ТЕМЕ, г. XLV, бр. 1, јануар – март 2021, стр. 95−109

Прегледни рад https://doi.org/10.22190/TEME201119006T
Примљено: 19. 11. 2020. UDK 323.28:28]:004.738.5
Ревидирана верзија: 5. 2. 2021.
Одобрено за штампу: 26. 2. 2021.

CYBERSECURITY – VIRTUAL SPACE AS AN AREA FOR COVERT TERRORIST ACTIVITIES OF RADICAL ISLAMISTS

Darko Trifunović*

University of Belgrade, Faculty of Security Studies, Belgrade, Serbia

Abstract

Over time, terrorism has evolved into different forms. One of the most dangerous is certainly cyber terrorism. There are many different motivations for terrorists to deploy cyber terrorism as a tool in their fight. Internet and computer networks are powerful resources on which contemporary society relies heavily. Terrorist groups have developed new tools and methods of the fight and they have become more effective, efficient, and unpredictable. Virtual, or cyberspace, is perfect and very safe ground for terrorist groups' various activities, such are secret encrypted communication, file sharing, indoctrination and recruitment of vulnerable individuals, fundraising and promotions of their future actions and accomplishments spreading fear among common people. Are we adequately aware of these facts and prepared for countermeasures? The fact is that terrorists use mostly open-source tools (software) for their purposes, widely available and free of charge, as well as video games, popular social networks (mostly Twitter), and software developed by their programmers. The purpose of this paper is to point out some of the methods radical Islamic terrorist groups have been using and underline the importance of responding to this new security challenge.

Key words: cyber terrorism, Islamic terrorists, Anonymous, steganography, the Islamic state.

САЈБЕР БЕЗБЕДНОСТ – ВИРТУЕЛНИ ПРОСТОР КАО ПОДРУЧЈЕ СКРИВЕНИХ ТЕРОРИСТИЧКИХ АКТИВНОСТИ РАДИКАЛНИХ ИСЛАМИСТА

Апстракт

Тероризам се током времена развио у различите облике. Један од најопаснијих је засигурно сајбер тероризам. Много је различитих мотивација за терористе да примене сајбер тероризам као оруђе у својој борби. Интернет и рачунарске мреже моћан су ресурс на који се модерно друштво увелико ослања. Терористичке групе развиле

[*] Аутор за кореспонденцију: Дарко Трифуновић, Факултет безбедности, Господара Вучића 50, 11118 Београд, Србија, galileja@yahoo.com

су нове алате и методе борбе и постале су ефикасније, унапређеније и непредвидљивије. Виртуелни или сајбер простор савршен је и врло сигуран терен за терористичке групе, њихове разне активности, као што су тајна шифрована комуникација, дељење датотека, индоктринација и регрутовање рањивих група, прикупљање средстава и промоција њихових будућих акција и достигнућа која шире страх међу обичним људима. Да ли смо довољно свесни ових чињеница и спремни за контрамере? Чињеница је да терористи у своје сврхе користе углавном алате отвореног кода (софтвер), широкодоступне и бесплатне као и видео-игре, популарне друштвене мреже (углавном Твитер) и софтвер који су развили њихови властити програмери. Сврха овог рада је да се укаже на неке методе које користе радикалне исламистичке терористичке групе и на важност реаговања на овај нови безбедносни изазов.

Кључне речи: сајбер тероризам, исламски терористи, Анонимуси, стеганографија, Исламска држава.

INTRODUCTION

Over the years, cyberspace has become an integral part of our lives. But also, what is more than notable is that this new ground, full of possibilities, is constantly under different attacks. Spies, criminals, state-sponsored hackers, are looking for efficient ways to penetrate computer systems to fulfill different objectives. These goals could be gaining illegal financial funds, stealing business or private information, industrial secrets, etc. Also, cyberspace can be used for sabotage activities, to conduct future war conflicts, or to transmit political, ideological, religious messages and propaganda. Over the years, these resources have become an increasingly powerful tool for radical Islamic terrorists who are using them to achieve their objectives. Cyberspace is also the place where their accomplishments and activities can be stopped. There are many different motivations for terrorists to deploy cyber terrorism as a tool in their fight to inflict damage or destruction to targets. Since cyberspace is borderless, attacks can originate anywhere in the world and are not limited by physical boundaries. Like any other form of terrorism, cyber terrorism is potentially a major global threat. This might be a serious threat that could endanger states and citizens. Terrorists, members of various radical Islamic organizations, have started using information technologies and the Internet increasingly. They have been using it as an instrument of the fight, but also as the target of the attack. This is a global problem and requires global attention. And yet, there is still no universal consensus about the definition or exact acts in cyberspace that could be listed as acts of cyber terrorism. Moreover, on the global level, academic and security experts have still not reached a unified definition of this illegal activity. Terrorism, as a method of radical Islamic groups, is motivated by political, objectives since they seek political power to compel society to conform to their extreme religious views. Therefore, it is important to underline and understand the better relationship between politics, religion, and society (Jevtić, 2017). Although there is no universal definition of cyber terrorism, security experts, academics, the IT sector, and politicians provide a myriad of definitions in an attempt to define it and it is quite noticeable that there are conflicting viewpoints on the term itself. Professor Dorothy Denning, one of the pioneers in the definition of cyber terrorism, argues that a particular act can be characterized as cyber terrorism if the attack results in violence against people or property, or causes damage that will cause fear (Denning, 2000). According to Denning "computer is the weapon of attack" in this case. Denning states that to understand the potential threat of cyber terrorism, two factors must be considered: first, whether there are targets that are vulnerable to the attack that could lead to violence or severe harm, and second, whether there are actors with the capability and motivation to carry them out.

The U.S. Federal Bureau of Investigation (FBI) defines cyber terrorism as any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents" (Tafoya, 2011). According to the U.S. Commission of Critical Infrastructure Protection, possible cyber-terrorist targets might include the banking industry, military installations, power plants, air traffic control centers, water systems, etc. On the other hand, professor Gabrial Weimann claims that cyber terrorism is used for recruitment, propaganda purposes, and gathering support through websites (Weimann, 2011).

Cyber terrorism is a threat to the international community as much as any other forms of terrorism (Iklody,2010). The fact is that both cyber terrorists and terrorists share the same political, ideological, and religious motives. What distinguishes them is a different type of tool and the different effects. In the case of cyber terrorists, those are the computer and the Internet. Cyber, as well as "classic terrorism", aims to attack and intimidate civilians by using computers, computer networks, and the Internet with the motive of spreading its ideals and political struggle (Arquilla & Ronfeldt, 2001).

The paper will explore the active use of cyberspace of extreme terrorist groups of radical Islamists for their goals. Terrorists are using cyberspace increasingly and there is possibly a great threat that the Internet and IT will play a significant role in the potential mass carnage and destruction through technological means by terrorist groups.

TOOLS AND METHODS FOR COVERT CYBER ACTIVITIES

There are numerous ways and tools by which terrorists use the Internet for communication, without fear that somebody might intercept them. Terrorists use the biggest advantage of cyberspace – anonymity – and different tools and methods to make strategies and plans for future attacks, but also to contact and activate their sleepers, to exchange important files, etc.

One of the most popular tools is the Tor network (The Onion Router). This is the most popular anonymizer software. The main advantage of this software is that it offers a technology that bounces internet users and website traffic through "relays" run by thousands of volunteers around the world. Thanks to its architecture, it renders it extremely hard for anyone to identify the source of the information or the location of the user. It is widely used by thousands of people who take care of their privacy, including journalists, the business sector, activities, different security agencies, etc. But also, it is more than popular among terrorist groups such are Al Nusra, Al-Qaida, ISIS, and others as well.

Tor hides the user's real IP address and changes it frequently for the fake one. Its main purpose is to hide the real identity of its users. Tor has its Darknet and that is a safe place for any kind of illegal activities. A Study published by NATO showed that there were about 300 forums of terrorist organizations in Tor's darknet (Ogun, 2015)

Tor can mask users' identities, but also host their websites via its "hidden services" capabilities, which is more than convenient for illegal activities and terrorists. Also, sites can only be accessed by people on the Tor network. Nowadays, there are speculations about Tor safety, since IT researchers found vulnerabilities that might be used for the de-anonymization of its users. However, there is still a need for further investigation of Tor's Darknet, but also deeper and better cooperation of law enforcement agencies around the world to track and prevent potentially illegal activities in this "hidden" place on the Internet.

I2p Darknet is another less popular Darknet but considered more secure than Tor (Akhgar, Bayerl & Sampson, 2016). Tor has a two-direction focus, on a clear/public net hiding identities of users and the focus on the Darknet, but the focus of I2p is only on the Darknet which is Encrypted Internet hidden in public/clear Internet. Its users can surf the public Internet much like Tor users, but that is a security issue and users mostly do not use it for that purpose. I2p in combination with other software can provide a perfectly secure way of communication through encrypted tunnels. Retroshare is another kind of software that can be used inside I2p Darknet connecting as many people as needed. Using Retroshare, users make hidden nodes of the network inside I2p Darknet and connect them, peer, to peer making encrypted tunnels between their computers. Interception of that way of communication is impossible at this point. No one can see the identities of participants and the content of the communication.

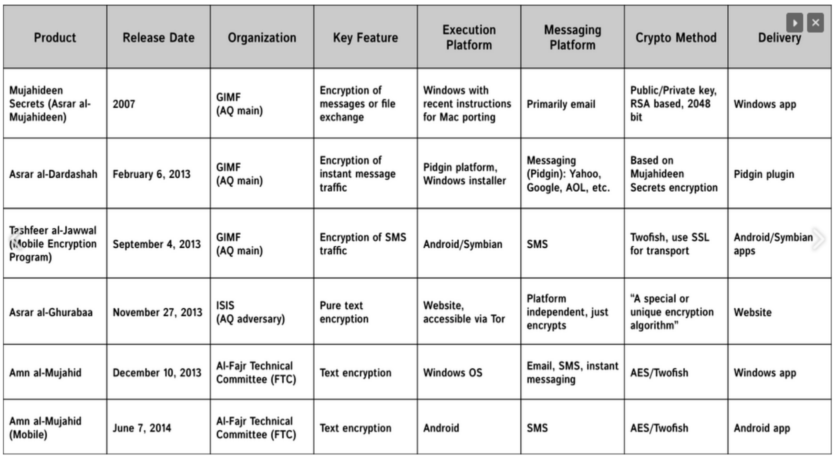
Cyber-attacks are one of the most serious security challenges in the 21st century. Hackers have already demonstrated weaknesses of the different systems by taking over control of crucial services, stealing sensitive information, or jeopardizing functions. The concern is that terrorists could also start applying these methods which could be a great security threat.

The question is whether cyber terrorism nowadays is a real danger. Islamic terrorists have their own software developing companies that make encrypted software for their purposes. The main software producers are GIMF (Global Islamic Media Front) and FTC (Al-FajrTechicalCommittee) (Axelrod, 2009).

Here is a timeline of software that ISIL, Al-Qaida, and other Islamic terrorist organizations have developed over the years:

- The original *Mujahideen Secrets* (*Asrar al-Mujahideen*) encryption software launched in 2007, primarily for use with email. Asrar has had multiple releases over time and is distributed by the Global Islamic Media Front.
- *Asrar al-Dardashah*, released by GIMF in February 2013, is an encryption plug-in for instant messaging based on the Pidgin platform – which connects to major US-based platforms.
- Tashfeer al-Jawwal is a mobile encryption program, again from GIMF, released in September 2013, based on Symbian and Android.
- *Asrar al-Ghurabaa* is yet another alternative encryption program, however, importantly, released in November 2013 by the Islamic State of Iraq And Al-Sham (ISIS), which coincides with ISIS breaking off from main AQ after a power struggle
- *Amn al-Mujahid* is an alternative encryption program released in December 2013. In this case from Al-Fajr Technical Committee (FTC) is also a mainstream AQ outfit.
- *Al-Fajr*, one of Al-Qaeda's media arms, released a new Android encryption application early June 2014 on their website, referring to how it follows the "latest technological advancements" and provides "4096-bit public key" encryption (Table 1).

Table 1.



Product	Release Date	Organization	Key Feature	Execution Platform	Messaging Platform	Crypto Method	Delivery
Mujahideen Secrets (Asrar al-Mujahideen)	2007	GIMF (AQ main)	Encryption of messages or file exchange	Windows with recent instructions for Mac porting	Primarily email	Public/Private key, RSA based, 2048 bit	Windows app
Asrar al-Dardashah	February 6, 2013	GIMF (AQ main)	Encryption of instant message traffic	Pidgin platform, Windows installer	Messaging (Pidgin): Yahoo, Google, AOL, etc.	Based on Mujahideen Secrets encryption	Pidgin plugin
Tashfeer al-Jawwal (Mobile Encryption Program)	September 4, 2013	GIMF (AQ main)	Encryption of SMS traffic	Android/Symbian	SMS	Twofish, use SSL for transport	Android/Symbian apps
Asrar al-Ghurabaa	November 27, 2013	ISIS (AQ adversary)	Pure text encryption	Website, accessible via Tor	Platform independent, just encrypts	"A special or unique encryption algorithm"	Website
Amn al-Mujahid	December 10, 2013	Al-Fajr Technical Committee (FTC)	Text encryption	Windows OS	Email, SMS, instant messaging	AES/Twofish	Windows app
Amn al-Mujahid (Mobile)	June 7, 2014	Al-Fajr Technical Committee (FTC)	Text encryption	Android	SMS	AES/Twofish	Android app

STEGANOGRAPHY

Besides the software mentioned above, one of the most popular techniques that terrorists widely use for secret communication and hidden messaging is steganography. Terrorist groups scramble their messages by applying open-source encryption programs that involve steganography techniques, and post hidden messages on existing photographs, text, or videos on almost any website or to directly send via e-mail (Trifunović, 2015). In short terms, steganography is a method of hiding a secret message in a public container or other words, putting messages inside pictures, pdf documents, videos, or almost any other format[1]. The implementation of the secret message and container is on a binary level. Steganography is widely used as a very sophisticated way of secret communication and it is almost impossible to detect. It provides a way of secret communication that is common to Islamic terrorists. Steganography is more subtle and more effective compared to encryption and could be combined with encryption as well (Trifunović, 2015).

It comes as no surprise that terrorist groups such as the Islamic State, Hezbollah, Hamas, and Al Qaeda, have been using emails, encryption, and steganography to support the work of their organizations and communication between members. There are numerous examples of terrorist attacks prepared and accomplished using this method. According to a former French defense ministry official, Islamic terrorists used steganography to prepare an attack on the United States embassy in Paris. He said that terrorists were instructed to communicate through pictures posted publicly on the Internet (Kolata, 2001).

Jamal Beghal, the leader of that terrorist plot and one of Al-Qaida's leading recruiters in Europe, was arrested in late July 2001. The reason for the arrest was a passport fraud at Dubai International Airport in the United Arab Emirates. Beghal was trying to travel back to Europe after receiving training in Afghanistan. After French intelligence agents' interrogation, he revealed details of the plot – the plan was to build a bomb out of sulfur and acetone and to destroy the embassy of the United States in Paris. The former professional football player in Germany, Tunisian Nizar Trabelsi was the designated suicide bomber. He planned to strap this bomb onto himself, cover it up with a business suit and detonate himself in the U.S. embassy. Then, a minivan full of explosives would be driven into the U.S. cultural center of Paris and the explosives would be detonated inside. Beghal was convicted in

[1] With the help of open source software, based on steganography technique, anyone can easily hide secret messages or malicious scripts into any digital format, such as: BMP, JPG, TXT, HTML/XML, PDF, PNG, GIF, AU, WAV, MP3, AVI, TIF, TGA, DLL and EXE. This technique manipulates the least significant bit of the pixels making up digital images to store hidden information.

March 2005 on terrorism charges and was sentenced to 10 years' imprisonment. He was released in 2009 but put under house arrest.[2]

The next case of using this technique by Islamic terrorists was revealed when in May 2011 a suspected al-Qaeda member, Maqsood Lodin, a 22-year-old Austrian was arrested. Lodin was traveling from Pakistan to Berlin via Hungary when German police detained him. The police officers found a USB memory stick on him. The USB was password protected. The information on it was invisible. After deep analysis, officers discovered that the USB stick was containing a video with pornographic content – "Kick Ass" and the file was marked under the name "Sexy Tanja".

Computer forensics experts from the German Federal Criminal Police extracted 141 hidden text files out of the videos detailing al-Qaeda operations and plans for future operations (Gallagher, 2012). Those documents contained plans to attack cruise ships as a distraction while other attacks were initiated in Europe, then PDF terrorist training manuals in German, English, and Arabic were found as well. Those files were just hidden inside with digital steganography technique, but not encrypted. Anyway, German specialists worked for several weeks to extract all hidden data. If those files were encrypted strong enough as well, it would have been much harder or even impossible to get readable content because it would give a second layer of protection. U.S. intelligence sources tell CNN that the documents uncovered are "pure gold" (Robertson, Cruickshank & Lister, 2012). One source says that they are the most important haul of al Qaeda materials, besides those found when U.S. Navy SEALs raided Osama bin Laden's compound in Abbottabad, Pakistan, in 2014 and killed the al Qaeda leader (Robertson et al., 2012).

Steganography combined with strong cryptography is a perfect and unbreakable way of secret communication. If those techniques are applied in Darknet, we would have a paranoid level of completely safe communication. That is why the members of different security sectors need to learn how to use steganography as well as other techniques for encryption. To fight terrorists on the Internet, it is imperative to know their strategies. Hence the need to stop possible cyber-terrorist acts of large dimensions is getting more important each day. It is also more than necessary for experts from different fields and countries to work together and deal with the issues of terrorists misusing the Internet and cyberspace in a joint effort.

[2] Beghal was one of the links between ChérifKouachi, one of the brothers behind the Charlie Hebdo massacre in 2015, and AmedyCoulibaly, who killed four hostages in a Paris kosher supermarket and also a policewoman.

ONLINE RECRUITMENT AND RADICALIZATION OF ISLAMIC TERRORISTS

Access to the Internet has become increasingly important for terrorists. Modern ways of communication have given terrorists the ability to facilitate the organization of groups. Radical Islamic terrorists successfully implement the recruiting of new members using modern ways of communication. Internet and social media platforms secure membership without directly approaching potential recruits across the world as it used to be done only a decade ago. What is more than obvious is that the target group for recruitment has become children (De Guttry, Capone & Paulussen, 2016). Child terrorists are getting recruited in different forms – via direct contact, the propaganda on social media from which they get inspiration, and even by playing computer games which are more than worrying and extremely dangerous.

Internet is terrorists' main tool for the recruitment and radicalization of vulnerable individuals all around the world. The most vulnerable ones are migrants from Syria, Iraq, Afghanistan, and other Muslim countries. They experienced the terror of war, lost their loved ones, traveled thousands of kilometers struggling to pass the borders, etc. These are the recruiters' main targets. In Germany, authorities reported 340 cases in which extremists tried to make contact with asylum seekers since October 2015. German interior ministry warned that jihadist sympathizers were targeting child asylum-seekers as potential recruits (European Union Agency for Fundamental Rights, 2016).

There are examples of successful recruitment. One of them is a 16-year-old Syrian refuge, Mohamed J. who was arrested at a refugee shelter in Cologne last year. Mohamed was in contact with an ISIS member from the Middle East who instructed him on how to make an explosive device and where to plant it (Huggler, 2016). In December, a 12-year-old German Iraqi boy — guided by an Islamic State contact in the Middle East who warmly addressed him as "brother" and groomed the boy via the encrypted messaging app. Telegram — built and tried to detonate a bomb near a shopping center in the western German city of Ludwigshafen. The device failed to explode (Anthony & Mekhenne, 2017).

In January 2017, a 15-year-old girl — the daughter of a German convert to Islam and a Moroccan mother — was sentenced to six years in prison for an attack last February on a German police officer in Hanover (Hall, 2017). She gouged him in the neck with a kitchen knife, causing life-threatening injuries after being befriended and cajoled by an Islamic State instructor via a text messaging service. It should be underlined that she was radicalized at the age of 7. Intelligence agencies here have identified at least 120 minors who have become dangerously radicalized — and some of them cannot be intensely monitored because of domestic laws protecting children, according to the officials (Anthony & Mekhenne, 2017).

As already mentioned earlier, terrorist recruiters use shooting video games to radicalize young people, especially children. The Islamic State has reached unprecedented success when it comes to this activity. In 2012, one of the world's most popular video games was Grand Theft Auto. The Islamic State propaganda machinery created its modifications. Players could role-play as members of IS engaged in combat on the battlefield. Players, as IS soldiers could be killing and shooting American soldiers and attack convoys, with lots of explosions (Clauson, 2014).

Two young British citizens were recruited by ISIL using Call of Duty. Their father, Ahmed Muthana refused to buy sons Nasser, 20, and Aseel, 17, copies of the first-person shooter game, but they managed to reach a copy of their own. Their father believes that the game was bought for them by the people who encouraged them to go to Syria. Nasser, who was a medical student, left Cardiff after borrowing £100 from his father, saying he was going to a Muslim conference in Shrewsbury. Instead, he flew to Syria to join IS rebels, formerly known as ISIS. His younger brother Aseel quit his studies at Cardiff Fitzalan High School. He is fighting in Syria while his older brother is in Iraq (Evans, 2014).

Another example of using video games for terrorist propaganda is using GTA 5. ISIS produced a game intro where Jihadists scream "Allahuakbar" while shooting and burning citizens alive[3].

CYBERWAR OF INDEPENDENT INTERNET COLLECTIVE ANONYMOUS AGAINST ISLAMIC TERRORISTS

Islamic State or ISIL became the dominant terrorist group when it comes to various activities in cyberspace, especially when it comes to propaganda, recruitment, fundraising the potential fear that hackers of the group could manage to successfully attack the national infrastructure of the "enemy" states by using sophisticate cyber-attacks. Fighting terrorist groups should include the fight on the ground, from the air, from the sea – and in cyberspace. There are a couple of Internet hacker groups fighting against Islamic terrorists in cyberspace. The most active ones are GhostSec and one of the most popular, most organized, and very well IT equipped hacker collectives known as Anonymous. Anonymous declared war against ISIS in 2015 after the Paris attacks (Aydinli, 2016). The hacker collective, which consists of unconnected volunteers, coders, and activists from around the world, launched its anti-Islamic State online campaign, called #OpISIS, after the Charlie Hebdo massacre in Paris in January 2015 (Lockhart, 2015). The main focus of the Anonymous collective is the disruption of terrorist

[3] Available at: https://www.youtube.com/watch?v=604aevo3MzM Retrieved, February 2017

communication with the public shutting down of their Twitter accounts, Facebook pages, Telegram channels, etc (Anonhq, 2015).

Anonymous' efforts have encompassed recruiting its online army of people devoted to identifying and shutting down the militant group's avenues of propaganda Anonhq (2015). The collective recently released instruction guides to help spread information about the basics of denial-off service attacks on websites and password cracking, as well as for instructions on how to create programs that identify Twitter accounts related to the Islamic State group and how to help Anonymous find terrorist-propaganda sites (Gilbert, 2015). Websites related to the militant group have been gravitating towards the dark Web, a region of the Internet whose constituents do not appear in the results of search engines and typically require login information, so Anonymous has been attempting to find and infiltrate these sites. An Anonymous sibling known as either Ghost Security or GhostSec took down a site associated with the Islamic State group on the Dark Web Friday, replacing calls for jihad against the infidels with an advertisement for an online pharmacy peddling Prozac and Viagra, as well as a snarky message to readers (Stainer, 2015).

Anonymous collective have taken down 149 Islamic State-related websites and exposed 101,000 Twitter accounts and 5900 propaganda videos (Khandelwal, 2015). Also, they have successfully mapped countries with the most ISIS supporters' Twitter accounts.

ISIS HACKER UNITS FOUNDER DRONED

A member of the hacker team TeaMp0ison, Junaid Hussain aka Trick who was arrested for hacking the email account of a staffer of the former UK Prime Minister Tony Blair and posted personal information of Blair's, as well as other government employees online, got radicalized and joined ISIS (Murphy, 2015). He became the group's most prominent hacker and the third person on the Pentagon's kill list after Jihadi John and the leader of ISIS Abu Bakr al-Baghdadi.

In Syria, where he arrived in 2013, Hussain initially became known for allegedly hacking the Twitter account of CENTCOM, though it has been reported that somebody else was behind that attack and the hacking group known as Cyber Caliphate (Guardian, 2015a). Hussain, however, was likely the leader, and perhaps the sole member, of another ISIS-linked hacking group known as the Islamic State Hacking Division, or IS Hacking Division (Spencer, 2015). His most important legacy is that he created the image of the powerful Islamic State in cyberspace. He was the one who had exceptional IT skills and very possibly, he had all the credit when it comes to IS's overtaking social media. He had the opportunity to recruit talented IT hackers to work in IS favor. But, although he was the public face of the Cyber Caliphate, he did not manage to accomplish the goal – creating a true, powerful, united cyber army of hackers who would be capable of attacking, destroying, or gaining the command and control systems of critical infrastructure.

Hiding behind the name of the IS Hacking Division, Hussain posted the names and personal information of 100 US military members, claiming to have obtained it from hacking Pentagon servers, though he likely got it most directly from the website. More importantly, he published the personal information of 1,400 American government workers, information likely culled from older breaches or open-source information (Alkhouri, Kassirer & Nixon, 2016:7).

Allegedly, the information of American personnel was delivered to Hussein by Kosovo citizen Ardit Ferizi, aka "Th3Dir3ctorY" who is believed to be the leader of the hacking collective "Kosova Hacker's Security" (Mickolus, 2016:458). But Hussain was not just pretending to dox government employees, or break into Twitter accounts for propaganda purposes. He developed a custom internet spy tool for ISIS (Coker, Yadron, & Palette, 2015), hacked into military members' Facebook accounts, and led the group's online recruitment. He was also allegedly involved in recruiting bombers in Western countries (Franceschi-Bicchierai, 2015).

Authorities knew Trick was somewhere in Raqqa, the *de facto* IS capital, though nailing down his exact location was a challenge. But unlike many others in ISIS, Trick had a heavy social media presence and was very active online. Britain's GCHQ got Trick's username on messaging app Surespot and its agent sent him a friend request that he accepted (Guardian, 2015b). This undercover agent, which has not been named in various stories in the British press, is believed to be a friend and a fellow hacker named Shm00p who wrote on Twitter, "F***ing guilty [of being an informant]," he wrote. ”And I'm sorry. I played their game and I shouldn't have." At some point, this undercover agent sent Trick a link to an unknown webpage known as a ”waterhole." It is called that because waterhole attacks involve ”poisoning“ the code on a website so that when a user visits, it will take over a system or modify it. In Trick's case, the page downloaded a virus to his phone. It is based on that that Surespot wrote of the incident. Subsequently, he made a phone call from his home in Raqqa that gave GCHQ the ability to pinpoint his location. The 21-year-old hacker was killed by a drone outside Raqqa in August 2015 (Szoldra, 2016).

SERBIAN ANONYMOUS JOINED FIGHTS AGAINST JIHADISTS

The Republic of Serbia has problems with Islamic extremists as well, especially in its southern region called Raška. The Serbian Anonymous collective has done its part in Operation ISIS in this region. First of all, they discovered the newly created Facebook page "Army of the Republic of Sandzak" (Sandzak is how they call the Raska region) with more than 7000 followers already. They asked their followers to report that page to Facebook and it was erased in half an hour. Serbian media followed the Anonymous post, informed the public about the existence of the extremists' page and the main Persecutor for hi-tech crime ordered the police to discover the individuals behind it. Meanwhile, Serbian Anonymous already found out who those people were, and revealed their identities on their page. The police arrested them the very same day.

The event that triggered the attention of Anonymous Serbia took place on 5th September. It was the military-styled parade that stirred the public. The group of about thirty men in green uniforms with red fezzes, and green berets on their heads, occupied the central streets of the city of Novi Pazar, in Sandžak (Serbia). They marched from the HQ of the Islamist community to the main city square, in their "foray into Hadžet" (village of Novi Pazar). This parade caused mostly negative comments of prominent individuals in the city of Novi Pazar and the surrounding area because the uniforms resembled those of war criminals who took part in the extermination of Serbs during the Second World War. The parade was led by the Islamist Chief Mufti and his associates (Cyber War Zone, 2017).

CONCLUSION

Islamic radicals and terrorist groups use the Internet in advanced and various ways to accomplish their goals. They have their IT professionals, programmers, hacker teams, and recruiters, fundraisers, etc. States and the security sector must find more efficient ways to identify the threats from the Internet, especially cyber terrorists, to track their members, intercept their communications, infiltrate them, etc. Cyber terrorism is a threat to the international community as much as any other form of terrorism. Extremists have adopted new skills to fight on a new ground – cyber ground and it will be a true challenge for the international community to fight back. Terrorists will continue to use the Internet to maintain their current methods. The question is whether or even when, they will start to utilize new, more effective ones. States, governmental, and security sectors are becoming more aware of this issue and have started creating their national cyber strategies, as well as systems of defense. But without international unified cooperation, the victory against terrorists on the Internet will not be gained.

REFERENCES

Akhgar, B., Bayerl, P. S., & Sampson, F. (Eds.). (2016). *Open Source Intelligence Investigation: From Strategy to Implementation*. Cham: SpringerInternational Publishing.

Alkhouri, L., Kassirer, A., & Nixon, A. (2016). *Hacking For ISIS: The Emergent Cyber Threat Landscape*. Flashpoint.

Anonhq. (2015). *Anonymous Finally Reveals How They Attack ISIS Militants|#opisis|ISIS|* Available at Anonymous. http://anonhq.com/anonymous-finally-reveals-attack-isis-militants-opisis-isis-anonymous/ Retrieved 19.03.2017.

Anthony, F.,&Mekhenne, S. (2017). They're young and lonely. The Islamic State thinks they'll make perfect terrorists.'What's happening to our children? *Washington Post.* Available at: http://www.washingtonpost.com/sf/world/2017/02/11/theyre-young-and-lonely Retrieved 19.01.2019.

Arquilla, J., &Ronfeldt, D. (2001). *Networks and netwars: The future of terror, crime, and militancy*. Santa Monica, CA: National Defense Research Institute.

Axelrod, E. M. (2009). *Violence goes to the Internet: Avoiding the snare of the Net*. Illinois: Charles C Thomas Publisher**.**

Aydinli, E. (2016). *Violent non-state actors: From Anarchists to Jihadists*. London: Routledge.

Clauson, J. (2014). ISIS use grand theft auto mock-up to recruit and boost morale, Inquisitr, Available at www.inquisitr.com/1486558/isis-uses-grand-theft-auto-mock-up-to-recruit-and-boost-morale Retrieved *19.03.2017*

Coker, M., Yadron, D., & Palette, D. (2015). Hacker killed by drone was Islamic State's "secret weapon". *Wall Street Journal*. Available at: http://www.wsj. com/articles/ hacker-killed-by-drone-was-secret-weapon-1440718560Retrieved 19.03.2018

CyberWarzone. (2017). *Anonymous Serbia identified jihadi groups in the Balkans #opIceISIS*, Available at https://cyberwarzone.com/anonymous-serbia-identified-jihadi-groups-balkans-opiceisis/Retrieved 10.02.2019.

De Guttry, A., Capone, F., &Paulussen, C. (Eds.). (2016). *Foreign fighters under international law and beyond*. The Hague: TMC Asser Press.

Denning, D. (2000). Cyber terrorism. Testimony Before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. In E.V. Linden (Ed.), *Focus on Terrorism* (pp.71-76). New York: Nova Science Publishers.

European Union Agency for Fundamental Rights, *Key migration issues: one year on from initial reporting*, Available at http://fra.europa.eu/en/publication/2016/key-migration-issues-one-year-initial-reporting/main-findings Retrieved 19.03.2017.

Evans, M. (2014). Call of Duty being used to recruit British Muslims', father of Welsh Jihadists claims. *Express.* Available at:http://www.express.co.uk/news/uk/503094/ Call-of-Duty-used-to-recruit-British-Muslims-father-of-Welsh-Jihadistsclaims Retrieved 19.03.2017

FranceschiBicchierai, L. (2015). How a Teenage Hacker Became the Target of a US Drone Strike. *MotherBoard.* Available at: https://motherboard.vice.com/en_us/article/ junaid-hussain-isis-hacker-drone Retrieved 19.03.2017

Gallagher, S. (2012). Steganography: how al-Qaeda hid secret documents in a porn video. Available at:*http://arstechnica.com/business/2012/05/steganography-how-al-qaeda-hid-secret-documentsin-a-porn-video*Retrieved 19.04.2018.

Gilbert, *D.* (2015). Anonymous #OpIsis: Hacktivists publish a how-to guide for identifying Islamic State Twitter accounts. *International Business Times*. Available at: http://www.ibtimes.co.uk/anonymous-opisis-hacktivists-publish-how-guide-identifying-islamic-state-twitter-accounts-1496378 Retrieved 19.03.2017

Guardian (2015a). Junaid Hussain: British hacker for Isis believed killed in US airstrike, *The Guardian.* Available at: https://www.theguardian.com/world/2015/aug/ 27/junaid-hussain-british-hacker-for-isis-believed-killed-in-us-airstrike Retrieved 19.03.2017

Guardian (2015a). US Central Command Twitter account hacked to read 'I love you Isis. *The Guardian,* Available at https://www.theguardian.com/us-news/2015/jan/12/ us-central-command-twitter-account-hacked-isis-cyber-attack Retrieved 19.03.2017

Hall, A. (2017). Teenage female ISIS fanatic was 'radicalized at the age of seven and stabbed a German police officer because she was unable to make it to Syria, *Mail Online*. Available at: https://www.dailymail.co.uk/news/article-3476986/Teenage-female-ISIS-fanatic-radicalised-age-seven-stabbed-German-police-officer-unable-make-Syria.html Retrieved 19.03.2018.

Huggler, J. (2016). Syrian teenager arrested in Germany 'was planning Isil bomb attack. *The Telegraph.*Available at:http://www.telegraph.co.uk/news/2016/09/22/syrian-teenager-arrested-in-germany-was-planning-isil-bomb-attac/ Retrieved 19.03.2017

Iklody, G. (2010). The New Strategic Concept and the Fight Against Terrorism: Challenges&Opportunities. *TerörizmleMücadeleDergisi*, *3*(2), 3-12.

Jevtic, M. (2007). Political Science and Religion. *The Politics and Religion Journal. 1*(1). 59-69.

Khandelwal, S. (2015). Anonymous has claimed to have taken down 20,000 ISIS-affiliated Twitter accounts, *The Hacker News* Available at http://thehackernews.com/2015/11/anonymous-hacker-isis_21.html Retrieved 19.03.2017

Kolata, G. (2001). Veiled messages of terrorists may lurk in cyberspace. *New York Times*. Available at: http://www.nytimes.com/2001/10/30/science/physical/30STEG.html Retrieved 19.03.2017

Lockhart, K (2015).#OpISIS: Why Anonymous has declared an online war against Isil - in 90 seconds. *The Telegraph*. Available at: http://www.telegraph.co.uk/news/worldnews/islamic-state/12003242/OpISIS-WhyAnonymous-has-declared-an-online-war-against-Isil-in-90-seconds.html Retrieved 19.03.2017

Mickolus, E. (2016). *Terrorism, 2013–2015: A Worldwide Chronology.* North Carolina, US**:** McFarland & Company Inc. Jefferson.

Murphy, L. (2015). The Curious Case Of The Jihadist Who Started Out As A Hacktivist**.** *Vanity Far*. Available at: http://www.vanityfair.com/news/2015/12/isis-hacker-junaid-hussain Retrieved 19.03.2017

Ogun, M. N. (Ed.). (2015). Terrorist Use of Cyberspace and Cyber Terrorism: New Challenges and Responses. Washington, DC: IOS Press.

Robertson, N., Cruickshank, P., & Lister, T. (2012). Documents reveal al Qaeda's plans for seizing cruise ships, the carnage in Europe. *CNN*: Assyrian International News Agency.

Spencer, R. (2015). *The complete infidel's guide to ISIS*. New York, NY: Simon and Schuster.

Stainer, M. (2015). Ghost Sec, an Anonymous affiliate, hacks ISIS site on the deep web with Viagra, Prozac ad. *Washington Times*. Available at: http://www.washingtontimes.com/news/2015/nov/26/ghost-sec-anonymous-affiliate-hacks-isis-site-deep/ Retrieved 19.03.2017

Szoldra, P. (2016). Here's how the military tracked down and killed the top hacker for ISIS. *Business Insider*. Available at: http://www.businessinsider.com/isis-hacker-trick-found-2016-6?IR=T Retrieved 19.03.2017

Tafoya, W. L. (2011). Cyberterror. *FBI Law Enforcement Bulletin(80)*1. 1-16.

Trifunović, D. (2015). Digital steganography in terrorist networks, *XLII International Symposium on Operations Research*, Belgrade: Faculty of Mathematics.

Weimann, G. (2011). Cyberterrorism: How Real is the Threat? United States Institute of Peace Special Report No. 119. Special Report, https://www.usip.org/publications/2004/05/cyberterrorism-how-real-threat Retrieved 19.03.2017

САЈБЕР БЕЗБЕДНОСТ – ВИРТУЕЛНИ ПРОСТОР КАО ПОДРУЧЈЕ СКРИВЕНИХ ТЕРОРИСТИЧКИХ АКТИВНОСТИ РАДИКАЛНИХ ИСЛАМИСТА

Дарко Трифуновић
Универзитет у Београду, Факултет безбедности, Београд, Србија

Резиме

Сајбер или кибернетички простор користи се и од стране носилаца терористичке претње. Већ годинама у сајбер простору одвијају се различите активности које могу да се окарактеришу као сајбер тероризам. Постоји много различитих мотива за терористе да примене сајбер тероризам као метод у својој борби за наношење штете или уништавање циљева. Будући да је сајбер простор без граница, напади могу потицати са било којег места на свету и нису ограничени физичким границама. Као и сваки други облик тероризма, сајбер тероризам је потенцијално главна глобална пријетња. Терористи који су чланови разних радикалних исламских организација почели су све више да користе информационе технологије и интернет. Користе га као инструмент борбе, али и као мету напада. Ово је глобални проблем и захтева глобалну пажњу и глобални одговор. Бројни су алати и начини како терористи користе интернет за комуникацију, без страха да би их неко могао пресрести или открити. Терористи користе највећу предност сајбер простора – анонимност – и различите алате и методе како би направили стратегије и планове будућих напада, затим да би контактирали и призвали своје „спаваче", разменили важне датотеке или још важније вршили радикализацију заинтересованих. Исламски радикали и терористичке групе користе интернет на напредне и различите начине како би постигли своје циљеве. Имају своје ИТ стручњаке, програмере, хакерске тимове и регрутере, прикупљаче средстава итд. Државе и сектор безбедности морају пронаћи ефикасније начине за препознавање претњи са интернета, посебно сајбер терориста, да би пратили своје чланове, пресретали њихове комуникације, инфилтрирали се међу њих итд.