

TERRORIST USE OF THE INTERNET

Terör Örgütlerinin İnternet Kullanımı

Ergül ÇELİKSOY*
Smith OUMA**

Abstract

This paper offers a brief overview of how and for what purposes the Internet is utilised by terrorists, and discusses whether it plays a vital role for today's terrorist organisations. For this aim, the paper examines how terrorists use the Internet for the purposes of disseminating their propaganda, of achieving the radicalisation of people and the recruitment of new supporters, and of providing online training for their supporters to carry out terrorist attacks as well as terrorist financing. It argues that the Internet is very important for today's terrorist groups for a variety of reasons.

Keywords: terrorism, internet, terrorist use of internet

Özet

Terör örgütleri interneti birçok amaç için kullanmaktadır. Bunların başında, terör propagandası yapmak, insanları radikalleştirmek, internet aracılığı ile uzaklardaki insanlara ulaşarak yeni üyeler devşirmek, terör saldırılarında kullanılmak üzere çeşitli patlayıcıların evde yapımını kolaylaştırıcı nitelikte bilgi içeren materyalleri

* PhD Researcher, School of Law, The University of Nottingham, Nottingham, NG7 2RD, UK. E-mail: ergul.celiksoy@nottingham.ac.uk, ORCID: 0000-0003-2980-710X.

** PhD Researcher, School of Law and Politics, Cardiff University, Cardiff, CF10 3AS, UK. E-mail: OumaSO@cardiff.ac.uk, ORCID: 0000-0002-0469-333X.

Makale Gönderim Tarihi: 01.04.2019.

Makale Kabul Tarihi: 16.12.2019.

internet üzerinden üyelerine ulaştırmak ve terör örgütlerinin internet aracılığı ile finanse edilmesi gelmektedir. Bu makale, terör örgütlerinin interneti hangi amaçlarla ve nasıl kullandığını inceleyerek internetin teröristlerin amacını gerçekleştirmede ne ölçüde etkili bir araç olduğunu tartışmayı amaçlamaktadır.

Anahtar Kelimeler: terörizm, internet, teröristlerin internet kullanımını

I. Introduction

The Internet is an important part of the daily life of many individuals and has brought with it many opportunities and challenges. Nowadays, over 3.3 billion people use the Internet.¹ This number not only include ordinary users, but also ill-wishers such as hackers, online fraudsters and terrorists. Researchers claim that terrorist organisations utilise the Internet for many reasons.² Benson states that terrorist groups exploit the Internet since it offers many opportunities such as anonymity, cheap and easy communication and an abundance of information.³ The Internet is also utilised by terrorists for a number of other purposes such as dissemination of propaganda, psychological warfare, gathering information, radicalisation and recruitment of individuals, online training and planning and preparing for attacks and terrorist financing.⁴ In this respect, terrorist use of the Internet is a broader term than

¹ "Individuals using the Internet (% of population)," The World Bank, accessed September 20, 2019, <https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2017&start=1960&view=chart>.

² Maura Conway, "Terrorism and the Internet: New Media - New Threat?," *Parliamentary Affairs* 59, no. 2 (2006): 283-298; Gabriel Weimann, "www.terror.net - How Modern Terrorism Uses the Internet," *USIP Special Report*, no. 116 (2004): 1-12.

³ David C Benson, "Why the Internet Is Not Increasing Terrorism," *Security Studies* 23, no. 2 (2014): 298.

⁴ Stuart Macdonald and David Mair, "Terrorism Online: A New Strategic Environment," in *Terrorism Online: Politics, Law and Technology*, ed. Lee Jarvis, Stuart MacDonald, and Thomas M. Chen (Abingdon: Routledge, 2015), 10-34.

'cyberterrorism' because the former refers to a wider range of online activities associated with terrorism, whereas the latter is linked to terrorist attacks against information infrastructures, computer systems and programmes and data.⁵ The purpose of this paper is to provide an overview of why and how the Internet is used by terrorist organisations for a variety of purposes. It contains four discussion sections: disseminating propaganda, radicalisation and recruitment, online training and attack and terrorist financing. Following the explanation of terrorist usage of the Internet under these four spheres, the conclusion arrived at will be evident: The use of the Internet is becoming vital for today's terrorist groups.

II. Propaganda Dissemination & Communication

Terrorist organisations use propaganda to legitimise their operations and to gain support or show the weakness of their enemies.⁶ To understand the importance of propaganda

⁵ Dorothy E. Denning provides best-known and widely used definition of cyberterrorism. According to her, 'Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt non-essential services or that are mainly a costly nuisance would not.' See Dorothy E. Denning, "Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services US House of Representatives," May 23, 2000, <https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm>. See also Lee Jarvis and Stuart Macdonald, "What Is Cyberterrorism? Findings from a Survey of Researchers," *Terrorism and Political Violence* 27, no. 4, (2015): 659, <https://doi.org/10.1080/09546553.2013.847827>; Lee Jarvis, Stuart Macdonald, and Andrew Whiting, "Unpacking Cyberterrorism Discourse: Specificity, Status, and Scale in News Media Constructions of Threat," *European Journal of International Security* 2, no. 1 (2017): 65, <https://doi.org/10.1017/eis.2016.14>.

⁶ Weimann, "How Modern Terrorism Uses the Internet," 6-8.

dissemination for terrorist organizations, it is worth noting that Osama bin Laden wrote, '[i]t is obvious that the media war in this century is one of the strongest methods; in fact, its ratio may reach 90 percent of the total preparation for the battles'.⁷ Similarly, in a letter that was sent by Ayman al-Zawahiri to Abu Musab al-Zarqawi, who was the leader of Al-Qaeda in Iraq at that time, al-Zawahiri wrote that '[w]e are in a battle, and more than half of this battle is taking place in the battlefield of the media. And that we are in a media battle in a race for the hearts and minds of our Ummah'.⁸ From these statements, it follows that propaganda dissemination is one of the priorities of terrorist organisations. Thus, terrorist groups utilise technology, especially the Internet, whose effectiveness rivals all the other methods of information dissemination. For example, Mohamed Jarmoune, who promoted jihadist ideology in his Facebook group, spent almost 15 hours a day disseminating terrorist propaganda online before eventually being arrested and sentenced to five years and four months in prison.⁹

Using the Internet for terrorist propaganda has many advantages. For example, prior to the advent of the Internet, terrorist groups depended on mainstream media such as television, radio and newspapers to express their policies and disseminate their propaganda.¹⁰ However, the Internet has freed terrorist groups from the dependency of mainstream media and allowed them to access their audience with little obstacles.¹¹ In addition to this, the Internet has increased the size of the potential audience of terrorist groups. For instance, the World Bank revealed that more than 45 per cent of the world population (more than 3.3 billion people) used the

⁷ Akil N. Awan, "The Virtual Jihad: An Increasingly Legitimate Form of Warfare," *CTC Sentinel* 3, no. 5 (2010): 10.

⁸ Jytte Klausen, "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq," *Studies in Conflict & Terrorism* 38, no. 1 (2015): 3.

⁹ Lorenzo Vidino, "The Evolution of Jihadism in Italy: Rise in Homegrown Radicals," *CTC Sentinel* 6, no. 11 (2013): 19.

¹⁰ Weimann, "How Modern Terrorism Uses the Internet," 6.

¹¹ Klausen, "Tweeting the Jihad," 3.

Internet in 2016 (See Figure 1). In addition, the number of social media users as of 2019 was over 2.7 billion, and it is estimated that this figure will increase to 3 billion by 2021 (See Figure 2). This means that terrorist organisations have billions of potential audiences which are impossible to access via mainstream media.

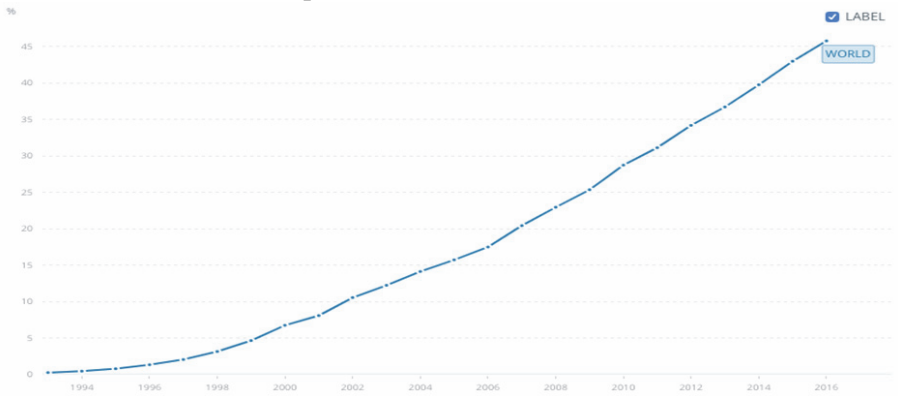


Figure 1: Individuals using the Internet (% of population) in the world.

This figure is reproduced from The World Bank’s website. See “Individuals using the Internet (% of population).”.

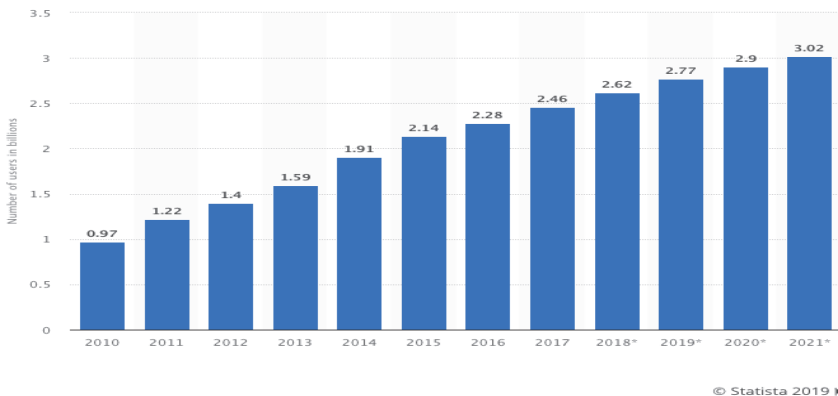


Figure 2: Number of social media users worldwide from 2010 to 2021 (in billions).

This figure is reproduced from Statista's website. See "Number of social Media users worldwide from 2010 to 2021 (in billions)," Statista, accessed March 20, 2019, <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users>.

It is known that almost all terrorist organisations have at least one website, and these are written in different languages.¹² For instance, PKK (*Partiya Karkerên Kurdistanê*), a terrorist organisation, mainly active in Turkey, has a website, called *Hêzên Parastina Gel*, written in Kurdish, Turkish, English, German and Arabic languages. This website includes a press release section, a list of terrorist leaders, a list of central commands, information about the terrorist group's legitimisation of activities, a link to the terrorist's group's online TV, book and article recommendations, interviews with individual terrorists and a contact form. Similarly, important messages of, so called terrorist group, Islamic State of Iraq and Al-Sham (ISIS), were published in English, French and German and translated into other languages to access a broader public.¹³ Al-Qaeda also has a web-based magazine in English called *Inspire*. This shows that terrorist groups try to access as wide an audience as possible to disseminate their propaganda. For this purpose, the Internet avails them many facilities that are easy to use and inexpensive in comparison with traditional methods.¹⁴ Today's terrorist organisations do not have to distribute hard copies of their publications to their supporters, which can be blocked and removed, because they can easily create a website to do so.¹⁵ Even if their website is banned or rendered inaccessible, creating another one is very easy and inexpensive.¹⁶ Although the content of publications

¹² Weimann, "How Modern Terrorism Uses the Internet," 3.

¹³ Anne Aly et al., "Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization," *Studies in Conflict & Terrorism* 40, no. 1 (2017): 5, <https://doi.org/10.1080/1057610X.2016.1157402>.

¹⁴ Benson, "Why the Internet Is Not Increasing Terrorism," 297.

¹⁵ Benjamin R. Davis, "Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance," *CommLaw Conspectus* 15, no. 1 (2006): 131.

¹⁶ Benson, "Why the Internet Is Not Increasing Terrorism," 297-298.

from today's terrorist organisations is like that of the past, the role of the Internet is in the content's distribution; the Internet allows for the 'digitalisation of information'.¹⁷

III. Radicalisation & Recruitment

Edwards and Gribbon have stated that, '[f]or reasons of security and safety, accessibility and anonymity, terrorists and extremists have shifted many of their activities from public spaces (such as mosques, in the case of Islamist extremist groups) to private residences, personal computers and tablets'.¹⁸ Similarly, Janbek and Williams stated that the Internet is an excellent tool for terrorist groups to contact and communicate with those who are vulnerable towards indoctrination attempts or who are already interested in terrorism.¹⁹ They also stated that the Internet is not only a good tool for indoctrination, but also consolidates 'existing radical ideology'.²⁰

It is claimed that terrorist groups use many facilities such as chat rooms, forums and websites to radicalise people.²¹ Keene suggests that 'Internet chat rooms are virtual meeting points for individuals to come together not only to enrol in the cause, and be further radicalised and recruited to the terrorist organisation'.²² With regards to the role played by online forums in radicalisation and recruitment, Marc Sageman wrote that '[i]t is the forums, not the images of the passive websites, which are crucial in the process of radicalization. People change their minds through discussion with

¹⁷ Martin Rudner, "Electronic Jihad: The Internet as Al-Qaeda's Catalyst for Global Terror," *Studies in Conflict & Terrorism* 40, no. 1 (2017): 12.

¹⁸ Charlie Edwards and Luke Gribbon, "Pathways to Violent Extremism in the Digital Era," *The RUSI Journal* 158, no. 5 (2013): 40.

¹⁹ Dana Janbek and Valerie Williams, "The Role of the Internet Post-9/11 in Terrorism and Counterterrorism," *Brown Journal of World Affairs* 20, no. 2 (2014): 299-300.

²⁰ Janbek and Williams, "The Role of the Internet Post-9/11 in Terrorism and Counterterrorism," 300.

²¹ Weimann, "How Modern Terrorism Uses the Internet," 8.

²² Shima D. Keene, "Terrorism and the Internet: A Double-edged Sword," *Journal of Money Laundering Control* 14, no. 4 (2011): 365.

friends, not by simply reading impersonal stories'.²³ Thus, it could be said that being active in chat rooms and forums, which involves joining a discussion rather than acting as a passive member who reads just personal stories or looks at pictures, has an important effect on the radicalisation process.

Websites also play an important role in online radicalisation. When an individual who wants to learn more about an ideology visits a website, he or she is led to 'the group's enlistment pages', which feature 'articles about religious beliefs and core ideologies'.²⁴ This is considered as the first step for the process of radicalisation online; the next step is indoctrination. The individuals who are radicalised try to find ways to act on 'their religious beliefs and core ideologies'.²⁵ These actions can involve joining terrorist groups to carry out their own attacks.²⁶ For example, a law student in London, Mohammed Gul, was radicalised after spending some time on cyberspace with people who already had radical views. Later, he made a decision to make some extremist videos and uploaded them onto YouTube and an Anti-Imperialist forum website.²⁷

More recently, it was discovered that a web-site called *8chan* was frequently used by the attackers of three terrorist attacks occurred in Christchurch, New Zealand on 15 March 2019; Poway, California on 27 April 2019 and El Paso, Texas on 02 August 2019.²⁸ *8chan* was a website, which contained a wide range of different

²³ Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century* (Philadelphia: University of Pennsylvania Press, 2008), 116.

²⁴ Aly et al., "Terrorist Online Propaganda and Radicalization," 5.

²⁵ Aly et al., "Terrorist Online Propaganda and Radicalization," 5.

²⁶ Aly et al., "Terrorist Online Propaganda and Radicalization," 5.

²⁷ "Islamic terrorist propaganda student Mohammed Gul jailed," BBC News, accessed March 25, 2019, <http://www.bbc.co.uk/news/uk-england-london-12576973>.

²⁸ Julia Carrie Wong, "8chan: the far-right website linked to the rise in hate crimes," *The Guardian*, accessed October 1, 2019, <https://www.theguardian.com/technology/2019/aug/04/mass-shootings-el-paso-texas-dayton-ohio-8chan-far-right-website>.

discussion groups about a number of different topics from anime and cryptocurrency to politics and video games.²⁹ *8chan's* /pol/ board was considered as 'a gathering place for extremely online neo-Nazis', and its purpose was, as described by its members, to radicalise anonymous members to carry out acts of violence in the physical world.³⁰

One of the Christchurch attackers posted a manifesto on *8chan*, which was titled 'The Great Replacement' referring to 'white genocide' conspiracy theories.³¹ He also posted link on this platform to his live-streamed attack on Facebook Live. His aim was to show his brutal attack to spread fear of his terrorism, and perhaps, to inspire other extremists to carry out their own attacks.³² His live-streamed attack posted in *8chan* attracted a number of members of this platform, and his manifesto was translated to different languages.³³ It was reported that the attacker's live-streamed video was watched by fewer than 200 people on Facebook before it was taken down by the social media site. However, the live footage posed on *8chan* allowed 'the grisly footage to reach millions'.³⁴ The El Paso shooter, who killed 22 people and injured 24 others, also

²⁹ "What is 8chan?," BBC News, accessed October 1, 2019, <https://www.bbc.co.uk/news/blogs-trending-49233767>.

³⁰ Robert Evans, "Ignore The Poway Synagogue Shooter's Manifesto: Pay Attention To 8chan's /pol/ Board," Bellingcat, accessed October 1, 2019, <https://www.bellingcat.com/news/americas/2019/04/28/ignore-the-poway-synagogue-shooters-manifesto-pay-attention-to-8chans-pol-board/>.

³¹ Kathy Gilsinan, "How White-Supremacist Violence Echoes Other Forms of Terrorism," The Atlantic, accessed October 1, 2019, <https://www.theatlantic.com/international/archive/2019/03/violence-new-zealand-echoes-past-terrorist-patterns/585043/>.

³² Isaac Stanley-Becker et al., "Primary Suspect, One Alleged Accomplice Identified in Terrorist Attack That Killed 49 in New Zealand," The Washington Post, accessed May 10, 2019, <https://www.washingtonpost.com/nation/2019/03/15/shootings-reported-mosques-christchurch-new-zealand/>.

³³ Evans, "Pay Attention To 8chan's /pol/ Board."

³⁴ Rachel Siegel, "8chan Is Back Online, This Time as 8kun," The Washington Post, accessed November 18, 2019, <https://www.washingtonpost.com/technology/2019/11/04/chan-is-back-online-this-time-kun/>.

posted an anti-immigrant manifesto decrying Hispanic migrants on *8chan*, which also expressed support for the gunman who killed 51 people in Christchurch, New Zealand.³⁵ Similarly, the attacker in Poway, California was also a user of this website to spread his hate speeches before conducting his attack.³⁶ Although *8chan* was knocked offline, its extremist users appeared to move other websites.³⁷

It is also important to note that the Internet has contributed to the radicalisation of ‘lone wolves’. Ramón Spaaij defines a lone wolf terrorist as someone who carries out attacks ‘individually and independently’ from the terrorist groups he or she sympathises with or supports.³⁸ Similarly, Gabriel Weimann suggests that ‘a lone wolf is someone who commits violent acts in support of some group, movement or ideology, but does so alone, outside of any command structure’.³⁹ However, it is sometimes questioned whether lone wolves are really alone in their radicalisation and operation process. It is argued that although lone wolves carry out their attacks individually and independently, they are radicalised and supported through the Internet.⁴⁰ Weimann states that ‘[l]one wolves connect, communicate and share information, know-how and guidance – all online – on the “Dark Web”’.⁴¹ Regarding the role played by the

³⁵ “Texas Walmart Shooting: El Paso Attack ‘Domestic Terrorism,’” BBC News, accessed September 12, 2019, <https://www.bbc.co.uk/news/world-us-canada-49226573>.

³⁶ Jill Cowan, “What to Know About the Poway Synagogue Shooting,” The New York Times, accessed September 12, 2019, <https://www.nytimes.com/2019/04/29/us/synagogue-shooting.html>.

³⁷ Joshua Fisher-Birch, “Users of *8chan*’s /Pol Board Move to Other Websites,” Counter Extremism Project, accessed September 10, 2019, <https://www.counterextremism.com/blog/users-8chan%E2%80%99s-pol-board-move-other-websites>.

³⁸ Ramón Spaaij, “The Enigma of Lone Wolf Terrorism: An Assessment,” *Studies in Conflict & Terrorism* 33, no. 9 (2010): 854.

³⁹ Gabriel Weimann, “Lone Wolves in Cyberspace,” *Journal of Terrorism Research* 3, no. 2 (2012): 77.

⁴⁰ Weimann, “Lone Wolves in Cyberspace,” 76.

⁴¹ Weimann, “Lone Wolves in Cyberspace,” 76.

Internet in lone wolves' radicalisation, Pantucci suggests that the Internet is 'an incubator or accelerator of the Lone Wolf phenomenon'.⁴² Additionally, that the Internet has considerable impact on the radicalisation of and attacks by lone wolves was shown in the report conducted by the General Intelligence and Security Service in the Netherlands (AIVD).⁴³

Dissemination may also take the form of terrorists broadcasting their activities in order to evoke sympathy or support from their intended targets and this phenomenon has increasingly become prevalent with the advent of online live-streaming platforms that are not subjected to the rigors of editorial processes.⁴⁴ This phenomenon is particularly attractive to lone wolf terrorists who may draw inspiration from terrorist organisations in jurisdictions beyond their reach or who may be radicalised by ideologies pursued by groups at a local level.

Terrorist use of the Internet is not only limited to the dissemination of terrorist propaganda or radicalisation of individuals. Terrorists also utilise the Internet to recruit new supporters.⁴⁵ Before the Internet, terrorist groups recruited individuals from certain geographic areas as communication with others from different countries or territories was too much of a challenge.⁴⁶ With the use of the Internet, the world is getting smaller for terrorist groups since they can contact others irrespective of where they live.⁴⁷ Today, terrorist groups can communicate with

⁴² Raffaello Pantucci, "A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists," *Developments in Radicalisation and Political Violence*, International Centre for the Study of Radicalisation and Political Violence (ICSR) (2011): 34.

⁴³ Netherlands: General Intelligence and Security Service (AIVD), *Jihadism on the Web: A Breeding Ground for Jihad in the Modern Age* (The Hague, 2012), 20-21.

⁴⁴ Maura Conway and Joseph Dillon, "Future Trends: Live-Streaming Terrorist Attacks?," *VOX-Pol*, accessed October 8, 2019, https://www.voxpol.eu/download/vox-pol_publication/Live-streaming_FINAL.pdf.

⁴⁵ Weimann, "How Modern Terrorism Uses the Internet," 8-9.

⁴⁶ Macdonald and Mair, "Terrorism Online," 16.

⁴⁷ Tom Holt et al., "Political Radicalization on the Internet: Extremist Content, Government Control, and the Power of Victim and Jihad Videos," *Dynamics of Asymmetric Conflict* 8, no. 2 (2015): 108-109.

people in countries and territories which were closed to them before the Internet.⁴⁸ For instance, ISIS used the Internet to recruit people from Europe, North America, Australia and the Muslim countries.⁴⁹ It appears that the Internet allows terrorist groups to live in a visible world in which there are no boundaries to prevent them from accessing people. This is also the case for sympathisers because they can easily contact these groups and join them via the Internet.⁵⁰

The Internet is more frequently used by young individuals than the older generation.⁵¹ Among young individuals, those who are socially deprived, angry and/or marginalised are online more often than others.⁵² By engaging these individuals, who are the major target for terrorist groups, and introducing terrorist literature to them, terrorist groups create new extremists and supporters.⁵³ This is another reason why terrorist groups exploit the Internet for recruitment purposes.⁵⁴ For example, PKK targeted young individuals aged between 15 and 25 in order to recruit them through social media. Ali Sahin, a Turkish MP, stated that 'the terrorist organization [PKK] uses it as a hunting field to recruit fighters for its mountain crew'. He noted that the average age of the PKK members 'has fallen to ages considered children' as young people are more vulnerable to be deceived, especially with the help of social media.⁵⁵

⁴⁸ Macdonald and Mair, "Terrorism Online," 16.

⁴⁹ Rudner, "Electronic Jihad," 16.

⁵⁰ Macdonald and Mair, "Terrorism Online," 16.

⁵¹ William H. Dutton, Grant Blank, and Darja Groselj, "Cultures of the Internet: The Internet in Britain, Oxford Internet Survey 2013 Report," Oxford Internet Surveys, accessed September 24, 2019, <http://oxis.oii.ox.ac.uk/wp-content/uploads/2014/11/OxIS-2013.pdf>.

⁵² Tina Frieberger and Jeffrey S. Crane, "A Systematic Explanation of Terrorist Use of the Internet," *International Journal of Cyber Criminology* 2, no. 1 (2008): 313-314.

⁵³ Macdonald and Mair, "Terrorism Online," 17.

⁵⁴ Macdonald and Mair, "Terrorism Online," 16.

⁵⁵ "AKP Warns on PKK Activities on Internet," *Hurriyet Daily News*, accessed September 14, 2019, <http://www.hurriyetdailynews.com/akp-warns-on-pkk-activities-on-internet-37572>.

IV. Online Training & Attack

In addition to radicalisation and recruitment, terrorist groups use the Internet for online training for their supporters and for planning and preparing for attacking their targets.⁵⁶ In *Inspire*, the Al-Qaeda web-based magazine, Al-Malahem, in an article entitled 'Make a bomb in the kitchen of your Mom', wrote the following:

My Muslim brother: we are conveying to you our military training right into your kitchen to relieve you of the difficulty of traveling to us. If you are sincere in your intentions to serve the religion of Allah then all what you have to do is enter your kitchen and make an explosive device that would damage the enemy if you put your trust in Allah and then use this explosive device properly.⁵⁷

It is obvious that the purpose of the extract above was to train and equip terrorist supporters with a desire to engage with 'leaderless jihad'.⁵⁸ Holbrook wrote that two individuals obtained some bomb-making materials and tried to make a homemade bomb to carry out an attack in the UK.⁵⁹ From the evidence, which was seized from the suspects' properties during the investigation, it was understood that they had downloaded many manuals and searched information online to make a bomb in their house.⁶⁰ Indeed, some researchers claim that the Internet is an 'online terrorism university' for people who seek this kind of information.⁶¹ For instance, Stenersen argues that many forums include some sub-forums dedicated solely to online training, and, in these sub-forums,

⁵⁶ Macdonald and Mair, "Terrorism Online," 17.

⁵⁷ Donald Holbrook, "A Critical Analysis of the Role of the Internet in the Preparation and Planning of Acts of Terrorism," *Dynamics of Asymmetric Conflict* 8, no. 2 (2015): 131.

⁵⁸ Rudner, "Electronic Jihad," 16.

⁵⁹ Holbrook, "A Critical Analysis of the Role of the Internet," 123-124.

⁶⁰ Holbrook, "A Critical Analysis of the Role of the Internet," 126.

⁶¹ Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, D.C.: United States Institute of Peace, 2006) 127.

members can ask questions and share their knowledge and experience with each other.⁶² Moreover, there are 'manuals and encyclopaedias, instruction videos, series and periodicals', which may be helpful for the online training of terrorists.⁶³

Some have contested that the Internet does not have an important role in the terrorists' training process because training requires hands-on experience along with technical information, and online materials may include misleading and incorrect information.⁶⁴ However, there have been some empirical examples of successful online training. For example, David Copeland and Anders Behring Breivik – the London 1999 and Oslo 2011 attackers, respectively – utilised the Internet to make their explosives, and they were successful in their attacks, even though they had no previous experience of making explosive devices.⁶⁵ These arguments also overlook the extent to which online training has facilitated acquisition of skills by mass shooters who have carried out acts of terrorism in different places.⁶⁶ Therefore, it can be argued that, notwithstanding the prevalence of wrong information on the Internet in terms of training, even an amateur attacker may obtain accurate information that he or she can use to make an explosive and carry out his or her attack.

The Internet can also be useful for terrorist groups in terms of planning an operation and attack. For example, Weimann wrote that

⁶² Anne Stenersen, "The Internet: A Virtual Training Camp?," *Terrorism and Political Violence* 20, no. 2 (2008): 228.

⁶³ Stenersen, "The Internet: A Virtual Training Camp?," 228.

⁶⁴ Michael Kenney, "Beyond the Internet: Mētis, Techne, and the Limitations of Online Artifacts for Islamist Terrorists," *Terrorism and Political Violence* 22, no. 2 (2010): 179.

⁶⁵ Gilbert Ramsay, "Relocating the Virtual War," *Defence against Terrorism Review* 2, no. 1 (2009): 45.

⁶⁶ Jillian Peterson and James Densley, "Op-Ed: We have Studied every Mass Shooting since 1966. Here's what we've Learned about the Shooters," *Los Angeles Times*, accessed September 22, 2019, <https://www.latimes.com/opinion/story/2019-08-04/el-paso-dayton-gilroy-mass-shooters-data>.

'Al Qaeda operatives relied heavily on the Internet in planning and coordinating the September 11 attacks'.⁶⁷ It was discovered that, in the 9/11 attack, Al-Qaeda was gathering information about the targets and sending messages through the Internet.⁶⁸ Terrorists planning the 9/11 attack used thousands of encrypted messages on a website that was accessed by password.⁶⁹ According to the United States Department of Justice: Office of Public Affairs, Najibullah Zazi, who tried to carry out an attack on the New York subway system in 2009, wrote 'Marriage is ready' to his contact in Pakistan via e-mail. 'Marriage', the word in his e-mail, refers to the attack and explosives.⁷⁰ Similarly, the members of Gülenist Terror Organisation (FETÖ) in Turkey used a messaging smartphone application, *ByLock*, to communicate via a private, encrypted connection.⁷¹

Planning an attack may require some preparatory acts such as 'target selection; reconnaissance; selection of entrance and exit routes; gaining knowledge of local peak times; and acquiring information on emergency service response times and effectiveness'.⁷² These kinds of preparatory acts require multiple visits to the possible target, which is highly risky, costly and time consuming. However, the Internet allows terrorists to decrease these risks and costs and to save time.⁷³ For example, in its twelfth issue,

⁶⁷ Weimann, "How Modern Terrorism Uses the Internet," 10.

⁶⁸ Keene, "Terrorism and the Internet," 363.

⁶⁹ Weimann, "How Modern Terrorism Uses the Internet," 10.

⁷⁰ The United States Department of Justice: Office of Public Affairs, "Charges Unsealed Against Five Alleged Members of Al-Qaeda Plot to Attack the United States and United Kingdom," The United States Department of Justice, accessed September 28, 2019, <https://www.justice.gov/opa/pr/charges-unsealed-against-five-alleged-members-al-qaeda-plot-attack-united-states-and-united>.

⁷¹ İsmail Saymaz, "ByLock use is an evidence of Gülen network links: Owner," *Hurriyet Daily News*, accessed September 3, 2019, <http://www.hurriyetdailynews.com/bylock-use-is-an-evidence-of-gulen-network-links-owner-105284>. For the analysis of 'Bylock' by the Republic of Turkey Court of Cassation, see General Criminal Division of the Republic of Turkey Court of Cassation, E.2019/312, K.2019/514, 02.07.2019.

⁷² Macdonald and Mair, "Terrorism Online," 21.

⁷³ Macdonald and Mair, "Terrorism Online," 21.

Al-Qaeda's magazine, *Inspire*, showed a 'country-by-country list of targets' and provided detailed information about these targets and how to carry out an attack on them.⁷⁴ Similarly, in the attack on British bases in Basra, attackers used photographs taken from Google Earth that showed the building and vulnerable areas in detail.⁷⁵ It has also been established that the Al Shaabab have in the past used social media platforms to generate propaganda and control the narrative during the course of an attack.⁷⁶ Part of the strategy has been to shape public opinion during an attack and to appeal to their perceived sympathisers. A similar strategy has been deployed by the Boko Haram in West Africa, who have not only employed the use of the Internet for propaganda, but also as a recruitment tool and to coordinate its activities.⁷⁷

The empirical evidence has shown the importance of the Internet in preparation for terrorist attacks. For example, Gill et. al. examined the cases of 223 convicted terrorists in the United Kingdom.⁷⁸ They found that terrorists used the Internet for a variety of activities including radicalisation and/or attack planning in 61 percent of these 223 cases.⁷⁹ More than half of the terrorists in their study specifically

⁷⁴ "Al-Qaeda urges followers to bomb the Savoy," The Telegraph, accessed September 29, 2019, <http://www.telegraph.co.uk/news/worldnews/al-qaeda/10704708/Al-Qaeda-urges-followers-to-bomb-the-Savoy.html>.

⁷⁵ "Terrorists use Google maps to hit UK troops," The Telegraph, accessed September 15, 2019, <http://www.telegraph.co.uk/news/worldnews/1539401/Terrorists-use-Google-maps-to-hit-UK-troops.html>.

⁷⁶ David Mair, "#Westgate: A Case Study: How al-Shabaab used Twitter during an Ongoing Attack," *Studies in Conflict & Terrorism* 40, no. 1 (2017): 24-43, <https://doi.org/10.1080/1057610X.2016.1157404>.

⁷⁷ Kate Cox et al., *Social Media in Africa: A Double-edged Sword for Security and Development* (UNDP, 2018), 22, https://www.undp.org/content/dam/rba/docs/Reports/UNDP-RAND-Social-Media-Africa-Research-Report_final_3%20Oct.pdf.

⁷⁸ Paul Gill et al., "Terrorist Use of the Internet by the Numbers: Quantifying Behaviors, Patterns, and Processes," *Criminology & Public Policy* 16, no. 1 (2017): 99-117, <https://doi.org/10.1111/1745-9133.12249>.

⁷⁹ Gill et al., "Terrorist Use of the Internet by the Numbers," 107.

employed the Internet to learn about their intended terrorist activities.⁸⁰ Importantly, more than a third used the Internet in preparation for their attacks, including watching bomb-making videos, reading poison manuals and assassination guidebooks, downloading plans for the London Underground, Buckingham Palace, and other symbolic landmarks and terrorist training manuals.⁸¹

V. Terrorist Financing

The Internet presents a platform where terrorists can easily obtain financing for acts of terrorism. The United Nation Office on Drugs and Crime has identified four different ways which terrorists use the Internet to obtain financing, to wit; direct solicitation, e-commerce, exploitation of online payment tools, and through charitable organisations.⁸² The Internet's attractiveness arises from the ease in which the platform offers a broad reach, timely efficiency, and a degree of anonymity and security to both the donor and recipient of the funds.⁸³ These considerations particularly become relevant within a context where access to properly regulated banking services is limited and where other alternatives such as mobile payments are prevalent. The situation is further exacerbated by the fact that few countries possess the technical know-how to detect and investigate online terrorist activities which means that this remains an area that will for a long time be attractive to terrorists and terrorist organisations.⁸⁴ To this end, it becomes challenging to assess the scale and impact of terrorist financing through the Internet, especially where encryption tools are deployed by the individuals.⁸⁵ Such complexities have heightened calls to

⁸⁰ Gill et al., "Terrorist Use of the Internet by the Numbers," 107.

⁸¹ Gill et al., "Terrorist Use of the Internet by the Numbers," 107.

⁸² United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes* (UNODC, 2012), 7, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

⁸³ Michael Jacobson, "Terrorist Financing on the Internet," *CTC Sentinel* 2, no. 6 (2009): 17-20.

⁸⁴ Jacobson, "Terrorist Financing on the Internet," 19.

⁸⁵ Tom Keatinge and Florence Keen, *Social Media and Terrorist Financing: What are the Vulnerabilities and how Could Public and Private Sectors Collaborate*

ensure collaboration amongst States and various stakeholders to collectively develop interventions for the threats occasioned from the use of the Internet for terrorist financing.⁸⁶ Efforts should particularly be driven towards expanding the capacities of low-income countries to be able to detect and investigate the use of the Internet for terrorist activities. Similarly. Efforts should be directed at strengthening the financial systems within these countries to ensure that financial transactions are monitored and regulated to prevent abuse of cash transfer platforms by terrorists and terrorist organisations. In Kenya for instance, the State vide The Kenya Information and Communications (Registration of SIM-CARDS) Regulations, 2015 has placed stringent regulations requiring proper records to be kept by telecommunication operators or their agents to keep in place a record of all the registered subscribers made by the telecommunications operator and to submit these records to the Communication Authority on a quarterly basis.⁸⁷ Such regulations essentially ensure that the regulatory agencies keep a record of all the users of communication devices utilising SIM cards and can enable the authorities monitor suspicious activities. Privacy and illegal surveillance concerns however cannot be overlooked whenever such interventions are deployed.

VI. Conclusion

The Internet has enormous importance for terrorists because it enables them to be independent from mainstream media, increase the size of their audience and benefit from the use of digitalised information, which is almost impossible to be blocked and removed from circulation. It also allows terrorist groups to shift their focus for radicalising people from public areas to online platforms such as websites, chatrooms and forums. In addition to radicalisation purposes, the Internet is also used by terrorist groups for the

Better? (Royal United Services Institute for Defence and Security Studies, 2019), 6, https://rusi.org/sites/default/files/20190802_grmtt_paper_10.pdf.

⁸⁶ Keatinge and Keen, *Social Media and Terrorist Financing*, 2.

⁸⁷ The Kenya Information and Communications (Registration of SIM-CARDS) Regulations, 2015. Section 3.

purposes of consolidating their sympathisers and inciting 'lone wolves' to carry out terrorist attacks. Importantly, it enables terrorist groups to access and potentially recruit those living in different countries where were not closed to them prior to the existence of the Internet. The Internet is seen as a library or even an 'online terrorism university' for terrorists to acquire knowledge and information. It is a source for planning and coordinating a terrorist attack. Although it includes a great deal of misleading or wrong information, there is empirical evidence that shows that even amateur attackers were able to successfully carry out attacks thanks to online training. This paper concludes that the Internet is a vital tool for today's terrorist organisations, especially in terms of disseminating their propagan-da, radicalising people, recruiting new supporters, providing online training materials for their followers and planning and preparing terrorist attacks and terrorist financing.

Bibliography

- Aly, Anne, Stuart Macdonald, Lee Jarvis, and Thomas M. Chen. "Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization." *Studies in Conflict & Terrorism* 40, no. 1 (2017): 1–9. <https://doi.org/10.1080/1057610X.2016.1157402>.
- Awan, Akil N. "The Virtual Jihad: An Increasingly Legitimate Form of Warfare." *CTC Sentinel* 3, no. 5 (2010): 10-13.
- BBC News. "Islamic terrorist propaganda student Mohammed Gul jailed." Accessed March 25, 2019. <http://www.bbc.co.uk/news/uk-england-london-12576973>.
- BBC News. "Texas Walmart Shooting: El Paso Attack 'Domestic Terrorism'." Accessed September 12, 2019. <https://www.bbc.co.uk/news/world-us-canada-49226573>.
- BBC News. "What is 8chan?." Accessed October 01, 2019. <https://www.bbc.co.uk/news/blogs-trending-49233767>.
- Benson, David C. "Why the Internet Is Not Increasing Terrorism." *Security Studies* 23, no. 2, (2014):293–328.
- Conway, Maura and Joseph Dillon. "Future Trends: Live-Streaming Terrorist Attacks?." VOX-Pol. Accessed October 8, 2019. https://www.voxpol.eu/download/vox-pol_publication/Live-streaming_FINAL.pdf.
- Conway, Maura. "Terrorism and the Internet: New Media - New Threat?." *Parliamentary Affairs* 59, no. 2 (2006): 283–298.
- Cowan, Jill. "What to Know About the Poway Synagogue Shooting." The New York Times. Accessed September 12, 2019. <https://www.nytimes.com/2019/04/29/us/synagogue-shooting.html>.
- Cox, Kate, William Marcellino, Jacopo Bellasio, Antonia Ward, Katerina Galai, Sofia Meranto, and Giacomo Persi Paoli. *Social Media in Africa: A Double-edged Sword for Security and Development*. UNDP, 2018. https://www.undp.org/content/dam/rba/docs/Reports/UNDP-RAND-Social-Media-Africa-Research-Report_final_3%20Oct.pdf.

- Davis, Benjamin R. "Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance." *CommLaw Conspectus* 15, no. 1 (2006): 119-135.
- Denning, Dorothy E. "Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services US House of Representatives." May 23, 2000. <https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm>.
- Dutton, William H., Grant Blank, and Darja Groselj. "Cultures of the Internet: The Internet in Britain, Oxford Internet Survey 2013 Report." Oxford Internet Surveys. Accessed September 24, 2019. <http://oxis.oii.ox.ac.uk/wp-content/uploads/2014/11/OxIS-2013.pdf>.
- Edwards, Charlie and Luke Gribbon. "Pathways to Violent Extremism in the Digital Era." *The RUSI Journal* 158, no. 5 (2013): 40-47.
- Evans, Robert. "Ignore The Poway Synagogue Shooter's Manifesto: Pay Attention To 8chan's /pol/ Board." Bellingcat. Accessed October 01, 2019. <https://www.bellingcat.com/news/americas/2019/04/28/ignore-the-poway-synagogue-shooters-manifesto-pay-attention-to-8chans-pol-board/>.
- Fisher-Birch, Joshua. "Users of 8chan's /Pol Board Move to Other Websites." Counter Extremism Project. Accessed September 10, 2019. <https://www.counterextremism.com/blog/users-8chan%E2%80%99s-pol-board-move-other-websites>.
- Frieburger, Tina and Jeffrey S. Crane. "A Systematic Explanation of Terrorist Use of the Internet." *International Journal of Cyber Criminology* 2, no. 1 (2008): 309-319.
- Gill Paul, Emily Corner, Maura Conway, Amy Thornton, Mia Bloom, and John Horgan. "Terrorist Use of the Internet by the Numbers: Quantifying Behaviors, Patterns, and Processes." *Criminology & Public Policy* 16, no. 1 (2017): 99-117. <https://doi.org/10.1111/1745-9133.12249>.
- Gilsinan, Kathy. "How White-Supremacist Violence Echoes Other Forms of Terrorism." The Atlantic. Accessed October 1, 2019. <https://www.theatlantic.com/international/archive/2019/03/violence-new-zealand-echoes-past-terrorist-patterns/585043/>.

- Holbrook, Donald. "A Critical Analysis of the Role of the Internet in the Preparation and Planning of Acts of Terrorism." *Dynamics of Asymmetric Conflict* 8, no. 2 (2015): 121–133.
- Holt, Tom, Joshua D. Freilich, Steven Chermak, and Clark McCauley. "Political Radicalization on the Internet: Extremist Content, Government Control, and the Power of Victim and Jihad Videos." *Dynamics of Asymmetric Conflict* 8, no. 2 (2015): 107–120.
- Hurriyet Daily News. "AKP Warns on PKK Activities on Internet." Accessed September 14, 2019. <http://www.hurriyetdailynews.com/akp-warns-on-pkk-activities-on-internet-37572>.
- Jacobson, Michael. "Terrorist Financing on the Internet." *CTC Sentinel* 2, no. 6 (2009): 17-20.
- Janbek, Dana and Valerie Williams. "The Role of the Internet Post-9/11 in Terrorism and Counterterrorism." *Brown Journal of World Affairs* 20, no. 2 (2014): 297–309.
- Jarvis, Lee and Stuart Macdonald. "What Is Cyberterrorism? Findings from a Survey of Researchers." *Terrorism and Political Violence* 27, no. 4, (2015): 657-678. <https://doi.org/10.1080/09546553.2013.847827>.
- Jarvis, Lee, Stuart Macdonald, and Andrew Whiting. "Unpacking Cyberterrorism Discourse: Specificity, Status, and Scale in News Media Constructions of Threat." *European Journal of International Security* 2, no. 1 (2017): 64-87. <https://doi.org/10.1017/eis.2016.14>.
- Keatinge, Tom and Florence Keen. *Social Media and Terrorist Financing: What are the Vulnerabilities and how Could Public and Private Sectors Collaborate Better?*. Royal United Services Institute for Defence and Security Studies, 2019. https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf.
- Keene Shima D. "Terrorism and the Internet: A Double-edged Sword." *Journal of Money Laundering Control* 14, no. 4 (2011): 359–370.
- Kenney, Michael. "Beyond the Internet: Mētis, Techne, and the Limitations of Online Artifacts for Islamist Terrorists." *Terrorism and Political Violence* 22, no. 2 (2010): 177–197.

- Klausen, Jytte. "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq." *Studies in Conflict & Terrorism* 38, no. 1 (2015): 1-22.
- Macdonald, Stuart and David Mair. "Terrorism Online: A New Strategic Environment." in *Terrorism Online: Politics, Law and Technology*, edited by Lee Jarvis, Stuart MacDonald, and Thomas M. Chen, 10-34. Abingdon: Routledge, 2015.
- Mair, David. "#Westgate: A Case Study: How al-Shabaab used Twitter during an Ongoing Attack." *Studies in Conflict & Terrorism* 40, no. 1 (2017): 24-43. <https://doi.org/10.1080/1057610X.2016.1157404>.
- Netherlands: General Intelligence and Security Service (AIVD). *Jihadism on the Web: A Breeding Ground for Jihad in the Modern Age*. The Hague, 2012.
- Pantucci, Raffaello. "A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists." *Developments in Radicalisation and Political Violence, International Centre for the Study of Radicalisation and Political Violence (ICSR)* (2011): 1-39.
- Peterson, Jillian and James Densley. "Op-Ed: We have Studied every Mass Shooting since 1966. Here's what we've Learned about the Shooters." Los Angeles Times. Accessed September 22, 2019. <https://www.latimes.com/opinion/story/2019-08-04/el-paso-dayton-gilroy-mass-shooters-data>.
- Ramsay, Gilbert. "Relocating the Virtual War." *Defence against Terrorism Review* 2, no. 1 (2009): 31-50.
- Rudner, Martin. "'Electronic Jihad': The Internet as Al-Qaeda's Catalyst for Global Terror." *Studies in Conflict & Terrorism* 40, no. 1 (2017): 10-23.
- Sageman, Marc. *Leaderless Jihad: Terror Networks in the Twenty-First Century*. Philadelphia: University of Pennsylvania Press, 2008.
- Saymaz, İsmail. "ByLock use is an evidence of Gülen network links: Owner." Hurriyet Daily News. Accessed September 3, 2019. <http://www.hurriyetdailynews.com/bylock-use-is-an-evidence-of-gulen-network-links-owner-105284>.

- Siegel, Rachel. "8chan Is Back Online, This Time as 8kun." The Washington Post. Accessed November 18, 2019. <https://www.washingtonpost.com/technology/2019/11/04/chan-is-back-online-this-time-kun/>.
- Spaaaj, Ramón. "The Enigma of Lone Wolf Terrorism: An Assessment." *Studies in Conflict & Terrorism* 33, no. 9 (2010): 854–870.
- Stanley-Becker, Isaac, Eli Rosenberg, Alex Horton, and Michael Brice-Saddler. "Primary Suspect, One Alleged Accomplice Identified in Terrorist Attack That Killed 49 in New Zealand." The Washington Post. Accessed May 10, 2019. <https://www.washingtonpost.com/nation/2019/03/15/shootings-reported-mosques-christchurch-new-zealand/>.
- Statista. "Number of social Media users worldwide from 2010 to 2021 (in billions)." Accessed March 20, 2019. <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users>.
- Stenersen, Anne. "The Internet: A Virtual Training Camp?." *Terrorism and Political Violence* 20, no. 2 (2008): 215–233.
- The Telegraph. "Al-Qaeda urges followers to bomb the Savoy." Accessed September 29, 2019. <http://www.telegraph.co.uk/news/worldnews/al-qaeda/10704708/Al-Qaeda-urges-followers-to-bomb-the-Savoy.html>.
- The Telegraph. "Terrorists use Google maps to hit UK troops." Accessed September 15, 2019. <http://www.telegraph.co.uk/news/worldnews/1539401/Terrorists-use-Google-maps-to-hit-UK-troops.html>.
- The United States Department of Justice: Office of Public Affairs. "Charges Unsealed Against Five Alleged Members of Al-Qaeda Plot to Attack the United States and United Kingdom." The United States Department of Justice. Accessed September 28, 2019. <https://www.justice.gov/opa/pr/charges-unsealed-against-five-alleged-members-al-qaeda-plot-attack-united-states-and-united>.
- The World Bank. "Individuals using the Internet (% of population)." Accessed September 20, 2019. <https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2017&start=1960&view=chart>.

- United Nations Office on Drugs and Crime. *The Use of the Internet for Terrorist Purposes*. UNODC, 2012. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.
- Vidino, Lorenzo. "The Evolution of Jihadism in Italy: Rise in Homegrown Radicals." *CTC Sentinel* 6, no. 11 (2013): 17-20.
- Weimann, Gabriel. "www.terror.net - How Modern Terrorism Uses the Internet." *USIP Special Report*, no. 116 (2004): 1-12.
- Weimann, Gabriel. "Lone Wolves in Cyberspace." *Journal of Terrorism Research* 3, no. 2 (2012): 75-90.
- Weimann, Gabriel. *Terror on the Internet: The New Arena, the New Challenges*. Washington, D.C.: United States Institute of Peace, 2006.
- Wong, Julia Carrie. "8chan: the far-right website linked to the rise in hate crimes." *The Guardian*. Accessed October 01, 2019. <https://www.theguardian.com/technology/2019/aug/04/mass-shootings-el-paso-texas-dayton-ohio-8chan-far-right-website>.