS executioner (Fig. 2). The cyber-attack did not have a significant impact on the online publication because all the data had backups. [11]

Although they claim to have greater attack capabilities, they have so far failed to compromise important companies such as Facebook, Google or Microsoft.

With access to the TOR and implicitly to the hidden part of the Internet, terrorist entities can play the role of financier in the development of cyber threats, they can act as a client in acquiring them, or both or by hiring Cybercrime-as-Service (CaaS) under anonymity.

As they develop their capabilities and adopt new attack vectors, terrorist entities will look to:

- damage electricity distribution networks by shutting down control systems;
- discontinue the services of the national electronic communications networks;
- sabotage air traffic systems;
- attack oil refineries and gas transmission systems by damaging control systems;
- destroy or alter bank information on a large scale, thus damaging the financial sector;
- remotely alter medical information;
- gain access to the dam control systems to cause massive flooding.

Fig. 2. Fake image posted on the SOHR site after being hacked.

Therefore, the use of cyber-attacks by terrorist entities involves the use of fewer resources and can cause more damage to a country than an army of several thousand people. The fact that a single computer through an Internet connection could cause as much damage as using a traditional weapon, such as a bomb is becoming more attractive to terrorists and I see an increasing interest in this area.

6. Conclusions

The operations carried out by terrorist groups in the cyberspace are very topical, and they will not disappear, but will, on the contrary, diversify and amplify. Terrorist acts are and will continue to be atypical, totally lacking in morality. The threat of terrorism has become increasingly pronounced, being proportional to the vulnerabilities of modern society, and evolving as the rifts widen, conflicts are amplified, and crises are multiplying.

Romania is subject to terrorist threats from at least three perspectives: as a member of the North-Atlantic Alliance and the European Union, as part of the Western civilization against which part of the terrorist attacks and especially those of Islamic fundamentalism are directed; as a country in the vicinity of the Muslim strategic flaw in the Black Sea and the Balkans, not far from the Caucasus and the Near East; as a direct participant in the war fought against terrorism in the United States-led anti-terrorist coalition.

The outlook for the evolution of the terrorist phenomenon in cyberspace needs to be the subject of strategic assessments both domestically and in consonance with those of the North Atlantic Alliance and those of the European Union, so that the best-appropriate formulas for discovering and combating terrorism or related activities in cyberspace.

Scientific research in the main defense, public order and national security structures can play an important role in developing a system of criteria and indicators for assessing threats, threats and terrorist threats, so that any terrorist attacks on Romania's territory.

References

[1] Robert GRAHAM, *How Terrorists Use Encryption*, CTC Sentinel, June 2016, Volume 9, Issue 6, pg. 20-26, http://www.dtic.mil/dtic/tr/fulltext/u2/1013820.pdf

[2] Vikram DODD, *British Airways worker Rajib Karim convicted of terrorist plot*, The Guardian,

February 28, 2011, https://www.theguardian.com/uk/2011/feb/28/british-airways-bomb-guilty-karim
[3] Jihadology, *New release from the Global Islamic Media Front: "Mobile Encryption Program: For Sending Encrypted SMS and Files and For Android and Symbian Mobiles"*, September 4, 2013, http://jihadology.net/2013/09/04/new-release-from-the-global-islamic-media-front-mobile-encryption-program-for-sending-encrypted-sms-and-files-and-for-android-and-symbian-mobiles/
[4] Siddik EKICI, Hüseyin AKDOGAN, Eman RAGAB, Ahmet EKICI, Richard WARNES, *Countering Terrorist Recruitment in the Context of Armed Counter-Terrorism Operations*, IOS Press, 2016, ISBN 978-1-61499-612-5, pg. 89
[5] Nic ROBERTSON, Paul CRUICKSHANK, Tim LISTER, *Documents reveal al Qaeda's plans for seizing cruise ships, carnage in Europe*, CNN, May 1, 2012, http://edition.cnn.com/2012/04/30/world/al-qaeda-documents-future/
[6] Michael T. RAGGO, Chet HOSMER, *Data Hiding: Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols*, Elsevier, 2012, ISBN 978-1-59749-743-5, pg. 193
[7] Dar al-Islam, *Sécurité Informatique*, April 26, 2016, nr.9, pg. 38-53
[8] Thomas Fox-BREWSTER, *ISIS Doesn't Trust Tor, Likes Snowden's Favorite Operating System (And Still Can't Hack Much)*, Forbes, April 28, 2016, https://www.forbes.com/sites/thomasbrewster/2016/04/28/isis-doesnt-trust-tor-likes-snowdens-favorite-operating-system-and-still-cant-hack-much/#7990fa85720b
[9] US Department of Energy, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004, https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf
[10] Faisal IRSHAID, *How ISIS is spreading its message online*, BBC, June 19, 2014, http://www.bbc.com/news/world-middle-east-27912569
[11] Syria Observatory for Human Rights, *ISIS Hacks Syria Observatory for Human Rights Website*, July 16, 2015, http://www.syriahr.com/en/?p=25012