

JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES ISSN 2029-7017 print/ISSN 2029-7025 online 2017 December Volume 7 Number 2 https://doi.org/10.9770/jssi.2017.7.2(1)

### **ROLE OF INTERNET IN LONE WOLF TERRORISM**

### Tomáš Zeman<sup>1</sup>, Jan Břeň<sup>2</sup>, Rudolf Urban<sup>3</sup>

<sup>1,2,3</sup>University of Defence in Brno, Faculty of Military Leadership, Department of Emergency Management, Brno, Czech Republic

*E-mails:*<sup>1</sup>*tomas.zeman2*@*unob.cz*; <sup>2</sup>*jan.bren*@*unob.cz*; <sup>3</sup>*rudolf.urban*@*unob.cz* 

Received 20 February 2017; accepted 26 November 2017

Abstract. For the last two decades, lone wolf terrorists in Western countries have been significantly changing their modus operandi. Part of these changes and possibly even one of their causes is the increasing use of the internet by lone wolves. This article reviews the role of the internet in the preparation of a terrorist attack as well as during the process of radicalisation of lone wolves. The possibilities and methodical flaws of lone wolf identification on the internet are also discussed. Based on current knowledge, it can be said that the Internet still has a limited role for lone wolves during the preparation of their terrorist attacks. However, it has been demonstrated, that as an efficient communication tool, the internet is of considerable importance in the process of lone wolf radicalisation. The internet is also a place where lone wolves may leak indications of their future actions. These leakages may be utilised for the identification of future lone wolf terrorists on discussion forums or radical websites using semi-automatic methods. However, the biggest drawbacks of these methods is their inability to distinguish between future lone wolf terrorists and common radical authors with no real intention on committing any terrorist act.

Keywords: terrorism; lone wolf; internet; identification; radicalisation; Internet; communication

**Reference** to this paper should be made as follows: Zeman, T.; Břeň, J.; Urban, R. 2017. Role of Internet in Lone Wolf Terrorism, *Journal of Security and Sustainability Issues* 7(2): 185-192. https://doi.org/10.9770/jssi.2017.7.2(1)

**JEL Classifications:** Q3

#### 1. Introduction

Although, lone wolf terrorism is not a new phenomenon, recent statistics show a significant increase in the number of terrorist attacks committed by lone wolves, as well as gradual changes in the technique of terrorist attacks during last two decades (Ellis et al., 2016; Hamm and Spaaij, 2015). Fig. 1 shows the annual statistics of terrorist attacks committed by lone wolves, resp. cases of lone wolf terrorists, based on published data for the European Union (EU) and United States (USA). In both regions, there is an obvious growing trend. In the USA, this trend reached its peak in 2010. In the EU, the highest amount of lone wolf terrorist attacks was reported in 2013. Although there is a slight decrease in 2014, it cannot be assessed if the growing trend actually stopped, or is only a random deviation, because newer data are not available. Ellis et al. (2016) pointed out that the growing trend may be partially caused by the expansion of digital archives, which significantly increase the media impact of newer terrorist attacks and improve their traceability. However, we assume that this may explain only a minor part of the observed increase in the numbers of terrorist acts committed by lone wolves in the EU, resp. lone wolf terrorists in the USA.



**Figure 1.** The number of terrorist attacks committed by lone wolves per year in Europe (EU, Norway and Switzerland) and the number of lone wolf terrorist in the USA from 2000 to 2014 (source of data: Ellis et al., 2016; Hamm and Spaaij, 2015)

Hamm and Spaaij (2015) pointed out the changes in modus operandi of lone wolves in the USA. They evidenced a significant increase of lone wolf terrorist attacks against uniformed police and military personnel since September 11, 2001. Since 2001, terrorist attacks by lone wolves against military bases and military facilities have emerged in the USA. Hamm and Spaaij (2015) reported important changes as well in the mechanism of lone wolf radicalisation in the USA. Whereas prior to September 11, 2001 the radicalization was most frequently connected with previous membership in an extremist group, since then this source of radicalisation has been gradually replaced by the internet. Ellis et al. (2016) noticed the fact that lone wolves are not necessarily so socially isolated as it has been sometimes assumed. Only 28% of lone wolves recorded in the Countering Lone Actor Terrorism (CLAT) database were socially isolated, while 46% of lone wolves somehow signalized their intentions or extremist attitudes to others before they actually committed a terrorist act. Previously, they expressed their opinions usually to their friends or family members; recently, the use of the internet as a tool for expressing views has been growing quickly.

## 2. The internet as an instrument used by lone wolves

The internet is often considered an effective communication tool for terrorist and terrorist groups giving them relative anonymity, a huge amount of information and very cheap connection compared to other communication tools (Benson, 2014; Bowman-Grieve, 2013; Holt et al., 2015; Ogun, 2012; Rudner, 2017; Torok, 2013; Tsfati and Weimann, 2002; Weimann, 2011; Tvaronavičienė, Černevičiūtė, 2015; Hilkevics, Hilkevics, 2017; Štitilis et al., 2016; Limba et al., 2017).

With regards to the lone wolves, the potential benefit for them is the availability of vital information on the internet such as instructions for bomb making, instructions for gaining weapons of mass destruction, or terrorist tactic guidelines. Benson (2014) even suggested that this information might actually enable lone wolves to prepare terrorist attacks and act truly independently.

On the other hand, whatever information a terrorist may obtain on the internet, internet communication seems to play only a marginal role during the actual preparation of terrorist attacks. Mueller and Stewart (2015) analysed 61 cases of Islamic terrorism in the USA from September 11, 2001 to 2015 and found out that truly important information was usually communicated face-to-face and not by using the internet. Benson (2014) argue that anonymity on the internet is only relative and user identity may often be tracked. Based on their results, Mueller and Stewart (2015) even question the significance of information gained on the internet. They highlight the fact that internet manuals are of poor quality and contain inaccuracies or even 'utter nonsense', for detailed

analysis see Stenersen (2008). In addition, Benson (2014) suggested that information on websites might be of limited use, even when they are correct, because learning of some skill requires practical experience that cannot be gained in this manner.

One source of information for lone wolves could be the websites of operating terrorist organisations. However, it seems that terrorist organisations focus their efforts on websites primarily for self-propagation, not for the transmission of practical knowledge, e.g. bomb construction instructions, to third parties (Brandon, 2008). Tsfati and Weimann (2002) analysed the contents of dozens of websites of different terrorist organisations. They reported that most of them avoid presenting their violent activities on their websites. Instead, they usually emphasise themes such as freedom of expression or political prisoners. Significant efforts are in most cases devoted to vindicating the use of violence. Tsfati and Weimann (2002) recognised four rhetorical structures used on terrorist organization websites that justify the use of violence:

- (1) The claim that there was 'no choice" other than the use of force.
- (2) Demonize the enemy, e.g. posting a video of children killed by US air raids.
- (3) Emphasize that terror is the weapon of the weak.
- (4) Made statements about how terrorist organizations are trying to reach a non-violent solution.

However, this rhetoric style may be an effective tool for the radicalization of website visitors, in fact, a more effective way than direct calls for terrorist attacks. Another important finding by Tsfati and Weimann (2002) is that terrorist organisations usually do not seek to mobilize visitors of websites directly into violent action. If they seek support on a website, it usually takes the form of economic support. Nevertheless, a website visitor may be indirectly encouraged towards violence, e.g. call for a Jihad.

As described above, the significance of the internet as a communication tool in the transfer of practical information or in the planning of a terrorist attack seems to be at least marginal. However, it is argued that the internet has a crucial role in transferring or changing theoretical information, e.g. ideology, opinions etc. Regarding the lone wolves, it is argued that information spreading throughout the internet may significantly contribute to their radicalization, however, if it is not its very source. A good example of this mechanism is Al-Qaeda's 'electronic jihad'. The goal of the 'electronic jihad' is to spread the idea of jihad among Muslim communities around the world, especially in the Western countries (Rudner, 2017). An 'electronic jihad' focuses specifically on turning moderate individuals into Islamic militants in Western countries. In this way, an 'electronic jihad' may influence the radicalization of lone wolves. Based on the analysis of an online discussion on the password-protected forum of the islambase.co.uk, the most significant websites for Islamic extremist in the UK, Brandon (2008) delimited three main functions of Islamic extremist websites:

(1) They work as online libraries of theoretical text, which includes violent interpretations of Islam.

(2) They act as a venue for preachers. On jihadi websites, radical preachers can communicate with their listeners unhindered.

(3) They act as a forum for radical Islamists where they can exchange their opinions, discuss their activities etc.

Part of the 'electronic jihad' Al-Qaeda strategy is also the publication of instruction manuals, e.g. for homemade bomb preparation, use of automatic rifles etc., intended especially for individually operated followers, which gives them inspiration and direction to engage, as suggested by Rudner (2017).

There are many different opinions on the involvement of internet in the radicalisation of lone wolves. Some authors, e.g. Benson (2014) or Mueller and Stewart (2015), attach only limited significance to the internet and agree on the fact that the internet in its current form provides more advantages to counter terrorists than to terrorists alone. Although Mueller and Stewart (2015) admit that the internet may have facilitated the function in the mechanism of terrorist radicalisation, they do not recognise it as unreplaceable tolls.

In contrast, Sageman (2008) sees the role of the internet as crucial in the development of a 'leaderless jihad'. Sageman suggested that the internet is transforming people's relationships and creating a new social structure. On the other hand, he denies that propaganda spread by extremist websites could create a new terrorist. They

may reinforce previously made-up minds and give them some inspiration at most. He emphasized the significance of web forums and chat rooms as a tool for an individual's radicalisation. Later, Tucker (2010) criticized many of the hypotheses formulated by Sageman (2008), especially the hypothesis about the influence of the internet on the transformation of the social relationship between people. Tucker (2010) considers this hypothesis baseless, arguing that even in the age of internet, people still prefer a face-to-face social life, which also applies to potential terrorists:

'Internet images sometimes appear to assist if not initiate the movement to extremism. Chat rooms play a role but rarely are the place terrorists first meet; face-to-face contact predominates. Mosques and other physical gathering places figure more prominently than the internet (Tucker, 2010, p. 5).'

In contrast, e.g. a report Roots of violent radicalisation: Nineteenth Report of Session 2010–12 by the UK House of Commons Home Affairs Commitee (2012) ascribes that the internet plays a large role in the process of radicalization, actually larger than religious institutions do. Similarly, Holt et al. (2015) emphasized the significance of the internet in the mechanism of terrorist radicalization.

As mentioned above, there are many published case studies of the internet's influence on terrorist radicalisation. However, there is almost a complete lack of quantitative studies on this subject. One exception is the statistical analysis of a sample of 223 lone wolf terrorists in the UK from 1990 to 2014, performed by Gill et al. (2017). They found out that in 61 % of them, there was evidence of online activity related to either their radicalization or attack planning:

- (1) 32 % used the internet for preparation of the attack
- (2) 29 % communicated with other radicals on the internet
- (3) 15 % via e-mail
- (4) 9 % via online chat rooms
- (5) 8 % via online discussion forum
- (6) 15 % spread propaganda online
- (7) 9 % tried to recruit others online
- (8) 6 % provided material support to others online
- (9) 5 % sought legitimization for their future action online
- (10) 5 % signalized their plans online

# 3. Searching for lone wolves on the internet

Although, there is still discussion about the extent and practical significance of internet use by lone wolves, the fact that lone wolves commonly use the internet is a matter of which there is little doubt. Even when they are not searching for terrorist tactic guidelines or not preparing a terrorist act, they may be expressing their opinions on the internet or leading discussions with other persons who have adopted a similar ideology. All these actions may be potentially utilized to identify future lone wolf terrorists before committing a terrorist attack. Unfortunately, some lone wolves are well aware of this risk, e.g. arguably one of the most successful lone wolf, Anders Breivik, wrote in his manifest (Berwick, 2011, p. 853).

'You will increase your chance of being apprehended by 100% for every person you involve. Don't trust anyone unless you absolutely need to (which should never be the case). Do absolutely everything yourself.'

Even if a lone wolf terrorist is able to remain anonymous and makes no leakages during his preparation of a terrorist attack, there is still the question of whether he could remain anonymous during the whole course of his radicalization. It is very probable that most lone wolves tend to express their attitudes sometimes during the phase of their radicalization. If the leakage took the place on the internet, it may be captured, possibly even before the radicalized person has become a lone wolf terrorist.

The overwhelming extent of the internet network makes it practically impossible to search manually for potential terrorist. In this situation, the use of automatic or semi-automatic computer search tools seems to be the only option. Cohen et al. (2014) suggested that fully automatic search tools are not likely to be sufficiently effective due to the fact, that deep knowledge of the context and large personal experience is often needed to detect a potential lone wolf terrorist. Moreover, the information may be expressed not only by words but also by other ways, e.g. by images. For these reasons, Cohen et al. (2014) view semi-automatic search engines as the most valuable tools for lone wolf identification.

Cohen et al. (2014) suggested that out of the eight warning behaviours formulated by Meloy et al. (2012), leakage, fixation and identification are the most likely to be found on the internet. Meloy and O'Toole (2011) define leakage as 'the communication to a third party of an intent to do harm to a target'. Based on the analysis of previously published case studies, Meloy and O'Toole (2011) noticed that some kind of leakage is especially common for adolescent mass murderers, e.g. spree shooters. In this group, the leakage is often accompanied by direct threats. These findings may also apply to adolescent lone wolves. Fixation is defined by Mullen et al. (2009, p. 34) as 'an intense preoccupation with an individual, activity, or idea'. As noticed by Cohen et al. (2014), the fixation compels the subject to gather extensive amounts of information about the target of attack. According to Cohen et al. (2014), the third of the most important warning behaviours is identification. Meloy and O'Toole (2011) define it as a behaviour that indicates the urge of the subject to project himself in the role of 'pseudo-commando'. It may take the shape of worshiping previous attackers or even identification with them, as well as strong personal interest in weapons or another military utility. Cohen et al. (2014) suggested that lone wolves tend to exhibit videos and pictures of themselves with weapons or in some kind of military context on the internet. As an example, they mentioned the case of Anders Behring Breivik, who showed himself in a picture with an automatic weapon.

Cohen et al. (2014) identified four main problems of searching for lone wolves on the internet: 1) Translation Services; 2) Sentiment Analysis; 3) Mapping Websites; 4) Author Recognition. The first step for a text not written in English is text translation. In principle, there are two basic approaches to translation. One option is manual translation by a human expert; the second is the use of an automatic translator, which leads to a lower quality translation but a very high translation speed compared to the first case. Sentiment analysis and mapping websites include text analysis whose main goal is to determine the 'problematic' users or websites. The last step is the identification of users, which is no less problematic. One way to identify the author of a 'problematic' post is to get into his registration details or locate his IP address. However, there are techniques allowing the concealment of these data, so the user may be very hard to detect when using these kind of methods. The other way to gain the identity of the user is by using text analysis. The basic idea behind this method is that the writing style of each individual is so unique, it is actually comparable to human fingerprints. At present, research is leading up to the development of algorithms that will be able to distinguish people based on the structure of their language. However, existing algorithms are not yet sufficiently effective for the task of large-scale language-based identification of persons on the internet.

Nevertheless, Cohen's et al. (2014) study was only theoretical, giving no practical guide for distinguishing lone wolves. Recently, Scrivens et al. (2018) analysed over 1 million posts on four online Islamic discussion forums. Based on performed sentiment analysis, they created a 'radical score', which rates each author according to his online activity. A 'radical score' is the sum of the following components: 1) Average sentiment score percentile; 2) Volume of negative posts; 3) Severity of negative posts; 4) Duration of negative posts. By using the 'radical score', Scrivens et al. (2018) were able to identify the most radical users on the analysed discussion forums. However, the authors themselves highlight the fact that the verbal radicalism of user does not imply that this user is preparing a terrorist act.

Many authors including Holt et al. (2015), Khalil (2014) or Schuurman & Eijkman (2015) consider this the most serious drawback of lone wolf identification based on their behaviour. They point out on the fact that a radical attitude and extreme action are not the same. There are many individuals with extreme opinions, however, only a slight fraction of them ever take the step to perform a terrorist attack. On the other hand, there are many terrorists who do not share their extreme opinions. Khalil (2014) argues that, whereas supportive attitudes for political violence are driven mainly by collective causes including repression, socioeconomic inequality etc., contribution to political violence is often caused by individual-level motives such as material gains, fear, craving for adventure or vengeance. If this would be true, what impact does the radicalization of an individual via the internet actually have on the probability of him performing some kind of terrorist act? Radicalisation may be only a necessary condition, not a direct cause of performing a terrorist act. However, as demonstrated by Gill et al. (2017), even the intention to perform a terrorist act might be gained on the internet. In their sample of 223 lone wolf terrorist in the UK from 1990 to 2014, they found that 14 % of them chose to use violence after witnessing something online.

# Conclusions

In review, it was pointed out that lone wolves are not necessarily so socially excluded as was sometimes suspected. Moreover, social isolation in real life does not exclude the possibility of social interaction with other people via the internet. Actually, these new online social structures mediated by the internet may be relatively common for lone wolves. Based on current knowledge, it can be said that the internet still plays a limited role for lone wolves during the preparation of their terrorist attacks. However, it is of considerable importance as an efficient communication tool. It is highly probable that the internet communication of lone wolves significantly participates in the process of their radicalisation. For example, the internet may serve as an environment, which allows future lone wolves to get acquainted with extremist opinions, search for ideological texts or easily establish contact with other radicals or preachers of an extreme ideology.

The internet is also a place where lone wolves may leak some indications of their future actions. These leakages may be utilised in the identification of future terrorists before carrying out his attack. Semi-automatic methods have recently begun to develop for the identification of radical websites and radical users on web discussion forums. These methods are still at the beginning of development, but they could be very effective in the future and should be further elaborated. Their biggest drawback, which is more serious than technical issues, is the fact that radicalism does not necessarily imply the implementation of terrorist attacks. Conversely, there have been many terrorist acts which were performed by actors who previously did not express any radical views.

## References

Benson, D.C., 2014. Why the Internet Is Not Increasing Terrorism. *Security Studies* 23: 293–328. https://doi.org/10.1080/09636412.2 014.905353

Berwick, A., 2011. 2083. A European Declaration of Independence.

Bowman-Grieve, L., 2013. A psychological perspective on virtual communities supporting terrorist & extremist ideologies as a tool for recruitment. *Security Informatics* 2(9). https://doi.org/10.1186/2190-8532-2-9

Brandon, J., 2008. Virtual Caliphate Islamic extremists and their websites. London: Published by Centre for Social Cohesion. ISBN 978-1-903386-68-2

Cohen, K., Johansson, F., Kaati, L., Mork, J.C., 2014. Detecting Linguistic Markers for Radical Violence in Social Media. *Terrorism and Political Violence* 26: 246–256. https://doi.org/10.1080/09546553.2014.849948

Ellis, C., Pantucci, R., van Zuijdewijn, J. de R., Bakker, E., Gomis, B., Palombi, S., Smith, M., 2016. Lone-Actor Terrorism Final Report.

Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., Horgan, J., 2017. Terrorist Use of the Internet by the Numbers: Quantifying Behaviors, Patterns, and Processes. *Criminology & Public Policy* 16: 99–117. https://doi.org/10.1111/1745-9133.12249

Hamm, M., Spaaij, R., 2015. Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies. Available on the Internet https://www.ncjrs.gov/pdffiles1/nij/grants/248691.pdf

Hilkevics, S.; Hilkevics, A. 2017. The comparative analysis of technology transfer models. *Entrepreneurship and Sustainability Issues* 4(4): 540-558. https://doi.org/10.9770/jesi.2017.4.4(11)

Holt, T., Freilich, J.D., Chermak, S., McCauley, C., 2015. Political radicalization on the Internet: Extremist content, government control, and the power of victim and jihad videos. *Dynamics of Asymmetric Conflict* 8: 107–120. https://doi.org/10.1080/17467586.2015.1065101

House of Commons Home Affairs Commitee, 2012. *Roots of violent radicalisation: Nineteenth Report of Session 2010–12*. London: Published by The Stationery Office Limited.

Khalil, J., 2014. Radical Beliefs and Violent Actions Are Not Synonymous: How to Place the Key Disjuncture Between Attitudes and Behaviors at the Heart of Our Research into Political Violence. *Studies in Conflict & Terrorism* 37: 198–211. https://doi.org/10.1080/1 057610X.2014.862902

Limba, T.; Plėta, T.; Agafonov, K.; Damkus, M. 2017. Cyber security management model for critical infrastructure. *Entrepreneurship and Sustainability Issues* 4(4): 559-573. https://doi.org/10.9770/jesi.2017.4.4(12)

Meloy, J.R., Hoffmann, J., Guldimann, A., James, D., 2012. The Role of Warning Behaviors in Threat Assessment: An Exploration and Suggested Typology. *Behavioral Sciences & the Law* 30: 256–279. https://doi.org/10.1002/bsl.999

Meloy, J.R., O'Toole, M.E., 2011. The concept of leakage in threat assessment. *Behavioral Sciences & the Law* 29: 513–527. https://doi.org/10.1002/bsl.986

Mueller, J., Stewart, M.G., 2015. Terrorism, counterterrorism, and the Internet: The American cases. *Dynamics of Asymmetric Conflict* 8: 176–190. https://doi.org/10.1080/17467586.2015.1065077

Mullen, P.E., James, D. V., Meloy, J.R., Pathé, M.T., Farnham, F.R., Preston, L., Darnley, B., Berman, J., 2009. The fixated and the pursuit of public figures. *The Journal of Forensic Psychiatry & Psychology* 20: 33–47. https://doi.org/10.1080/14789940802197074

Ogun, M.N., 2012. Terrorist Use of Internet: Possible Suggestions to Prevent the Usage for Terrorist Purposes. *Journal of Applied Security Research* 7: 203–217. https://doi.org/10.1080/19361610.2012.656252

Rudner, M., 2017. "Electronic Jihad": The Internet as Al Qaeda's Catalyst for Global Terror. *Studies in Conflict & Terrorism* 40: 10–23. https://doi.org/10.1080/1057610X.2016.1157403

Sageman, M., 2008. Leaderless Jihad: Terror Networks in the Twenty-First Century. Philadelphia: Published by University of Penn-sylvania Press.

Schuurman, B., Eijkman, Q., 2015. Indicators of terrorist intent and capability: Tools for threat assessment. *Dynamics of Asymmetric Conflict* 8: 215–231. https://doi.org/10.1080/17467586.2015.1040426

Scrivens, R., Davies, G., Frank, R., 2018. Searching for signs of extremism on the web: an introduction to Sentiment-based Identification of Radical Authors. *Behavioral Sciences of Terrorism and Political Aggression* 10(1): 1–21. https://doi.org/10.1080/19434472.20 16.1276612

Stenersen, A., 2008. The Internet: A Virtual Training Camp? Terrorism and Political Violence 20: 215–233. https://doi.org/10.1080/09546550801920790

Štitilis, D.; Pakutinskas, P.; Malinauskaitė, I. 2016. Preconditions of sustainable ecosystem: cyber security policy and strategies. *Entre*preneurship and Sustainability Issues 4(2): 174-182. https://doi.org/10.9770/jesi.2016.4.2(5)

Torok, R., 2013. Developing an explanatory model for the process of online radicalisation and terrorism. *Security Informatics* 2: 6. https://doi.org/10.1186/2190-8532-2-6

Tsfati, Y., Weimann, G., 2002. www.terrorism.com: Terror on the Internet. *Studies in Conflict & Terrorism* 731: 317–332. https://doi. org/10.1080/1057610029010121

Tucker, D., 2010. Jihad Dramatically Transformed? Sageman on Jihad and the Internet. Homeland Security Affairs 6: 1-7.

Tvaronavičienė, M.; Černevičiūtė, J. 2015. Technology transfer phenomenon and its impact on sustainable development,. *Journal of Security and Sustainability Issues* 5(1): 87–97. DOI: http://dx.doi.org/10.9770/jssi.2015.5.1(7)

Weimann, G., 2011. Cyber- Fatwas and Terrorism. Studies in Conflict & Terrorism 34: 765-781. https://doi.org/10.1080/105761 0X.2011.604831

JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES ISSN 2029-7017 print/ISSN 2029-7025 online

### Tomáš Zeman

ORCID ID: orcid.org/0000-0001-7269-4994

Jan Břeň ORCID ID: orcid.org/0000-0003-1565-4050

Rudolf Urban ORCID ID: orcid.org/0000-0003-1893-4648

This is an open access journal and all published articles are licensed under a Creative Commons Attribution 4.0 International License