ZOLTÁN ANDRÁS NAGY

Terrorists who make their mark online

The opportunities provided by the Internet (Internetworking System) are used and exploited by criminals and criminal groups.

The question is whether there are differences between the use of the Internet by the terrorist organizations or their members and the lone terrorists?

There are similarities between the actions of the two groups of criminals:

- The aims and/or motivations. Typically, there is no difference between the two groups of offenders. The goals and motives can include national, ethnic, separatist aspirations, neo-Nazi, white supremacy racist or other extreme political or politically rooted ideology.
- The aims and motives can be intertwined. Violence used in the name of neo-Nazi ideology can be both politically motivated and directed against Jews. The actions of Muslim extremists can also be directed against the Western world's denial of the Christian religion (its political system, lifestyle and value system.)
- The site of potential attacks of both groups of perpetrators can be both the real and the virtual world.

In the case of attacks carried out in the natural sphere, the reasons why Internet monitoring is so important include the clarification of the target, the method of the attack, the communication before and after the commission, the timing of terrorist attacks against the same target and the same method, which can help the investigation in real space with other evidence.

Both the terrorist organization and the lone terrorist can remain hidden during an attack carried out online and offline. Traces and hints of their actions can be found by evaluating the identifiers used (pseudonym, monogram, tricks, TC/IP number, etc.), the method and purpose of the network attack, although other tools are also needed to identify them in this context. There are typical network attacks, such as hacking, malware, DoS, DDoS, blackmails - attacks, the defacing etc.[1]

Differences can also be discovered between two groups of perpetrators:

– Concerning the aims and motives mentioned above, in addition to political and religious motives, as well as similar reasons and goals, attacks carried out with an individual goal, for themselves, e.g. for profit, kidnapping, asserting a particular claim, and motiveless or irrational attacks are characteristic of lone perpetrators.

Psychopaths are especially dangerous.[2]

At the same time, actions aimed at disrupting the social-economic-political order or exchanging hostages can be characterized as the goal of terrorist organizations.

– Attacks carried out by mail are typical of the lone terrorist.[3] Theodore John "Ted" Kaczynski (called Unabomber) was a specialist in letter bombs. But letters containing anthrax are also known cases.

[1] Dornfeld, L. (2019): Kiberterrorizmus – a jövő terrorizmusa? [Cyberterrorism - the terrorism of the future?]. In: Mezei Kitti (ed) A bűnügyi tudományok és az informatika, Budapest – Pécs. 47-63
Nagy, Z. (2016): Kiberbűncselekmények, kiberháború, kiberterrorizmus [Cybercrime, cyberwar, cyberterrorism]. Magyar Jog 63. 2016/1. 17 - 24

[2] Fanatical psychopaths hide the danger in their name, but so do affective psychopaths, who are characterized by emotional fluctuations and excessive emotional reactions, hysterical psychopaths who often hide from the world, but are often unable to form social relationships, etc.

[3] Simon, J. (2013): Lone Wolf Terrorism: Understanding the Growing Threat, Prometheus Book, New York. 87-88

In terms of appearance on the networks, the differences are:

Organizations declared terrorists by the Western world have a greater personal and material potential in their appearance on the Internet:

- Maintenance of own servers, server parks or raid servers.
- False, so-called use of "traveling" TC/IP numbers to measure computers and servers and prevent their paralyzing.
- Editing and maintenance of an own website in order to provide fast, multilingual, comprehensive multimedia information. The propaganda about their activities exaggerates their successes and trivializes their losses (For example, Chechen kavkazcenter.com – it has not been reached). Remember that there is a solid Wahhabi community in the province of Sandzak in southern Serbia, who, together with their Wahhabi brothers, aspire to create an Islamist state that includes Kosovo, Sandzak and Muslim Bosnia. Many Chechens and al-Qaeda members are Wahhabis belonging to the radical Muslim reformer movement.
- Their pages, with their profoundly religious content (this is typically the case with jihadist sites), also serve as a means of recruiting members with the possibility of exchanging files with young people. In more than one case, a movie can be downloaded from Palestinian sites before it has been shown in Hollywood.[4]
- Information can be hidden on web pages without encryption (steganography – a well-known, established solution), which may contain instructions and information. Images downloaded from websites, for example, can hide completely different content.
- Other options are also known, for example, an FTP network protected by a password or other identifier. Communication takes place through this hidden network, or by opening an e-mail account that does not distribute, but the entrants send their written messages to

[4] Source: https://www.cnet.com/tech/home-entertainment/in-refugee-camp-a-p2p-outpost/
Accessed: 02.05.2022

the "they communicate by leaving" draft. It is worth paying attention to existing e-mail accounts from which there is no outgoing data traffic.
– Providing news information about the organization, their activities, battles, victories and losses ("their heroes").

News can be published on legal news sites and content providers, the sympathy of the Basque and Northern Irish sites for ETA and the IRA is noticeable. Often ("cover") websites appear, not under the name of a terrorist organization, but essentially promoting their propaganda.[5]

The communication interfaces of lone terrorists on the Internet can be their own web pages, blogs, forums, on social media sites, but – presumably due to the relative complexity of this (creation, maintenance, payment of fees to the service provider and other reasons) – it is more practical to use options that provide space for further communication.

The solitary offender is often characterized by sociability, they are unable to keep their views, opinions and future actions to themselves, they expect confirmation from others or feel compelled to share them and want to brag about their idea.[6]

Anonymity "offers" personality change on a tray. Users often put off their insignificance and greyness, break out of it and hide in a new personality, and they can promote radical views, "create order" and write

[5] Nagy, Z. (2009): Bűncselekmények számítógépes környezetben. [Computer-related crime]. Ad-Librum, Budapest. 224-226

[66] In addition to the following cases, an example is the crime of ex-Yugoslav origin Muharem Kurbegovic, who carried out the first bombing at Los Angeles airport (hence his name, the so-called "Alphabet Bomber"). In August 1974, he set off an explosive device containing flammable materials, which killed three people. 36 people were injured in the attack.
Source: http://hadmernok.hu/2009_4_horvatha.pdf
Accessed: 20.05.2022
Kurbegovic spoke about his plans on tapes and shared them over the phone with a close friend. It would be worthwhile to carry out extensive psychological studies in this area as well.

about solving the problems of society, which they will resolve themselves or contribute to the solution. Then this "noble mission" created by them can become a fixed idea, fixed in their psyche, which can be confirmed by others. Ultimately, this obsession typically culminates in an act committed in the real world, such as an armed attack against an enemy fixed in the offender's imagination.

– Apart from web pages, writing blogs, comments on blog posts, communication on video-sharing portals, in "forum sections" organized around the same topic and chat rooms based on the same interests can potentially reach many users, although their range may be smaller in rooms. Still, this communication reaches an unsuspecting audience (sympathetic to him or his actions). And in e-mail, two or a few people can have access to what the lone terrorist has to say.

Let's look at one case from the recent past. An example of communication on someone's own page: Joseph Stack published his farewell letter, which concluded: "violence is not only an answer, that's the only answer" 18 February 2010, on his website, embeddedArt.com. He drove his small airplane to the building of the tax authorities next day.[7] Was his suicidal individual action the inspiration for the coordinated al-Qaeda terrorist attacks on several cities in the United States 11 September 2011? Did al-Qaeda learn from the incident, unlike the CIA?

The various social and video sharing portals are suitable for the exposure of users – often in the strict sense of the word. The messages "Palestine we are with you" and "Sympathy with Gaza" first appeared on the myspace.com profile of Colleen LaRose (later known as Jihad Jane), and then on another social site Dailymotion.com and the video sharing portal Youtube.com. She condemned the Israeli occupation of

[7] Source: http://kitekinto.hu/amerika/2010/02/20/kamikaze-tamadas_erte_az_amerikai_adohivatal/#.UkCgAtIvnSs.
Accessed: 05.20.2022

Arab territories, the policy of the state of Israel towards the Arabs and its tools, all the while referring to the killing of the Swedish graphic artist Lars Vilks, who made ironic drawings of the defining figures of the Mohammedan religion.[8]

In blogs (web-logs "diaries of the web") communication is typically thematic. Therefore, they are also suitable for forming a community among those with the same interests. The communication can be uploaded in any file format (there are video, music, image blogs). Blogs can bring, „collect" like-minded users together. The criminal proceedings against Ábel Somogyi are still ongoing, it may be proven that he tried to kill several fellow students, and then fired shots in a fast food restaurant in Budapest. However, it is a fact that he wrote hateful and slanderous posts on blog.hu under the pseudonym "Arszák". His writings, which can still be read on the blog and on iviv, bear witness to his hatred: *"I have boundless hatred for all the bastards who stand in front of me in line."*[9]

The Norwegian Breivik also expressed himself in forum columns. On Document.no he voiced his opinion 75 times, which could be classified as extreme. James von Brunn openly voiced his Anti-Semitic views on several forums, operated a Jew-hating website, and later wrote a book with such a tone. He came under the purview of the FBI, but it was deemed that his communications did not exceed the limits of freedom of expression. His hatred of Jews culminated in a murder, 10 June 2009; he killed a guard at the Holocaust Memorial Museum in Washington.

Stormfront, one of the chat-rooms that give room to extreme ideologies, which is still operating today, is where Richard Poplawski often chatted. His antisocial behaviour was indicated by the worst rating he received from the army, when he was discharged. 4 April 2009 Poplawski shot and wounded three police officers.

---

[8] n.a. (2012): Internet Radicalization: Actual Threat of Phantom Menace? Analysis and cases. US. Gov. Dep. of Defense, Naval Postgraduate School. 45-49

[9] Sources: http://blog.hu/user/114820/tab/activity,
and http://iwiw.hu/pages/user/userdata.jsp?userID=9344869.
Accessed: 05.20.2022

Nidal Malik Hasan of the United States served as a Navy psychiatrist. His relatives still live in Ramallah, the seat of the Palestinian National Authority, in the West Bank. In the United States, he attended the Muslim community that included the two perpetrators of the 9/11 terrorist attack, Hani Handzur and Nawaf al-Hazmi. The latter also fought in Bosnia, on the side of the Wahhabis there and the Chechen and other Arab Wahhabi volunteers who fought with them. At that time, the leader of the Muslim community was called Anwar Al-Awlaki,[10] who left the USA in 2004 and went to Yemen, where he was imprisoned. Awlaki's perception had already been radicalized at the time of the 2001 terrorist attacks, and later this became even more complete. From 2008, Al-Awlaki and Hasan exchanged twenty e-mails with each other (that is all they found on his computer), as a result of the profoundly religious messages, 5 November 2009 twelve soldiers and one civilian were killed in Fort Hood, Texas, which was preparing soldiers for deployment in Afghanistan, and another nineteen people were injured.

Bruce Ivins, a doctor at the US Army Institute of Infectious Diseases, recommended anthrax to his colleagues in an e-mail in 2001. That year, 5 people died in the United States from anthrax powder sent in the mail. Ivins committed suicide at the time of his indictment. The innocence of Ivins is raised, but the investigating authority is convinced of the guilt of the scientist, classified as a sociopath. Ivins researched and perfected anthrax for 18 years. Maybe he wanted to test the killer effect in a real environment? No one else was willing to do it, so he did it?

[10] Until his death, Anwar al-'Awlakī was one of the most dangerous and effective Islamic proselytes, his name came up due to his contact with the perpetrators, for example, in the 2005 London, 2006 Toronto, 2007 Fort Dix, and 2010 New York assassination attempts and in other cases.

Perhaps the opinion that the chat-room is the most popular and dangerous area for communicating ideas and persuasion on Internet communication deserves attention.[11] Sadly, information about how to create weapons and bombs are easily available on the internet.

However, not all the terrorists appear on some surface of the Internet. We can also find plenty of examples of introverted criminals.

How can users hide? The most obvious is that they register with a fake e-mail address, or they use a mail system that is not located in some remote country, remote island, where they will not be able to catch up.

For anonymity, additional options are also provided.

– using the computer of a real user left on by someone else or sharing their IDs.
– Internet cafes.
– via WiFi connection. In this case, the called server only logs the router's TC/IP number, but the server cannot "know" which of the several users connected to the router's signal (who is behind the router). The router should log in, but there are still technical obstacles to this today.
– In this case, the identity of the users can be found out by using other methods, e.g. testimonies (e.g. in premises, on trains, long-distance buses) or camera recordings of premises (schools, universities, office buildings, catering establishments) and public areas. (If users in public areas do not hide in the camera's blind spot.)

Users can also hide by using an anonymous public proxy server. By the way, it is extremely easy to hide "behind" these servers. The so-called anonymous public proxy is one "degree" more secure. Other methods include:

[11] Sagemon, M. (2008): Leaderless Jihad: Terror Networks in the Twenty-First Century, University of Pennsylvania Press, Philadelphia. 115-116

- distorting proxy servers. This type of proxy intentionally provides a fake IP, i.e. it also hides the location of the proxy server. The "safest" though is:
- the high anonymity proxy. These don't even show themselves as proxies to the outside, it appears as if the user himself were calling the targeted server, at most the TC/IP number is either fake (does not match the country assigned by the geographic-mathematical formula) or does not exist.

Communication can be easily hidden if the messages are left in the "draft" application of the e-mail account, and then they can be read and deleted after logging in, or a new one can be written to others. However, a common difficulty during the investigation is that, although the subscriber's name and address can be clarified based on the IP number – in a matter of seconds –, the question is still who used the computer (and the Internet) at the time in question. To find this out, classic forensic methods, tools and methods are used. Manipulation (forgery) of the TC/IP number requires more serious preparation.

What can we do against threats from virtual space?

The fight against terrorism, like the phenomenon itself, is complex in nature, and it is necessary to "fight the battle" simultaneously in real and virtual space.

1. Theoretical knowledge of IT dangers and abuses.
2. Defence and prevention are not different from the otherwise necessary physical protection of electronic data processing and transmission systems.
3. Part of the anti-terrorist strategy is the unification of national databases, the mutual and rapid exchange of information about terrorist manifestations appearing and available on the networks.
4. The monitoring of networks should extend to destructive web pages (blogs, forum sections), WAP and chat rooms, especially the chats of people exchanging ideas about extreme views. Attention should

be paid to radicalizing users, e.g. to identical or nearly identical aliases on different forums, blogs and chat rooms. The content of communication, the same expressions and turns of phrase can help with identifying the perpetrator's profile.

5. Monitoring and limiting the Internet in democratic conditions is not an easy issue. German Minister of the Interior Hans-Peter Friedrich stated after Breivik's "rampant" that this assassination made it obvious that the general anonymity of internet blogs and online speech must be abolished, just as the spread of "horde ideas" must somehow be restrained.
6. Continuous training of "good hackers" and increasing their numbers in the various services, national defence, and the police by promoting them to status. (Priority scholarships for students at technical faculties, students majoring in computer science.)[12]
7. More frequent advertising of tenders (e.g. fight against destructive websites, involvement of the Internet community in the fight against them).
8. It is clear that the fight against terrorism involves the possibility of increased control over members of society. There is no such thing as a "what if" question, i.e. asking if Breivik's horrific assassination plan had been known sooner, perhaps his actions could have been prevented. However, regarding the future, serious, reasoned thinking is needed in order to detect the dangers (views, harmful content) and dangerous people inherent in the World Wide Web, and to create legal frameworks against them.
9. This harmful effect of the Internet must also be presented. It is necessary to illustrate with concrete examples and cases why it is important to curb the freedom of the Internet (credible, real registration of the authors of blogs, and even so the user could write or upload data files under a pseudonym or phantom name). It could be paralleled with other, albeit restrictive, measures that serve our

[12] Ibid. 115-116

safety, e.g. with airport baggage inspection. These could perhaps help to establish the rules for acceptance of control.

It is an interesting contrast that while one part of society is eager to guard personal data and information belonging to the intimate sphere, another part freely shares their personal data, horribile dictum – their current locations, helping criminals to obtain information. Education in responsibility would be needed in this area as well.

Terrorism is today's reality, terrorists live here, walk and are brought up among us. They differ from us only in their vile thoughts, in their intent to do horrible destruction. The lone perpetrators are mentally ill, struggling with personality disorder, "grey" people who find their evil selves on the Internet, wanting to break out of their insignificance. It is there that they shout out their distorted, crazy thoughts to the world, there they find companions who are the same or are close to them, and with whom they can shout together, ... so that they can then go to their doom, to kill and drag many with them .... into death.

In order for society to be able to protect itself, these shouters must be detected and isolated. Let us not regret the price. The loss of fellow human beings would cost much more than that!