

**Darko Trifunovic**

## **Cyber security – Virtual Space as an area for Covert Terrorist Activities of Radical Islamist**

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

**Keywords:** cyber terrorism, Islamic terrorists, Anonymous, steganography, Islamic state

### **Introduction**

Over the years, cyberspace became integrated 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 a efficient way to penetrate computer systems in order to fulfill different objectives. There goals could be gaining illegal financial funds, to steel business or private information, industrial secrets. Also, cyber space can be used for sabotage activities, to conduct future war conflict, or to transmit political, ideological, religious messages and propaganda. Over the years, these resources have become an increasingly powerful tool for terrorists radical Islamist who are using them in order to achieve their objectives. Cyber space is also 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. Because cyberspace is borderless, attacks can originate from anywhere in the world and are not limited by physical boundaries. As any other form of terrorism, cyber terrorism is potentially major global threat. This might be the serious threat that could endanger the states and citizens. Terrorists, member of various radical Islamic

organizations, started using information technologies and the Internet increasingly. They are 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 definition or exact acts in cyber space that could be listed as acts of cyber terrorism. Moreover, on the global level, academic and security experts still have not reached a unified definition of this illegal activity. Terrorism as 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 better relationship between politics, religion and society<sup>1</sup>.

Although there is no universal definition of cyber terrorism, from security experts, academics, IT sector, politicians came myriad of definitions in attempt to define it and it is quite noticeable that there are conflicting viewpoints of 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 result in violence against people or property, or make that causes damage that will cause fear<sup>2</sup>”. According to Professor 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 attack that could lead to violence or severe harm, and second, whether there are actors with the capability and motivation to carry them out<sup>3</sup>”.

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 results in violence against non-combatant targets by sub-national groups or clandestine agents<sup>4</sup>”. 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

---

<sup>1</sup> Miroљub Jevtic, *Political Science and Religion*, The Politics and Religion Journal, Volume 1 No.1, Belgrade, Serbia, 2017, p. 59-69

<sup>2</sup> Dorothy E. Denning, *Cyber terrorism*, Testimony Before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives - May 23, Washington D.C.US. 2000.

<sup>3</sup> Ibid

<sup>4</sup> William L. Tafoya, *Cyber Terror*, FBI Law Enforcement Bulletin, <https://leb.fbi.gov/2011/november/cyber-terror> Retrieved 19.03.2017

control centers, water systems, etc. On the other side, professor Gabriel Weimann claims that cyber terrorism is used for recruitment, propaganda purposes and gathering support through websites<sup>5</sup>.

Cyber terrorism is a threat to the international community as much as any other forms of terrorism<sup>6</sup>. The fact is that both cyber terrorists and terrorists share the same political, ideological, religious motives. What distinguish them is different type of tool and different effect. In the case of cyber terrorists it is computer and 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<sup>7</sup>.

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

### **Tools and methods for covert cyber activities**

There are numerous ways and tools how terrorist are using Internet for communication, without fear that somebody might intercepted them. Terrorist are using the biggest advantage of cyber space – anonymity – and different tools and methods in order to make strategies and plans of the future attacks, then to contact and evoke their sleepers, to exchange important files, etc.

One of the most popular tools is **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 websites' traffic through "relays" run by thousands of volunteers around the world. Thanks to it's architecture it is making 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 are taking care of their privacy, including journalists, business sector, activities, different

---

<sup>5</sup> Gabriel Weimann, *Cyberterrorism: How Real Is the Threat?*, United States Institute for Peace, Special Report, <https://www.usip.org/publications/2004/05/cyberterrorism-how-real-threat> Retrieved 19.03.2017

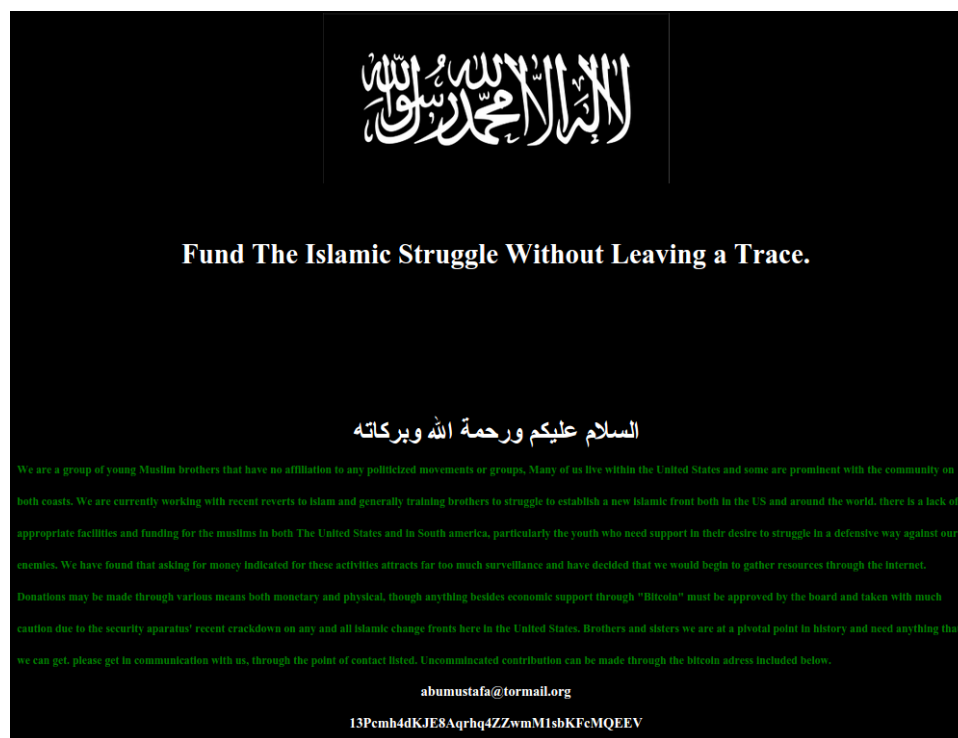
<sup>6</sup>Gábor IKLÓDY, *The New Strategic Concept and the Fight Against Terrorism: Challenges & Opportunities*, Defence Against Terrorism Review, COE-DAT, NATO, Vol.3, No. 2, Fall 2010, Brussels, Belgium, page 5

<sup>7</sup> John Arquilla, David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, RAND, Santa Monica, CA, US, 2001, page 281

security agencies, etc. But also, it is more than popular among terrorist groups such as Al Nusra, Al-Qaida, ISIS and others as well.

Tor hides user's real IP address and changes it frequently for the fake one. Its main purpose is to hide real identity of its users. Tor has its own **Darknet** and that was a safe place for any kind of illegal activities. Study published Y2011 showed that there were about 300 forums of terrorist organizations in Tor's darknet<sup>8</sup>.

There are examples of fund raising for Jihad in Tor's Darknet. Here is one:



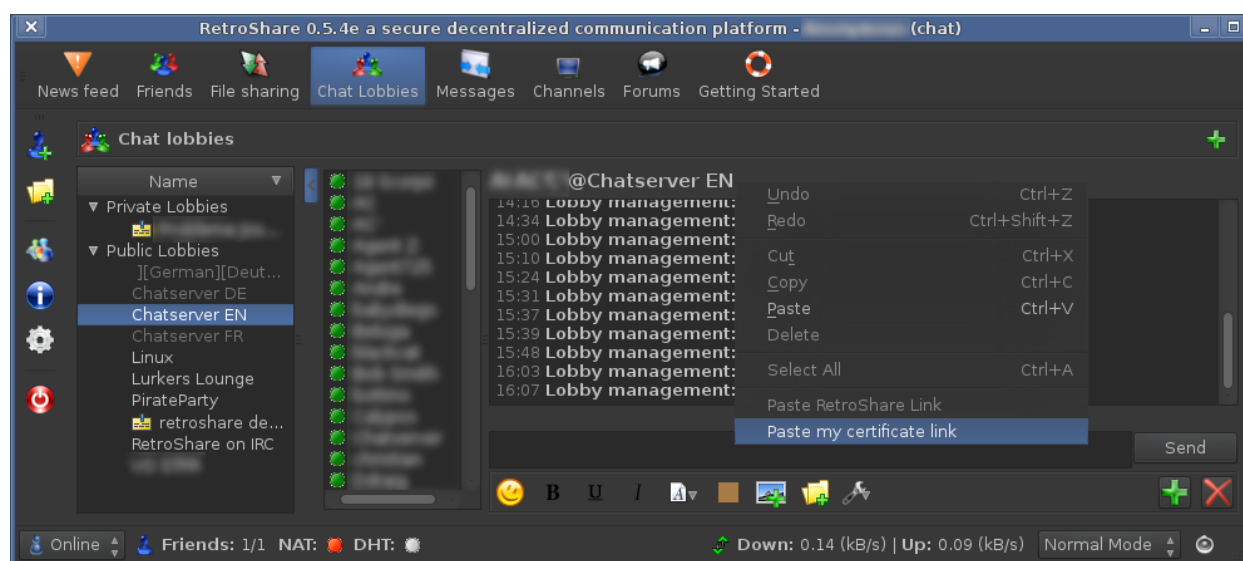
**Photo 1.** Fond The Islamic Struggle Without Leaving a Trace

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 how indeed the Tor is actually safe as it used to be since IT researchers found vulnerabilities that might be used for

<sup>8</sup> See: M.N. Ogun, *Terrorist Use of Cyberspace and Cyber Terrorism: New Challenges and Responses*, IOS Press, NATO – Emerging Security Challenges Division, Washington D.C. US, 2015.  
Also: <http://canadafreepress.com/article/backdoor-plots-the-darknet-as-a-field-for-terrorism>

deanonymization of its users. However, here is still need for further investigation of Tor's darknet but also deeper and better cooperation of law enforcement agencies round the world in order to track and prevent potential illegal activities in this "hidden" place on the Internet.

**I2p Darknet** is another less popular Darknet but considered more secure than Tor's one<sup>9</sup>. Tor has two direction focus, on a clear/public net hiding identities of users and focus on a Darknet but focus of I2p is only on a Darknet which is Encrypted Internet hidden in public/clear Internet. Its users have possibility to surf public Internet as well like a Tor users but that is a security issue and users mostly do not use it for that purpose. I2p in combination with other softwares can provide perfectly secure way of communication through encrypted tunnels. **Retroshare** is one of those softwares that can be used inside I2p Darknet connecting as many people as needed. Using Retroshare, users make hidden nodes of 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 is able to see identities of participants and the content of communication.



**Photo 2.** Retroshare – Encrypted social network

<sup>9</sup> Babak Akhgar, P. Saskia Bayerl, Fraser Sampson, *Open Source Intelligence Investigation: From Strategy to Implementation*, Springer, Cham, Switzerland, 2017, p.114

Cyber attacks are one of the most serious security challenges in the 21<sup>st</sup> century. Hackers have already demonstrated weaknesses of the different systems by taking over control of the crucial services, stealing sensitive information or by 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 softwares for their purposes. Main software producers are GIMF (Global Islamic Media Front) and FTC (Al-Fajr Technical Committee)<sup>10</sup>.

Here is a timeline of softwares that ISIL, Al-Qaida and other Islamic terrorist organization 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, which 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 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) which is also a mainstream AQ outfit.*
- ***Al-Fajr**, one of Al-Qaeda's media arms, released a new Android encryption application early*



---

<sup>10</sup> Evan M. Axelrod, *Violence Goes to the Internet: Avoiding the Snare of the Net*, Charles C Thomas Publisher, Springfield, IL, US, 2009, p.174

June 2014 on their website, referring to how it follows the “latest technological advancements” and provides “4096 bit public key” encryption.



**Photo 3.** Encrypted softwares GIMF (Global Islamic Media Front)

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

**Summary Table 1.**

## Steganography

Besides softwares mentioned above, one of the most popular technique that terrorists are widely using for secret communication and hiding 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<sup>11</sup>. In short terms, steganography is method of hiding secret message in a public container or in other words, putting message inside picture, pdf document, video or almost any other format<sup>12</sup>. Implementation of 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<sup>13</sup>.

It comes as no surprise that terrorists groups such as Islamic State, Hezbollah, Hamas, Al Qaeda, are and were using emails, encryption, and steganography to support work of their organizations and communication between members. There are numerous examples of terrorist attacks prepared and successfully accomplished using this method. According to former French defense ministry official, Islamic terrorists used steganography to prepare attack on the United States embassy in Paris. He said that terrorists were instructed to communicate through pictures posted on publicly on internet<sup>14</sup>.

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 arrest was 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 built a bomb out of sulfur and acetone and to destroy embassy of United States in Paris. 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

---

<sup>11</sup> Darko Trifunović, *Digital steganography in terrorist networks*, SYM-OP-IS 2015: XLII International Symposium on Operations Research, Belgrade, Serbia, 2015, Vol.V(1)

<sup>12</sup> 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.

<sup>13</sup> Darko Trifunović, *Digital steganography in terrorist networks*, SYM-OP-IS 2015: XLII International Symposium on Operations Research, Belgrade, Serbia, 2015, Vol.V(1)

<sup>14</sup> *Veiled Messages of Terror May Lurk in Cyberspace*, Gina Kolata, New York Times, <http://www.nytimes.com/2001/10/30/science/physical/30STEG.html> Retrieved 19.03.2017



business suit and detonate himself in the U.S. embassy. Then, 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 March 2005 on terrorism charges and was sentenced to 10 years' imprisonment. He was released in 2009 but put under house arrest<sup>15</sup>.

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 in. Lodin was traveling from Pakistan to Berlin via Hungary when German police detained him. The police officers found with him USB memory. The USB was password protected. The information on it was invisible. After deep analysis, officers discovered that USB stick was containing video with pornographic content - "Kick Ass" and the file was marked under the name "Sexy Tanja". Computer forensics experts from German Federal Criminal Police extracted out of videos 141 hidden text files detailing al-Qaeda operations and plans for future operations<sup>16</sup>. Those documents contained plans to attack cruise ships as a distraction while other attacks were initiated in Europe, than PDF terrorist training manuals in German, English and Arabic were found as well<sup>17</sup>. 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 be 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"<sup>18</sup>. 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 2011 and killed the al Qaeda leader<sup>19</sup>. Steganography combined with strong cryptography is perfect and unbreakable way of secret

---

<sup>15</sup> Beghal was one of the links between Chérif Kouachi, one of the brothers behind the Charlie Hebdo massacre in 2015, and Amedy Coulibaly, who killed four hostages in a Paris kosher supermarket and also a policewoman.

<sup>16</sup> *Steganography: How al-Qaeda hid secret documents in a porn video*, Sean Gallagher - <http://arstechnica.com/business/2012/05/02/steganography-how-al-qaeda-hid-secret-documents-in-a-porn-video/> Retrieved 19.03.2017

<sup>17</sup> *Al Qaeda Porn Video: Terrorist Attack Plot Hidden In Pornographic Movie File*, [http://www.huffingtonpost.com/2012/05/01/al-qaeda-porn-video-terrorist-group-plans-hidden\\_n\\_1467775.html](http://www.huffingtonpost.com/2012/05/01/al-qaeda-porn-video-terrorist-group-plans-hidden_n_1467775.html), Al Qaeda Porn Video: Terrorist Attack Plot Hidden In Pornographic Movie File, Retrieved 19.03.2017

<sup>18</sup> Documents reveal al Qaeda's plans for seizing cruise ships, carnage in Europe, CNN, <http://edition.cnn.com/2012/04/30/world/al-qaeda-documents-future/> Retrieved 19.03.2017

<sup>19</sup> Ibid.

communication. If those techniques are applied in Darknet, we would have a paranoid level of completely safe communication. That is why it is extremely important for the members of a different security sectors to learn how to use steganography as well as other techniques for encryption. In order to fight terrorist on Internet, it is imperative to know their strategies. Hence the need to stop possible cyber terrorist acts of large dimension is getting more important each day, it is also more than necessary for the experts from the different fields and countries work together and with join forces deal with the issues of terrorist misusing Internet and cyber space.

### **Online Recruitment and Radicalization of Islamic terrorists**

Access to the Internet is increasingly important for terrorists. Modern ways of communication have given the terrorists the ability to facilitate the organization of groups. Radical Islamic terrorists successfully implement recruiting of the 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 target group for recruitment became children<sup>20</sup>. Child terrorists are getting recruited in different forms – from direct contact, from propaganda on social media from which they get inspiration and even by playing computer games which is more than worrying and extremely dangerous.

Internet is terrorists' main tool for recruitment and radicalization of vulnerable individuals all around the Globe. The most vulnerable ones are migrants from Syria, Iraq, Afghanistan and other Muslim Countries. They experienced terror of war, lost their loved ones, traveled thousands of kilometers struggling to pass the borders, etc. These are recruiter the main target. In Germany, authorities reported of 340 cases in which extremists tried to make contact with asylum seekers since October 2015. German interior ministry warned that jihadist sympathisers were targeting child asylum-seekers as potential recruits<sup>21</sup>.

---

<sup>20</sup> Andrea De Guttry, Francesca Capone, Christophe Paulussen, *Foreign Fighters under International Law and Beyond*, Springer, Cham, Switzerland, 2016, p.200

<sup>21</sup> European Union Agency for Fundamental Rights, *Key migration issues: one year on from initial reporting*, <http://fra.europa.eu/en/publication/2016/key-migration-issues-one-year-initial-reporting/main-findings> Retrieved 19.03.2017

There are examples of successful recruitment. One of them is Syrian 16 years old refuge, Mohamed J. who was arrested at a refuge shelter in Cologne last year. Mohamed was in contact with an ISIS member from Middle East who instructed him how to make an explosive device and where to plant it<sup>22</sup>. 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<sup>23</sup>.

In January this year, 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<sup>24</sup>. 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, officials said<sup>25</sup>.

As it was mentioned above, terrorist recruiters are using shooting video games as well to radicalize young people, especially children. Islamic state has reached unprecedented success when it comes to this activity. In 2012 one of the world’s most popular video game was Grand Theft Auto. Islamic State propaganda machinery created its own modifications. Players can role-

---

<sup>22</sup> *Syrian teenager arrested in Germany 'was planning Isil bomb attack*, The Telegraph, By Justin Huggler <http://www.telegraph.co.uk/news/2016/09/22/syrian-teenager-arrested-in-germany-was-planning-isil-bomb-attack/> Retrieved 19.03.2017

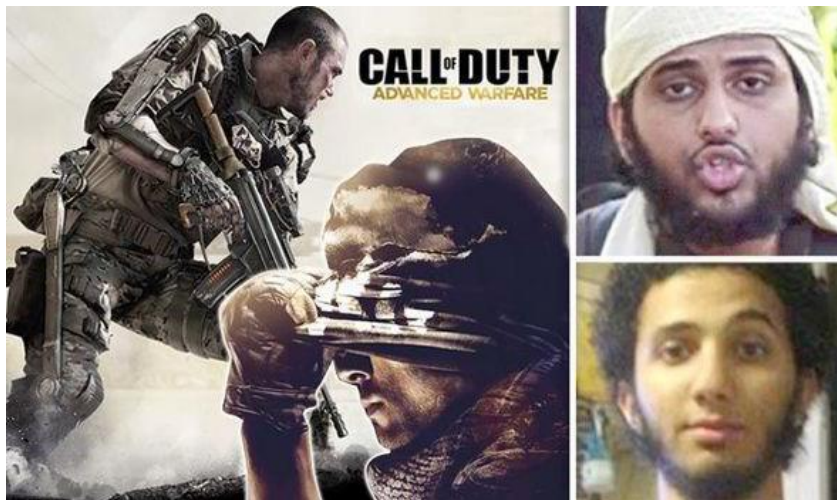
<sup>23</sup> *They're young and lonely. The Islamic State thinks they'll make perfect terrorists. 'What's happening to our children?*, Washington Post, Story by Anthony Faiola, Souad Mekhenne, [http://www.washingtonpost.com/sf/world/2017/02/11/theyre-young-and-lonely-the-islamic-state-thinks-theyll-make-perfect-terrorists/?utm\\_term=.7d8415eb9d60](http://www.washingtonpost.com/sf/world/2017/02/11/theyre-young-and-lonely-the-islamic-state-thinks-theyll-make-perfect-terrorists/?utm_term=.7d8415eb9d60) Retrieved 19.03.2017

<sup>24</sup> *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, By Allan Hall <http://www.dailymail.co.uk/news/article-3476986/Teenage-female-ISIS-fanatic-radicalised-age-seven-stabbed-German-police-officer-unable-make-Syria.html#ixzz4boTyI0UH> Retrieved 19.03.2017

<sup>25</sup> *They're young and lonely. The Islamic State thinks they'll make perfect terrorists. 'What's happening to our children?*, Washington Post, Story by Anthony Faiola, Souad Mekhenne, [http://www.washingtonpost.com/sf/world/2017/02/11/theyre-young-and-lonely-the-islamic-state-thinks-theyll-make-perfect-terrorists/?utm\\_term=.7d8415eb9d60](http://www.washingtonpost.com/sf/world/2017/02/11/theyre-young-and-lonely-the-islamic-state-thinks-theyll-make-perfect-terrorists/?utm_term=.7d8415eb9d60) Retrieved 19.03.2017

play as as members of IS engaged in combat on battlefield. Players, as IS soldiers are killing and shooting American soldiers and attack convoys, with lots of explosions<sup>26</sup>.

Two young British citizens were recruited by ISIL with Call of Duty game. 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 game was bought for them by the people who encouraged them to go to Syria. Nasser, who was the 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<sup>27</sup>.<sup>7</sup>



**Photo 4.** Video game for children and youths GTA 5

Another example of using video games for terrorists propaganda is using GTA 5. ISIS produced game intro where Jihadists screaming “Allahu akbar” while burning alive and shooting civilians<sup>28</sup>.

---

<sup>26</sup> *ISIS use grand theft auto mock up to recruit and boost morale*, Inquisitr, By Jonathan Clauson, [www.inquisitr.com/1486558/isis-uses-grand-theft-auto-mock-up-to-recruit-and-boost-morale](http://www.inquisitr.com/1486558/isis-uses-grand-theft-auto-mock-up-to-recruit-and-boost-morale) Retrieved 19.03.2017

<sup>27</sup> *Call of Duty being used to recruit British Muslims', father of Welsh Jihadists claims*, Sunday Express, <http://www.express.co.uk/news/uk/503094/Call-of-Duty-used-to-recruit-British-Muslims-father-of-Welsh-Jihadistsclaims> Retrieved 19.03.2017

<sup>28</sup> Available at: <https://www.youtube.com/watch?v=604aevo3MzM>



**Photo 5.** GTA 5 Radical Islamic terrorists kill civilians

### **Cyber war of Independent Internet Collective Anonymous against Islamic Terrorists**

Islamic state or ISIL became quite dominant terrorist group when it comes to various activities in cyber space, especially when it comes to propaganda, recruitment, fund raising with the potential fear that hackers of the group could manage to successfully attack national infrastructure of the ‘‘enemy’’ states by using sophisticate cyber attacks. Fighting terrorist groups should include fight on the ground, from the air, from the sea – and in cyber space. There are a couple of Internet hacker groups fighting against Islamic terrorists in a cyberspace. The most active ones are GhostSec and one of most popular, most organized and very well IT equipped hacker collective known as Anonymous. Anonymous declared war against ISIS 2015 after Paris attacks<sup>29</sup>. The hacker collective, which consists of unrelated 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<sup>30</sup>. Main focus of Anonymous collective is disruption of terrorist’s communication with public shutting down their Twitter accounts, Facebook pages, Telegram channels, etc<sup>31</sup>.

<sup>29</sup> Ersel Aydinli, *Violent Non-State Actors: From Anarchists to Jihadists*, Taylor & Francis, Abingdon, UK, 2016. P.138

<sup>30</sup> #OpISIS: Why Anonymous has declared an online war against Isil - in 90 seconds, *The Telegraph*, By Keely Lockhart

<http://www.telegraph.co.uk/news/worldnews/islamic-state/12003242/OpISIS-Why-Anonymous-has-declared-an-online-war-against-Isil-in-90-seconds.html> Retrieved 19.03.2017

<sup>31</sup> *Anonymous Finally Reveals How They Attack ISIS Militants |#opisis | ISIS | Anonymous*

<http://anonhq.com/anonymous-finally-reveals-attack-isis-militants-opisis-isis-anonymous/> Retrieved 19.03.2017

Anonymous' efforts have encompassed recruiting its own online army of people devoted to identifying and shutting down the militant group's avenues of propaganda<sup>32</sup>. The collective recently released instruction guides to help spread information about the basics of denial-of-service attacks on websites and password cracking, as well as 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<sup>33</sup>. Websites related to the militant group have been gravitating to 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<sup>34</sup>. Anonymous collective have taken down 149 Islamic State related websites and exposed 101,000 Twitter accounts and 5900 propaganda videos<sup>35</sup>. Also, they successfully mapped countries with the most ISIS supporters' Twitter accounts.

### **ISIS Hacker Units Founder Droned**

Member of hacker team TeaMp0ison, Junaid Hussain aka Trick who was arrested for hacking email account of a staffer of former UK Prime Minister Tony Blair and posted personal information of Blair, as well as other government employees online, got radicalized and joined ISIS<sup>36</sup>. He became 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.

---

<sup>32</sup> *Anonymous Finally Reveals How They Attack ISIS Militants* /#opisis | ISIS | Anonymous  
<http://anonhq.com/anonymous-finally-reveals-attack-isis-militants-opisis-isis-anonymous/> Retrieved 19.03.2017

<sup>33</sup> *Anonymous #OpIsis: Hacktivists publish how-to guide for identifying Islamic State Twitter accounts*  
<http://www.ibtimes.co.uk/anonymous-opisis-hacktivists-publish-how-guide-identifying-islamic-state-twitter-accounts-1496378> Retrieved 19.03.2017

<sup>34</sup> *Ghost Sec, Anonymous affiliate, hacks ISIS site on deep web with Viagra, Prozac ad*, Washington Times, By Maria Stainer  
<http://www.washingtontimes.com/news/2015/nov/26/ghost-sec-anonymous-affiliate-hacks-isis-site-deep/> Retrieved 19.03.2017

<sup>35</sup> *Anonymous has claimed to have taken down 20,000 ISIS-affiliated Twitter accounts*, The Hacker News  
[http://thehackernews.com/2015/11/anonymous-hacker-isis\\_21.html](http://thehackernews.com/2015/11/anonymous-hacker-isis_21.html) Retrieved 19.03.2017

<sup>36</sup> *The Curious Case Of The Jihadist Who Started Out As A Hacktivist*, Vanity Fair, BY Lorraine Murphy,  
<http://www.vanityfair.com/news/2015/12/isis-hacker-junaid-hussain> Retrieved 19.03.2017





**Photo 6.**Member of hacker team TeaMp0ison, Junaid Hussain aka Trick

In Syria, where he arrived in 2013, Hussain initially became known for allegedly hacking the Twitter account of CENTCOM, though it's been reported that somebody else was behind that attack and the hacking group known as Cyber Caliphate<sup>37</sup>. Hussain, however, was likely the leader, and perhaps sole member, of another ISIS-linked hacking group known as Islamic State Hacking Division, or IS Hacking Division<sup>38</sup>. What is his most important legacy – he created image of powerful Islamic State in cyber space. He was the one who had exceptional IT skills and very possible, he had all the credit when it comes to IS's overtaking social medias. He had an opportunity to recruit talented IT hackers to work in IS favor. But apparently, although he was public face of Cyber caliphate, he did not manage to accomplish the goal – creating true, powerful, united cyber army of hackers who would be capable of attacking, destroying or gaining the commands and control systems of critical infrastructure that could paralyze their operations.

Hiding behind the name of the IS Hacking Division, Hussain posted the names and personal

---

<sup>37</sup> *US Central Command Twitter account hacked to read 'I love you Isis*, The Guardian, <https://www.theguardian.com/us-news/2015/jan/12/us-central-command-twitter-account-hacked-isis-cyber-attack> Retrieved 19.03.2017

<sup>38</sup> Robert Spencer, *The Complete Infidel's Guide to ISIS*, Regnery Publishing, New York, NY, 2015. Chapter III

information's of 100 US military members, claiming to have obtained it from hacking Pentagon servers, though he likely got most directly from the website. More important, he published the personal information of 1,400 American government workers, information likely culled from older breaches or open source information<sup>39</sup>. Allegedly, information of American personal was delivered to Hussein by Kosovo citizen Ardit Ferizi, aka 'Th3Dir3ctorY' who is believed to be the leader of hacking collective "Kosova Hacker's Security"<sup>40</sup>. But Hussain wasn't just pretending to dox government employees, or breaking into Twitter accounts for propaganda purposes. He apparently developed a custom internet spy tool for ISIS<sup>41</sup>, hacked into military members' Facebook accounts, and led the group's online recruitment drive. He was also allegedly involved in recruiting bombers in Western countries<sup>42</sup>.

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 friend request that he accepted<sup>43</sup>. This undercover agent, which wasn't named in various stories in the British press, is believed to be a friend and 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 web page known as a "waterhole." It's 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, according to what Surespot wrote of the incident. Then later, he made a phone call from his

---

<sup>39</sup> Laith Alkhouri, Alex Kassirer, & Allison Nixon, *Hacking for ISIS: The Emerging Cyber Threat Landscape*, Flashpoint, Inc, 2016, str. 7  
[http://fortunascorner.com/wp-content/uploads/2016/05/Flashpoint\\_HackingForISIS\\_April2016-1.pdf](http://fortunascorner.com/wp-content/uploads/2016/05/Flashpoint_HackingForISIS_April2016-1.pdf) Retrieved 19.03.2017

<sup>40</sup> Edward Mickolus, *Terrorism, 2013-2015: A Worldwide Chronology*, McFarland, Jefferson, North Carolina, US, 2016, p.458

<sup>41</sup> *Hacker Killed by Drone Was Islamic State's 'Secret Weapon'* *Wall Street Journal*, By Margaret Coker in London, Danny Yadron in San Francisco and Damian Paletta in Washington  
<https://www.wsj.com/articles/hacker-killed-by-drone-was-secret-weapon-1440718560> Retrieved 19.03.2017

<sup>42</sup> *How a Teenage Hacker Became the Target of a US Drone Strike*, By Lorenzo Franceschi-Bicchierai  
[https://motherboard.vice.com/en\\_us/article/junaid-hussain-isis-hacker-drone](https://motherboard.vice.com/en_us/article/junaid-hussain-isis-hacker-drone) Retrieved 19.03.2017

<sup>43</sup> *Junaid Hussain: British hacker for Isis believed killed in US air strike*, The Guardian,  
<https://www.theguardian.com/world/2015/aug/27/junaid-hussain-british-hacker-for-isis-believed-killed-in-us-airstrike> Retrieved 19.03.2017



home in Raqqa that gave GCHQ the ability to pinpoint his location. The 21-year-old hacker was killed by drone outside Raqqa in August 2015<sup>44</sup>.

### **Serbian Anonymous Joined Fights Against Jihadists**

Republic of Serbia has problems with Islamic extremists as well, especially on its south region called Raška. Serbian Anonymous collective had done their part of Operation ISIS in this region. First of all, they discover newly create Facebook page “Army of Republic of Sandzak” (Sandzak is how they call Raska region) with more than 7000 followers already. They asked their followers to report that page to Facebook and it was erased in a half an hour. Serbian medias following Anonymous post, informed public about existence of extremists’ page and main Persecutor for hi-tech crime ordered the police to discover individuals behind it. In meanwhile, Serbian Anonymous already found out who are those people and reveled their identities on their page. Police arrested them very same day.

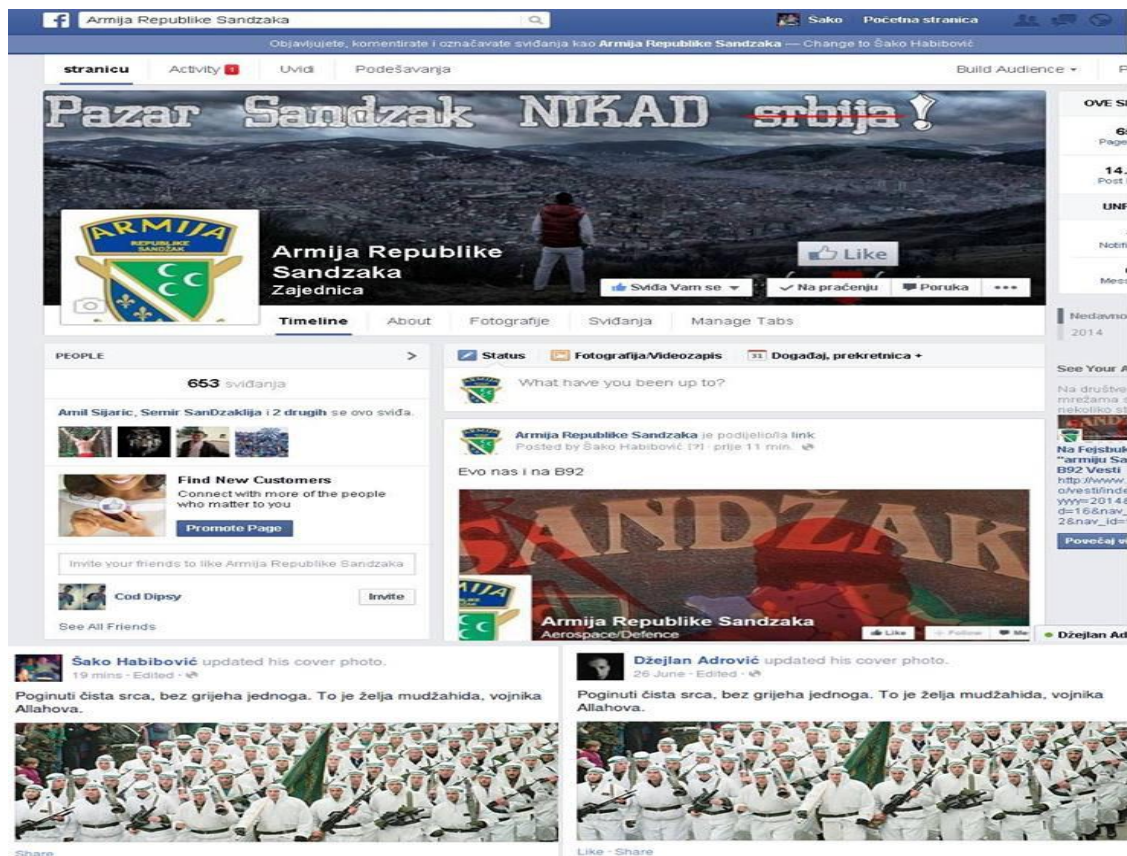
Event that triggered the attention of Anonymous Serbia took place on 5<sup>th</sup> September. It was military styled parade that stirred the public. The group of about thirty men in green uniforms with red fezzes, and green berets on their heads, occupied the central streets of the city of Novi Pazar, in Sandzak (Serbia). They marched from HQ of Islamist community to 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 surrounding area, because of uniforms resembled those of war criminals who took part in the extermination of Serbs during the Second World War. The parade was lead by Islamist Chief Mufti and his associates<sup>45</sup>.

---

<sup>44</sup> *Here’s how the military tracked down and killed the top hacker for ISIS*, Business Insider, By Paul Szoldra,

<http://www.businessinsider.com/isis-hacker-trick-found-2016-6?IR=T> Retrieved 19.03.2017

<sup>45</sup> *Anonymous Serbia identified jihadi groups in the Balkans #opIceISIS*, CyberWarzone, <http://cyberwarzone.com/anonymous-serbia-identified-jihadi-groups-balkans-opiceisis/> Retrieved 19.03.2017



**Photo 7.** Radical Islamic terrorists in Raska -Serbia

## Conclusion

Islamic radicals and terrorist groups use Internet in advanced and various ways to accomplish their goals. They have their IT professionals, programmers, hacker teams, and recruiters, fund raisers, etc. States and security sector must find more efficient ways to identify the threats from Internet, especially cyber terrorists, to track their members, intercept their communications, infiltrate among them, etc. Cyber terrorism is a threat to the international community as much as any other forms of terrorism. Extremists have adopted new skills in order to fight on a new ground – cyber ground and it will be a true challenge for international community to fight back. Terrorist will continue to use the Internet to maintain their current methods. The question is will 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 started creating their national cyber

strategies as well as systems of defense. But without international unified cooperation, the victory against terrorist on Internet will not be gained.

### **Literature:**

1. Miroljub Jevtic, *Political Science and Religion*, The Politics and Religion Journal, Volume 1 No.1, Belgrade, Serbia, 2017
2. Dorothy E. Denning, *Cyber terrorism*, Testimony Before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives - May 23, Washington D.C.US. 2000.
3. Gábor IKLÓDY, *The New Strategic Concept and the Fight Against Terrorism: Challenges & Opportunities*, Defence Against Terrorism Review, COE-DAT, NATO, Vol.3, No. 2, Brussels, Belgium, 2010.
4. John Arquilla, David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, RAND, Santa Monica, CA, US, 2001.
5. M.N. Ogun, *Terrorist Use of Cyberspace and Cyber Terrorism: New Challenges and Responses*, IOS Press, NATO – Emerging Security Challenges Division, Washington D.C. US, 2015.
6. Babak Akhgar, P. Saskia Bayerl, Fraser Sampson, *Open Source Intelligence Investigation: From Strategy to Implementation*, Springer, Cham, Switzerland, 2017.
7. Evan M. Axelrod, *Violence Goes to the Internet: Avoiding the Snare of the Net*, Charles C Thomas Publisher, Springfield, IL, US, 2009.
8. Darko Trifunović, *Digital steganography in terrorist networks*, SYM-OP-IS 2015: XLII International Symposium on Operations Research, Belgrade, Serbia, 2015.
9. Andrea De Guttry, Francesca Capone, Christophe Paulussen, *Foreign Fighters under International Law and Beyond*, Springer, Cham, Switzerland, 2016.
10. Ersel Aydinli, *Violent Non-State Actors: From Anarchists to Jihadists*, Taylor & Francis, Abingdon, UK, 2016.
11. Robert Spencer, *The Complete Infidel's Guide to ISIS*, Regnery Publishing, New York, NY, 2015.

12. Edward Mickolus, *Terrorism, 2013-2015: A Worldwide Chronology*, McFarland, Jefferson, North Carolina, US, 2016.