Utrecht University

# Updating terrorism

## The changing uses of the internet by terrorists in the West

Matthijs Kock | 5996198

Master thesis in International Relations in Historical Perspective
Supervised by Prof. dr. Beatrice de Graaf & dr. Frank Gerits
Utrecht University | 15 August 2020

“The fact that we’re all connected, the fact that we’ve got this information space, does change the parameters. It changes the way people live and work. It changes things for good and for bad.”[1]

- Tim Berners-Lee, inventor of the World Wide Web

[1] Scott Laningham, ‘Tim Berners-Lee. Originator of the Web and director of the World Wide Web Consortium talks about where we’ve come, and about the challenges and opportunities ahead’, *IBM Developed,* August 22, 2006, https://www.ibm.com/developerworks/podcast/dwi/cm-int082206txt.html (accessed May 14, 2020).

# Abstract

This thesis analyses how the technological development of the internet has changed the use of the internet by terrorists in the West between 2003 and 2009. The role of the internet for terrorism is often, but incorrectly, perceived as a static one without progress. This thesis however emphasises the historical development of the internet by analysing how the internet was used by terrorists in three technological phases of the web. Each Web phase is studied using a detailed qualitative approach in which the online activities of individual members of a terrorist network are examined. The networks selected for this analysis are the Dutch Hofstad Network, the Islamic State in Iraq and Syria (ISIS) and the fluid network of far-right terrorists. The careful choice for each of these networks is based on their active use of the respective technological phase of the internet. The analysis shows that on the one hand, shifts in the type of content and used platforms can be distinguished over the years. Additionally, an increase in the sophistication of online activities of terrorists and the importance of online communities can be seen. On the other hand, the online activities were merely an expansion to the offline activities of terrorists, as they could not replace the physical violence that is essential to terrorism. This online expansion did however further increase the (potential) audience of terrorists and decrease the importance of ideology.

**Keywords** *Online terrorism, History of Internet, Hofstad Network, ISIS, Far-Right terrorism, counterterrorism*

# Acknowledgements

I would like to express my great appreciation to my supervisors, Prof. dr. Beatrice de Graaf and dr. Frank Gerits. The advice, insights, and support from a renowned researcher in the field of terrorism studies like Beatrice de Graaf, has greatly enhanced the quality of my thesis. Dr. Frank Gerits helped me to improve the overall structure of this research and kept me focussed on answering the main research question.

I would also like to thank Esther Heldenbergh-Bode, personal assistant to Beatrice de Graaf, for managing my progress, and organising my meetings with Beatrice, which was not an easy feat due to the current coronavirus pandemic.

Additionally, I want to thank my fellow students of the thesis seminar, Jordy van Beek, Dawid Fusiek, Alex Hampton, Connie Meza and Jannes Pittermann. We all shared the struggles of writing a master thesis and they kept me motivated while also providing me with new insights and perspectives.

And finally, I am grateful for the advice, support and encouragements of my parents and friends throughout the process of writing this master thesis.

# Table of contents

**List of abbreviations** ........ 1

1.1 Introduction to the topic ........ 2

1.2 Research question ........ 3

1.3 Theoretical justification ........ 6

1.4 Methodological framework ........ 10

**The Hofstad Network's exploration of the internet** ........ 14

2.1 The internet at the start of the century ........ 14

2.2 The Hofstad Network ........ 14

2.3 The internet of the Hofstad Network ........ 16

2.3.1 Propaganda ........ 16

2.3.2 Finance ........ 18

2.3.3 Training ........ 19

2.3.4 Planning ........ 20

2.3.5 Execution ........ 23

2.3.6 Cyberattacks ........ 24

2.4 Looking in the wrong direction ........ 24

2.5 Conclusion ........ 25

**The online ubiquity of ISIS** ........ 27

3.1 The user-based internet ........ 27

3.2 Creating an Islamic caliphate ........ 28

3.3 ISIS electronic jihad ........ 30

3.3.1 Propaganda ........ 30

3.3.2 Finance ........ 33

3.2.3 Training ........ 35

3.3.4 Planning ........ 36

3.3.5 Execution ........ 37

3.3.6 Cyberattacks ........ 39

3.4 Notice and take down ........ 41

3.5 Conclusion ........ 42

**Lone actor terrorism and the Web 3.0** ........ 44

4.1 The ever-expanding internet ........ 44

4.2 Right-wing terrorism ........ 45

4.3 An online community ........ 47

4.3.1 Propaganda ........ 47

4.3.2 Finance ........ 50

4.3.3 Training ........ 51
4.3.4 Planning ........ 52
4.3.5 Execution ........ 54
4.3.6 Cyberattacks ........ 57
4.4 Automated counterterrorism ........ 58
4.5 Conclusion ........ 60
**Transitions and trends in the online activities of terrorists.** ........ 61
Transitions ........ 61
5.1 The visualisation of terrorist content ........ 61
5.2 Choosing the audience ........ 62
5.3 From amateurs to professionals ........ 63
5.4 Offline versus online communities ........ 64
Trends ........ 65
5.5 The role of the internet for terrorism ........ 65
5.6 Offering an expanded audience ........ 66
**Conclusion** ........ 68
General conclusion ........ 68
The relevance of this thesis ........ 71
Recommendations for further research ........ 71
**Bibliography** ........ 73
Primary sources ........ 73
Academic sources ........ 74
Online sources ........ 78

# List of abbreviations

| | |
|---|---|
| AQI | al-Qaeda in Iraq |
| AI | Artificial Intelligence |
| FPS | First-person shooter |
| ISI | Islamic State in Iraq |
| ISIS | Islamic State in Iraq and Syria |
| US | United States (of America) |
| UUC | United Cyber Caliphate |
| UNODC | United Nations Office on Drugs and Crime |
| WWW | World Wide Web**Introduction** |

## 1.1 Introduction to the topic

By downloading the free Telegram app, everybody can communicate with others via highly secure encryption. This safety feature has made the app extremely popular with terrorists, who could communicate without worrying about counter-terrorism agencies secretly reading along. The terrorist affection for Telegram changed in November 2019 when the company behind the app, in cooperation with Europol, removed the accounts belonging to terrorists. Within a day, terrorists had lost one of their primary means of communications. However, academic researchers witnessed the quick transition of these terrorists to other, similarly encrypted apps, such as TamTam, Nandbox, Surespot and Hoop Messenger. According to one of these researchers, Pieter van Ostaeyen, the operation from Telegram and Europol resulted in the fragmentation of terrorist communication platforms, with terrorists now using at least ten different applications on which intelligence services do not yet have a hold.[2] This quick transition shows that terrorists are often early adopters of new technologies and how well the internet is integrated into terrorism (and vice versa).

Because terrorists constantly adopt new technologies, their online activities have changed over time. Whereas the phenomenon of modern terrorism dates to 1878,[3] terrorists first came into content with the internet once became publicly available in the 1990s[4] and gained mass popularity after 2000.[5] Starting as a collection of relatively simple webpages, the World Wide Web quickly evolved and expanded with new features, including images, videos and social media platforms, and continues to do so every day. Terrorists have adopted these new features of the internet into their acts, with examples such as the digital publication of the magazine *Inspire* by al-Qaeda in the Arabian Peninsula in the mid-2010s,[6] and the livestreaming of the Christchurch Mosque attacks in New Zealand in 2019, which was viewed approximately four thousand times before it was removed from Facebook[7]. However, the

[2] *Europol*, 'Europol and Telegram take on terrorist propaganda online', November 25, 2019, https://www.europol.europa.eu/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online (accessed April 7, 2020).

[3] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 2017) 5-6.

[4] Barry Leiner et al., *Brief History of the Internet* (n.d.: Internet Society, 1997) 16.

[5] Max Roser, Hannah Ritchie, and Estaban Ortiz-Ospina, 'Internet', *OurWorldInData*, 2020, https://ourworldindata.org/internet#the-internet-s-history-has-just-begun (accessed April 14, 2020).

[6] Haroro J. Ingram, 'An Analysis of *Inspire* and *Dabiq*: Lessons from AQAP and Islamic State's Propaganda War', *Studies in Conflict & Terrorism* 40 (2017) 5: 357-375, here: 358.

[7] Graham Macklin, 'The Christchurch Attacks: Livestream Terror in the Viral Video Age', *CTC Sentinel* 13 (2019) 6: 18-29, here: 20.

option of publicly livestreaming an act of terrorism was not available until the 2010s.[8] Instead, the first generation of online active terrorists could only rely on webpages and e-mail-based communication. The constant addition of new features to the internet implies that the terrorist use of the internet is subjected to the technological advancement of the internet at a certain time. Therefore, terrorists from different periods in time dealt with different versions of the internet. These variations raise the question of how the technological development of the internet has changed the use of the internet by terrorists over the years.

## 1.2 Research question

The purpose of this master thesis is to explicate the way in which the technological development of the internet has impacted the use of the internet by terrorists. As the historiography below will show, multiple studies into the role of the internet have already been undertaken. In these studies, the internet is often perceived as static and has therefore not changed over time. This is incorrect, as the internet is constantly changing and so are the ways in which terrorists use the internet. This thesis, therefore, focusses on this dynamic and fluid nature of the internet and analyses how the technological development of the internet has changed the use of the internet by terrorists in the West between 2003 and 2019.

To analyse the technological development of the internet, this research uses three different phases of the World Wide Web as distinguished by other researchers, which are referred to as Web 1.0, Web 2.0 and Web 3.0. Each of these stages has an approximate duration of ten years, with the Web 1.0 starting in 1996.[9] We are currently around halfway through the timespan of the Web 3.0, but scholars have already started discussing the Web 4.0 would.[10] Each phase has distinct technological advancements compared to the previous versions, which changed how the internet was used by everybody, including terrorists.[11] The

[8] Video website YouTube was one of the first to offer livestreaming services to its users in 2010, having experimented with the feature in 2009, see: Dough Gross, 'YouTube testing live streaming', *CNN*, September 13, 2010, http://edition.cnn.com/2010/TECH/web/09/13/youtube.livestreaming/index.html (accessed April 7, 2020).

[9] Umesha Naik and D. Shivalingaiah, 'Comparative Study of Web 1.0, Web 2.0 and Web 3.0', paper presented at the *6th International CALIBER Conference* (Odisha, March 2009).

[10] Nupur Choudhury, 'World Wide Web and Its Journey from Web 1.0 to Web 4.0', *International Journal of Computer Science and Information Technologies* 5 (2014) 6: 8096-8100, here: 8099-8100.

[11] Johnny Ryan, *A History of the Internet and the Digital Future* (London: Reaktion Books, 2010) 137-150.

impact of each Web phase on society and its corresponding features will be discussed at the beginning of each chapter.

To answer the main research question of this master thesis, each chapter focusses on a specific terrorist organisation or group[12] whose existence corresponds with a specific Web phase of the Internet. To fully analyse the impact of a certain Web phase on terrorism, prominent terrorist groups from the end of each Web phase have been chosen. In doing this, the full extent of a Web phase's impact on terrorism can be analysed, due to the incorporation of developments within a phase. By analysing and comparing the online activities of terrorists in each Web phase, the technological development of the internet is emphasised and an answer to the main research question can be formulated.

The first chapter examines how the Web 1.0 was used by the members of the Dutch Jihadist Hofstad Network, which was active between 2003 and 2005.[13] In contrast to groups that had already been founded before the public availability of the internet, such as al-Qaeda[14], the members of the Hofstad Network all came into contact with the internet before their group was formed. Focussing on the members of the Hofstad Network and their use of the Web 1.0 therefore enables this research to also examine the radicalising impact of the Web 1.0 phase of the internet.

The second chapter focusses on the Web 2.0 phase of the internet. When in 2006 the World Wide Web transitioned to the Web 2.0, internet consumers became internet users. New features that allowed user interactions were created, such as sharing videos on YouTube and posting multimedia messages on Twitter and Facebook. This was however not only used by innocent individuals, as terrorists of The Islamic State in Iraq and Syria (ISIS) effectively used these Web 2.0 features for terrorist purposes. ISIS became one of the biggest terrorist

[12] The structural organisation of terrorists is debated, with some scholars referring to organisations, while others argue for the use of *networks* or *groups*. See for example: Martha Crenshaw, *Explaining terrorism: causes, processes and consequences* (New York/ Abingdon: Routledge, 2011) 69; Marc Sageman, *Leaderless jihad: terror networks in the twenty-first century* (Philadelphia: University of Pennsylvania Press, 2008) 140-143; Gina Scott Ligon et al., 'Putting the 'O' in VEOs: What makes an organization?', *Dynamics of Asymmetric Conflict* 6 (2013) 1-3: 110-134, here: 120.

[13] Bart Schuurman, *Becoming a European homegrown jihadist: A multilevel analysis of involvement in the Dutch Hofstadgroup, 2002-2005* (Amsterdam: Amsterdam University Press, 2018) 11-13.

[14] When al-Qaeda was founded in 1988, only 32,400 computers worldwide were connected to the internet. Its explosive grow started around 1995, with an increase of three million new computers in only 10 months. Ryan, *A History of the Internet*, 115; Rohan Gunarata, *Inside Al Qaeda* (New York: Columbia University Press, 2002) 3-4.

threats to the West after the fall of al-Qaeda.[15] Centred around Syria and Iraq the organisation exclaimed its own Islamic caliphate in 2014 which attracted Muslims from all over the world, including the West. Supporters of ISIS were also called upon to commit terrorist attacks in Europe and the United States, in which some of them succeeded and of which the Paris and Brussels attacks of 2015 and 2016 were the most prominent. In the second chapter, the online activities of ISIS terrorists in the West in the Web 2.0 phase of the internet will be analysed.

The third and final chapter examines the most recent developments of the internet and its uses by terrorists. The introduction of the Web 3.0 in 2016 focussed on improving the underlying computer processes of the internet and the immersion of users and services.[16] During this phase of the internet, anonymous imageboard websites such as 4chan, 8chan and Reddit which have become infamous for the presence of openly racist and radical ideas, gained prominence. Imageboards are especially popular with far-right lone actor terrorists, whose extremist worldviews are often censored on other websites.[17] This last chapter will, therefore, focus on the use of the internet by these far-right terrorists in the most recent technological phase of the internet.

Whereas both the internet and terrorism have a global nature, [18] this research focusses on the online activities of terrorists in the West, and in particular in the Netherlands, France the United States and New Zealand. Multiple definitions for the "Western world" exist, but within this thesis the "West" refers to the Western civilisation as defined by Samuel Huntington and includes Western and Central-Europe, the United States, Canada, Australia and New Zealand.[19] Terrorists from all three of the selected case studies were active in the West, but despite this geographical demarcation, analysed information might have a link to other regions. This can however not be prevented because of the global natures of both terrorism and the internet. But in instances where a geographical specification is possible, this will be done accordingly.

[15] Thomas Hegghammer and Petter Nesser, 'Assessing the Islamic State's Commitment to Attacking the West', *Perspectives on Terrorism* 9 (2015) 4: 14-30, here: 27.

[16] Naik and Shivalingaiah, 'Comparative Study of Web 1.0, Web 2.0 and Web 3.0', 503.

[17] Elizabeth T. Harwood, 'Terrorism and the Digital Right-Wing', *Contexts* 18 (2019) 3: 60-62, here: 60-61.

[18] David Rapoport, 'The Four Waves of Modern Terrorism', in Audrey Kurth Cronin and James M. Ludes (eds.), *Attacking Terrorism. Elements of a Grand Strategy* (Washington, D.C.: Georgetown University Press, 2004) 46-73, here: 47.

[19] Samuel P. Huntington, 'The Clash of Civilizations?', *Foreign Affairs* 72 (1993): 22-49, here: 24.

This demarcation in time and space allows for the analysis of the impact of the technological development of the internet on the use of the internet by terrorists in the West. The conclusions of these chapters provide insight into the overarching main research question.

It is likely that the analysis of the internet activities of terrorists in the three different internet phases, will show an expansion of the online features that are used by terrorists over the years. Public use of online data has kept increasing over the years[20] and research by Van Deursen, Van Dijk, and Ten Klooster already indicated an increase in the time spent on the internet between 2010 and 2013.[21] It is expected that this trend will continue. Additionally, a change in the nature of services and platforms used by terrorists is expected, as the platforms of the Web 1.0 did not offer opportunities for interactions like current-day social media platforms do.

### 1.3 Theoretical justification

Terrorism is not a new phenomenon. But while terrorism has been present throughout history, the nature of the phenomenon changed over the course of history. David Rapoport defined a clear difference between terrorism before and after the 1880s. According to him, terrorism became better organised and terrorist attacks with similar tactics and from comparable motives were committed internationally. This started in the 1880s with the introduction of the telegraph, mass newspapers and trains, introducing a transformation in communication and transportation methods.[22] The emergence of the internet could similarly pose a new phase in the history of terrorism with the introduction of even newer communication technologies.

The presence of an audience is essential for labelling an act of violence as terrorism. Without an audience, an act of violence has no social meaning and cannot be used to instil

[20] *Cisco*, 'VNI Mobile Forecast Highlights Tool', n.d., https://www.cisco.com/c/m/en_us/solutions/service-provider/forecast-highlights-mobile.html (accessed April 8,2020).

[21] Alexander van Deursen, Jan van Dijk, and Peter ten Klooster, 'Increasing inequalities in what we do online: A longitudinal cross section analysis of Internet activities among the Dutch population (2010 to 2013) over gender, age, education, and income', *Telematics and Informatics* 32 (2015): 259-272, here: 263.

[22] Rapoport, 'The Four Waves of Modern Terrorism', 48-49.

fear.[23] Creating fear among (a part of) society is one of the key elements of terrorism.[24] In the words of terrorism expert Brian Jenkins: "Terrorists want a lot of people watching, not a lot of people dead."[25] Whereas the Zealots and Assassins from centuries ago already used terrorist tactics to impact an audience beyond the immediate victims of their attacks,[26] the invention of the steam-powered printing press in the nineteenth century greatly expanded the potential audience for terrorism. Featured in mass-produced newspapers, information on acts of terrorism was distributed quicker than ever before. Newspaper coverage on terrorism has proven to be successful in reporting on the grievances and causes of terrorists, but this medium was only of limited use for gaining respectability and legitimacy.[27] The introduction of broadcast media such as the radio and television changed this. When the first American television satellite was launched in 1968, news media was revolutionised. News broadcast quickly became popular and within ten years television had become the primary source of news information for 67 per cent of Americans.[28] News channels competed with each other to deliver new information first, creating a culture where "scoops" were more important than providing context. This was exploited by terrorists who got offered a podium that had previously been inaccessible to them but could be used to gain respect and legitimacy. The terrorists' need for an audience combined with the news media's lust for new events resulted in the creation of a symbiotic relationship between terrorism and the media and greatly increased the potential audience for terrorists.

But according to Walter Laqueur, the biggest change in communication methods for terrorists was the introduction of the internet. In his book *The New Terrorism: Fanaticism and the Arms of Mass Destruction* Laqueur argues that the nature of terrorism has changed in the 1990s and became more complex, global and destructive.[29] This is supported by Faisal Devji, who states that: "This jihad is global not because it controls people, places and circumstances over vast distances […], but precisely the opposite reason: because it is too weak to participate

[23] Bettina Schmidt and Ingo Schroeder, 'Violent imaginaries and violent practices', in Bettina Schmidt and Ingo Schroeder (eds.), *Anthropology of Violence and Conflict* (London: Routledge, 2001) 1-24, here: 5-6.

[24] Charles Tilly, 'Terror, Terrorism, Terrorists', *Sociological Theory* 22 (2004) 1: 5-13, here: 9.

[25] Brian Jenkins, *Will Terrorists Go Nuclear?* (Santa Monica, CA: RAND Corporation, 1975) 5.

[26] Hoffman, *Inside Terrorism*, 186.

[27] Brigitte Nacos, David Fan, and John Young, 'Terrorism and the Print Media: The 1985 TWA Hostage Crisis', *Terrorism* 12 (1989) 2: 107-115.

[28] Hoffman, *Inside Terrorism*, 187; 191.

[29] Walter Laqueur, *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (Oxford: Oxford University Press, 1999).

in such a politics of control."[30] Proponents of this 'New Terrorism' theory have pointed at the internet as an amplifying factor for this change.[31] And while this New Terrorism theory is heavily contested by academics in the field of terrorism studies,[32] most scholars agree that the internet has influenced the new nature of terrorism.

However, the relation between the internet and terrorism is often, possibly unintentional, seen as a static one, in the sense that the internet is circumscribed as an autonomous factor with specific characteristics that do not seem to change over time. James A. Lewis, for example, uses examples from different periods to substantiate his argument that the internet is a tool used by terrorists across the world.[33] Similarly, Maura Conway, who has written multiple articles on terrorism and the internet, wrote about ""old" [terrorists] groups with very lengthy and active online presences" without distinguishing the gradual technological development of the internet.[34] However, the internet is constantly expanded and new features and possibilities for its users are added. This master thesis analyses the role of the internet for terrorism from a historic point of view, to incorporate this development of the internet into the scholarly understanding of terrorism. By emphasising this development, this research will furthermore show that the relation between the internet and terrorism has been a dynamic one because the internet itself is an effervescent and ever-changing, highly adaptable technology.

Additionally, this master thesis leans on different concepts from the actor-network theory. In the 1960s, Canadian philosopher and social scientist McLuhan noted changes in the traditional (offline) society. Technical developments became encompassed in all fields of human affairs, resulting in the creation of a "global" village. In his view, people were no longer limited to exposure to one single culture, language, or technology, but could live in a plurality of worlds and cultures simultaneously. Everybody could inhabit a house in this globally shared

[30] Faisal Devji, *Landscapes of the Jihad* (Ithaca, NY: Cornell University Press, 2005) 1.

[31] Thomas R. Mockaitis, *The "new" terrorism: myths and reality* (Westport, Connecticut/ London: Praeger Security International, 2007) xii.

[32] See for example: Martha Crenshaw, 'The Debate over "New" vs. "Old" Terrorism', paper presented at the *Annual Meeting of the American Political Science Association* (Chicago, August 30 – September 2, 2007); Isabelle Duyvesteyn, 'How New Is the New Terrorism?', *Studies in Conflict & Terrorism* 27 (2004) 5: 439-454.

[33] James A. Lewis, 'The Internet and Terrorism', *American Society of International Law Proceedings* 99 (2005): 112-115.

[34] Maura Conway, 'Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research', *Studies in Conflict & Terrorism* 40 (2017) 1: 77-98, here: 83; Maura Conway, 'Terrorism and the Internet: New Media – New Threat?', *Parliamentary Affairs* 59 (2006) 2: 283-298.

village by using the new technological advancements according to this theory.[35] While his theory had already been coined before the origins of the internet, it became even more relevant due to the new possibilities of the internet. Dutch media sociologist Jan van Dijk went even further when he witnessed the first steps of the internet in 1984. While working on a project for a Dutch bank which had connected multiple workstations via a single computer network, Van Dijk realised that this would eventually be integrated into the entire society.[36] The emergence of new media would lead to the creation of what he called a *Network Society*. According to Van Dijk, "the network society concept emphasizes the form and organization of information processing and exchange. An infrastructure of social and media networks takes care of this."[37] In turn, this would allow all levels of society to access the prime mode of organisation. In three phases individuals would become more connected, leading to the ultimate form of a network society according to Van Dijk. First, he predicted the far-reaching impact of the internet and the rise of social media, which has become a reality. We are currently experiencing the second phase, in which more and more appliances, such as watches, lamps and refrigerators, are connected to the internet. The first steps into a third phase have been made by connecting human bodies to the internet through smart pacemakers for example.[38] Thus, while the Global Village theory of McLuhan focusses on the internet as a type of infrastructure, allowing individuals to access a more extensive world, Van Dijk's concept of a network society is concerned with the underlying relations between individuals and groups as a result of this expanded world and is already better attuned to the post-2001 world than McLuhan's approach was.

More recently, Spanish sociologist Manuel Castells stated that:

> The Internet, as all technologies, does not produce effects by itself. Yet, it has specific effects in altering the capacity of the communication system to be organized around flows that are interactive, multimodal, asynchronous or synchronous, global or local, and from many to many,

[35] Marshall McLuhan, *The Gutenberg Galaxy: The Making of Typographic Man* (Toronto: University of Toronto Press, 2011) 36.

[36] Twente University, 'Hoogleraar pleit voor nieuw sociaal netwerk dat wél let op privacy', *Emerce*, April 4, 2018, https://www.emerce.nl/wire/hoogleraar-pleit-nieuw-sociaal-netwerk-dat-wl-let-privacy (accessed April 6, 2020).

[37] Jan van Dijk, *The Network Society. Social Aspects of New Media* (London/ Thousand Oaks/ New Delhi: SAGE Publications, 2006) 19.

[38] Ibid.

> from people to people, from people to objects, and from objects to objects, increasingly relying on the semantic web.[39]

Here, Castells proposes the idea of an even more immersive internet, that affects humans as well as objects. The connection between the internet and objects is already starting to take shape with the introduction of smart home appliances and self-driving cars. While this is still in an early phase, both Castells' idea and the theories and concepts from McLuhan and Van Dijk are important for understanding the role of the internet because they provide a context to the relations between individual actors, such as terrorists, and computer networks, like the internet. Therefore, the ideas of McLuhan, Van Dijk and Castells are essential for this master thesis. In the conclusion of this research, these theories and concepts are used to reflect on the results of the analysis.

## 1.4 Methodological framework

Analysing the developing role of the internet for terrorist purposes in the twenty-first century is as complicated as it sounds. Because the internet is extremely complicated, with a plethora of features and functions spanning enormous amounts of data, it first needs to be clearly defined. This thesis therefore makes use of the description of the Oxford English Dictionary, which defines the internet as:

> The global network comprising a loose confederation of interconnected networks using standardized communication protocols, which facilitates various information and communication systems such as the World Wide Web and email. Also: the resources accessible via this global network, esp. the World Wide Web.[40]

The various information and communication systems mentioned here are at the centre of this research. The online activities of terrorists throughout the years will be analysed using a detailed qualitative approach, in which the online activities of individual terrorists are analysed. Different uses of the internet for terrorist purposes have been distinguished by

[39] Manuel Castells, 'The impact of the internet on society: a global perspective', in Manuel Castells (ed.), *19 Key Essays on how Internet is Changing Our Lives* (Bilbao: BBVA, 2013) 127-148.

[40] *Oxford English Dictionary*, 'Terrorism, *n*.', n.d., https://www-oed-com.proxy.library.uu.nl/view/Entry/199608?redirectedFrom=terrorism#eid (accessed March 31, 2020).

researchers. In 2006, Maura Conway defined five prominent contemporary uses of the internet by terrorists: information provision, financing, networking, recruitment and information gathering.[41] Despite her expertise, this paper will instead use the means in which the internet is used for terrorist purposes as defined by the United Nations Office on Drugs and Crime (UNODC) as it is more comprehensive and each function is better demarcated. The UNODC has identified a total of six different means by which the internet is utilized for terrorist purposed: 1) *propaganda*, 2) *financing*, 3) *training*, 4) *planning*, 5) *execution*, and 6) *cyberattacks*.[42]

By publishing online content terrorists try to propagate their ideas and to create support for their actions. Additionally, spreading *propaganda* can incite, radicalise, or even recruit others for their cause. Propaganda can take on various forms, such as video or text, but its nature is always contested and based on a certain framing.[43] It can be expected that the ways in which the internet has been used by terrorists for spreading their propaganda have radically changed over the years, to incorporate the addition of new internet features.

Terrorists also use the internet for *financing* their operations. This aspect of terrorists' internet use will analyse how terrorist networks use the internet to raise funds for their cause and for what purposes such financial support is used.

Many Western terrorists visited camps in the Middle East for *training* purposes in the previous century, but due to the internet, this was no longer necessary in the twenty-first century. Online videos and texts could provide terrorists with instructions without having to travel to the Middle East, and information on how to build weapons could be digitally exchanged over as well. These exchanges of tactics and digital training will be examined while focussing on the training aspect of the internet.

The internet is also used by terrorists for *planning* attacks. Online platforms and services have allowed terrorists to (secretly) communicate with others and to discuss plans for a terrorist attack. Additionally, certain internet services enable terrorists to gather information on the location of a terrorist attack, such as street view images and floorplans.

[41] Maura Conway, 'Terrorist 'use 'of the internet and fighting back', *Information & Security. An International Journal* 19 (2006): 9-30.

[42] United Nations Office of Drugs and Crime (hereafter: UNODC), 'The use of the Internet for terrorist purposes', paper in collaboration with the United Nations Counter-Terrorism Implementation Task Force (New York, 2012) 3-12.

[43] Michael V. Bhatia, 'Fighting Words: Naming Terrorists, Bandits, Rebels and Other Violent Actors'. *Third World Quarterly* 26 (2005) 1: 5-22, here: 12.

The fifth function of the internet for terrorist purposes is called *execution* by the UNODC. This entails all internet activities right before a terrorist attack and during the act itself. In the middle of an attack, perpetrators have used the internet to communicate with accomplices or to live stream the event. Additionally, the internet has also been used as the place of the terrorist attack itself, with many countries having criminalised the making of terrorist threats under counterterrorism legislation. Publishing a terroristic threat on the internet can therefore in some cases be seen as an act of terrorism in itself.

The sixth and last function for which the internet is used by terrorists is *cyberattacks*. These are new forms of terrorist attacks with a purely digital nature, targeting computer networks to disrupt a digital infrastructure via hacking, overloading, or corrupting those networks.

This division by the UNODC will be used to analyse the role of the internet in the different periods. Each chapter analyses how the internet is used by terrorists for these six specific functions, which allows for a historical comparison between the different technological phases of the internet.

To execute this detailed qualitative analysis, multiple types of sources were used for this research. Both online publications by terrorists and counterterrorism agencies served as primary sources. Texts by Mohammed Bouyeri and the manifestos of terrorists like Breivik, Tarrant, and Crusius illustrate the online activities of terrorists. The different forms of these online publications and their contents have been analysed in their corresponding web phase. Posts in Arabic could unfortunately not be included in this research due to the language barrier. However, most terrorists in the West relied on online content in either English or their native language. The absence of Arabic sources is therefore not a problem to this thesis, as it focusses on terrorists in the West. To provide an unbiased understanding, sources from counterterrorism agencies have also been taken into account. Especially, the yearly reports from the Dutch AIVD and Directorate-General for External Policies of the European Parliament have proven to be insightful. The analysis of these primary sources is further substantiated by several articles on the online activities of terrorists in different periods. The articles that have been used for this thesis were written by esteemed researchers in the field of terrorism studies and have been published in dedicated peer-reviewed journals such as *Studies in Conflict & Terrorism* and *Terrorism and Political Violence*. Additionally, other publications such as books, doctoral dissertations, and reports, by terrorism experts have been consulted to provide a context.

# The Hofstad Network's exploration of the internet

## 2.1 The internet at the start of the century

After the internet had been introduced to the broad public in the mid-1990s in the form of the World Wide Web, companies worldwide quickly started to invest in internet-related start-ups. The internet was booming, and everybody wanted to profit from it. For the average internet user in 2000, the internet was equal to the World Wide Web (WWW) and email. While the process of sending emails has not changed much over the years, the WWW of 2002 differed greatly from today's internet. Before 2004, the WWW functioned as another one-way broadcasting medium providing information, similar to mass-produced newspapers and television broadcasts. Furthermore, this phase of the internet had limited to no options for interaction between different users of the WWW.[44] Web 1.0 websites were mainly created to establish an online presence and to publish information. A personal experience was therefore lacking, and users could not interact with these websites and other users. As a result, the webpages were often static and updated infrequently.[45] Despite these limited functions for internet users, the Web 1.0 offered new possibilities for early adopters of such new information and communication technologies, such as the terrorists of the Dutch Hofstad Network.

## 2.2 The Hofstad Network

On the morning of November 2, 2004, Dutch filmmaker, director and columnist Theo van Gogh was brutally murdered on the streets of Amsterdam by Mohammed Bouyeri.[46] According to the Dutch General Intelligence and Security Service (Dutch: Algemene Inlichtingen en Veiligheidsdiensten, AIVD), Bouyeri was part of a group of Jihadists radicals, which was dubbed the "Hofstad Network" or "Hofstadgroup" by the agency.[47] Active between 2002 and 2005, this Salafi-Jihadist group was located around The Hague and Amsterdam and

[44] Ryan, *A History of the Internet*, 136.

[45] Sareh Aghaei, Mohammad Ali Nematbakhsh, and Hadi Khrosravi Farsani, 'Evolution of the World Wide Web: From Web 1.0 to Web 4.0', *International Journal of Web & Semantic Technology* 3 (2012) 1: 1-10, here: 2-3.

[46] Beatrice de Graaf, 'The Van Gogh Murder and Beyond', in Bruce Hoffman and Fernando Reinares (eds.), *The Evolution of the Global Terrorist Threat: From 9/11 to Osama bin Laden's Death* (New York: Columbia University Press, 2014) 144-187, here: 103.

[47] J.P.H. Donner and J.W. Remkes, 'Kamerstukken 2, 2004-2005, 29854, nr. 3', (The Hague: Sdu Publishers, 2004) 5.

strove to disturb the Rule of Law in the Netherlands by targeting opponents of Islam, such as Van Gogh and politician Ayaan Hirsi Ali, following the practice of 'takfir'.[48]

Members of the Hofstad Network have been suspected of planning multiple attacks against Dutch politicians and the headquarters of the AIVD. All of these plans were however prevented by the Dutch police, except for the assassination of Van Gogh. Despite the group fitting into a global pattern of radicalised Islamic youths, the Hofstad Network did not maintain close relations with Islamic terrorist groups in other countries.[49]

The terrorist status of the Hofstad Network is however contested, as arrested members have been acquitted of membership of a terrorist organisation.[50] This was however revoked by the Dutch Supreme Court in 2010 on a wrong interpretation by the appeals judge of the Dutch definition of a terrorist organisation.[51] The organisational aspect of terrorist groups is subjected to academic debate as well. According to Martha Crenshaw, terrorist groups are organised along structured lines and should, therefore, be seen as organisations.[52] Marc Sageman, however, argues that jihadist groups are ambiguously defined interconnected networks of individuals without clear hierarchical structures and should therefore not be called organisations.[53] While each group of radicals is different, the Hofstad Network leans more towards Sagerman's network structure according to research by Renée van der Hulst. He concludes that there is no central leadership of the Hofstad Network, but instead makes a distinction between thirteen core members and 54 supporters.[54]

[48] Schuurman, *Becoming a European homegrown jihadist*, 71.

[49] Bart Schuurman, Quirine Eijkman, and Edwin Bakker, 'The Hofstadgroup Revisited: Questioning its Status as a "Quintessential" Homegrown Jihadist Network', *Terrorism and Political Violence* 27 (2015) 5: 906-925, here: 911.

[50] The Hague District Court, 'ECLI:NL:GHSGR:2008:BC2576', January 23, 2008, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHSGR:2008:BC2576 (accessed March 14, 2020).

[51] Dutch Supreme Court, 'ECLI:NL:PHR:2010:BK5193', February 2, 2010, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:PHR:2010:BK5193 (accessed March 14, 2020).

[52] Crenshaw, *Explaining Terrorism*, 69.

[53] Sageman, *Leaderless Jihad*, 140-143.

[54] Renée van der Hulst, 'Terroristische netwerken en *intelligence*: een sociale netwerkanalyse van de Hofstadgroep', *Tijdschrift voor Veiligheid* 8 (2009) 2: 8-27, here: 15-16.

## 2.3 The internet of the Hofstad Network

### 2.3.1 Propaganda

The internet played an important role in the creation of the Hofstad Network. The core members of the group had already been influenced by the internet in their radicalisation process. This is clearest in the case of Samir Azzouz, whose sister stated that his radicalisation process started through television reports and images attached to e-mails.[55] By watching these images and hearing about the situation in the Middle East, his interest was piqued and Azzouz started to delve into these topics on the internet.[56] Other members started radicalising after the events of 9/11 and were driven to the internet in search of answers. To understand how he, as a Muslim, was supposed to feel about these events, Jason Walters studied primary sources on the Islamic religion.[57] Due to the increasing accessibility of the internet and the rapidly expanding amount of available information, Walters was able to access (translated versions of) radical sources from his computer. Via the internet, he delved into different schools of thought within Islamic jurisprudence and fatwas including those of al-Qaeda scholars.[58] Additionally, the AIVD later discovered that publications by Bouyeri contained argumentation that had long circulated online.[59] which is a clear indication that his radicalisation was influenced via the internet.

The online search for answers did not only lead the members of the Hofstad Network to websites with one-way information on Islam, but also to text-based web fora and chat messaging platforms. These services were the first form of user-based interaction on the internet and precursors to the social media platforms of the Web 2.0. On websites such as maroc.nl, members of the Hofstad Network expressed their opinion on the situation of the Muslim communities around the world and discussed the interpretation of Islam, often

[55] *Portret*, 'Samir A.: staatsvijand nr. 1, exclusief interview met Nederlands bekendste terreurverdachte', *KRO*, October 1, 2005, [0:11:45], https://www.vpro.nl/speel~KRO_1233054~samir-a-staatsvijand-nummer-1-reporter~.html (accessed March 24, 2020).

[56] Marion van San and Stijn Sieckelinck, *Idealen op drift. Een pedagogische kijk op radicaliserende jongeren* (Amsterdam: Boom Lemma Uitgevers, 2010) 46.

[57] David Boogerd and Jason Walters, 'Jason Walters, van terrorist to filosoof', August 18, 2019, *De Ongelofelijke Podcast*, produced by the Evangelische Omroep, podcast, [0:14:15], https://www.nporadio1.nl/podcasts-uitgelicht/18165-de-ongelooflijke-podcast-met-ex-terrorist-jason-walters-ik-zei-tegen-de-politie-schiet-maar (accessed March 25, 2020).

[58] Janny Groen, 'Deze man wilde sterven als martelaar, deradicaliseerde en wil nu helpen islamisten te begrijpen', *De Volkskrant*, September 28, 2018, https://www.volkskrant.nl/nieuws-achtergrond/deze-man-wilde-sterven-als-martelaar-deradicaliseerde-en-wil-nu-helpen-islamisten-te-begrijpen~b38864cd/ (accessed June 7, 2020).

[59] Algemene Inlichtingen- en Veiligheidsdienst, *Jaarverslag 2004* (The Hague: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties: 2005) 20.

agreeing with the arguments of extremists.[60] Samir Azzouz even met his wife, Abida K., on such a web forum.[61] Their contact with other Muslims through these internet fora helped to consolidate the idea of an imaginary *ummah*,[62] establishing a connection through a common cause with individuals they would most likely never meet in real life.[63] The idea of this global community via the internet was clearly felt by Azzouz, whose sister stated that he was concerned with the situation of his Muslim “brothers” in Bosnia, Chechnya and Palestine.[64]

The internet was for a short time also used by Walters to find new members for the Hofstad Network. Like-minded people were contacted via web fora and chats, but Azzouz eventually stopped this recruitment as he was unsatisfied with the level of commitment from these recruits.[65] The local nature and centralised core limited the use of the internet for recruitment as well, as the group was looking for recruits closer to home.[66] This secretive character increased even further after five members of the Hofstad Network were arrested and temporarily held in custody in 2003.[67]

Radicalisation and recruitment were however not the only functions of the internet for the Hofstad Network. From their homes, both Walters and Bouyeri used the internet to spread the ideology of the Hofstad Network by writing, translating, editing and publishing inciting texts.[68] Rudolph Peters has studied over fifty publications by Bouyeri (under the pseudonyms ‘Abu Zubair’ or ‘Sayf al-Dîn al-Muwahidd’) and concluded that they showed a chronological process of political radicalisation. He noted a clear shift in Bouyeri’s radicalisation, calling for violent jihad against democracy.[69] This is voiced most clearly in Bouyeri’s text *To Catch a Wolf*, in which he called on others to wake up and free themselves. In the same text, he also threatens that it is only a matter of time before the knights of Allah

[60] Boogerd and Walters, ‘Jason Walters, van terrorist to filosoof’, [0:15:25].
[61] Beatrice de Graaf, *Gevaarlijke vrouwen. Tien militante vrouwen in het vizier* (Amsterdam: Boom, 2012) 254.
[62] Frazer Egerton, *Jihad in the West. The Rise of Militant Salafism* (Cambridge: Cambridge University Press, 2011) 124-125.
[63] Schuurman, *Becoming a European homegrown jihadist*, 85-86.
[64] *Portret*, ‘Samir A.: staatsvijand nr. 1, exclusief interview met Nederlands bekendste terreurverdachte’, [0:11:45].
[65] Jaco Alberts and Steven Derix, ‘Hoe georganiseerd waren Samir A. en zijn vrienden?’, *NRC Handelsblad*, April 9, 2005, https://www.nrc.nl/nieuws/2005/04/09/hoe-georganiseerd-waren-samir-a-en-zijn-vrienden-10461552-a102432 (accessed March 23, 2020).
[66] Van der Hulst, ‘Terroristische netwerken en *intelligence*’, 16.
[67] Emerson Vermaat, *De Hofstadgroep. Portret van een radicaal-islamitisch netwerk* (Soesterberg: Uitgeverij Aspect, 2017) 77.
[68] Van der Hulst, ‘Terroristische netwerken en *intelligence*’, 25.
[69] Rudolph Peters, ‘Dutch extremist Islamism: Van Gogh’s murderer and his ideas’, in R. Coolsaet (ed.), *Jihadi terrorism and the radicalisation challenge in Europe* (Aldershot: Ashgate, 2008) 115-127, here: 119-120.

would enter the Binnenhof in The Hague and establish Sharia Law in the Netherlands.[70] These texts show that the Hofstad Network's presence on the internet mainly functioned as a method to incite others, whereas recruitment played only a limited role.

Although most of the Web 1.0 was text-based, the members of the Hofstad Network also encountered images and videos on the internet, albeit on a very limited scale. When Bouyeri's house was searched after the murder of Van Gogh, a CD-ROM was found with a compilation of 28 men whose throats were cut. Most core members of the Hofstad Network watched videos of beheadings of infidels and shared their fascination with others.[71] It is, however, unclear how these videos found their way to the Hofstad Network as videoclips were not as prominent on the internet as nowadays. Video site YouTube would for instance only be created a year after the murder of Van Gogh for example.[72]

Despite these efforts, the Hofstad Network lacked popular support because of its Takfir ideology, radical interpretation of Islam and intimidation of potential supporters.[73] While the World Wide Web offered a big audience to Hofstad Network, the group could not benefit from this for their propaganda purposes, due to the limited attraction of its ideology.

This paragraph has shown that the online content accessed, published, and distributed by members of the Hofstad Network was text-based. The focus of these texts was on the message they conveyed, not on the visual aspect. This changed however with the introduction of the Web 2.0 as will be shown in chapter 3.

### 2.3.2 Finance

Limited information is available on the financial situation of the Hofstad Network. In contrast to terrorist organisations of the 20th century, the Hofstad Network was not dependent on international contacts for financial resources.[74] Due to the small scale and local nature of the

[70] Rudolph Peters, 'Overzicht teksten geschreven of vertaald door Mohammed B.', attachment to the report 'De ideologische en religieuze ontwikkeling van Mohammed B.', 1-31, here: 20.

[71] Samir Azzouz showed such videos to his sister early in his radicalisation process radicalisation, whereas Nouriddin El Fahtni reportedly even watched videos of infidels being slaughtered on his wedding night. De Graaf, *Gevaarlijke vrouwen*, 255; Ian Buruma, *Murder in Amsterdam: The Death of Theo Van Gogh and the Limits of Tolerance* (London: Atlantic Books, 2007) 212.

[72] Paige Leskin, 'The incredible story of YouTube's early days and how it rose to become the world's most popular place to watch', *Business Insider*, December 18, 2019, https://www.businessinsider.nl/history-of-youtube-in-photos-2015-10?international=true&r=US (accessed April 16, 2020).

[73] Schuurmans, *Becoming a European homegrown jihadist*, 87-88.

[74] Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004) 120.

network, the members of the group did not require large amounts of money to keep their organisation functioning. Furthermore, terrorist attacks also became cheaper in the twenty-first century, so the Hofstad Network required no financial support for their attacks.[75] This is illustrated by the murder of Van Gogh, which was the only successful terrorists attack by a member of the Hofstad Network. For this assassination, Bouyeri used a cheap pistol and two knives.[76] Additionally, dealing with financial matters via the internet was just becoming popular in the Netherlands, with less than thirty per cent of the population using online banking services in 2004.[77] Furthermore, the fact that Bouyeri handed an envelope with 1650 euros in cash to Zakaria T. the weekend before the murder of Van Gogh, instead of transferring this money online, indicates that the internet did not have a financial purpose for the members of the Hofstad Network.[78]

### 2.3.3 Training

In the 20th century, many European terrorists travelled to the Middle East to follow military training from organisations such as Al-Qaida and the Palestine Liberation Organization.[79] Whereas foreign training camps are still visited in the twenty-first century, the internet has increasingly facilitated the training of terrorists. This duality in training terrorist was also present within the Hofstad Network.

Samir Azzouz was the first of the (future) Hofstad Network members who travelled abroad country to follow military training. As a sixteen-year-old, he left the Netherlands with a high school friend to join the Chechnyan cause at the beginning of 2003, but they were refused entry at the Russian border and returned home.[80] Jason Walter and Ismail A. successfully travelled to Pakistan for a month in the summer of 2003 to undergo jihad training

[75] Lorenzo Vidino, 'The Hofstad Group: The New Face of Terrorist Networks in Europe', *Studies in Conflict & Terrorism* 3 (2007) 7: 579-592, here: 589.

[76] See for an extensive and factual overview of the murder of Van Gogh: Amsterdam District Court, 'ECLI:NL:RBAMS:2005:AU0025', July 26, 2005, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2005:AU0025 (accessed March 14, 2020).

[77] *De Nederlandsche Bank*, 'Internetbankieren nu en in de toekomst', kwartaalbericht, June 2007, https://www.dnb.nl/binaries/Internetbankieren%20nu%20en%20in%20de%20toekomst_tcm46-156864.pdf (accessed April 16, 2020).

[78] Vermaat, *De Hofstadgroep*, 38.

[79] James J.F. Forest, 'Terrorist Training Centers Around the World: A Brief Review', in James J.F. Forest (ed.), *The Making of a Terrorist: Volume Two* (Westport, CT: Praeger Security International, 2005) 296-311.

[80] *Portret*, 'Samir A.: staatsvijand nr. 1, exclusief interview met Nederlands bekendste terreurverdachte', [0:05:05].

there. Zakaria T. followed them later but only stayed for a week. Walters and T. went again in December of the same year but were deported from the country after nine days.[81] Whereas the AIVD is unclear about the activities of the men in Pakistan, Walters spoke about his experiences with a friend via chat messaging. In multiple texts, he stated that he had undergone basic training and had learnt to handle guns, grenades and rocket launchers there.

Other members of the Hofstad Network did not visit foreign training camps but instead turned to the internet for instructions. Multiple printed manuals in English were found in the houses of Hofstad Network members. These manuals covered subjects like 'how to use a combat kit', 'preparations for a terrorist attack', and contained instructions for creating explosives and dealing with police interrogations.[82]

In this Web 1.0 phase, terrorists started to explore the possibilities of online training. Most members preferred the physical training in foreign training camps, as the focus of major terrorist networks like al-Qaeda was still on these local training camps. [83] The online facilitation of training was just starting to get embraced by such organisations at this time in history, but the internet would soon become the "online terrorism university" that it is today.[84]

### 2.3.4 Planning

A key aspect of the Hofstad Network were the living room meeting, in which members gathered to discuss religious aspects of Islam and the activities of people such as Theo van Gogh, Ayaan Hirsi Ali, and Geert Wilders.[85] The AIVD suspected that the murder of Van Gogh had been discussed at one of these meetings, as Jason Walters and Ismail A. were secretly recorded speaking about details of the assassination that had not yet been discussed in the media.[86] This shows that they must have had pre-existing knowledge on (aspects of) the assassination.

[81] Vermaat, *De Hofstadgroep*, 89-91.

[82] Ibid., 54-63.

[83] Anne Stenersen, 'The Internet: A Virtual Training Camp?', *Terrorism and Political Violence* 20 (2008) 2: 215-233, here: 216.

[84] Gabriel Weimann, 'Virtual Training Camps: Terrorists' Use of the Internet', in James J.F. Forest (ed.), *Teaching Terror: Strategic and Tactical Learning in the Terrorist World* (Lanham, MD: Rowman & Littlefield, 2006) 110-132, here: 112.

[85] Vermaat, *De Hofstadgroep*, 33.

[86] Ibid., 95

However, whereas these living room meetings were a trademark of the Hofstad Network's activities, the internet was also actively used by members of the Hofstad Network for planning acts of terror.[87] Email accounts and MSN-groups were used for internal communication between different members.

Most members of the Hofstad Network had Hotmail accounts. Hotmail and other web-based email services were a popular means of communications for terrorists in the first few years of the twenty-first century, who often used a dead drop system to avoid detection. By sharing a Hotmail account between members, they were able to communicate without actually sending the messages. One terrorist would write an email and save it as a draft, allowing another terrorist to read the message by logging into the same account and reading the draft. This way, no email traffic between these individuals existed, which made it difficult for intelligence agencies to discover connections between terrorists. Multiple accounts were also shared as to avoid discovery by intelligence services.[88] This tactic was also successfully adopted by other European terrorists who were active around the same time as the Hofstad Network, such as the suspects of the 2004 Madrid train bombings.[89] A list containing 78 different email accounts found on Mohammed B.,[90] indicates that the members of the Hofstad Network likely used this system as well. Unfortunately, the emails that could serve as evidence for this were destroyed due to negligence of the AIVD.[91]

For instant communication, the members of the Hofstad Network relied on MSN Messenger and MSN Groups. These online services from Microsoft allowed people to send messages to each other and create online communities. Members and supporters of the Hofstad Network were united in an MSN-group called 'Muwahiddin' (Arabic for 'the True Muslims') and communicated in private chats. On these platforms, they openly spoke about their terroristic intentions, but at the same time only undertook limited actions to hide their identities. In a chat with a friend, Jason Walters bragged about his jihad training in Pakistan

[87] *Trouw*, 'Hof krijgt internetles in Hofstadzaak', June 14, 2007, https://www.trouw.nl/nieuws/hof-krijgt-internetles-in-hofstadzaak~bea5ca66/?referer=https%3A%2F%2Fwww.google.nl%2F (accessed April 19, 2020).
[88] UNODC, 'The use of the Internet,' 55.
[89] Renwick McLean, 'Madrid suspects tied to e-mail ruse', *The New York Times*, April 27, 2006, https://www.nytimes.com/2006/04/27/world/europe/madrid-suspects-tied-to-email-ruse.html (accessed April 20, 2020).
[90] *Trouw*, 'E-mail Hofstadgroep vernietigd door fout AIVD', November 2, 2006, https://www.trouw.nl/nieuws/e-mails-hofstadgroep-vernietigd-door-fout-aivd~bf139238/ (accessed April 20, 2020).
[91] Ibid.

and his 'to-kill-list' using the pseudonym "Mujaheed".[92] The online aliases used by Walters and other members of the Hofstad Network could, however, be easily traced back to them according to two experts on digital crime.[93] Additionally, the MSN messages and groups were constantly deleted and re-established under different names to avoid detection.[94] These chats were however ignored for a long time by the security services and the AIVD was only able to confirm that the members of the Hofstad Network had openly discussed acts of terrorism online.[95]

Regarding the planning of an attack, terrorists not only rely on the internet for communication purposes but also benefit from the information that is publicly available on the internet. The Hofstad Network is no exception to this. When Samir Azzouz, who is often perceived as the mastermind of the Hofstad Network,[96] was arrested in June 2004, the police discovered a collection of maps and photos of high-profile buildings in the Netherlands. These included the Headquarters of the AIVD in Schiedam, barracks of the Dutch Commando's in Roosendaal, the House of Representatives in The Hague, Amsterdam Airport Schiphol, and a nuclear powerplant in Borssele.[97] Many of these floorplans and photographs of their surroundings had been downloaded from the internet. Additionally, photographs of other coal-fired power stations and nuclear powerplants were downloaded for a better understanding of the maps.[98] It should be noted that this was a difficult job at this time, considering that easy to use web mapping services, such as Google Maps, were still in development and required an understanding of different programming languages.[99]

Whereas this shows that the members of the Hofstad Network (or at least Samir Azzouz) benefitted from the publicly available information online for planning a terrorist

[92] Vermaat, *De Hofstadgroep*, 86-91.
[93] Janny Groen en Annieke Kranenberg, 'Vrij spel voor de jihad', *De Volkskrant*, February 13, 2006, https://www.volkskrant.nl/cultuur-media/vrij-spel-voor-de-jihad~b5f4773c/ (accessed April 19, 2020).
[94] Nationaal Coördinator Terrorismebestrijding, 'Jihadisten en het internet' (phenomenon report to the Dutch parliament, 2007), 60-61, https://www.aivd.nl/documenten/publicaties/2007/01/18/jihadisten-en-het-internet (accessed April 20, 2020).
[95] Janny Groen and Annieke Kranenberg, *Strijdsters van Allah: radicale moslima's en het Hofstadnetwerk* (Kobo e-book, 2013) 11-12 (Chapter 3).
[96] Van der Hulst, 'Terroristische netwerken en *intelligence*', 21.
[97] De Graaf, *Gevaarlijke vrouwen*, 263.
[98] The Hague District Court, 'ECLI:NL:GHSGR:2005:AU6181', November 18, 2005, https://linkeddata.overheid.nl/front/portal/document-viewer?ext-id=ECLI:NL:GHSGR:2005:AU6181 (accessed March 25, 2020).
[99] Samuel Gibbs, 'Google Maps: a decade of transforming the mapping landscape', *The Guardian*, February 8 2015, https://www.theguardian.com/technology/2015/feb/08/google-maps-10-anniversary-iphone-android-street-view (accessed April 20, 2020).

attack, they primarily kept relying on offline means. Some of the maps at the house of Azzouz were not downloaded but hand-drawn and notes were added on security measures, presumably by Azzouz himself.[100] Furthermore, witnesses have stated that Mohammed B. had visited the Linnaeusstraat multiple times in the month before the murder of Van Gogh in that same street.[101] This still had to be done physically due to the limited availability of online mapping services that allowed the user to study the targeted location on the internet.[102]

This analysis of the internet uses by the Hofstad Network regarding planning purposes has shown that the group's members were adept in getting the most out of the available technology. In addition to the physical living room meetings and offline reconnaissance, the member of the Hofstad Network used online methods of communication and services to prepare for terrorist attacks, albeit in an amateurish manner and on a small scale. Their online activities were limited by the of the technology available, but the first steps into the use of the internet for planning purposes had been taken.

### 2.3.5 Execution

Fortunately for the Dutch society, but unfortunately for this master thesis, the lack of terrorist attacks by the Hofstad Network has made it difficult to analyse the use of the internet for the execution of an act of terrorism. The only successful act of terrorism committed by a member of the Hofstad Network was the murder of Van Gogh by Bouyeri, for which no accomplices were ever convicted. It was however suspected that other members of the Hofstad Network were aware of the attack before it happened.[103] Despite the uncertainty about possible accomplices, no evidence was found for online communication or the use of other online services by Bouyeri in the execution of this terrorist attack.[104]

However, the internet was frequently used by members of the Hofstad Network to publish threats of a terrorist attack. In MSN-groups they discussed the of killing "fake Muslims" and stated that politician Geert Wilders, who had criticised Islam, should be murdered.[105]

[100] The Hague District Court, 'ECLI:NL:GHSGR:2005:AU6181'.

[101] Vermaat, *De Hofstadgroep*, 37.

[102] Drew Olanoff, 'Inside Google Street View: From Larry Page's Car To The Depths Of The Grand Canyon', *TechCrunch*, March 8, 2013, https://techcrunch.com/2013/03/08/inside-google-street-view-from-larry-pages-car-to-the-depths-of-the-grand-canyon/ (accessed April 20, 2020).

[103] Amsterdam District Court, 'ECLI:NL:RBAMS:2005:AU0025'.

[104] Vermaat, *De Hofstadgroep*, 39-42.

[105] Schuurman, Eijkman and Bakker, 'The Hofstadgroup Revisited', 913-914; 916.

Additionally, many of the texts that were published online by members of the Hofstad Network contained terrorist threats against the Dutch society or specific individuals.[106] Whereas this is seen as freedom of speech in some Western countries, threatening with a terrorist attack is prosecutable as an act of terrorism in the Netherlands.[107] In publishing these threats online, the members of the Hofstad Network were therefore committing acts of terrorism via the internet. These threats did not impact the Dutch society similar to the murder of Van Gogh,[108] but this shows that the internet was used for the execution of acts of terrorism by the Hofstad Network, albeit in a primitive way.

### 2.3.6 Cyberattacks

The evidence found at the homes of the members of the Hofstad Network indicates that they focussed on physical and violent acts of terrorism. No cyberattack has been undertaken by the group and there has been no evidence suggesting that the group was interested in cyberterrorism at all. Other terrorist organisations of that time did give attention to the opportunities that cyberterrorism could provide, even though it was still in its initial phase. For example, a few weeks after 9/11, a Pakistani hacking group linked themselves to al-Qaeda and established the "al-Qaeda Alliance Online". Fear that this collective would commit acts of cyberterrorism was however unfounded, as the group quickly declared that it was "not a group of Cyber terrorists" and disappeared from the internet.[109] Despite the existence of a cyberterrorist threat, no cyberattacks have been recorded during the Web 1.0 phase of the internet.[110]

## 2.4 Looking in the wrong direction

Despite it not being at the centre of this research, the online actions by counterterrorism agencies need to be discussed as their activities have an impact on the online activities of

[106] See for example: Peters, 'Overzicht teksten geschreven of vertaald door Mohammed B'.
[107] AIVD, 'Terrorisme', n.d., https://www.aivd.nl/onderwerpen/terrorisme (accessed April 21, 2020).
[108] After the murder of Van Gogh, public fear due to terrorism increased in the Netherlands, see: Edwin Bakker, *Terrorism and Counterterrorism Studies. Comparing Theory and Practice* (Leiden: Leiden University Press, 2015) 41.
[109] Dorothy Denning, 'A View of Cyberterrorism 5 Years Later', in Kenneth Himma (ed.), *Internet Security: Hacking, Counterhacking, and Society* (Burlington, Massachusetts: Jones & Barlett Publishers, 2007) 123-141, here: 131.
[110] Gabriel Weimann, 'Cyberterrorism: The Sum of All Fears', *Studies in Conflict & Terrorism* 28 (2005) 2: 129-149, here: 131.

terrorists. This impact was however limited in the case of the Hofstad Network. The AIVD struggled with incorporating the internet activities of terrorists in its intelligence-gathering operations, which was highlighted in a report by the supervisory committee stating:

> Online intelligence gathering had in this period [before November 2004] no clear position within the operational process of the AIVD and the technological opportunities to shape online intelligence gathering were not yet optimal. Where available, the AIVD found it difficult to evaluate information from the internet as it was such an open source.[111]

Whereas the internet had been publicly accessible for ten years, the world was not as entangled with the internet as it is today. The importance of online activities by terrorists was underestimated, based on the limited technological capabilities of the Web 1.0. Additionally, counterterrorism agencies had focussed their attention on offline intelligence gathering and even downplayed the impact of the emerging internet on terrorist activities.[112] After the murder of Van Gogh in November 2004, the AIVD increased its intelligence-gathering efforts on the internet and slowly embraced the expanding role of the internet for terrorist activities.[113]

## 2.5 Conclusion

The main function of the Web 1.0 was the provision of information to a broad public. This was exploited by terrorists who could use the internet for publishing their own messages. These also reached the members of the Hofstad Network, contributing to their radicalisation process. As terrorists themselves, the members of the Hofstad Network explored how the internet could be used for terrorist purposes. This chapter has shown that they not only used the Web 1.0 for spreading their own radical texts as propaganda but also used the internet to communicate with others via web fora, email services and messenger platforms. Because the Hofstad Network focussed on strict ideological principles, with the text-based nature of the Web 1.0. Their radical ideology was at the core of their texts and needed no visual additions.

[111] (own translation) Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (hereafter: CTIVD), 'Toezichtsrapport inzake de afwegingsprocessen van de AIVD met betrekking to Mohammed B.', CTIVD report (The Hague, 2008) 39-40.

[112] John L. Hennessy, David Patterson, and Herbert Lin, *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities* (Washington D.C.: National Academies Press, 2003) 18.

[113] CTIVD, 'Toezichtsrapport inzake de afwegingsprocessen van de AIVD met betrekking to Mohammed B.', 40.

On a small scale, images and videos were used by the Hofstad Network for gathering intelligence, but only in addition to the offline methods that were preferred by the members. Whereas the members of the Hofstad Network took the first steps into integrating the internet into their terrorist activities, they were still limited by the capabilities of the available technologies. It is therefore not surprising that they had no use for the internet in matters of finance and cyberattacks and only limited use in the execution of terrorist attacks. Whenever the members of the Hofstad Network did use the internet, they acted in an amateurish way and it was only due to the lack of online investigation by the AIVD that the group could remain hidden for a long time

Whereas the internet of the Web 1.0 offered new opportunities to the terrorists of the Hofstad Network, the internet was not yet the gamechanger that it would become with the introduction of the Web 2.0.

# The online ubiquity of ISIS

## 3.1 The user-based internet

The transition to the Web 2.0 phase radically changed the nature of the internet for its users. Whereas the Web 1.0 centred around the provision of information in a one-way approach, the Web 2.0 can be seen as a web of continuous interactive communication with a transition from written texts to visualised imagery and videos.[114] With the Web 2.0, users were no longer restricted by obstacles such as time, electricity or intermediates (such as individuals who distributed physical propaganda content over the world) and each user could become a 'broadcasting company'. Whereas user-based interaction was not an entirely new phenomenon in 2006, with web forums and websites like Wikipedia implementing options for limited user-interaction in the Web 1.0 phase,[115] other websites increasingly started to add similar options for their users in the Web 2.0 phase. Dale Dougherty was the first to speak about the Web 2.0 in 2004, noting that instead of crashing, the internet had become more important than ever after the dot-com collapse.[116] Whereas the Web 1.0 internet was often perceived as a digital counterpart of paper,[117] the shift to the Web 2.0 meant that the internet differentiated itself from previous media and would impact the world in a revolutionary manner.[118]

The concept of 'social media' is inextricably linked with the Web 2.0. Defined by Andreas Kaplan and Michael Haenlein: "Social Media is a group of Internet-based applications that build on the ideological and technological foundations of the Web 2.0, and that allow the creation and exchange of User Generated Content."[119] Around 2006 many new social media platforms were launched of which the impact on society would only increase in the years to come. The rise of content management systems, such as WordPress and individual blogs, made it easier for internet users to express their opinions and worldviews on the internet. Furthermore, the creation of video website YouTube in 2005 and community-based platforms

[114] Aghaei, Nematbakhsh, and Farsani, 'Evolution of the World Wide Web', 1.

[115] Wikipedia.org is a free online encyclopaedia that can be edited by anyone and was founded in 2001. Jim Giles, 'Internet encyclopaedias go head to head', *Nature* 438 (2005): 900-901, here: 900.

[116] Tim O'Reilly, 'What is Web 2.0', *O'Reilly Media*, September 30, 2005, https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html (accessed April 23, 2020).

[117] Ted Nelson, 'Mission statement', *Project XANADU*, 1960, http://xanadu.com/ (accessed April 23, 2020.

[118] Johnny Ryan, *A History of the Internet*, 137.

[119] Andreas Kaplan and Michael Haenlein, 'Users of the world, Unite! The challenges and opportunities of Social Media', *Business Horizons* 53 (2010) 1: 59-68, here: 61.

such as Facebook and Twitter in 2004 and 2006 allowed for easier distribution of multimedia content and communication on the internet.

This interactive internet attracted more users, doubling the total number of individuals on the internet to almost two billion worldwide between 2005 and 2010.[120] According to a study by Van Deursen, Van Dijk and Ten Klooster, the internet's use for social interaction kept increasing between 2010 and 2013, but the provision of information still remained the most popular function.[121] From 2013 onwards, the three most popular social media platforms have been Facebook, YouTube and WhatsApp.[122]

Because these new features of the Web 2.0 were not only used for innocent purposes, this chapter analyses how the interactive technologies of the Web 2.0 were used by jihadist terrorists from Islamic State in Iraq and Syria.

## 3.2 Creating an Islamic caliphate

Founded in 1999 by Abu Musab al Zarqawi, ISIS precursor Jama'at al-Tawhid wal-Jihad allied itself with al-Qaeda in Iraq (AQI) in 2004. Based on a Salafist jihadist interpretation of Islam, this group strove to create an Islamic state in the Middle East. After Zarqawi was killed in a United States (US) drone attack, Abu Ayyub al Masri took his place and cooperated with other jihadist groups in the region to establish the overarching Islamic State in Iraq (ISI) organisation with Abu Omar al Baghdadi as its leader. Due to the increased number of US troops in Iraq from 2007 onwards, ISI moved its centre of operations from Baghdad to Mosul but faded into obscurity. When both al Masri and al Baghdadi were killed by a US intervention in 2010, Abu Bakr al Baghdadi assumed the role of leader for the organisation and under his rule, the ISI quickly expanded. By maintaining contact with other terrorist organisations in the region, such as Jabhat al-Nusra in Syria, al Baghdadi transformed ISI from an Iraqi organisation into an international terrorist organisation. Benefitting from the eruption of the Syrian Civil War in 2011, ISI quickly expanded its operations and got a foothold in this country as well.[123]

[120] Roser, Ritchie and Ortiz-Ospina, 'Internet'.

[121] Van Deursen, Van Dijk, and Ten Klooster, 'Increasing inequalities in what we do online', 264.

[122] Esteban Ortiz-Ospina, 'The rise of social media', *OurWorldinData*, September 18, 2019, https://ourworldindata.org/rise-of-social-media (accessed April 30, 2020).

[123] *Wilson Center*, 'Timeline: the Rise, Spread, and Fall of the Islamic State', October 28, 2019, https://www.wilsoncenter.org/article/timeline-the-rise-spread-and-fall-the-islamic-state (accessed April 25, 2020).

In the early 2010s, the population in much of the Arab world revolted against their governments and demanded reforms. Syria's population demonstrated peacefully in 2011 against the dictatorship of President Bashar al-Assad, but when these protests were met with military crackdowns, the situation escalated into a Civil War. Due to ethnic, sectarian and ideological differences, the opposition fragmented into more radical groups including, Jabhat al-Nusra and ISI.[124] These groups were extremely successful in combating the Syrian military due to their organisational capabilities, fearlessness and experienced fighters.[125] On April 11, 2011, ISI declared that it had merged with al-Nusra and formed the new "Islamic State in Iraq and Syria." This merger was however contested by the leader of al-Nusra who declared allegiance to al-Qaeda.[126] Despite this, ISIS quickly gained ground in Syria and took control over the city of Raqqa, declaring it the capital of its emirate. After conquering the city of Mosul in northern Iraq, ISIS declared the establishment of its Islamic caliphate on June 29, 2014 and renamed itself to "Islamic State."[127]

Whereas ISIS' caliphate was not recognised as a state by any sovereignty, ISIS consolidated its control over the region by establishing ministries and collecting taxes from its population.[128] In line with research by Niels Terpstra and Georg Frerks into rebel governance practices, ISIS concerned itself with the welfare of its population and established a legal system based on Sharia Law and created a police force.[129] And similar to the Stasi in East Germany, ISIS set up an organization for internal intelligence, called Emni.[130]

Shortly after the declaration of the caliphate, a US-led international coalition against ISIS was formed and began attacking the territory of ISIS. As a result of their actions, the

[124] Maurits Berger and Masha Rademakers, 'Allahoe Akbar! – de jihadisten', in Maurits Berger (ed.), *Nederlanders in de heilige oorlog: zoeaven, brigadisten en jihadisten* (The Hague: Boom Juridische uitgevers, 2015) 67-96, here: 72-73.

[125] Edwin Bakker, Christophe Paulussen, and Eva Entenmann, 'Dealing with European Foreign Fighters in Syria: Governance Challenges & Legal Implications', ICCT research paper (The Hague, December 2013) 2.

[126] *Wilson Center*, 'Timeline'.

[127] *BBC*, 'ISIS rebels declare 'Islamic state' in Iraq and Syria', June 30, 2014, https://www.bbc.com/news/world-middle-east-28082962 (accessed April 25, 2020).

[128] Kareem El Damanhoury, 'The Daesh State: The Myth Turns into a Reality', *Center for Global Communication Studies*, July 26, 2016, https://global.asc.upenn.edu/the-daesh-state-the-myth-turns-into-a-reality/ (accessed April 25, 2020).

[129] Niels Terpstra and Georg Frerks, 'Rebel Governance in Sri Lanka's 'Uncleared' Territories during 1990s and 2000s', paper presented at the *9th Pan-European Conference on International Relations* (Giardini Naxos, Italy, September 23-26, 2014); *Vice*, 'The Islamic State', special news video, 2014, https://video.vice.com/nl/video/the-islamic-state/559ea2a9884e6b677d5e2b25 (accessed April 25, 2020).

[130] Beatrice de Graaf and Saskia Pothoven, 'De islamitische inlichtingenstaat – De Stasi als leermeester?', *Militaire Spectator* 187 (2018) 9: 453-465, here: 465.

caliphate's expansion was halted and eventually pushed back in 2014. Subsequently, ISIS called on its supporters to commit acts of terrorism in the combatting countries as a form of retaliation. This call was not only aimed at its members within the caliphate but was also directed at homegrown terrorists who supported ISIS.

Whereas the Islamic caliphate of ISIS was located in the Middle East, the group's cause resonated with Muslims worldwide. After the declaration of the Islamic caliphate, Muslims from all over the world travelled to the area occupied by ISIS to live under Sharia Law and became fighters for ISIS. Western-European governments feared that these foreign fighters would receive militant training from ISIS and would commit acts of terrorism upon their eventual return.[131] Major attacks in Paris, Brussels and London were committed in the name of ISIS, showing that this fear was not unfounded.[132] The major impact of these terrorist acts on the world can be explained by the effective use of the Web 2.0 by ISIS.

## 3.3 ISIS electronic jihad

### 3.3.1 Propaganda

Nearly all terrorist organisations were active on social media platforms in the 2010s. ISIS is however unique in this regard. In the words of cyber-expert James P. Farwell "[…] ISIS stands apart for its sophisticated use and understanding of social media to achieve its goals."[133] To maintain this level of sophistication, ISIS created a decentralised media apparatus. Consisting of different media units, such as the al-Furqan Foundation and the al-Hayat Media Centre, this system was responsible for the constant production and distribution of media content. As a result of this decentralised but institutionalised structure, ISIS was able to narrowcast its content to a specific target audience.[134]

Most of the content created by ISIS was published on Twitter but could also be found on other social media platforms, such as Facebook, YouTube, and other websites. These

[131] Daniel Byman, 'The Homecomings: What Happens When Arab Foreign Fighters in Iraq and Syria Return?', *Studies in Conflict & Terrorism* 38 (2015) 8:581-602, here: 584-586.

[132] For more information on the Paris and Brussels attack and an assessment, see: Mario Arturo Ruiz Estrada and Evangelos Koutronas, 'Terrorist attack assessment: Paris November 2015 and Brussels March 2016', *Journal of Policy Modeling* 38 (2016) 3: 553-571; For an overview of the London Bridge attack of 2017, see: *BBC*, 'Westminster attack: What happened', April 7, 2017, https://www.bbc.com/news/uk-39355108 (accessed April 26, 2020).

[133] James P. Farwell, 'The Media Strategy of ISIS', *Survival* 56 (2015) 6: 49-55, here: 49.

[134] Pieter Nanninga, 'Branding a Caliphate in Decline: The Islamic State's Video Output (2015-2018)', ICCT research paper (The Hague, 2019) 4.

platforms and websites had and open nature and anyone interested could read published messages, look at discussion boards, click on links to propaganda videos, or join specific groups.[135] This potentially unlimited audience explains why ISIS chose those digital mediums for publishing its propaganda messages. The published content assumed different forms, ranging from written statements to news reports. However, visualised content, such as images and videos was most prominent, accounting for 88% of publications by ISIS on twitter in 2015.[136] Whereas the video content of ISIS did not always have a violent nature, the organisation's online activities gained notoriety through the videos in which they showed the execution of captured foreigners. This resulted in Twitter taking down the official accounts of ISIS on its platform, but new accounts were created almost instantly. It is estimated that between September and December 2014 at least 46.000 twitter accounts were used by ISIS.[137] This constant change made it difficult to track the propaganda from ISIS and to analyse the audience of their messages.

ISIS countered these takedowns by developing a free mobile application called "The Dawn of Glad Tidings" or simply "Dawn". This app allowed its users to monitor tweets from ISIS and automatically copied the information to the user's own feed.[138] In doing so, ISIS was able to send out 44.000 tweets on the day the organisation conquered the city of Mosul in 2014.[139]

The languages used for the propaganda content on the social media accounts of ISIS do however indicate that the organisation mostly targeted Arabic speaking individuals, with English being the second most used language, only accounting for 6.5 per cent of the content.[140] For non-Arabic speakers, ISIS published a digital magazine between 2014 and 2017 in different languages. Changing its name from *Islamic State News* to *Islamic State Report* in

[135] Gabriel Weimann, 'Terror on Facebook, Twitter, and YouTube', *Brown Journal of World Affairs* 16 (2010) 2: 45-54, here: 50.

[136] Aaron Y. Zelin, 'Picture Or It Didn't Happen: A Snapshot of the Islamic State's Official Media Output', *Perspectives on Terrorism* 9 (2015) 4: 85-97, here: 89.

[137] J.M. Berger and Jonathon Morgan, 'The ISIS Twitter Census. Defining and describing the population of ISIS supporters on Twitter', analysis paper no. 20 for *The Brookings Project on U.S. Relations with the Islamic World* (Washington D.C., March 2015) 7.

[138] Imran Awan, 'Cyber-Extremism: Isis and the Power of Social Media', *Social Science and Public Policy* 54 (2017): 138-149, here: 139.

[139] Farwell, 'The Media Strategy of ISIS', 51.

[140] Zelin, 'Picture Or It Didn't Happen', 89.

June 2014 and *Dabiq* in July 2014, before finally settling on *Rumiyah* in 2016.[141] The online magazine focussed on concepts from jihadist ideology and politico-military aspects of Islam. The publications were mostly targeted at Muslims in the United States and the United Kingdom, urging them to move to the Islamic Caliphate.[142] The different issues of this magazine were, however, difficult to access online. Instead of looking for a specific page via a search engine (such as Google or Bing), the magazine was published on the deep web. The deep web is also known as the 'hidden web' as its contents do not show up on search engines. The issues of ISIS's online magazine could therefore only be accessed by typing in a specific URL (also known as a web address) or IP address. This made the magazine hard to find for counterterrorism agencies but impacted the number of readers. However, quickly after their publication on the deep web, the issues could also be found on other more, more accessible, platforms and were even available on Amazon for a short time.[143]

Additionally, the Web 2.0 allowed supporters of ISIS to create their own accounts which could distribute content even further than the official ISIS accounts. As a result, the terrorist organisation no longer depended on faltering technology or physical distribution as had been the case with previous terrorist organisations, such as al-Qaeda, which transported physical cassettes with the teachings of Osama bin Laden all over the world.[144]

ISIS also used anonymous sharing portals on the deep web to distribute their content to others. Using services like Justpaste.it, Sendvid.com and Dump.to ISIS was able to "disseminate its online videos, brutal images of beheadings, texts that aim to spread its radical ideology, and […] the ISIS online magazine *Dabiq*."[145] Compared to social media platforms, especially Facebook, these deep web services reduced the risk of having the identity of ISIS supporters or members leaked and were therefore preferred by ISIS.[146] On the downside, the content distributed this way reached as a smaller, selected audience. Such deep web

[141] Haroro J. Ingram, 'Islamic State's English-language magazines, 2014-2017: Trends & implications for CT-CVE strategic communications. A quick reference guide to Islamic State News (issues 1-3), Islamic State Report (issues 1-4), Dabiq (issues 1-15) and Rumiyah (issues 1-13)', ICCT research report (The Hague, 2018) 6.

[142] Ingram, 'An Analysis of *Inspire* and *Dabiq*', 368.

[143] Alessandria Masi, 'ISIS propaganda Magazine Dabiq For Sale On Amazon Gets Taken Down', *International Business Times*, October 6, 2015, https://www.ibtimes.com/isis-propaganda-magazine-dabiq-sale-amazon-gets-taken-down-1961036 (accessed April 30, 2020).

[144] David Killcullen, 'Countering global insurgency', *Journal of Strategic Studies* 28 (2005) 4: 597-617, here: 601.

[145] Ahmad Shehabat and Teodor Mitew, 'Black-boxing the Black Flag: Anonymous Sharing Platforms and ISIS Content Distribution Tactics', *Perspectives of Terrorism* 12 (2018) 1: 81-99, here: 88.

[146] Weimann, 'Terror on Facebook, Twitter, and YouTube', 48.

platforms were therefore used by ISIS to narrowcast specific messages and types of content to its supporters, whereas publicly available social media platforms served to reach a large audience regardless of whether this audience supported ISIS.

The propaganda content of ISIS eventually found its way to a large, global audience, increasing the number of ISIS sympathisers and members around the globe. Great Britain alone counted around 23 thousand jihadist sympathisers in 2015, and similar numbers can be seen in other countries in the West.[147] Whereas these are staggering numbers, the small number of foreign fighters that have heeded the call to emigrate to the Islamic caliphate and became fighters for ISIS pose a bigger threat. It is estimated that around 30.000 individuals from over the world have joined ISIS, of which four thousand came from Europe.[148] These foreign fighters will be further analysed in the third subsection of this chapter which deals with the training of ISIS terrorist.

This paragraph has shown that ISIS has developed a complex duality in its distribution of propaganda. The organisation relied on publicly accessible platforms for broadcasting their messages, whereas more restricted and hidden platforms, such as those on the deep web, have been used to reach a smaller, selected audience of supporters. The type of content had changed as well, with more emphasis on the visual aspects of content. This dual approach and visualised content benefitted from the sophisticated media centres that ISIS established, which dedicated to themselves to the online output of the terrorist organisation.

### 3.3.2 Finance

Terrorist organisations have never been very open about their sources of income and ISIS is no exception to this.[149] Images from inside the caliphate however showed that ISIS collected Zakat, Islamic taxation for the wealthy. The money is often collected after prayers and is usually provided in cash.[150] Cash is preferred by terrorists as offline money transfers are

[147] Ian Kershaw, *Een naoorlogse achtbaan. Europa 1950-2017* (Houten: Unieboek|Het Spectrum bv, 2018) 582.
[148] Beatrice de Graaf, 'Foreign fighters on trial: Sentencing risk, 2013 – 2017', in Nadia Fadil, Martijn de Koning and Francesco Ragazzi (eds.), *Radicalization in Belgium and the Netherlands – Critical Perspective on Violence and Security* (London/ New York: I.B. Tauris, 2019) 97-130, here: 99.
[149] Michael Freeman, 'The Sources of Terrorist Financing: Theory and Typology', *Studies in Conflict & Terrorism* 34 (2011) 6: 461-475, here: 463-464.
[150] Vice, 'The Islamic State'.

impossible to track by counterterrorism agencies.[151] Furthermore, the United Nations Security Council's Resolution 1373, that was adopted in the wake of the 9/11 attacks, called upon member states to combat the financing of terrorist activities by freezing their financial assets, which further complicated the use of the internet for financial matters.[152] Despite this, online banking has been being used to provide ISIS with international funding. Multiple supporters of ISIS in Western Europe collected money through non-profit organisations. They wired the money to contacts in Turkey and Jordan, where it was withdrawn and smuggled into the caliphate.[153] In other instances, money was wired to individual members of ISIS by friends or family members.[154]

ISIS also experimented with using cryptocurrencies for financing. Cryptocurrencies are digital currencies based on highly secure blockchain technology and can be traded over the internet. A Twitter account controlled by ISIS published multiple tweets on how the cryptocurrency Bitcoins could be used to finance the organisations and explained how an anonymous donation system using cryptocurrencies could be set up.[155] This extra attention to secure digital funding of ISIS might have been a result of the caliphate's loss of ground in Iraq and Syria from 2016 onwards.[156] Its loss in territory also meant less profit from the oil resources, that had previously been the organisation's primary source of income.[157] As a result, ISIS had to rely more on secure methods of international financing, which was extremely complex.

[151] Cynthia Dion-Schwarz, David Manheim, and Patrick B. Johnston, *Terrorist Use of Cryptocurrencies. Technical and Organisational Barriers and Future Threats* (Santa Monica, CA: RAND Corporation, 2019) 1-2.

[152] United Nations Security Council, 'Security Council Unanimously Adopts Resolution Calling upon Member States to Combat, Criminalize Financing of Terrorists, Their Activities', *United Nations Meetings Coverage and Press Releases*, March 28, 2019, https://www.un.org/press/en/2019/sc13754.doc.htm (accessed April 27, 2020).

[153] Directorate-General for External Policies of the European Parliament, 'In-depth analysis: The financing of the 'Islamic State' in Iraq and Syria (ISIS)', paper requested by the European Parliament's Committee on Foreign Affairs (Brussels, 2017) 16.

[154] See for example: Caroline Davies, 'Isis suspect Jack Letts' parents found guilty of funding terrorism', *The Guardian*, June 21, 2019, https://www.theguardian.com/uk-news/2019/jun/21/jack-letts-isis-suspect-parents-found-guilty-of-funding-terrorism-oxford-syria (accessed April 27, 2020).

[155] Financial Action Task Force, *Emerging Terrorist Financing Risks* (Paris: FAFT, 2015), 36.

[156] Martin Chulov, 'Losing ground, fighters and morale – is it all over for Isis?', *The Guardian*, September 7, 2016, https://www.theguardian.com/world/2016/sep/07/losing-ground-fighter-morale-is-it-all-over-for-isis-syria-turkey, (accessed April 17, 2020).

[157] Willem Theo Oosterveld and Willem Bloem, 'The Rise and Fall of ISIS: From Evitability to inevitability', security report of the The Hague Centre for Strategic Studies (The Hague, 2017) 12.

### 3.2.3 Training

Whereas the Islamic Caliphate of ISIS was located in the Middle East, it attracted supporters from all over the world. Some of these international supporters migrated to peacefully live in the caliphate governed by Sharia Law, while others joined the fighting at the side of ISIS. Because many countries in the West restricted travelling to the Islamic Caliphate, foreign fighters from these countries had to take detours to arrive in the territory of ISIS. This has made it difficult to get a clear image of the number of foreign fighters that joined ISIS, but estimates of foreign fighters from Europe placed the number around five thousand individuals in 2016.[158] As fighters for ISIS in Syria and Iraq, these volunteers pick up experience in waging a violent conflict. The acquired tactics and skills made the return of foreign fighters a risk in the eyes of their former governments. Additionally, these foreign fighters created networks of terrorists while in Syria and Iraq, which could become the basis of future terrorist networks in the West.[159] As a result, governments and societies were afraid of the potential risk such trained individuals might pose when they return to the West and did therefore not want to facilitate their returns.

However, foreign fighters did not pose the only risk to Western societies. As was shown in the chapter on the Hofstad Network, terrorists no longer required physical training to launch a terrorist attack. Because of the information provided via the internet, jihadist could easily access terrorist manuals. Whereas such handbooks had previously been published on websites and forums, ISIS relied on Telegram to disperse these manuals. These training guides were written in multiple languages including Arabic, English and Turkish.[160] In 2017, the Turkish franchise of ISIS even published a 66-page e-book, titled *Lone Wolf's Handbook*, which instructed readers to carry out attacks in the West and providing detailed information on burning parked cars, making bombs, suicide-truck attacks on pedestrians and detonating entire buildings. Containing over 170 illustrations and charts, this manual was unusually comprehensive and visual compared to similar manuals from other terrorist groups.[161] But

[158] Tanya Mehra, 'Foreign Terrorist Fighters. Trends Dynamics and Policy Responses', ICCT research report (The Hague, 2016) 6.

[159] Byman, 'The Homecomings', 584-585.

[160] Ahmet Yayla, 'Manhattan Bike-Path murderer Followed to the Letter ISIS' Latest 'Terrorism for Dummies'', *The Daily Beast*, November 1, 2017, https://www.thedailybeast.com/manhattan-bike-path-murderer-followed-to-the-letter-isiss-latest-terrorism-for-dummies (accessed May 1, 2020).

[161] Ahmet Yayla, 'Islamic State e-book released to home-school 'lone wolves'', *The Washington Times*, July 10, 2017, https://www.washingtontimes.com/news/2017/jul/10/islamic-state-e-book-released-to-home-school-lone-/ (accessed May 1, 2020).

not all training manuals from ISIS were focussed on instructions for acts of terrorism. A manual published in 2014 instructed readers how to navigate the internet securely by removing metadata, such as names and location, from their posts, and explained to them how to access the deep web.[162]

### 3.3.4 Planning

Similar to online activities of members of the Hofstad Network, members of ISIS in the West used the internet to acquire publicly available information. After the 2016 Brussels bombing, a laptop of one the perpetrators was found by the Belgian police, which discovered that the device contained plans and images on the Belgian Prime Minister's home and office.[163] Whereas the Prime Minister had not been targeted in the attacks, the presence of such files on a terrorist's computer was worrying. This shows that the ISIS-inspired terrorists of 2016, used the internet to access publicly available information as an alternative to offline reconnaissance, similar to the terrorists of the Web 1.0 phase of the internet. However, not all the images on the computer were downloaded from the internet. Photos taken by the perpetrators themselves show that terrorists still relied on physical reconnaissance to a certain extent, despite the extensive abilities of the Web 2.0.

Whereas acts of terrorism by individuals remained the most common, from 2013 onwards the number of terrorist attacks committed by groups has increased.[164] As a result, communication between terrorists became more important, which was reflected in the increased use in digital communication methods by terrorists. Before 2015, individual members of ISIS made use of popular social media platforms such as Facebook and Twitter, but due to rising security concerns, supporters of ISIS started to focus more on encrypted communication services instead.[165] Most popular of these were WhatsApp, Telegram, and

[162] Johnlee Varghese, 'ISIS Releases Training Guide on 'How to Tweet Safely, Without Giving out Your Location to NSA'', *International Business Times*, October 19, 2014, https://www.ibtimes.co.in/isis-releases-training-guide-how-tweet-safely-without-giving-out-your-location-nsa-611734 (accessed May 1, 2020).

[163] Jennifer Ranking, 'Laptop containing plans of Belgian PM's home found near terrorists' flat', *The Guardian*, March 30, 2016, https://www.theguardian.com/world/2016/mar/30/laptop-containing-plans-belgian-pms-charles-michel-home-terrorists-flat (accessed May 4, 2020).

[164] Petter Nesser, Anne Stenersen, and Emilie Ofteda, 'Jihadi Terrorism in Europe: The IS-Effect', *Perspectives on Terrorism* 10 (2016) 6: 3-24, here: 12-13.

[165] Mia Bloom, Hicham Tiflati, and John Horgan, 'Navigating ISIS's Preferred Platform: Telegram', *Terrorism and Political Violence* 31 (2019) 6: 1242-1254, here: 1242.

more recently, Surespot. All of these messaging services were free and offered end-to-end encryption to its users. [166]

However, Telegram gradually became the app of choice for ISIS terrorists from 2014 onwards. This could be a result of WhatsApp being acquired by Facebooks which had a bad reputation regarding privacy violations. Additionally, Telegram allowed users to create secret chatrooms and have messages self-destruct, which is a big plus if you are a terrorist and are looking for a secure method of communication.[167] Furthermore, Telegram was used for communicating with the leadership of ISIS. Whereas it is difficult to prove due to the previously mentioned encryption and self-destruction features, it is suspected that some attacks in the West have been coordinated by high-ranking members of ISIS from within the Caliphate.[168] Evidence for such involvement in the Western countries is still lacking, but the perpetrator of the 2017 Istanbul nightclub shooting openly spoke about the directions he had received from an 'emir' and a commander of ISIS in Raqqa via Telegram.[169] Jihadist research Nico Prucha even states that Telegram group chats have been used to connect assailants, targets and tactics for larger attacks.[170]

ISIS thus switched from very public communication media, such as Facebook and Twitter, to more selective and secure services like WhatsApp and Telegram for their internal communications. Furthermore, terrorists not only used such services to communicate with their direct accomplices, but these services were also used by high-ranking members of ISIS to supervise the attacks from within the caliphate.

### 3.3.5 Execution

The Web 2.0 phase of the internet made it easier to use the internet for the execution of a terrorist attack. Whereas the number of online published terrorist threats by members of the Hofstad Network was limited, this changed in the new Web 2.0 phase. Because more

[166] Previous methods of encryption secured the data only until it reached the server from the corresponding company, where it could still be accessed by hackers and intelligence services. End-to-end encryption however secures data in such a way that only the sender and receiver can access it. This is therefore a much safe method of communication for terrorists.

[167] Bloom, Tiflati, and Horgan, 'Navigating ISIS's Preferred Platform: Telegram', 1243.

[168] Tanya Mehra, 'Foreign Terrorist Fighters. Trends, Dynamics and Policy Responses', 13-15.

[169] Ahmet Yayla, 'The Reina Nightclub Attack and the Islamic State Threat to Turkey', *CTCSentinel* 10 (2017) 3: 9-16, here: 10.

[170] Nico Prucha, 'IS and the Jihadist Information Highway – Projecting Influence and Religious Identity via Telegram', *Perspectives on Terrorism* 10 (2016) 6: 48-58, here: 55.

radicalised individuals gained access to the internet and because the interactive Web 2.0 made it easier for them to publish their own content, an increase in the number of online published terrorist threats could be witnessed. Despite at least 30.000 Twitter accounts supporting ISIS' cause in March 2015,[171] only 1.264 tweets containing terroristic threats from ISIS supporters were found in research from 2017.[172] Ignoring the heavily fluctuating number of active accounts due to restrictive measures undertaken by Twitter, this would mean that not even five per cent of the tweets from ISIS supporters contained terrorist threats. A possible explanation for this small percentage is the fact that the tweets could serve multiple different purposes for terrorists and the strict definition of a terrorist threat by the researchers.

Whereas the number of terrorist threat messages in the name of ISIS might be limited, the terrorist organisation compensated with the use of the internet in the execution of physical acts of terrorism. ISIS shocked the world in August 2014 when Al-Hayat, one of the organisations official media centres, published a video of four minutes and 40 seconds on social media platform Diaspora. In the video American journalist James Wright Foley, who had been abducted two years earlier while reporting on the Syrian Civil War, was shown kneeling in the desert in an orange jumpsuit next to an executioner from ISIS. After a scripted statement by Foley, the member of ISIS put a knife to his throat after which a beheaded body and head were shown.[173] This brutal and gruesome video, titled 'A Message to America', was the first of many videos showing beheadings by ISIS. These execution videos were distributed on multiple different platforms including YouTube, Twitter, and lesser-known platforms such as VKontakte, Diaspora, and Liveleak.[174] The publication of these horrible videos served a dual function. On the one hand, these publications generated attention for ISIS and functioned therefore as a form of propaganda. On the other hand, the publication of these executions on the internet greatly expanded the audience of the act. Whereas such beheadings usually had only a limited audience of the members of ISIS present at the act, these executions became a public event by publishing these videos on the internet with a potential audience of millions

[171] Berger and Morgan, 'The ISIS Twitter Census', 37.

[172] Ibid., 23.

[173] Because the original videos has been removed from most public available platforms, and news sites only use parts of the original video, this description is derived from: Simone Molin Friis, ''Beyond anything we have ever seen': beheading videos and the visibility of violence in the war against ISIS', *International Affairs* 91 (2015) 4: 725-746, here: 725.

[174] Ibid., 740.

worldwide. The audience of such content in the Web 1.0 phase of the internet was smaller as individual internet-users were not as interconnected as with the Web 2.0 phase and they had to access a specific website to watch these videos. Due to the interactive nature of the Web 2.0, such content could easily be published on multiple platforms and accounts and could be further distributed by individual accounts of ISIS supporters.

Another use of the internet in the execution of a physical terrorist attack is the use of online means of communications. Like the services used for planning a terrorist attack, terrorists relied on secure methods of communications during a terrorist attack. Most notable of these is the messaging application Telegram. The advantage terrorists received from using this app is demonstrated in the investigation of the November Paris attacks. When the phone of one of the perpetrators was found near the Bataclan theatre, the police discovered that Telegram had only been installed seven hours before the attack. Due to the use of end-to-end encryption by Telegram, and the self-destruct feature of the app, the French police was unable to analyse what had been discussed by the terrorists via the application. As a result, no content from these messages was mentioned in the investigation report.[175]

Compared to the more public functions of the internet for terrorism, such as the dispersion of propaganda content, terrorists from ISIS relied on more secure methods of communications during a physical act of terrorism. However, ISIS also used the imagery of terrorist attacks as a form of propaganda content, for which it used more public services. As a result, a complex duality between more open and restricted services was created.

### 3.3.6 Cyberattacks

Whereas cyberattacks had not been a viable threat using the Web 1.0, this changed with the introduction of the Web 2.0. In this phase of the internet, multiple hacker groups allied themselves with terrorist organisations, including ISIS. The organisations made use of multiple of these groups at the same time, creating a semi-independent network of hackers. Many of these groups were headed by people who had enjoyed Western education but who had travelled to Syria to support ISIS.[176] Most prominent of these hacker collectives was a group called United Cyber Caliphate (UCC), which was created in 2016 as a merger of three smaller

[175] Robert Graham, ‘How Terrorists Use Encryption’, *CTCSentinel* 9 (2016) 6:20-25, here: 23.

[176] Dominika Giantas and Dimitrios Stergiou, ‘From Terrorism to Cyber-Terrorism: The Case of ISIS’, *SSRN Electronic Journal*, March 7, 2018, 9-12, https://dx.doi.org/10.2139/ssrn.3135927 (accessed May 5, 2020).

hacker groups. The UCC stands out among the other hacker groups of ISIS as it was "the most coordinated and essential actor in ISIS' cyber-terrorism" according to Giantas and Dimitrios.[177]

The first act of cyberterrorism claimed by the UCC was hacking the website of the Indonesian Embassy in France. Once the hackers had accessed the website, the members of the UCC deface the website's interface, by adding pictures of a fallen Eiffel Tower and a text stating:

> Now our fighting has come! We don't negotiate except with cannon, we don't have dialogues except with guns, we will not talk except strength. And we will not stop the fighting until we make Athan [call for prayer] and pray in Rome by Allah's will in a conquest, as a promise from Allah, and Allah does not break his promise.[178]

Whereas the audience of this specific cyberattack was limited, ISIS hackers also attacked roughly 19.000 French websites after the physical terrorist attack at the office of satirical newspaper Charlie Hebdo in 2015.[179] As a result of these attacks, some of these websites were inaccessible for a short time and others redirected users to websites with ISIS content, which impacted a way larger audience.[180]

Although these cyberattacks by ISIS should not be neglected, the more pressing attacks focussed on the hacking of government information. UCC gained notoriety by hacking into government databases and subsequently publishing the retrieved data on government and military officials as well as ordinary civilians in extensive "kill lists". These lists contained names, home addresses and IP addresses of over fifteen thousand individuals. These lists were published in Telegram group chats and called upon supporters to commit acts of terrorism against these individuals with phrases such as "shoot them down", "Kill them immediately. Enter [their] home and slay", and "Wanted to kill. KILL THEM ALL".[181] In some

[177] Ibid., 14.

[178] Laith Alkhouri, Alex Kassirer, and Allison Nixon, *Hacking for ISIS: The Emergent Cyber Threat Landscape* (n.p.: Flashpoint, Inc., 2016) 18.

[179] Andrew Griffin, 'Charlie Hebdo: France hit by 19,000 cyberattacks since Paris shootings in unprecedented hacking onslaught', *Independent*, January 15, 2015, https://www.independent.co.uk/life-style/gadgets-and-tech/news/charlie-hebdo-france-hit-by-19000-cyberattacks-since-paris-shootings-in-unprecedented-hacking-9980634.html (accessed May 5, 2020).

[180] Such attacks where websites are temporarily inaccessible as a result of the amount of data requests are more commonly known as distributed denial of service or DDoS-attacks.

[181] Giantas and Stergiou, 'From Terrorism to Cyber-Terrorism', 15-16.

instances, high-ranking members of governments from countries in the West were specifically targeted by these hackers of ISIS. Which was for example shown when in 2015 ISIS hackers temporarily had access to top-secret emails from senior members of the British government, including the Home Secretary Theresa May, discussing information on events that high-ranking members of the British government and royal family would attend. [182]

Whereas hacking websites and changing their interfaces was an addition to the more regular methods in which ISIS used the internet to spread propaganda, the cyberattacks against the personal information of citizens, military personnel and senior government officials were directly aimed at increasing the fear of ISIS in a society. In doing this, these cyberattacks became cyberterrorism. And although these cyberattacks in the name of ISIS did not cause any casualties or infrastructural disturbances,[183] it is unclear whether this will change in the future.

## 3.4 Notice and take down

Terrorists were not the only ones who increasingly used the internet to achieve their goals, as the use of the internet by counterterrorism agencies also increased in the Web 2.0 phase of the internet. When the use of the internet by terrorists increased from 2004 onwards, counterterrorism agencies initially struggled with how they should act. This terrorist 'battlefield' was new for counterterrorism agencies, and their operational structure had not yet been optimised for this, as was already shown in paragraph 2.4 which discussed the lack of counterterrorism actions against the Hofstad Network. In adapting to the new domain of terrorism, the counterterrorism agencies struggled with legislation that did not yet allow them to operate in this domain. Before 2012, government institutions were not allowed to take a website with terroristic content offline. This gradually changed from 2012 onwards, with the adoption of new legislation and counterterrorism agencies contacting the website's provider to shut it down.[184] Slowly, counterterrorism agencies adopted new strategies for dealing with the online activities of terrorists, which centred around notice and take down

[182] Keith Perry, 'ISIS hackers intercept top secret British Government emails in major security breach uncovered by GCHQ', *Mirror*, September 12, 2015, https://www.mirror.co.uk/news/uk-news/isis-hackers-intercept-top-secret-6428423 (accessed May 5, 2020).

[183] Giantes and Stergiou, 'From Terrorism to Cyber-Terrorism', 24.

[184] Edwin Bakker and Peter Grol, *Nederlandse Jihadisten. Van naïeve idealisten tot geharde terroristen* (Amsterdam: Hollands Diep, 2017) 121.

actions. This meant that counterterrorism institutions could get a court order that forced the provider of terrorist websites, to remove all content from a website or have it taken down. However, notice and take down approaches were only useful when the targeted provider of a website lived in the same country as the counterterrorism agency was located in. Because this is not always the case, due to the global nature of terrorism, and an international counterterrorism effort is needed, but this is still lacking.[185]

However, government institutions were not alone in combatting the online presence of ISIS. Multiple non-governmental groups, such as Ghost Security, were established with the sole goal of attacking ISIS websites and the social media accounts of jihadists.[186] Other groups and individuals used a different approach in which they tried to expose accounts that supported the message of ISIS or reported these accounts to the violations departments of social media platforms.[187] This shows that the Web 2.0 not only offered interactive and user-based opportunities to terrorists but also to individuals and groups who supported the counterterrorism of government agencies.

## 3.5 Conclusion

This analysis of the online activities of ISIS has shown that whereas ISIS still relied on offline means of operation, the internet was increasingly used for all six distinguished functions albeit in various degrees. Especially regarding the creation and distribution of propaganda content, ISIS benefited from the Web 2.0 phase of the internet. ISIS has shown to make effective use of the internet for spreading propaganda content, using publicly accessible social media platforms, such as Twitter, Facebook, VKontakte and Telegram. ISIS even created multiple professional media centres that were responsible for the creation and distribution of content. The real power of ISIS' online propaganda campaign was generated by the large number of followers who further distributed the organisation's messages. Additionally, ISIS greatly expanded the use of the internet for online training through the dissemination of digital

[185] Bartosz Kozłowski, 'Fighting ISIS Online: Is a co-regulatory system the most effective approach to fight ISIS online when using the NTD procedure', (Master thesis in Crisis and Security Management, Leiden University, 2018) 24.

[186] Giantas and Stergiou, 'From Terrorism to Cyber-Terrorism', 18.

[187] Rick Gladstone, 'Behind a Veil of Anonymity, Online Vigilantes Battle the Islamic State', *The New York Times*, March 24, 2015, https://www.nytimes.com/2015/03/25/world/middleeast/behind-a-veil-of-anonymity-online-vigilantes-battle-the-islamic-state.html?_r=1 (accessed May 13, 2020).

manuals and the use internet for financing, planning, execution and training purposes, using multiple internet platforms, both publicly accessible and restricted. ISIS immersed itself into the internet, being active on a plethora of websites, platforms, and other internet services. Combined with a sophisticated and professional approach, ISIS was able to reach a large, global audience.

This online ubiquity of ISIS was largely owed to the technological development of the Web 2.0. This new internet phase brought new users to the internet, increasing the potential audience of terrorists, with Twitter removing 235.000 ISIS-friendly accounts in the first half-year of 2016.[188] Additionally, user-based and user-created content was at the heart of ISIS' online presence. Online interactions between supporters of ISIS made it possible to distribute propaganda on a scale that had been unimaginable in the Web 1.0 phase of the internet.  As a result, it is with this Web 2.0 phase that the internet really took off as a new medium for terrorism and greatly impacted the nature of terrorism. By using visual content to reach a previously inaccessible audience of millions of individuals, while at the same time taking advantage of the more selective online platforms to target specific groups, ISIS fully exploited the technological opportunities of the Web 2.0 phase. This carried over to the online activities of terrorist networks that were active in the Web 3.0 phase of the internet, as the next chapter will show.

[188] Nicky Woolf, 'Twitter suspends 235.000 accounts in six months for promoting terrorism', *The Guardian*, August 18, 2016, https://www.theguardian.com/technology/2016/aug/18/twitter-suspends-accounts-terrorism-links-isis (accessed June 8, 2020).

# Lone actor terrorism and the Web 3.0

## 4.1 The ever-expanding internet

A new phase of the internet emerged in 2016: the Web 3.0.[189] Although this Web phase is set to continue for another five years, some of the effects it has had on the internet and terrorism can already be discussed. Compared to the previous phases of the web, the Web 3.0 focussed less on changes for the internet users and more on the technological structures at the back end of the internet. In doing so, the Web 3.0 aimed at "transforming the Web into a database, a move towards making content accessible by multiple non-browser applications, and the introduction of artificial intelligence technologies."[190] This Web phase therefore strove to create a 'semantic web', in which different sets of data could automatically be connected.[191] One of the online services that illustrated the advantages of such technological development was Microsoft's PhotoSynth. This discontinued application analysed digital photographs of multiple users and combined them to generate three-dimensional models of buildings and landscapes. The main difference between the Web 3.0 and Web 2.0 is therefore that the Web 2.0 focusses on the agency of the humans who made us of the internet, whereas the Web 3.0 centres on automatic and autonomous processes.[192]

Although the Web 3.0 thus focusses on the technology underlying the internet, this new phase also impacted internet users and therefore terrorists. New features, such as Artificial Intelligence (AI) services and virtual assistants (like Apple's Siri, Google Assistant and Amazon's Alexa) were introduced to the internet to make it a more connected, comprehensive and smarter system.

The way in which internet users accessed the internet also changed in the last few years owing to the introduction of new 'smart' devices that are connected to the internet and offer new opportunities. Yet, these devices were not always useful for terrorist purposes and most smartphones, tablets and computers remained the most popular in the West.[193] Internet-

[189] Naik and Shivalingaiah, 'Comparative Study of Web 1.0, Web 2.0 and Web 3.0', 503.

[190] Ibid., 505.

[191] *W3C*, 'W3C Semantic Web Frequently Asked Questions', November 12, 2009, https://www.w3.org/RDF/FAQ (accessed May 14, 2020).

[192] Aghaei, Nematbakhsh, and Farsani, 'Evolution of the World Wide Web: From Web 1.0 to Web 4.0', 6.

[193] See for example: *Statista*, 'Which is the most important device you use to connect to the internet, at home or elsewhere?', April 2019, https://www.statista.com/statistics/387447/consumer-electronic-devices-by-internet-access-in-the-uk/ (accessed May 14, 2020).

connected devices were used by a total of 3.4 billion worldwide users in 2016, with countries in the West having particular high percentages of internet users among its population.[194]

Whereas the Web 3.0 offered new technologies to terrorists to use on the internet, the following analysis of the internet's use by Far-Right terrorists will show that both the Web 2.0 and Web 3.0 were interchangeably used by these terrorists.

## 4.2 Right-wing terrorism

According to David Rapoport's four waves theory on modern terrorism, the world is currently experiencing the last few years of the Religious Wave.[195] At the same time, a new terrorist threat slowly emerged with attacks from far-right individuals in places like El Paso, Christchurch, and Halle. Whereas the perpetrators of these attacks were all seen as far-right terrorists, this political conviction is rather diverse and is constituted of multiple right-wing ideologies, including fascism, antisemitism, national-socialism, white supremacy, nationalism and alt-right.[196] As a result, far-right terrorism was directed at individuals with multiple diverse backgrounds. However, most of these subcategories of the far-right have a shared understanding of the themes of the White Race, political climate, and the threat to Europe and European culture by invaders[197] and aim at the creation of a nationalist/fascist regime.[198]

In recent years, the threat of far-right terrorists has grown in the West, with an increase in far-right attacks of 320 per cent in the last five years.[199] However, far-right terrorism was not a new phenomenon. During the wave of New Left terrorism between the 1960s and 1990s, right-wing terrorist organisations were created to counter left-wing narratives. Especially in Italy, during the *Anni di piombo* (Years of Lead) of 1968-1982, multiple terrorist attacks were committed by far-right terrorist groups, like the fascist Ordine Nuovo and neo-Nazi Avanguardia Nazionale.[200] However, from the 1990s onwards, attention shifted to Islamic

[194] Roser, Ritchie, and Ortiz-Ospina, 'Internet'.

[195] Rapoport, 'The Four Waves of Modern Terrorism', 61-65.

[196] Stefan Aubrey, *The New Dimension of International Terrorism* (Zürich: VDF Hochschulverlag AG, 2004) 45.

[197] Jacob Ware, 'Testament to Murder: The Violent Far-Right's Increasing Use of Terrorist Manifestos', ICCT policy brief (The Hague, 2020) 4.

[198] Aubrey, *The New Dimension of International Terrorism*, 45.

[199] *Vision of Humanity*, 'Far-right attacks in the West surge by 320 per cent', n.d., http://visionofhumanity.org/global-terrorism-index/far-right-attacks-in-the-west-surge-by-320-per-cent/ (accessed May 14, 2020).

[200] Beatrice de Graaf, *Theater van Angst. De strijd tegen terrorisme in Nederland, Duitsland, Italië en Amerika* (Amsterdam: Boom, 2010) 101.

terrorism and far-right terrorism's prominence decreased.[201] It gained renewed attention in the 2010s, with an attack by Norwegian far-right terrorist Anders Breivik in Oslo and on the small island of Utøya.

The new attacks by far-right terrorists were mostly committed by lone actor individuals. Lone actor terrorism, also known as lone wolf terrorism, is defined by Gabriel Weimann as:

> A lone wolf is an individual or a small group of individuals who uses traditional terrorist tactics – including the targeting of civilians – to achieve explicitly political or ideological goals, but who acts without membership in, or cooperation with, an official or unofficial terrorist organization, cell, or group.[202]

As a result of their position as outsiders, these lone wolves experienced no social constraints and could therefore be more creative and innovative in their attacks.[203] Due to this lack of a social environment, online interaction was extremely influential in the creation of a personal ideology of grievances for far-right lone wolves.[204] Lone wolf terrorism is however not limited to the far-right but has also been used as a tactic by terrorists motivated by other ideologies, such as left-wing and Islamic terrorists. However, compared to other groups, lone-actor terrorism is most prominent with far-right terrorists.[205] But despite the popularity of lone actor terrorism, far-right terrorists were still united in a community of like-minded individuals. For instance, in his manifesto, *2083: A European Declaration of Independence*, Breivik stated that he was part of a large organisation called the 'Pauperes commilitones Christi Templique Solomonici'.[206] The Norwegian intelligence services could however not find any evidence for this claim.[207] Whereas some far-right groups that met in person existed, most far-right communities were virtual communities which used the internet to stay connected.

[201] Florian Hartleb, *Lone Wolves. The New Terrorism of Right-Wing Single Actors* (Basel: Springer Nature Switzerland AG, 2020) 1.

[202] Gabriel Weimann, 'Lone Wolves in Cyberspace', *Journal of Terrorism Research* 3 (2012) 2: 75-90, here: 75.

[203] Jeffrey Simon, *The Alphabet Bomber. A Lone Wolf Terrorist ahead of his time* (Lincoln, Nebraska: University of Nebraska Press, 2019) 172.

[204] Peter Neumann, 'Kaum ein Terrorist ist ein einsamer Wolf', *NTV*, October 14, 2016, https://www.n-tv.de/politik/Kaum-ein-Terrorist-ist-ein-einsamer-Wolf-article18854546.html (accessed May 16, 2020); Hartleb, *Lone Wolves*, 47.

[205] Hartleb, *Lone Wolves*, 7-10.

[206] This was the official name of the Knights Templar, a prominent catholic military order that took part in the Crusades but was dissolved in 1312.

[207] Anders Breivik, '2083: A European Declaration of Independence', (online distributed manifesto, 2011), https://info.publicintelligence.net/AndersBehringBreivikManifesto.pdf (accessed May 15, 2020).

These virtual communities were present on different anonymous platforms, most prominently imageboard websites such as Reddit, 4Chan and 8Chan, and websites like DailyStormer.su and altright.com, far-right individuals communicated with like-minded people. Between them, different types of far-right content, including memes[208] and deepfake videos[209] from a radical nature were shared and discussed. These communities functioned as "echo chambers" in which arguments were not met by counterarguments but were amplified by a reverberation effect.[210] This internet culture has been extremely important for far-right terrorists as will be shown in the analysis below.

## 4.3 An online community

### 4.3.1 Propaganda

Because of their previously established preference for lone-actor terrorism, most far-right terrorists did not aim at recruiting new members, as they operated alone. However, they did call upon others to follow their examples and commit terrorist attacks. Online, some radical individuals acted as recruiters and tried to persuade sympathisers to join their radical perception of the world. To achieve this, the far-right 'weaponised' and claimed internet culture references ranging from Japanese anime and singer-songwriter Taylor Swift, to cult films and books such as *Fight Club* and George Orwell's *1984*.[211] The radicalisation process itself was referred to as 'redpilling' by the far-right, which in itself is a reference to the 1999 movie *The Matrix* in which a character tells the protagonist: "You take the blue pill, the story ends. […] You take the red pill, you stay in Wonderland, and I show you how deep the rabbit hole goes." Far-right individuals saw this as a metaphor for the unpleasant reality that the world was to them.[212] Despite the lack of a demarcated group and a well-defined ideology, redpilling was a clear form of radicalisation for the far-right.

[208] Defined by the Oxford English Dictionary as: "An image, video, piece of text, etc., typically humorous in nature, that is copied and spread rapidly by internet users, often with slight variations." *Oxford English Dictionary*, 'Meme, *n*.', n.d., https://www-oed-com.proxy.library.uu.nl/view/Entry/239909?redirectedFrom=meme#eid (accessed May 16, 2020).

[209] Deepfakes videos are videos that have been edited to replace a person in the video with the likeness of somebody else.

[210] Sanne Geeraerts, 'Digital radicalization of youth', *Social Cosmos* 3 (2012) 1: 25-32, here: 26.

[211] Julia Ebner, *Going Dark. The Secret Social Lives of Extremists* (London: Bloomsbury, 2020) 21; 41-42.

[212] Ebner, *Going Dark*, 20.

Although the internet offered them a potential audience of millions, propaganda by far-right terrorists was mostly directed at a small and selective group of like-minded people. Similar to terrorists the terrorists of ISIS, far-right individuals were active on the more popular social media platforms, such as Twitter and Facebook, on which they expressed their worldviews in restricted groups.[213] However, far-right individuals also explored new platforms, including imageboard website. These interactive multimedia websites were rather similar to the for a used by terrorists in the Web 1.0 but allowed users to post their messages anonymously and defended the posted content by referring to the freedom of speech. This, combined with the non-hierarchical relations between users, attracted many radicals.[214] Well-known imageboard websites on which far-right individuals were active include Reddit, 4Chan and the more radical 8Chan (later 8kun).[215] Furthermore, far-right terrorists were also in contact with others through the chats and servers of videogames, primarily first-person shooters (FPS) games.[216] Terrorists from all ideological backgrounds have a long history with FPS, but the far-right has expanded on this with a high notion of gamification, but this will be discussed further in paragraph 4.3.5.[217] By narrowcasting their propaganda on these lesser-known platforms, far-right terrorists could tailor their content to specific groups or individuals with whom the message would resonate.

The content that was distributed on these platforms also assumed new forms. Whereas the previous chapter has shown that ISIS gained notoriety through its videos of beheadings, far-right content centred around edited images and videos containing inside jokes, transgressive humour, and irony. This increased the appeal of the far-right ideology among young people.[218] Especially memes and deepfakes supporting far-right ideas and concepts were shared frequently. Memes are images or short videos with a humorous nature that can easily be edited to reflect certain worldviews. Deepfakes can be on the other hand be

[213] Imogen Richards, 'A Dialectical Approach to Online Propaganda: Australia's United Patriots Front, Right-Wing Politics, and Islamic State', *Studies in Conflict & Terrorism* 42 (2019) 1-2: 43-69, here: 45.

[214] Angela Nagle, 'Paleocons for porn', *Jacobin*, February 22, 2017, https://www.jacobinmag.com/2017/02/paleocons-for-porn (accessed May 17, 2020).

[215] Christopher Knauw, ''A perfect platform': Internet's abyss becomes a far-right breeding ground', *The Guardian*, March 19, 2019, https://www.theguardian.com/world/2019/mar/19/a-perfect-platform-internets-abyss-becomes-a-far-right-breeding-ground (accessed May 17, 2020).

[216] See for example: Ahmed Al-Rawi, 'Video games, terrorism, and ISIS's Jihad 3.0', *Terrorism and Political Violence* 30 (2018) 4: 740-760.

[217] Michael Hitchens, Bronwin Patrickson, and Scherman Young, 'Reality and Terror, the First-Person Shooter in Current Day Settings', *Games and Culture* 9 (2014) 1:3-29, here: 19-21.

[218] Ebner, *Going Dark*, 16.

described as extremely realistic fake videos that have been adjusted using artificial intelligence.[219] By using artificial intelligence, these deepfakes made use of new technologies benefitting from the Web 3.0. These deepfake videos and memes by far-right radicals often contained anti-Semitic, anti-Muslim, and xenophobic messages intended to create a shared understanding of an outsider group.[220]

This content was targeted at an audience of like-minded individuals, which results in the online platforms acting as "echo chambers". No counterarguments were presented in these communities and members spiralled into radicalisation. This was further enhanced by the computer-generated algorithms that were integrated into online services, such as YouTube's recommendations section which suggested more radical videos to viewers after watching videos on political issues.[221]

In addition to radicalisation purposes, propaganda was also used to incite others to commit terrorist attacks. In the case of far-right terrorism, this was done through the publication and distribution of manifestos shortly before an act of terrorism was committed, in which the perpetrator calls onto others to follow his example and commit terrorist attacks themselves. Anders Breivik's document of over fifteen hundred pages titled *2083: A European Declaration of Independence*, is one of the most well-known examples. Breivik initially tried to email this document to 8,109 radical far-right activists whose email addresses he had collected via Facebook, but his email server only allowed him to send one thousand e-mails, due to the limits of a spam filter. However, his manifesto quickly became available to the public via hyperlinks on other platforms such as Twitter.[222] In this manifesto, Breivik explained his worldview and actions and called onto others to follow his example by stating:

> "It is not only our right but also our duty to contribute to preserve our identity, our culture and out national sovereignty by preventing the ongoing Islamisation. There is no Resistance Movement if individuals like us refuses to contribute…"[223]

[219] Peter Daou, *Digital Civil War: Confronting the Far-Right Menace* (London: Melville House, 2019) 60.
[220] Marc Tuters and Sal Hagen, '(((They))) rule: Memetic antagonism and nebulous othering on 4chan', *New Media & Society* (November 2019), 1-20, here: 15-16.
[221] Harwood, 'Terrorism and the digital right-wing', 60.
[222] Hartleb, *Lone Wolves*, 83.
[223] Breivik, '2083: A European Declaration of Independence', 15.

This call to arms was answered by other far-right terrorists, who in turn published their own manifestos, such as Brenton Tarrant who committed the Christchurch mosque attacks of 2019. The inspiring effect these documents have had on other far-right radicals is clearly shown by the fact that these manifestos often directly refer to the works and actions of previous terrorists. In his manifesto, titled *The Great Replacement*, Tarrant, for example, states that he decided on the attack himself, but that he had contacted the "reborn Knights Templar" for a blessing.[224] This referred to the group that Breivik claimed to be a part of in his manifesto. Furthermore, in the first line of the manifesto published by Patrick Crusius, the perpetrator of the El Paso shooting, Crusius writes that he supported the Christchurch shooter and his manifesto. Additionally, he states that Tarrant's manifesto convinced him to target Hispanics.[225] This shows that such manifestos directly incited others to commit similar acts of terrorism and whereas the documents were originally narrowcasted on platforms with like-minded individuals, they were quickly shared outside these domains and became publicly available.

### 4.3.2 Finance

Evidence for specific uses of the internet by far-right terrorists to gain financial resources could not be found. Like the attack on Van Gogh by a member of the Hofstad Network, acts of terrorism by lone wolves do not require financial support. Due to the small scale of the operations and the lack of an overarching organisation that required financial stability, far-right lone wolves did not need the internet to gain financial assets. Multiple far-right terrorists even had debts when they committed their attack. Which was for example the case with Frank Steffen, who stabbed a candidate for mayor in Cologne, Germany in 2015, whose financial situation and unemployment were important drivers for his act.[226]

There are however exceptions to this, as Brenton Tarrant stated that he had acquired a fortune through his investments in the cryptocurrency Bitconnect in 2016.[227] Whereas

[224] Brenton Tarrant, 'The Great Replacement', (online distributed manifesto, 2019), 10, https://commons.wikimannia.org/images/Tarrant_Brenton_-_The_Great_Replacement.pdf (accessed May 17, 2020).
[225] Patrick Crusius, 'The Inconvenient Truth', (online distributed manifesto, 2019), https://grabancijas.com/patrick-crusius-manifesto-the-inconvenient-truth/ (accessed May 17, 2020).
[226] Ibid., 68.
[227] Hartleb, *Lone Wolves*, 86.

cryptocurrencies had already been used by terrorists of Islamic States in previous years, this financial system' blockchain technology was based on early Web 3.0 technologies. Tarrant did however not invest in the cryptocurrency to fund his terrorist attack. Instead, he used the acquired money to fund his travels to other countries, as well as donated over two thousand euros to the Austrian and French chapters of the far-right Identitarian Movement.[228]

It should also be noted, concerning the focus of this thesis on the connection between the internet and terrorism, that Breivik financed his acts of terrorism in 2011 with revenue he made from a digital software company. This business was quite successful but went bankrupt as a result of the Financial crisis of 2008. Despite his company going under, Breivik revealed that he had forty thousand euros at his disposal on multiple offshore accounts prior to his attack.[229] This shows that whereas financial support was not required for attacks by far-right terrorists, some perpetrators were familiar with online banking and digital financial systems, yet funding their forthcoming attacks was only an indirect use for this.

### 4.3.3 Training

Whereas the publication of training manuals was prevalent with the terrorists of ISIS in the Web 2.0 phase of the internet, far-right terrorists of the Web 3.0 relied on other media to instruct others. In their manifestos, they not only explained the motives for their acts to incite others, but these texts also contained information on the preparations of the subsequent attack. Breivik, for instance, dedicated 108 pages of his manifesto to instructions for others.[230] Consequently, these manifestos also acted as online instruction manuals for other terrorists.

Far-right terrorists also played videogames as a form of training. Breivik specifically mentioned first-person shooter (FPS) videogames, such as *Call of Duty Modern Warfare*, as a good simulation for target practice.[231] After his arrest, he told the court that he even used a holographic aiming device for a more realistic experience while playing these games.[232] This method of training was adopted by many far-right terrorists, with the perpetrator of the 2016

[228] Reuters, 'Suspected New Zealand attacker donated to Austrian far-right group, officials say', *NBCnews*, March 27, 2019, https://www.nbcnews.com/news/world/new-zealand-attacker-linked-austrian-far-right-group-officials-n987846 (accessed May 17, 2020).
[229] Breivik, '2083: A European Declaration of Independence', 1380-1384.
[230] Ibid., 848-956.
[231] Ibid., 908.
[232] Helen Pidd, 'Anders Breivik 'trained' for shooting attacks by playing Call of Duty', *The Guardian*, April 19, 2012, https://www.theguardian.com/world/2012/apr/19/anders-breivik-call-of-duty (accessed May 18, 2020).

Munich shooting even clocking over four thousand hours on the game *Counter-Strike* before his attack.[233] Whereas the impact of violent games on individuals is a hotly debated subject,[234] Tarrant clearly states in his manifesto that the videogame Fortnite trained him to be a killer.[235] This shows that FPS videogames therefore became a new online medium used by far-right terrorists for training opportunities.

However, videogames did not become the primary means of training for a far-right terrorist. Physical training remained at the top of the lists of far-right terrorists, with Breivik stating that sympathisers should "try to get some practice with a real assault rifle (with red point optic) if possible."[236] Both Breivik and Tarrant also acquired gun permits through legal channels and could therefore train with the weapons they would later use in their attacks without suspicion.[237]

This paragraph has shown that whereas far-right terrorists found new online mediums to train in preparation for their terrorist attacks, physical training was not abandoned. This was likely a result of the efforts by counterterrorism agencies to better monitor terrorist(-like) behaviour online, and the need of the terrorists to remain undiscovered. This will further be discussed in paragraph 4.4 focusing on the counterterrorism measures in this phase of the internet.

### 4.3.4 Planning

Tracking the planning activities of far-right terrorists on the internet is a difficult task. Most terrorists tried to stay under the radar by deliberately limiting their communications with others.[238]  However, this did not mean that they were completely shut off from the internet while preparing for a terrorist attack. As examined in the paragraph above, the online

[233] Isaac Kfir, 'Gaming platforms – a breeding ground for violence?', *Policy Forum*, October 10, 2019, https://www.policyforum.net/gaming-platforms-a-breeding-ground-for-violence/ (accessed May 17, 2020).

[234] See for example: Raul Ramos, Christopher Ferguson, and Kelly Frailing, 'Violent Entertainment and Cooperative behavior: Examining Media Violence Effects on Cooperation in Primarily Hispanic Sample', *Psychology of Popular Media Culture* 5 (2016): 119-132.

[235] Tarrant, 'The Great Replacement', 17.

[236] Breivik, '2083: A European Declaration of Independence', 908.

[237] Hartleb, *Lone Wolves*, 89.

[238] Lasse Lindekilde, Francis O'Connor, and Bart Schuurman, 'Radicalization patterns and modes of attack planning and preparation among lone-actor terrorists: an exploratory analysis', *Behavioral Sciences of Terrorism and Political Aggression* 11 (2019) 2: 113-133, here: 120.

manifestos of far-right terrorists already contained instructions on preparing for a terrorist attack.  But these instructions also dealt with other aspects of the preparatory phase.

Breivik, for instance, stated that terrorists should plan on how they would distribute the message of their attacks. As manifestos were the most popular form of propaganda, the internet was extensively used by far-right terrorists to research different topics to be included in these documents. Breivik spent a total of nine years preparing for his act of terrorism, of which three years were dedicated to compiling his manifesto of 1515 pages. While this document represents his personal ideology of grievances, many parts of the text were copied from other online sources. Some paragraphs were even directly copied and pasted from the manifestos of other far-right terrorists.[239] The personal ideology of grievances that was constructed through the use of selected resources recurred in the manifestos of many far-right terrorists, as Tarrant for example mentions that he had read the writings of other far-right terrorists, such as Dylan Roof Breivik and supported the visions of Luca Traini, Anton Lundin Pettersson, Darren Osbourne.[240] This shows that while preparing for their attacks, far-right terrorists used the internet to access information for writing their manifestos.

Another use of the internet by far-right terrorists in the preparatory stage was finding information on the targets and locations of their forthcoming terrorist attacks. Crusius decided to target Hispanics after reading Tarrant's manifesto, whereas he did not have a specific target in mind before.[241] The far-right perpetrator of the assassination of British Labour MP Jo Cox in 2016 had meticulously researched information on his target online.[242] Tarrant even explained that he initially wanted to target a mosque in Dunedin after seeing a video of it on Facebook.[243] He however switched the location of his attack after a visit to the mosques in Christchurch, which had a higher number of attendees and a more iconic and Islamic architecture, which he suspected would result in a bigger impact of his attack.[244]  This indicates that whereas the internet was accessed to find information on locations and targets, offline reconnaissance was still highly influential for the final decision.

[239] Hartleb, *Lone Wolves*, 83.
[240] Tarrant, 'The Great Replacement', 18.
[241] Crusius, 'The Inconvenient Truth'.
[242] Ian Cobain, Nazia Parveen, and Matthew Taylor, 'The slow-burning hatred that led Thomas Mair to murder Jo Cox', *The Guardian*, November 23, 2016, https://www.theguardian.com/uk-news/2016/nov/23/thomas-mair-slow-burning-hatred-led-to-jo-cox-murder (accessed May 18, 2020).
[243] Tarrant, 'The Great Replacement', 18.
[244] Idem.

Furthermore, the internet was also used by Tarrant to acquire the weapons used in his attack. Shortly after receiving a firearms licence in New Zealand, Tarrant bought four guns and the necessary ammunition online.[245] Crusius and Breivik acquired their guns legally as well, albeit from offline retailers.[246] Their legal possession of these weapons was only possible due to the inconspicuousness of these individuals both online and offline, as they did not possess a criminal record that prevented them from owning a gun. Whereas these three terrorists had legal gun permits, other far-right extremists relied on the deep web to acquire weapons. The required URL's to these illegal markets were shared between far-right users on previously mentioned platforms such as 8chan.[247]

In the preparatory phase, far-right terrorists mainly used the internet for acquiring information on targets and locations and researching topics for their manifestos. Additionally, weapons for terrorist attacks could be purchased online, both lawful and illegally. This paragraph has shown that whereas the technologies underlying the internet developed, one of the primary uses of the internet for terrorists remained the accessing of (publicly available) information that could be used to plan an act of terrorism.

### 4.3.5 Execution

Because of the individual nature of lone wolf operatives from the far-right, there was no communication with others during acts of terrorism. Despite this lack of online communication, the internet was extensively used in the execution of such acts for other purposes.

Just before an act of terrorism was committed, far-right terrorists announced the event online. Minutes before his attack, Breivik sent out a cryptic tweet stating that "One person with a belief is equal to the force of 100,000 with merely interests".[248] Similarly, 45 minutes before the El Paso attack, an anonymous user posted a statement on 8chan in which he

[245] Rachel Pannett, Rob Taylor, and Rhiannon Hoyle, 'New Zealand Shootings: Brenton Tarrant Bought Four Guns Legally Online', *The Wall Street Journal*, March 18, 2019, https://www.wsj.com/articles/australian-police-raid-two-homes-in-hunt-for-clues-on-brenton-tarrant-11552872377 (accessed May 19, 2020).

[246] Jack Healy and Sarah Mervosh, 'El Paso Suspect Ordered Gun and Moved Out in Weeks Before Attack', *The New York Times*, August 8, 2019, https://www.nytimes.com/2019/08/08/us/el-paso-suspect.html? (accessed May 19, 2020); Hartleb, *Lone Wolves*, 82.

[247] Maura Conway, Ryan Scrivens, Logan Macnair, 'Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends', ICCT Policy Brief (The Hague, 2019) 16.

[248] Hartleb, *Lone Wolves*, 1-2.

mentions an attack and the possibility that he would die that day. Attached to the post was a four-page manifesto, signed by Patrick Crusius.[249] The most daring of these announcements was the distribution of Tarrant's manifesto fifteen minutes before his act via email. One of the recipients of this email was namely the office of New Zealand's Prime Minister, Jacinda Ardern.[250] Informing the others, especially government officials, on the attack that is about the happen seems unwise. This was however essential to lone-actor terrorism, as perpetrators could not rely on other members of their terrorist group to distribute the reasoning behind the attack. Whereas Breivik urged others to carry physical copies of their announcements on them during their attacks, he also emphasised the importance of publishing the announcement online, as to prevent counterterrorism agencies from discrediting these texts.[251] Additionally, the online publication of such documents just before an attack was committed, the perpetrator and author assured himself of an audience for his attack.

Furthermore, right-wing terrorists also utilized Web 3.0 livestreaming functions that had been incorporated in digital platforms, such as Facebook and YouTube, and specific livestreaming services such as Twitch, to directly show their attack to a live audience. While driving towards the Al Noor Mosque in Christchurch, Tarrant activated an action camera attached to his helmet. The video captured by this device was livestreamed directly to Facebook for over seventeen minutes before being removed by the platform. Stephan Balliet also livestreamed his attack on a synagogue in Halle, Germany, via streaming platform Twitch. According to Jason Burk, the point of such livestreamed attacks was not to kill Jews or Muslims, "but to make a video of someone killing Muslims [and Jews]."[252]

These livestreams contributed to the increasing resemblance between terrorism and videogames, a process referred to as the gamification of terrorism. By mounting the camera on his helmet, Tarrant's live stream resembled a first-person shooter game, such as *Call of Duty*. Furthermore, the manifesto of Stephan Balliet, the perpetrator of the Halle synagogue

[249] Evans, 'The El Paso Shooting and the Gamification of Terror'.
[250] Macklin, 'The Christchurch Attacks: Livestream Terror in the Viral Video Age', 18.
[251] Breivik, '2083: A European Declaration of Independence', 924.
[252] Jason Burk, 'Technology is terrorism's most effective ally. It delivers a global audience', *Guardian*, March 17, 2019, https://www.theguardian.com/commentisfree/2019/mar/17/technology-is-terrorisms-most-effective-ally-it-delivers-a-global-audience (accessed June 7, 2020).

attack in 2019, included a list of 'achievements', similar to videogames.[253] Whereas terrorism was often referred to as a theatre, it has slowly changed into terrorism as a game according to Graham Macklin.[254] This gamification is not merely a reference to popular culture, but structures reality for both perpetrators and sympathisers of far-right terrorist attacks. Breivik, for instance, recalled how it felt like he became his on-screen character during his act of terrorism. Moreover, Balliet, Crusius, and Tarrant all adopted visual styles found in first-person shooters for their terrorist attacks.[255] Tarrant even picked background music for his livestream that was popular with far-right extremists.[256] The audience of these terrorists also contributed to the gamification of terrorism, as, for example, a man from New Zealand edited crosshairs onto the video of Tarrant's terrorist act to make the livestream resemble a videogame even more.[257] Furthermore, sympathisers of far-right terrorist attacks compared the number of victims from one terrorist attack with other terrorist attacks, speaking of "beating the highscore".[258] Whereas Tarrant was praised for the high number of casualties he had caused, the perpetrators of far-right terrorist attacks with limited numbers of casualties, such as the perpetrator of the Poway Synagogue shooting in 2019, were on the other hand ridiculed by their online audience.[259]

The gamification of terrorism was however not limited to far-right terrorism, as references to gaming culture have also been made by Islamic terrorists in the past, albeit on a small scale compared to far-right terrorists.[260] Although gamification of terrorism had already been present in the Web 2.0 phase of the internet, it increased in the Web 3.0 phase due to the emergence of new technologies, such as livestreaming, that could quickly be adapted and distributed. Moreover, the gamification of terrorism built upon the visualisation

[253] Stephan Balliet, 'Manifest', (online distributed manifesto), October 9, 2019, https://www.docdroid.net/oEfJ0a3/manifesto-pdf (accessed May 27, 2020).
[254] Macklin, 'The Christchurch Attacks: Livestream Terror in the Viral Video Age', 19.
[255] Linda Schlegel, 'Can You Hear Your Call of Duty? The Gamification of Radicalization and Extremist Violence', *European Eye on Radicalization*, March 17, 2020, https://eeradicalization.com/can-you-hear-your-call-of-duty-the-gamification-of-radicalization-and-extremist-violence/ (accessed May 28, 2020).
[256] Robert Evans, 'The El Paso Shooting and the Gamification of Terror', *Bellingcat*, August 4, 2019, https://www.bellingcat.com/news/americas/2019/08/04/the-el-paso-shooting-and-the-gamification-of-terror/ /(accessed May 17, 2020).
[257] Hartleb, *Lone Wolves*, 2.
[258] Evans, 'The El Paso Shooting and the Gamification of Terror'.
[259] Conway, Scrivens, and Macnair, 'Right-Wing Extremists' Persistent Online Presence', 13.
[260] Schlegel, 'Can You Hear Your Call of Duty?'.

of terroristic content that arose in the Web 2.0 phase with the prominence of livestreaming and the appropriation of visual styles from videogames in terrorist attacks.

### 4.3.6 Cyberattacks

In a 1999 report by the Center for the Study of Terrorism and Irregular Warfare, the prospects and implications of cyberterrorism were analysed. From this analysis, the authors concluded that only religiously inspired terrorist groups were likely to seek the capacity to inflict massive damage via a cyberattack. Additionally, the report specifically stated that "it is unlikely that far-right extremists will desire cyberterrorism", as they lack the incentives, means and financial capability to set up such complicated attacks.[261]

Whereas this conclusion seemed to be correct as no major cyberattacks by the far-right were committed, spontaneously coordinated mass mobilisation of far-right sympathisers online did occur in multiple instances.[262] Such organised actions often took the shape of trolling and distributing fake news.

Internet trolls referred to individuals who tried to provoke an online community through inflammatory messages. Whereas internet trolls were not limited to far-right sympathisers, troll culture was an essential part of the online presence of the far-right.[263] Trolling is not a crime in itself but took the shape of online harassment in some instances, which is a form cybercrime

Far-right sympathisers were also connected to the publication and distribution of fake news. Recently, the far-right has capitalized on the Corona Pandemic by "promoting conspiracy theories, scapegoat refugees, and advance the argument for closed borders."[264] Such articles with disinformation served as propaganda and aimed at convincing others of the dangers for which the far-right has warned, like the replacement of the white race and the threats of Islam and Judaism.

[261] Bill Nelson et al., 'Cyberterror: Prospects and Implications', Report for the Intelligence Agency Office for Counterterrorism Analysis (Monterey, California: Center for the Study of Terrorism and Irregular Warfare of the Naval Postgraduate School, 1999) 72-74.

[262] Evan Malmgren, 'Don't Feed the Trolls', *Dissent* 64 (2017) 2: 9-12, here: 9.

[263] Edwin Hodge and Helga Hallgrimsdottir, 'Networks of Hate: The Alt-right, "Troll Culture", and the Cultural Geography of Social Movement Space Online', *Journal of Borderlands Studies* (February 2019): 1-18, here: 13.

[264] Gabriel Weimann and Natalie Masri, 'The Virus of Hate: Far-Right Terrorism in Cyberspace', report for the International Institute for Counter-Terrorism (Herzliya, March 5, 2020) 12.

To promote such fake news content, supporters often utilize software applications that controlled internet bots. These were online accounts that were partly or fully controlled by computer algorithms and interacted with human users. Bot software could be harmless and beneficial in certain situations, but far-right sympathisers aimed at manipulating human behaviour and public discourse with these bots.[265] The use of algorithms by far-right sympathisers was not possible in the Web 1.0 and Web 2.0 phases of the internet and is therefore a clear example of the impact the Web 3.0 had on the online activities of terrorists.

## 4.4 Automated counterterrorism

Terrorists were not the only ones impacted by the technological developments of the Web 3.0. Counterterrorism efforts by both government agencies and the companies behind online platforms also benefited from the technologies of this phase of the Web. New computer algorithms were used by government counterterrorism agencies to flag and monitor terrorist activities on the internet. The Dutch intelligence legislation of 2017 specifically states that the intelligence and security services, including the Dutch counterterrorism agency, are allowed to make use of "automated processes" for gathering and analysing online communications.[266] Such automated algorithms proved extremely useful to counterterrorism agencies as they enabled to map the structures of terrorist networks.[267] Furthermore, international conferences and summits were held to create an international policy to counteract the online activities of terrorists. The most recent of these conferences was the Christchurch Call Summit on May 15, 2019. Initiated by New Zealand and France, a total of 48 countries signed an international agreement on addressing online extremism content at this summit. Alongside these countries, eight online service providers, including Amazon, Facebook, Google, Microsoft, and Twitter were signatories to this pact.[268]

[265] Kai-Cheng Yang et al., 'Arming the public with artificial intelligence to counter social bots', *Emerging Technologies: Perspectives from Technology Pioneers*, special issue, *Human Behaviour and Emerging Technologies* 1 (2019) 1: 48-61, here: 48.

[266] Wet op de Inlichtingen- en Veiligheidsdienst 2017, paragraph 3.2.5, January 1, 2020, https://wetten.overheid.nl/BWBR0039896/2020-01-01 (accessed May 31, 2020).

[267] Leslie Ball and Matthew Craven, 'Automated Counter-Terrorism', poster paper presented at the European Intelligence and Security Informatics Conference (Uppsala 2013).

[268] *Christchurch Call*, 'Supporters', n.d., https://www.christchurchcall.com/supporters.html (accessed May 31, 2020).

During the Web 3.0 phase the role of these and other online service providers for countering terrorist activities on their platforms expanded. Because these online platforms were owned by companies instead of states, government counterterrorism agencies had no authority here. As a result, the companies behind these services were tasked with removing terroristic content on their platforms. All users of online platforms accepted certain codes of conduct in which the creation and distribution of terroristic content are prohibited. Online service providers were therefore constantly analysing the content published on their platforms to take such content down as quickly as possible and delete or suspend the accounts of these users. Research by Berger and Perez shows that these counterterrorism efforts by companies were effective, as counterterrorism measures by Twitter led to a 25 per cent decline in the number of terrorist accounts over time.[269] More recently Facebook followed this example and removed approximately 190 accounts of far-right extremists.[270] Twitter also implemented a fact-checking policy to counter fake news.[271] Whereas far-right terrorists were mostly active on anonymous platforms on which suspensions of accounts was not possible, counterterrorism efforts still impacted their use of the internet. After the El Paso shooting, a cybersecurity company that had been protecting the popular far-right platform 8Chan, ended its services for the platform and within a few minutes multiple cyber-attacks rendered the website unavailable.[272]

Lastly, new technologies enabled individual citizens to protect themselves from terroristic propaganda. To counter the activities of bots, software, like Botometer, could be downloaded to detect the activities of bots.[273]

This paragraph showed that automated counterterrorism processes were used by government institutions, online service providers and individual internet users alike. This would not have been possible without the technological developments of the Web 3.0. As a

[269] J.M. Berger and Heather Perez, ‘The Islamic State’s Diminishing Returns on Twitter: How suspensions are limiting the social networks of English -speaking ISIS supporters’, occasional paper for the Program on Extremism (Washington D.C.: Georgetown University, 2016) 4.

[270] David Klepper, ‘Facebook removes nearly 200 accounts tied to hate groups’, *ABCNews*, June 6, 2020, https://abcnews.go.com/Business/wireStory/facebook-removes-200-accounts-tied-hate-groups-71101914 (accessed June 15, 2020).

[271] *BBC*, ‘Twitter tags Trump tweet with fact-checking warning’, May 27, 2020, https://www.bbc.com/news/technology-52815552 (accessed June 15, 2020).

[272] Dave Lee, ‘8chan far-right forum offline as Cloudflare cuts support’, *BBC*, August 5, 2019, https://www.bbc.com/news/technology-49232333 (accessed May 31, 2020).

[273] Yang et al., ‘Arming the public with artificial intelligence to counter social bots’, 50-51.

result, counterterrorism benefitted most from Web 3.0 technologies compared to the technologies of the Web 1.0 and Web 2.0 phases of the internet.

## 4.5 Conclusion

Whereas the distinction between the Web 2.0 and Web 3.0 was not as clear cut as the previous transition, the Web 3.0 has brought some changes to the online activities of terrorists. New platforms were used by far-right terrorists, preferring non-traditional platforms, such as imageboards and gaming communities. The biggest change however is found in the type of content that is exchanged online by far-right terrorists and sympathisers. The virtual aspect of content became increasingly important, with memes and deepfake videos rising to prominence. The decrease in textual content also resulted in terrorism becoming more idiosyncratic instead of ideological. A clear example of this is the emergence of the Boogaloo movement which incorporated aspects from both the political left and right.[274] The gamification of terrorism and the humorous references to internet culture created a strong online community of like-minded individuals. Compared to the terrorist networks from the previous chapters of this thesis, far-right terrorists had no physical territory for their community. The internet replaced physical or geographical spaces for interaction for far-right extremist. This increasing importance of the internet as a substitute for a physical community will be further analysed in the next chapter.

Yet, not only terrorism benefited from the Web 3.0 phase of the internet. both government and corporate counterterrorism efforts took advantage of the Web 3.0 technologies and adopted autonomous and automated processes to monitor and counteract the online activities of terrorists.

[274] Robert Evans and Jason Wilson, 'The Boogaloo Movement Is Not What You Think', *Bellingcat*, May 27, 2020, https://www.bellingcat.com/news/2020/05/27/the-boogaloo-movement-is-not-what-you-think/ (accessed June 15, 2020).

# Transitions and trends in the online activities of terrorists.

In each of the three previous chapters the internet uses by specific terrorist networks have been analysed. This fourth and final chapter compares the findings of these chapters and discusses the trends that can be distinguished through all three chapters as to answer the main research question of this thesis of how the technological development of the internet has changed the use of the internet by terrorists in the West between 2003 and 2019. Multiple changes in how the internet has been used over the years can be recognized. In this chapter, I will briefly discuss the following four transitions that impacted terrorism:

1. From plain text to humorous images;
2. From one-directional broadcasting to picking an audience;
3. From amateurs to professionals;
4. From hybrid breeding grounds to virtual nurseries of terrorism.

As well as these four transitions, two trends can be distinguished in the analysis of this thesis. After discussing the transitions, this chapter will examine the following two trends:

1. The internet expands offline terrorism, but does not replace it;
2. The main purpose of using the internet by terrorists was expanding their (potential) audience.

## Transitions

### 5.1 The visualisation of terrorist content

A shift can be distinguished in the types of content that were published and accessed by terrorists over the years. In the Web 1.0 phase of the internet, the members of the Hofstad Network focussed on text-based content, with the publication of translated and radical texts. This changed with the introduction of visual content with the Web 2.0 phase of the internet. Images and videos prominently featured in the online output of ISIS and the organisation grew infamous with the publication of beheading videos. This visual aspect helped to deliver a message of terror as images and sounds better grasp a larger audience compared to the plain texts of the Web 1.0.[275] This visual turn was continued into the Web 3.0 phase of the internet, with over fifty per cent of the posts on twitter containing visual media.[276] At the same time,

[275] Hoffman, *Inside Terrorism*, 182-183.

[276] Mary Meeker, 'Internet Trends 2019', *Bond Capital Report on Internet Trends*, June 11, 2019, 78, https://www.bondcap.com/report/itr19/#view/title (accessed June 1, 2020).

an expansion took place with the adaption of memes, internet culture references and livestreaming of acts of terrorism. Whereas the online content of Islamic terrorism focussed on horror and shock to capture the attention of its audience, far-right terrorism added humour to its online messages. Jokingly referring to Youtuber PewDiePie[277] and creating 'funny' memes that depicted Tarrant as a saint and far-right terrorists as reincarnations of the medieval crusaders,[278] are forms of such dark humour that were used by the far-right. By using humour in their online content, these terrorists show their wit and creativity to attract attention from a wider audience.[279] Far-right terrorists however still made use of a shock-effect in their online content, with the livestreaming of terrorist attacks.

The type of online content used by terrorists has therefore changed over the years and the visual aspect became more important. As a result, the strict ideology that was central to the Islamic terrorists of the Hofstad Network and ISIS was slowly replaced by a more idiosyncratic nature of terrorism that centred around internet culture.

### 5.2 Choosing the audience

Throughout the development of the internet, the online platforms that were utilized by terrorists also changed. In the Web 1.0 phase of the internet, user interaction was limited and the online activities of terrorist focussed on information-based webpages. As a result, the internet offered terrorists a new medium that they could use to broadcast their messages.

Whereas the number of people on the internet was still limited, the members of the Hofstad Network had no options to narrowcast messages to specific audiences. Although certain websites attracted a specific audience, such as maroc.nl, these could still be visited by everyone. This changed with the introduction of social media platforms in the Web 2.0 phase of the internet. Whereas these platforms still allowed terrorists to broadcast their messages to a broad public, they also offered the ability to narrowcast messages to groups on these platforms. Additionally, terrorists from ISIS' used encrypted and difficult to trace online services, like Telegram and anonymous file-sharing portals to interact with selected individuals. The Web 2.0 technologies therefore introduced a dual approach to terrorism, in

[277] Macklin, 'The Christchurch Attacks: Livestream Terror in the Viral Video Age', 19.

[278] Ben Cook, 'Deus Vult: ISIS & the White Nationalist Shooters', *Redpill Strategies*, December 9, 2019, https://redpillstrategies.co/blog/deus-vult-isis-and-the-white-nationalist-shooters (accessed June 2, 2020).

[279] Marta Dynel and Fabio Poppi, 'In tragoedia risus: Analysis of dark humour in post-terrorist attack discourse', *Discourse & Communication* 12 (2018) 4: 382-400, here: 397.

which terrorists broadcasted online content on public platforms to spread fear but used more secure channels to narrowcast tactical information to their supporters. This duality continued to be used by far-right terrorists in the Web 3.0 phase of the internet, but the clear distinction was fading. Whereas popular and public platforms were still used to spread messages of fear through livestreaming, far-right terrorists made use of public but less popular platforms to narrowcast their messages to like-minded individuals.

The technological development of the intent therefore allowed terrorists to choose between a broad audience and a selected target audience for each online message. This enabled them to tailor each message to a specific audience. These messages could be aimed at a broad uncommitted audience to win support, or an audience of sympathisers to strengthen its commitment.[280] Whereas this was extremely useful for propaganda purposes, it also allowed terrorists to communicate with their supporters in a secure manner.[281] This expansion of the opportunities for targeting specific audiences therefore greatly impacted the online activities of terrorists.

## 5.3 From amateurs to professionals

This dual approach called for sophisticated use of the internet by terrorists. Additionally, the internet became increasingly diverse and complicated for its users, but this also allowed terrorists to adopt more sophisticated methods for using the internet. Whereas the terrorists of the Hofstad Network acted foolishly and amateurish online, they benefited from the lack of interest in the online activities of terrorists by the Dutch counterterrorism agency.[282] With the increased online presence of counterterrorism services from the Web 2.0 onwards, terrorists were forced to adopt more sophisticated methods for their online activities. ISIS set up dedicated media centres and allied itself with hacker collectives to commit cyberattacks. This was however only possible due to a large amount of (skilled) supporters within the Islamic Caliphate and the networks financial capacity.[283] The far-right terrorists of the Web 3.0 were not structured as well and lacked the financial assets required for such institutionalised online strategies, but were sophisticated in their use of the internet as well, albeit in a different way.

[280] Hoffman, *Inside Terrorism*, 207.

[281] Ibid.

[282] CTIVD, 'Toezichtsrapport inzake de afwegingsprocessen van de AIVD met betrekking to Mohammed B.', 40.

[283] Nelson et al., 'Cyberterror: Prospects and Implications', 72-74.

By using platforms that allowed them to remain anonymous track, far-right terrorists were able to stay under the radar of counterterrorism agencies. Thus, over the years both the technologies of the internet and the activities of terrorists became more sophisticated.

### 5.4 Offline versus online communities

With the development of the internet, the importance of online communities also increased, peaking with the far-right terrorists of the Web 3.0. Whereas the Islamic terrorists of the Hofstad Network and ISIS still met each other in the 'offline world' at living room meetings and in the Islamic Caliphate, physical interactions between far-right terrorists were limited. Instead, far-right terrorists abandoned the idea of a geographical-based community in favour of an online community. Such online communities benefitted from the internet being an ungoverned space. The term 'ungoverned spaces' has long focussed on the absence of state governance but it is more recently defined as places "where territorial state control has been voluntarily or involuntarily ceded in whole or part to actors other than the relevant legally recognized sovereign authorities."[284] The ever-expanding size of the internet made it impossible for states (and consequently government counterterrorism agencies) to monitor all online activities. This was exploited by terrorists, as their online community therefore functioned as a sort of safe-haven. Counterterrorism efforts against such online communities were further hindered by the unstructured nature of modern terrorist networks. As terrorist attacks by lone actor operators increased over the years,[285] terrorist networks became more fluid with its members lacking previous connections and their acts becoming more spontaneous.[286] Whereas this was most prominent with far-right extremists, Islamic terrorist networks also called on its supporters to strike alone from 2005 onwards.[287]

With the organisational structure of terrorist networks becoming more fluid, the internet's facilitation of community interaction became increasingly important for connecting different sympathisers. As online communities provide a safer environment to terrorists

[284] Anne Clunan and Harold Trinkunas, *Ungoverned Spaces: Alternatives to State Authority in an Era of Softened Sovereignty* (Palo Alto, California: Stanford University Press, 2010) 17.

[285] Edwin Bakker and Beatrice de Graaf, 'Lone Wolves. How to Prevent this Phenomenon?', Expert Meeting Paper presented at the ICCT Expert Meeting: Lone Wolves (The Hague, November 2010) 3.

[286] Daniel Koehler, 'The Halle, Germany, Synagogue Attack and the Evolution of the Far-Right Terror Threat', *CTCSentinel* 12(2019) 11: 14-20, here: 15.

[287] Charles Townsend, *Terrorism. A Very Short Introduction* (Oxford: Oxford University Press, 2018) 15.

compared to offline communities, it would not be surprising if this trend continues in the years to come.

### Trends

Whereas the four paragraphs above dealt with the transitions that impacted terrorism, the next two sections focus on the aspects of terrorism that were not impacted by the technological development of the internet.

## 5.5 The role of the internet for terrorism

Although the uses of the internet by terrorists were at the centre of this thesis' analysis, it also became clear that the online activities of terrorists were merely an extension to their physical acts. The analysis above has shown that physical acts were at the basis of all online activities of terrorists, regardless of their corresponding stage of the internet. Both descriptions and depictions of terrorist acts, such as written threats of violence or videos of terrorist attacks, feature prominently in the online propaganda content distributed by terrorists. The finances gained via the internet were used by terrorists of ISIS and the far-right for travelling to the Caliphate and acquiring the means required for a physical terrorist attack. And whereas digital instructions eventually replaced the training camps of the Middle East, the online manuals with instructions still prepared terrorists for a physical terrorist attack. The online dimension of terrorism served therefore only as an extension to the physical domain of terrorism. In his revised academic consensus definition of terrorism, Alex P. Schmid also specifically emphasises the physical aspect of terrorist violence.[288] Without the physical aspects of terrorism, the internet served no purpose for terrorists. The only exception to this was the use of the internet for cyberattacks by the hacker groups that had allied themselves to ISIS. Whereas these groups only committed attacks in the virtual world, this cyberterrorism was extremely limited and was only viable because of the institutionalised organisational structure of ISIS' caliphate. With the far-right terrorists of the Web 3.0, the cyberterrorism purposes of the internet disappeared again. In all three analysed phases of the web, the internet thus mainly served as an extension to the physical nature of terrorism.

[288] Alex P. Schmid, 'The Revised Academic Consensus Definition of Terrorism', *Perspectives on Terrorism* 6 (2012) 2: 158-159, here: 159.

## 5.6 Offering an expanded audience

Lastly, and quite remarkably (and contrary to what I expected when I started this research) only small changes in the different functions for which the internet was used by terrorists have occurred over the years. This is not to say that the development of the internet to the Web 3.0 phase we are in now is irrelevant, but it is to state that the internet's functionality per se has not changed much. Obviously, within the functions that were there form the beginning, the professionalisation and modernisation of the internet meant a great deal, which has been described above. But it is important to stress that the type of functions per se has not changed

Throughout all phases of the web, the primary use of the internet by terrorists was the *creation and distribution of propaganda content*. This is not surprising as the internet was originally created as a new (and nuclear-proof) method of communication.[289] The technological development of the internet also resulted in an increased use of the internet in the execution of an act of terrorism and planning and training of terrorists. Whereas the members of the Hofstad Network still preferred physical training camps in foreign countries and limited their online acts of terrorism to threats, this changed with the widespread distribution of digital instruction manuals on terrorism and the emergence of visual content from the Web 2.0 onwards.

In contrast and despite the technological developments, the use of the internet for cyberattacks remained minimalistic. Of the studied terrorist networks, only ISIS possessed the means and financial capacity to make use of cyberattacks through allied hacker collectives. Similarly, the internet's function for financing terrorism saw only a minor increase through the development of the internet, with the emergence of cryptocurrencies. This use of the internet by the terrorists studied in this research was however limited, with both the Hofstad Network and terrorists from the far-right not requiring digital financial support. The minimal use of the internet for financing terrorism can be explained through the previously mentioned concept of ungoverned spaces. Whereas the internet is often perceived as an ungoverned space, digital money transfers are still controlled by central banks and digital aspects of financing are therefore governed.[290] As a result, online transfer of money would increase the

[289] Ryan, *A History of the Internet*, 13-17.

[290] Clunan and Trinkunas, *Ungoverned Spaces*, 17.

risk of terrorists being discovered by government counterterrorism agencies. Overall, the most important functions of the internet for terrorists were those that expanded the potential audience for the messages of terrorists.

# Conclusion

## General conclusion

From its release to the public in the mid-1990s, terrorists have made use of the internet. But for a long time, the role of the internet has been perceived as a static one by researchers in the field of terrorism studies. However, the constant addition of new features of the internet that were exploited by terrorists, such as social media platforms and live streaming functions, indicated that this is incorrect. This master thesis therefore set out to analyse how the technological development of the internet has changed the use of the internet by terrorists in the West between 2003 and 2019. To find an answer to this research question, a detailed qualitative approach was used to analyse the online activities of terrorists from three consecutive technological phases of the internet, labelled the Web 1.0, Web 2.0 and Web 3.0. Each phase lasted about ten years and brought new technological opportunities to the internet, which were incorporated by terrorist networks active at the time. The individual terrorists, whose acts were analysed in this research were members of the Dutch Hofstad Network, the Islamic State in Iraq and Syria (ISIS) and the far-right extremists.[291] Each of these terrorist networks was selected on its active use of the respective technological phase of the internet. The analysis of each chapter was structured using the six different functions of the internet for terrorism according to the UNODC: Propaganda, finance, training, planning, execution and cyberattacks.

From the analysis of the internet's uses by terrorists over the years, four transitions and two trends could be distinguished.

Firstly, a gradual transition towards visual terrorist content could be distinguished online. Whereas the online activities of members of the Hofstad Network were mostly text-based, this changed with the introduction of Web 2.0 technologies that offered users more visual-based content options. This was exploited by terrorists, who increasingly visualised their content with for instance the use of images, videos by ISIS and the adoption of livestreaming services by the terrorists of the far-right. As the visual aspect became more important over the years, the strict ideology that had been central to the terrorism of the Hofstad Network and ISIS was slowly replaced by a more idiosyncratic nature of terrorism that

[291] Here, 'members' is used in the most basic understanding of the word, as the studied far-right network lacks an organisational structure and is best treated as a fluid network.

centred around internet culture. This is illustrated by the rise of the Boogaloo movement that lacks a well-defined ideology.

Secondly, a complex duality emerged in the approach used by terrorists to select an audience. During the Web 1.0 phase of the internet, terrorists from the Hofstad Network relied on one-way websites and internet fora with limited options for interactions. With the transition to the Web 2.0 phase, internet consumers became internet users, due to the interaction possibilities of the internet that had previously been unavailable. ISIS operated on both popular social media platforms and secure, encrypted platforms. Social media platforms were used for broadcasting messages of fear to a large audience, whereas encrypted services offered the ability to narrowcast content tailored to a specific audience. This combined approach was continued by the far-right terrorists of the Web 3.0 phase, although they also expanded their activities to previously neglected gaming-platforms and imageboard websites. This allowed terrorists to choose between a broad audience and a selective audience and tailor each online message to the chosen audience. This expansion of the opportunities for targeting specific audiences therefore greatly impacted the online activities of terrorists.

Thirdly, the ever-expanding nature of the internet and the developing online efforts of counterterrorism agencies required terrorists to become more sophisticated in their online activities. Although the terrorists of the Hofstad Network acted foolishly online, they benefitted from a lack of interest by the AIVD. From the Web 2.0 onwards, both counterterrorism agencies and terrorists became increasingly sophisticated in their online activities as to deal with the growing complexity of the internet. This dedication to online activities by terrorists indicates how important the internet as a field of operations has become for terrorism.

The fourth and final transition that impacted terrorism was the increasing importance of online communities. The Islamic terrorists of both the Hofstad Network and ISIS met each other in the real world and their communities were respectively centred around The Hague and the Islamic caliphate in Iraq and Syria. The far-right terrorists of the Web 3.0 only met in their online communities and lacked a physical location that tied them together. With the organisational structure of terrorist networks becoming more fluid, the internet's facilitation of community interaction became increasingly important for connecting individual sympathisers from all over the world. As online communities provide a safer environment to terrorists compared to offline communities, it would not be surprising if this trend continues in the years to come.

Whereas these transitions help to understand how the technological development of the internet has impacted the use of the internet by terrorists in the West between 2003 and 2019, two trends have been distinguished that have remained constant over the years.

Although this thesis focussed on the online activities of terrorists, the offline aspect of terrorism remained essential. The analysis of online terrorist activities has shown that physical acts of terrorism have been at the basis of nearly all the online activities of terrorists of the Hofstad Network, ISIS, and the far-right. Without the physical aspects of terrorism, the internet would therefore serve no purpose for these terrorists. So, despite the importance of the online field of terrorism, offline activities have remained at the centre of terrorism through the years.

Additionally, propaganda remained the most important of the six internet functions for terrorism that have been studied in this research. Gradually, internet uses for training, planning, and execution purposes were also incorporated by terrorists. Online financing and the internet's use for cyberterrorism remained minimal. This is not surprising as the first four of purposes all benefitted from the extended audience that could be reached via the internet and as stated in the introduction, an audience is essential to terrorism.[292] Similar to the impact of the introduction of the mass media in the 1880s, the introduction of the internet expanded the potential audience of terrorists, which substantiates the idea of a dynamic nature of terrorism as proposed by both Walter Laqueur and David Rapoport.[293] But if the internet has indeed been responsible for a change in the nature of terrorism, the introduction of the internet in the 1990s should not be regarded as the breaking point. Instead, the introduction of the Web 2.0, that changed internet consumers into internet users and allowed user interactions on a large scale via social media, was responsible for the biggest change in the online behaviour of terrorists.

[292] Schmidt and Schroeder, 'Violent imaginaries and violent practices', 5-6; Tilly, 'Terror, Terrorism, Terrorist', 9; Jenkins, *Will Terrorists Go Nuclear,* 5.

[293] Laqueur, *The New Terrorism*; Rapoport, 'The Four Waves of Modern Terrorism', 48-49.

## The relevance of this thesis

This thesis has shown that the development of the internet has an impact on terrorism. terrorists are early adopters of online technologies and were therefore present on multiple platforms. The development of the internet however continues to this day and terrorists adapt their strategies to new online platforms. By studying how the internet is used by terrorists, future threats can be better assessed. This subject has become extremely relevant, with multiple scholars researching the online activities of terrorists on multiple platforms. In a study yet to be published in *Studies in Conflict & Terrorism*, Gabriel Weimann and Natalie Masri analyse how far-right extremists have used the new social media platform TikTok to spread its hateful content to an extremely young audience. Whereas TikTok was only released worldwide in 2017, the app amassed an enormous user base and was downloaded over two billion times. [294] The research by Weimann and Masri contributes to the conclusions of this thesis by highlighting new transitions in terrorism such as the shifting focus of far-right extremists to radicalising a young audience. By understanding how terrorists make use of the ever-evolving internet, society becomes more aware of the risks of such online services. A clear image of the online activities of terrorists furthermore contributes to the understanding of terrorism by counterterrorism actors, such as government agencies and corporations, as well as individual civilians. The conclusions of research into new online activities of terrorists help them to create approaches for their counterterrorism efforts suited to these new developments.

## Recommendations for further research

This thesis analysed the uses of the internet for terrorist purposes up until 2019. However, the Web 3.0 phase of the internet is expected to continue for at least another five years according to the research by Naik and Shivalingaiah.[295] As a result, the entire technological developments of the Web 3.0 phase could not be analysed in this thesis. The impact of the

[294] Aaron Reich, 'TikTok rife with racist, antisemitic content aimed at children – study', *The Jerusalem Post*, June 18, 2020, https://www.jpost.com/diaspora/antisemitism/tiktok-rife-with-racist-antisemitic-content-aimed-at-children-study-631808?fbclid=IwAR1pLgtUZmhgn0ke5ewx9B6tmzxSR8p32k_ho3xnDhp5h-5gd4KZARrdYF8 (accessed June 24, 2020).

[295] Naik and Shivalingaiah, 'Comparative Study of Web 1.0, Web 2.0 and Web 3.0', 503.

Web 3.0 technology on the online activities of terrorists should therefore be revisited once this phase has entirely concluded.

Whereas it might seem that all terrorists from the twenty-first century used the internet for one or more terroristic purposes, this is not the case. There is, for instance, no evidence that the perpetrator of the Utrecht tram shooting in the Netherlands on March 18, 2019, used the internet for terrorist purposes at any stage of his attack.[296] Furthermore, for a small number of the 2.226 radicalised individuals included in the Profiles of Individual Radicalization in the United States Database, the internet did not play any role in their radicalisation process.[297] Whereas this thesis focussed on the technological development of the internet and its impact on terrorism, some information on the relationship between terrorism and the internet is still lacking. Sociological research into the reasoning of terrorists for using the internet can explain why some terrorists deliberately refrain from using the internet for any aspect of their terrorist attack and help to understand the relation between terrorists and the internet.

The authors of such further research should however build on this thesis and be aware of the dynamic nature of the internet and its impact on terrorism as researched within this thesis.

[296] Utrecht District Court, 'ECLI:NL:RBMNE:2020:1046', March 20, 2020, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBMNE:2020:1046 (accessed June 6, 2020).

[297] START, 'Profiles of Individual Radicalization in the United States – Internet Radicalization', 2018, https://www.start.umd.edu/data-tools/profiles-individual-radicalization-united-states-pirus (accessed June 6, 2020).

# Bibliography

## Primary sources

Algemene Inlichtingen- en Veiligheidsdienst. *Jaarverslag 2004*. The Hague: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties: 2005.

Amsterdam District Court. 'ECLI:NL:RBAMS:2005:AU0025'. July 26, 2005, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2005:AU0025 (accessed March 14, 2020).

Balliet, Stephan. 'Manifest'. Online distributed manifesto, October 9, 2019, https://www.docdroid.net/oEfJ0a3/manifesto-pdf (accessed May 27, 2020).

Boogerd, David, and Jason Walters. 'Jason Walters, van terrorist to filosoof'. August 18, 2019, *De Ongelofelijke Podcast*, produced by the Evangelische Omroep, podcast, [0:14:15], https://www.nporadio1.nl/podcasts-uitgelicht/18165-de-ongelooflijke-podcast-met-ex-terrorist-jason-walters-ik-zei-tegen-de-politie-schiet-maar (accessed March 25, 2020).

Breivik, Anders. '2083: A European Declaration of Independence'. Online distributed manifesto, 2011, https://info.publicintelligence.net/AndersBehringBreivikManifesto.pdf (accessed May 15, 2020).

*Christchurch Call*. 'Supporters'. N.d., https://www.christchurchcall.com/supporters.html (accessed May 31, 2020).

Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (hereafter: CTIVD). 'Toezichtsrapport inzake de afwegingsprocessen van de AIVD met betrekking to Mohammed B.'. CTIVD report. The Hague, 2008.

Crusius, Patrick. 'The Inconvenient Truth'. Online distributed manifesto, 2019, https://grabancijas.com/patrick-crusius-manifesto-the-inconvenient-truth/ (accessed May 17, 2020).

Directorate-General for External Policies of the European Parliament. 'In-depth analysis: The financing of the 'Islamic State' in Iraq and Syria (ISIS)'. Paper requested by the European Parliament's Committee on Foreign Affairs. Brussels, 2017.

Donner, J.P.H. and J.W. Remkes. 'Kamerstukken 2, 2004-2005, 29854, nr. 3'. The Hague: Sdu Publishers, 2004.

Dutch Supreme Court. 'ECLI:NL:PHR:2010:BK5193'. February 2, 2010, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:PHR:2010:BK5193 (accessed March 14, 2020).

Nationaal Coördinator Terrorismebestrijding. 'Jihadisten en het internet'. Phenomenon report to the Dutch parliament, 2007. 60-61, https://www.aivd.nl/documenten/publicaties/2007/01/18/jihadisten-en-het-internet (accessed April 20, 2020).

Peters, Rudolph. 'Overzicht teksten geschreven of vertaald door Mohammed B.'. Attachment to the report 'De ideologische en religieuze ontwikkeling van Mohammed B.'.

START. 'Profiles of Individual Radicalization in the United States – Internet Radicalization'. 2018, https://www.start.umd.edu/data-tools/profiles-individual-radicalization-united-states-pirus (accessed June 6, 2020).

Tarrant, Brenton. 'The Great Replacement'. Online distributed manifesto, 2019, https://commons.wikimannia.org/images/Tarrant_Brenton_-_The_Great_Replacement.pdf (accessed May 17, 2020).

The Hague District Court. 'ECLI:NL:GHSGR:2005:AU6181'. November 18, 2005, https://linkeddata.overheid.nl/front/portal/document-viewer?ext-id=ECLI:NL:GHSGR:2005:AU6181 (accessed March 25, 2020).

———. 'ECLI:NL:GHSGR:2008:BC2576'. January 23, 2008, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHSGR:2008:BC2576 (accessed March 14, 2020).

United Nations Office of Drugs and Crime (hereafter: UNODC). 'The use of the Internet for terrorist purposes'. Paper in collaboration with the United Nations Counter-Terrorism Implementation Task Force. New York, 2012.

Utrecht District Court. 'ECLI:NL:RBMNE:2020:1046'. March 20, 2020, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBMNE:2020:1046 (accessed June 6, 2020).

Wet op de Inlichtingen- en Veiligheidsdienst 2017. Paragraph 3.2.5, January 1, 2020, https://wetten.overheid.nl/BWBR0039896/2020-01-01 (accessed May 31, 2020).

## Academic sources

Aghaei, Sareh, Mohammad Ali Nematbakhsh, and Hadi Khrosravi Farsani. ‘Evolution of the World Wide Web: From Web 1.0 to Web 4.0’. *International Journal of Web & Semantic Technology* 3 (2012) 1: 1-10.

Alkhouri, Laith, Alex Kassirer, and Allison Nixon, *Hacking for ISIS: The Emergent Cyber Threat Landscape*. N.p.: Flashpoint, Inc., 2016.

Al-Rawi, Ahmed. ‘Video games, terrorism, and ISIS’s Jihad 3.0’. *Terrorism and Political Violence* 30 (2018) 4: 740-760.

Aubrey, Stefan. *The New Dimension of International Terrorism*. Zürich: VDF Hochschulverlag AG, 2004.

Awan, Imran. ‘Cyber-Extremism: Isis and the Power of Social Media’. *Social Science and Public Policy* 54 (2017): 138-149.

Bakker, Edwin, and Beatrice de Graaf. ‘Lone Wolves. How to Prevent this Phenomenon?’. Expert Meeting Paper presented at the ICCT Expert Meeting: Lone Wolves. The Hague, November 2010.

Bakker, Edwin, and Peter Grol. *Nederlandse Jihadisten. Van naïeve idealisten tot geharde terroristen*. Amsterdam: Hollands Diep, 2017.

Bakker, Edwin, Christophe Paulussen, and Eva Entenmann. ‘Dealing with European Foreign Fighters in Syria: Governance Challenges & Legal Implications’. ICCT research paper. The Hague, December 2013.

Bakker, Edwin. *Terrorism and Counterterrorism Studies. Comparing Theory and Practice*. Leiden: Leiden University Press, 2015.

Ball, Leslie, and Matthew Craven. ‘Automated Counter-Terrorism’. Poster paper presented at the European Intelligence and Security Informatics Conference. Uppsala 2013.

Berger, J.M., and Heather Perez. ‘The Islamic State’s Diminishing Returns on Twitter: How suspensions are limiting the social networks of English -speaking ISIS supporters’. Occasional paper for the Program on Extremism. Washington D.C.: Georgetown University, 2016.

Berger, J.M., and Jonathon Morgan. ‘The ISIS Twitter Census. Defining and describing the population of ISIS supporters on Twitter’. Analysis paper no. 20 for *The Brookings Project on U.S. Relations with the Islamic World*. Washington D.C., March 2015.

Berger, Maurits, and Masha Rademakers. ‘Allahoe Akbar! – de jihadisten’. In Maurits Berger (ed.), *Nederlanders in de heilige oorlog: zoeaven, brigadisten en jihadisten*. The Hague: Boom Juridische uitgevers, 2015. 67-96.

Bhatia, Michael V. ‘Fighting Words: Naming Terrorists, Bandits, Rebels and Other Violent Actors’. *Third World Quarterly* 26 (2005) 1: 5-22.

Bloom, Mia, Hicham Tiflati, and John Horgan. ‘Navigating ISIS’s Preferred Platform: Telegram’. *Terrorism and Political Violence* 31 (2019) 6: 1242-1254

Buruma, Ian. *Murder in Amsterdam: The Death of Theo Van Gogh and the Limits of Tolerance*. London: Atlantic Books, 2007.

Byman, Daniel. ‘The Homecomings: What Happens When Arab Foreign Fighters in Iraq and Syria Return?’. *Studies in Conflict & Terrorism* 38 (2015) 8:581-602.

Castells, Manuel. ‘The impact of the internet on society: a global perspective’. In Manuel Castells (ed.), *19 Key Essays on how Internet is Changing Our Lives*. Bilbao: BBVA, 2013. 127-148.

Choudhury, Nupur. ‘World Wide Web and Its Journey from Web 1.0 to Web 4.0’. *International Journal of Computer Science and Information Technologies* 5 (2014) 6: 8096-8100.

Clunan, Anne, and Harold Trinkunas. *Ungoverned Spaces: Alternatives to State Authority in an Era of Softened Sovereignty*. Palo Alto, California: Stanford University Press, 2010.

Conway, Maura, Ryan Scrivens, Logan Macnair. ‘Right-Wing Extremists’ Persistent Online Presence: History and Contemporary Trends’. ICCT Policy Brief. The Hague, 2019.

Conway, Maura. ‘Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research’. *Studies in Conflict & Terrorism* 40 (2017) 1: 77-98.

———. ‘Terrorism and the Internet: New Media – New Threat?’. *Parliamentary Affairs* 59 (2006) 2: 283-298.

———. ‘Terrorist ‘use ‘of the internet and fighting back’. *Information & Security. An International Journal* 19 (2006): 9-30.

Crenshaw, Martha. ‘The Debate over “New” vs. “Old” Terrorism’. Paper presented at the *Annual Meeting of the American Political Science Association*. Chicago, August 30 – September 2, 2007.

———. *Explaining terrorism: causes, processes and consequences*. New York/ Abingdon: Routledge, 2011.

Daou, Peter. *Digital Civil War: Confronting the Far-Right Menace*. London: Melville House, 2019.

De Graaf, Beatrice, and Saskia Pothoven. ‘De islamitische inlichtingenstaat – De Stasi als leermeester?’. *Militaire Spectator* 187 (2018) 9: 453-465.

De Graaf, Beatrice. ‘Foreign fighters on trial: Sentencing risk, 2013 – 2017’. In Nadia Fadil, Martijn de Koning and Francesco Ragazzi (eds.), *Radicalization in Belgium and the Netherlands – Critical Perspective on Violence and Security*. London/ New York: I.B. Tauris, 2019. 97-130.

———. ‘The Van Gogh Murder and Beyond’. In Bruce Hoffman and Fernando Reinares (eds.), *The Evolution of the Global Terrorist Threat: From 9/11 to Osama bin Laden’s Death*. New York: Columbia University Press, 2014. 144-187.

———. *Gevaarlijke vrouwen. Tien militante vrouwen in het vizier*. Amsterdam: Boom, 2012.

———. *Theater van Angst. De strijd tegen terrorisme in Nederland, Duitsland, Italië en Amerika*. Amsterdam: Boom, 2010.

Denning, Dorothy. ‘A View of Cyberterrorism 5 Years Later’. In Kenneth Himma (ed.), *Internet Security: Hacking, Counterhacking, and Society*. Burlington, Massachusetts: Jones & Barlett Publishers, 2007. 123-141.

Devji, Faisal. *Landscapes of the Jihad*. Ithaca, NY: Cornell University Press, 2005.

Dion-Schwarz, Cynthia, David Manheim, and Patrick B. Johnston. *Terrorist Use of Cryptocurrencies. Technical and Organisational Barriers and Future Threats*. Santa Monica, CA: RAND Corporation, 2019.

Duyvesteyn, Isabelle. ‘How New Is the New Terrorism?’. *Studies in Conflict & Terrorism* 27 (2004) 5: 439-454.

Dynel, Marta, and Fabio Poppi. ‘In tragoedia risus: Analysis of dark humour in post-terrorist attack discourse’. *Discourse & Communication* 12 (2018) 4: 382-400.

Ebner, Julia. *Going Dark. The Secret Social Lives of Extremists*. London: Bloomsbury, 2020.

Egerton, Frazer. *Jihad in the West. The Rise of Militant Salafism*. Cambridge: Cambridge University Press, 2011.

Estrada, Mario Arturo Ruiz, and Evangelos Koutronas. ‘Terrorist attack assessment: Paris November 2015 and Brussels March 2016’. *Journal of Policy Modeling* 38 (2016) 3: 553-571.

Farwell, James P. ‘The Media Strategy of ISIS’. *Survival* 56 (2015) 6: 49-55.

Financial Action Task Force. *Emerging Terrorist Financing Risks*. Paris: FAFT, 2015.

Forest, James J.F. ‘Terrorist Training Centers Around the World: A Brief Review’. In James J.F. Forest (ed.), *The Making of a Terrorist: Volume Two*. Westport, CT: Praeger Security International, 2005. 296-311.

Freeman, Michael. ‘The Sources of Terrorist Financing: Theory and Typology’. *Studies in Conflict & Terrorism* 34 (2011) 6: 461-475.

Friis, Simone Molin. ‘‘Beyond anything we have ever seen’: beheading videos and the visibility of violence in the war against ISIS’. *International Affairs* 91 (2015) 4: 725-746.

Geeraerts, Sanne. ‘Digital radicalization of youth’. *Social Cosmos* 3 (2012) 1: 25-32.

Giantas, Dominika, and Dimitrios Stergiou. ‘From Terrorism to Cyber-Terrorism: The Case of ISIS’. *SSRN Electronic Journal*, March 7, 2018, 9-12, https://dx.doi.org/10.2139/ssrn.3135927 (accessed May 5, 2020).

Giles, Jim. ‘Internet encyclopaedias go head to head’. *Nature* 438 (2005): 900-901.

Graham, Robert. ‘How Terrorists Use Encryption’. *CTCSentinel* 9 (2016) 6:20-25.

Groen, Janny, and Kranenberg, Annieke. *Strijdsters van Allah: radicale moslima’s en het Hofstadnetwerk* .Kobo e-book, 2013.

Gunarata, Rohan. *Inside Al Qaeda*. New York: Columbia University Press, 2002.

Hartleb, Florian. *Lone Wolves. The New Terrorism of Right-Wing Single Actors*. Basel: Springer Nature Switzerland AG, 2020.

Harwood, Elizabeth T. ‘Terrorism and the Digital Right-Wing’. *Contexts* 18 (2019) 3: 60-62.

Hegghammer, Thomas, and Petter Nesser. ‘Assessing the Islamic State’s Commitment to Attacking the West’. *Perspectives on Terrorism* 9 (2015) 4: 14-30.

Hennessy, John L., David Patterson, and Herbert Lin., *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities*. Washington D.C.: National Academies Press, 2003.

Hitchens, Michael. Bronwin Patrickson, and Scherman Young, ‘Reality and Terror, the First-Person Shooter in Current Day Settings’. *Games and Culture* 9 (2014) 1:3-29.

Hodge, Edwin, and Helga Hallgrimsdottir. ‘Networks of Hate: The Alt-right, “Troll Culture”, and the Cultural Geography of Social Movement Space Online’. *Journal of Borderlands Studies* (February 2019): 1-18.

Hoffman, Bruce. *Inside Terrorism*. New York: Columbia University Press, 2017.

Huntington, Samuel P. ‘The Clash of Civilizations?’ *Foreign Affairs* 72 (1993): 22-49.

Ingram, Haroro J. ‘An Analysis of *Inspire* and *Dabiq*: Lessons from AQAP and Islamic State’s Propaganda War’. *Studies in Conflict & Terrorism* 40 (2017) 5: 357-375.

———. ‘Islamic State’s English-language magazines, 2014-2017: Trends & implications for CT-CVE strategic communications. A quick reference guide to Islamic State News (issues 1-3), Islamic State Report (issues 1-4), Dabiq (issues 1-15) and Rumiyah (issues 1-13)’. ICCT research report. The Hague, 2018.

Jenkins, Brian. *Will Terrorists Go Nuclear?* Santa Monica, CA: RAND Corporation, 1975.

Kaplan, Andreas, and Michael Haenlein. ‘Users of the world, Unite! The challenges and opportunities of Social Media’. *Business Horizons* 53 (2010) 1: 59-68.

Kershaw, Ian. *Een naoorlogse achtbaan. Europa 1950-2017*. Houten: Unieboek|Het Spectrum bv, 2018.

Killcullen, David. ‘Countering global insurgency’. *Journal of Strategic Studies* 28 (2005) 4: 597-617.

Koehler, Daniel. ‘The Halle, Germany, Synagogue Attack and the Evolution of the Far-Right Terror Threat’. *CTCSentinel* 12(2019) 11: 14-20.

Kozłowski, Bartosz. ‘Fighting ISIS Online: Is a co-regulatory system the most effective approach to fight ISIS online when using the NTD procedure’. Master thesis in Crisis and Security Management, Leiden University, 2018.

Laqueur, Walter. *The New Terrorism: Fanaticism and the Arms of Mass Destruction*. Oxford: Oxford University Press, 1999.

Leiner, Barry, vinton Cerf, David Clark, Robert Kahn, Leonard Kleinrock, Daniel Lynch, Jon Postel, Larry Roberts, and Stephen Wolff. *Brief History of the Internet*. N.d.: Internet Society, 1997.

Lewis, James A. ‘The Internet and Terrorism’. *American Society of International Law Proceedings* 99 (2005): 112-115.

Ligon, Gina Scott, Pete Simi, Mackenzie Harms, and Daniel J. Harris. ‘Putting the ‘O’ in VEOs: What makes an organization?’. *Dynamics of Asymmetric Conflict* 6 (2013) 1-3: 110-134.

Lindekilde, Lasse, Francis O’Connor, and Bart Schuurman. ‘Radicalization patterns and modes of attack planning and preparation among lone-actor terrorists: an exploratory analysis’. *Behavioral Sciences of Terrorism and Political Aggression* 11 (2019) 2: 113-133.

Macklin, Graham. ‘The Christchurch Attacks: Livestream Terror in the Viral Video Age’. *CTC Sentinel* 13 (2019) 6: 18-29.

Malmgren, Evan. ‘Don’t Feed the Trolls’. *Dissent* 64 (2017) 2: 9-12.

McLuhan, Marshall. *The Gutenberg Galaxy: The Making of Typographic Man*. Toronto: University of Toronto Press, 2011.

Mehra, Tanya. ‘Foreign Terrorist Fighters. Trends Dynamics and Policy Responses’. ICCT research report. The Hague, 2016.

Mockaitis, Thomas R. *The “new” terrorism: myths and reality*. Westport, Connecticut/ London: Praeger Security International, 2007.

Nacos, Brigitte, David Fan, and John Young. ‘Terrorism and the Print Media: The 1985 TWA Hostage Crisis’. *Terrorism* 12 (1989) 2: 107-115.

Naik, Umesha, and D. Shivalingaiah. ‘Comparative Study of Web 1.0, Web 2.0 and Web 3.0’. Paper presented at the *6th International CALIBER Conference*. Odisha, March 2009.

Nanninga, Pieter. ‘Branding a Caliphate in Decline: The Islamic State’s Video Output (2015-2018)’. ICCT research paper. The Hague, 2019.

Nelson, Bill, Rodney Choi, Michael Lacobucci, Mark Mitchell, and Greg Gagnon. ‘Cyberterror: Prospects and Implications’. Report for the Intelligence Agency Office for Counterterrorism Analysis. Monterey, California: Center for the Study of Terrorism and Irregular Warfare of the Naval Postgraduate School, 1999.

Nesser, Petter, Anne Stenersen, and Emilie Ofteda. ‘Jihadi Terrorism in Europe: The IS-Effect’, *Perspectives on Terrorism* 10 (2016) 6: 3-24.

Oosterveld, Willem Theo, and Willem Bloem. ‘The Rise and Fall of ISIS: From Evitability to inevitability’. Security report of the The Hague Centre for Strategic Studies. The Hague, 2017.

Peters, Rudolph. ‘Dutch extremist Islamism: Van Gogh’s murderer and his ideas’. In R. Coolsaet (ed.), *Jihadi terrorism and the radicalisation challenge in Europe*. Aldershot: Ashgate, 2008. 115-127.

Prucha, Nico. ‘IS and the Jihadist Information Highway – Projecting Influence and Religious Identity via Telegram’. *Perspectives on Terrorism* 10 (2016) 6: 48-58.

Ramos, Raul, Christopher Ferguson, and Kelly Frailing. ‘Violent Entertainment and Cooperative behavior: Examining Media Violence Effects on Cooperation in Primarily Hispanic Sample’. *Psychology of Popular Media Culture* 5 (2016): 119-132.

Rapoport, David. ‘The Four Waves of Modern Terrorism’. In Audrey Kurth Cronin and James M. Ludes (eds.), *Attacking Terrorism. Elements of a Grand Strategy*. Washington, D.C.: Georgetown University Press, 2004. 46-73.

Richards, Imogen. ‘A Dialectical Approach to Online Propaganda: Australia’s United Patriots Front, Right-Wing Politics, and Islamic State’. *Studies in Conflict & Terrorism* 42 (2019) 1-2: 43-69.

Ryan, Johnny. *A History of the Internet and the Digital Future*. London: Reaktion Books, 2010.

Sageman, Marc. *Leaderless jihad: terror networks in the twenty-first century*. Philadelphia: University of Pennsylvania Press, 2008.

———. *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press, 2004.

Schmid, Alex P. ‘The Revised Academic Consensus Definition of Terrorism’. *Perspectives on Terrorism* 6 (2012) 2: 158-159.

Schmidt, Bettina, and Ingo Schroeder. ‘Violent imaginaries and violent practices’. In Bettina Schmidt and Ingo Schroeder (eds.), *Anthropology of Violence and Conflict*. London: Routledge, 2001. 1-24.

Schuurman, Bart, Quirine Eijkman, and Edwin Bakker. ‘The Hofstadgroup Revisited: Questioning its Status as a “Quintessential” Homegrown Jihadist Network’. *Terrorism and Political Violence* 27 (2015) 5: 906-925.

Schuurman, Bart. *Becoming a European homegrown jihadist: A multilevel analysis of involvement in the Dutch Hofstadgroup, 2002-2005*. Amsterdam: Amsterdam University Press, 2018.

Shehabat, Ahmad, and Teodor Mitew. ‘Black-boxing the Black Flag: Anonymous Sharing Platforms and ISIS Content Distribution Tactics’. *Perspectives of Terrorism* 12 (2018) 1: 81-99.

Simon, Jeffrey. *The Alphabet Bomber. A Lone Wolf Terrorist ahead of his time*. Lincoln, Nebraska: University of Nebraska Press, 2019.

Stenersen, Anne. ‘The Internet: A Virtual Training Camp?’. *Terrorism and Political Violence* 20 (2008) 2: 215-233.

Terpstra, Niels, and Georg Frerks. ‘Rebel Governance in Sri Lanka’s ‘Uncleared’ Territories during 1990s and 2000s’. Paper presented at the *9th Pan-European Conference on International Relations*. Giardini Naxos, Italy, September 23-26, 2014.

Tilly, Charles. ‘Terror, Terrorism, Terrorists’. *Sociological Theory* 22 (2004) 1: 5-13.

Townsend, Charles. *Terrorism. A Very Short Introduction*. Oxford: Oxford University Press, 2018.

Tuters, Marc, and Sal Hagen. ‘(((They))) rule: Memetic antagonism and nebulous othering on 4chan’. *New Media & Society* (November 2019), 1-20.

Van der Hulst, Renée. ‘Terroristische netwerken en *intelligence*: een sociale netwerkanalyse van de Hofstadgroep’. *Tijdschrift voor Veiligheid* 8 (2009) 2: 8-27.

Van Deursen, Alexander, Jan van Dijk, and Peter ten Klooster. ‘Increasing inequalities in what we do online: A longitudinal cross section analysis of Internet activities among the Dutch population (2010 to 2013) over gender, age, education, and income’. *Telematics and Informatics* 32 (2015): 259-272.

Van Dijk, Jan. *The Network Society. Social Aspects of New Media*. London/ Thousand Oaks/ New Delhi: SAGE Publications, 2006.

Van San, Marion, and Stijn Sieckelinck. *Idealen op drift. Een pedagogische kijk op radicaliserende jongeren*. Amsterdam: Boom Lemma Uitgevers, 2010.

Vermaat, Emerson. *De Hofstadgroep. Portret van een radicaal-islamitisch netwerk*. Soesterberg: Uitgeverij Aspect, 2017.

Vidino, Lorenzo. ‘The Hofstad Group: The New Face of Terrorist Networks in Europe’. *Studies in Conflict & Terrorism* 3 (2007) 7: 579-592.

Ware, Jacob. ‘Testament to Murder: The Violent Far-Right’s Increasing Use of Terrorist Manifestos’. ICCT policy brief. The Hague, 2020.

Weimann, Gabriel, and Natalie Masri. ‘The Virus of Hate: Far-Right Terrorism in Cyberspace’. Report for the International Institute for Counter-Terrorism. Herzliya, March 5, 2020.

Weimann, Gabriel. ‘Cyberterrorism: The Sum of All Fears’. *Studies in Conflict & Terrorism* 28 (2005) 2: 129-149.

———. ‘Lone Wolves in Cyberspace’. *Journal of Terrorism Research* 3 (2012) 2: 75-90.

———. ‘Terror on Facebook, Twitter, and YouTube’. *Brown Journal of World Affairs* 16 (2010) 2: 45-54.

———. ‘Virtual Training Camps: Terrorists’ Use of the Internet’. In James J.F. Forest (ed.), *Teaching Terror: Strategic and Tactical Learning in the Terrorist World* (Lanham, MD: Rowman & Littlefield, 2006) 110-132.

Yang, Kai-Cheng, Onur Varol, Clayton A. Davis, Emilio Ferrara, Alessandro Flammini, and Filippo Menczer. ‘Arming the public with artificial intelligence to counter social bots’. *Emerging Technologies:*

*Perspectives from Technology Pioneers*, special issue, *Human Behaviour and Emerging Technologies* 1 (2019) 1: 48-61.

Yayla, Ahmet. 'The Reina Nightclub Attack and the Islamic State Threat to Turkey'. *CTCSentinel* 10 (2017) 3: 9-16.

Zelin, Aaron Y. 'Picture Or It Didn't Happen: A Snapshot of the Islamic State's Official Media Output'. *Perspectives on Terrorism* 9 (2015) 4: 85-97.

## Online sources

AIVD. 'Terrorisme'. N.d., https://www.aivd.nl/onderwerpen/terrorisme (accessed April 21, 2020).

Alberts, Jaco, and Steven Derix. 'Hoe georganiseerd waren Samir A. en zijn vrienden?'. *NRC Handelsblad*, April 9, 2005, https://www.nrc.nl/nieuws/2005/04/09/hoe-georganiseerd-waren-samir-a-en-zijn-vrienden-10461552-a102432 (accessed March 23, 2020).

*BBC*. 'Twitter tags Trump tweet with fact-checking warning'. May 27, 2020, https://www.bbc.com/news/technology-52815552 (accessed June 15, 2020).

———.. 'ISIS rebels declare 'Islamic state' in Iraq and Syria'. June 30, 2014, https://www.bbc.com/news/world-middle-east-28082962 (accessed April 25, 2020).

———.. 'Westminster attack: What happened'. April 7, 2017, https://www.bbc.com/news/uk-39355108 (accessed April 26, 2020).

Burk, Jason. 'Technology is terrorism's most effective ally. It delivers a global audience'. *Guardian*, March 17, 2019, https://www.theguardian.com/commentisfree/2019/mar/17/technology-is-terrorisms-most-effective-ally-it-delivers-a-global-audience (accessed June 7, 2020).

Chulov, Martin. 'Losing ground, fighters and morale – is it all over for Isis?'. *The Guardian*, September 7, 2016, https://www.theguardian.com/world/2016/sep/07/losing-ground-fighter-morale-is-it-all-over-for-isis-syria-turkey, (accessed April 17, 2020).

*Cisco*. 'VNI Mobile Forecast Highlights Tool'. N.d., https://www.cisco.com/c/m/en_us/solutions/service-provider/forecast-highlights-mobile.html (accessed April 8,2020).

Cobain, Ian. Nazia Parveen, and Matthew Taylor, 'The slow-burning hatred that led Thomas Mair to murder Jo Cox'. *The Guardian*, November 23, 2016, https://www.theguardian.com/uk-news/2016/nov/23/thomas-mair-slow-burning-hatred-led-to-jo-cox-murder (accessed May 18, 2020).

Cook, Ben. 'Deus Vult: ISIS & the White Nationalist Shooters'. *Redpill Strategies*, December 9, 2019, https://redpillstrategies.co/blog/deus-vult-isis-and-the-white-nationalist-shooters (accessed June 2, 2020).

Davies, Caroline. 'Isis suspect Jack Letts' parents found guilty of funding terrorism'. *The Guardian*, June 21, 2019, https://www.theguardian.com/uk-news/2019/jun/21/jack-letts-isis-suspect-parents-found-guilty-of-funding-terrorism-oxford-syria (accessed April 27, 2020).

*De Nederlandsche Bank*. 'Internetbankieren nu en in de toekomst'. Kwartaalbericht, June 2007, https://www.dnb.nl/binaries/Internetbankieren%20nu%20en%20in%20de%20toekomst_tcm46-156864.pdf (accessed April 16, 2020).

El Damanhoury, Kareem. 'The Daesh State: The Myth Turns into a Reality'. *Center for Global Communication Studies*, July 26, 2016, https://global.asc.upenn.edu/the-daesh-state-the-myth-turns-into-a-reality/ (accessed April 25, 2020).

*Europol*. 'Europol and Telegram take on terrorist propaganda online'. November 25, 2019, https://www.europol.europa.eu/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online (accessed April 7, 2020).

Evans, Robert, and Jason Wilson. 'The Boogaloo Movement Is Not What You Think'. *Bellingcat*, May 27, 2020, https://www.bellingcat.com/news/2020/05/27/the-boogaloo-movement-is-not-what-you-think/ (accessed June 15, 2020).

Evans, Robert. ‘The El Paso Shooting and the Gamification of Terror’. *Bellingcat*, August 4, 2019, https://www.bellingcat.com/news/americas/2019/08/04/the-el-paso-shooting-and-the-gamification-of-terror/ /(accessed May 17, 2020).

Gibbs, Samuel. ‘Google Maps: a decade of transforming the mapping landscape’. *The Guardian*, February 8 2015, https://www.theguardian.com/technology/2015/feb/08/google-maps-10-anniversary-iphone-android-street-view (accessed April 20, 2020).

Gladstone, Rick. ‘Behind a Veil of Anonymity, Online Vigilantes Battle the Islamic State’. *The New York Times*, March 24, 2015, https://www.nytimes.com/2015/03/25/world/middleeast/behind-a-veil-of-anonymity-online-vigilantes-battle-the-islamic-state.html?_r=1 (accessed May 13, 2020).

Griffin, Andrew. ‘Charlie Hebdo: France hit by 19,000 cyberattacks since Paris shootings in unprecedented hacking onslaught’. *Independent*, January 15, 2015, https://www.independent.co.uk/life-style/gadgets-and-tech/news/charlie-hebdo-france-hit-by-19000-cyberattacks-since-paris-shootings-in-unprecedented-hacking-9980634.html (accessed May 5, 2020).

Groen, Janny, en Annieke Kranenberg. ‘Vrij spel voor de jihad’. *De Volkskrant*, February 13, 2006, https://www.volkskrant.nl/cultuur-media/vrij-spel-voor-de-jihad~b5f4773c/ (accessed April 19, 2020).

Groen, Janny. ‘Deze man wilde sterven als martelaar, deradicaliseerde en wil nu helpen islamisten te begrijpen’. *De Volkskrant*, September 28, 2018, https://www.volkskrant.nl/nieuws-achtergrond/deze-man-wilde-sterven-als-martelaar-deradicaliseerde-en-wil-nu-helpen-islamisten-te-begrijpen~b38864cd/ (accessed June 7, 2020).

Gross, Dough. ‘YouTube testing live streaming’. *CNN*, September 13, 2010, http://edition.cnn.com/2010/TECH/web/09/13/youtube.livestreaming/index.html (accessed April 7, 2020).

Healy, Jack, and Sarah Mervosh. ‘El Paso Suspect Ordered Gun and Moved Out in Weeks Before Attack’. *The New York Times*, August 8, 2019, https://www.nytimes.com/2019/08/08/us/el-paso-suspect.html? (accessed May 19, 2020);

Kfir, Isaac. ‘Gaming platforms – a breeding ground for violence?’. *Policy Forum*, October 10, 2019, https://www.policyforum.net/gaming-platforms-a-breeding-ground-for-violence/ (accessed May 17, 2020).

Klepper, David. ‘Facebook removes nearly 200 accounts tied to hate groups’. *ABCNews*, June 6, 2020, https://abcnews.go.com/Business/wireStory/facebook-removes-200-accounts-tied-hate-groups-71101914 (accessed June 15, 2020).

Knauw, Christopher. ‘’A perfect platform’: Internet’s abyss becomes a far-right breeding ground’. *The Guardian*, March 19, 2019, https://www.theguardian.com/world/2019/mar/19/a-perfect-platform-internets-abyss-becomes-a-far-right-breeding-ground (accessed May 17, 2020).

Laningham, Scott. ‘Tim Berners-Lee. Originator of the Web and director of the World Wide Web Consortium talks about where we’ve come, and about the challenges and opportunities ahead’. *IBM Developed,* August 22, 2006, https://www.ibm.com/developerworks/podcast/dwi/cm-int082206txt.html (accessed May 14, 2020).

Lee, Dave. ‘8chan far-right forum offline as Cloudflare cuts support’. *BBC*, August 5, 2019, https://www.bbc.com/news/technology-49232333 (accessed May 31, 2020).

Leskin, Paige. ‘The incredible story of YouTube’s early days and how it rose to become the world’s most popular place to watch’. *Business Insider*, December 18, 2019, https://www.businessinsider.nl/history-of-youtube-in-photos-2015-10?international=true&r=US (accessed April 16, 2020).

Masi, Alessandria. ‘ISIS propaganda Magazine Dabiq For Sale On Amazon Gets Taken Down’. *International Business Times*, October 6, 2015, https://www.ibtimes.com/isis-propaganda-magazine-dabiq-sale-amazon-gets-taken-down-1961036 (accessed April 30, 2020).

McLean, Renwick. ‘Madrid suspects tied to e-mail ruse’. *The New York Times*, April 27, 2006, https://www.nytimes.com/2006/04/27/world/europe/madrid-suspects-tied-to-email-ruse.html (accessed April 20, 2020).

Meeker, Mary. ‘Internet Trends 2019’. *Bond Capital Report on Internet Trends*, June 11, 2019, https://www.bondcap.com/report/itr19/#view/title (accessed June 1, 2020).

Nagle, Angela. ‘Paleocons for porn’. *Jacobin*, February 22, 2017, https://www.jacobinmag.com/2017/02/paleocons-for-porn (accessed May 17, 2020).

Nelson, Ted. ‘Mission statement’. *Project XANADU*, 1960, http://xanadu.com/ (accessed April 23, 2020.

Neumann, Peter. ‘Kaum ein Terrorist ist ein einsamer Wolf‘. *NTV*, October 14, 2016, https://www.n-tv.de/politik/Kaum-ein-Terrorist-ist-ein-einsamer-Wolf-article18854546.html (accessed May 16, 2020)

O'Reilly, Tim. 'What is Web 2.0'. *O'Reilly Media*, September 30, 2005, https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html (accessed April 23, 2020).

Olanoff, Drew. 'Inside Google Street View: From Larry Page's Car To The Depths Of The Grand Canyon'. *TechCrunch*, March 8, 2013, https://techcrunch.com/2013/03/08/inside-google-street-view-from-larry-pages-car-to-the-depths-of-the-grand-canyon/ (accessed April 20, 2020).

Ortiz-Ospina, Esteban. 'The rise of social media'. *OurWorldinData*, September 18, 2019, https://ourworldindata.org/rise-of-social-media (accessed April 30, 2020).

*Oxford English Dictionary*. 'Meme, *n*.'. N.d., https://www-oed-com.proxy.library.uu.nl/view/Entry/239909?redirectedFrom=meme#eid (accessed May 16, 2020).

*Oxford English Dictionary*. 'Terrorism, *n*.'. N.d., https://www-oed-com.proxy.library.uu.nl/view/Entry/199608?redirectedFrom=terrorism#eid (accessed March 31, 2020).

Pannett, Rachel, Rob Taylor, and Rhiannon Hoyle. 'New Zealand Shootings: Brenton Tarrant Bought Four Guns Legally Online'. *The Wall Street Journal*, March 18, 2019, https://www.wsj.com/articles/australian-police-raid-two-homes-in-hunt-for-clues-on-brenton-tarrant-11552872377 (accessed May 19, 2020).

Perry, Keith. 'ISIS hackers intercept top secret British Government emails in major security breach uncovered by GCHQ'. *Mirror*, September 12, 2015, https://www.mirror.co.uk/news/uk-news/isis-hackers-intercept-top-secret-6428423 (accessed May 5, 2020).

Pidd, Helen. 'Anders Breivik 'trained' for shooting attacks by playing Call of Duty'. *The Guardian*, April 19, 2012, https://www.theguardian.com/world/2012/apr/19/anders-breivik-call-of-duty (accessed May 18, 2020).

*Portret*. 'Samir A.: staatsvijand nr. 1, exclusief interview met Nederlands bekendste terreurverdachte'. *KRO*, October 1, 2005, [0:11:45], https://www.vpro.nl/speel~KRO_1233054~samir-a-staatsvijand-nummer-1-reporter~.html (accessed March 24, 2020).

Ranking, Jennifer. 'Laptop containing plans of Belgian PM's home found near terrorists' flat'. *The Guardian*, March 30, 2016, https://www.theguardian.com/world/2016/mar/30/laptop-containing-plans-belgian-pms-charles-michel-home-terrorists-flat (accessed May 4, 2020).

Reich, Aaron. 'TikTok rife with racist, antisemitic content aimed at children – study'. *The Jerusalem Post*, June 18, 2020, https://www.jpost.com/diaspora/antisemitism/tiktok-rife-with-racist-antisemitic-content-aimed-at-children-study-631808?fbclid=IwAR1pLgtUZmhgn0ke5ewx9B6tmzxSR8p32k_ho3xnDhp5h-5gd4KZARrdYF8 (accessed June 24, 2020).

Reuters. 'Suspected New Zealand attacker donated to Austrian far-right group, officials say'. *NBCnews*, March 27, 2019, https://www.nbcnews.com/news/world/new-zealand-attacker-linked-austrian-far-right-group-officials-n987846 (accessed May 17, 2020).

Roser, Max, Hannah Ritchie, and Estaban Ortiz-Ospina. 'Internet'. *OurWorldInData*, 2020, https://ourworldindata.org/internet#the-internet-s-history-has-just-begun (accessed April 14, 2020).

Schlegel, Linda. 'Can You Hear Your Call of Duty? The Gamification of Radicalization and Extremist Violence'. *European Eye on Radicalization*, March 17, 2020, https://eeradicalization.com/can-you-hear-your-call-of-duty-the-gamification-of-radicalization-and-extremist-violence/ (accessed May 28, 2020).

*Statista.* 'Which is the most important device you use to connect to the internet, at home or elsewhere?'. April 2019, https://www.statista.com/statistics/387447/consumer-electronic-devices-by-internet-access-in-the-uk/ (accessed May 14, 2020).

*Trouw*. 'E-mail Hofstadgroep vernietigd door fout AIVD'. November 2, 2006, https://www.trouw.nl/nieuws/e-mails-hofstadgroep-vernietigd-door-fout-aivd~bf139238/ (accessed April 20, 2020).

———. 'Hof krijgt internetles in Hofstadzaak'. June 14, 2007, https://www.trouw.nl/nieuws/hof-krijgt-internetles-in-hofstadzaak~bea5ca66/?referer=https%3A%2F%2Fwww.google.nl%2F (accessed April 19, 2020).

Twente University. 'Hoogleraar pleit voor nieuw sociaal netwerk dat wél let op privacy'. *Emerce*, April 4, 2018, https://www.emerce.nl/wire/hoogleraar-pleit-nieuw-sociaal-netwerk-dat-wl-let-privacy (accessed April 6, 2020).

United Nations Security Council. 'Security Council Unanimously Adopts Resolution Calling upon Member States to Combat, Criminalize Financing of Terrorists, Their Activities'. *United Nations Meetings Coverage and Press Releases*, March 28, 2019, https://www.un.org/press/en/2019/sc13754.doc.htm (accessed April 27, 2020).

Varghese, Johnlee. 'ISIS Releases Training Guide on 'How to Tweet Safely, Without Giving out Your Location to NSA''. *International Business Times*, October 19, 2014, https://www.ibtimes.co.in/isis-releases-training-guide-how-tweet-safely-without-giving-out-your-location-nsa-611734 (accessed May 1, 2020).

*Vice*. 'The Islamic State'. Special news video, 2014, https://video.vice.com/nl/video/the-islamic-state/559ea2a9884e6b677d5e2b25 (accessed April 25, 2020).

*Vision of Humanity*. 'Far-right attacks in the West surge by 320 per cent'. N.d., http://visionofhumanity.org/global-terrorism-index/far-right-attacks-in-the-west-surge-by-320-per-cent/ (accessed May 14, 2020).

*W3C*. 'W3C Semantic Web Frequently Asked Questions'. November 12, 2009, https://www.w3.org/RDF/FAQ (accessed May 14, 2020).

*Wilson Center*. 'Timeline: the Rise, Spread, and Fall of the Islamic State'. October 28, 2019, https://www.wilsoncenter.org/article/timeline-the-rise-spread-and-fall-the-islamic-state (accessed April 25, 2020).

Woolf, Nicky. 'Twitter suspends 235.000 accounts in six months for promoting terrorism'. *The Guardian*, August 18, 2016, https://www.theguardian.com/technology/2016/aug/18/twitter-suspends-accounts-terrorism-links-isis (accessed June 8, 2020).

Yayla, Ahmet. 'Islamic State e-book released to home-school 'lone wolves''. *The Washington Times*, July 10, 2017, https://www.washingtontimes.com/news/2017/jul/10/islamic-state-e-book-released-to-home-school-lone-/ (accessed May 1, 2020).

———. 'Manhattan Bike-Path murderer Followed to the Letter ISIS' Latest 'Terrorism for Dummies''. *The Daily Beast*, November 1, 2017, https://www.thedailybeast.com/manhattan-bike-path-murderer-followed-to-the-letter-isiss-latest-terrorism-for-dummies (accessed May 1, 2020).

Faculty of Humanities
*Version September 2014*

PLAGIARISM RULES AWARENESS STATEMENT

## Fraud and Plagiarism

Scientific integrity is the foundation of academic life. Utrecht University considers any form of scientific deception to be an extremely serious infraction. Utrecht University therefore expects every student to be aware of, and to abide by, the norms and values regarding scientific integrity.

The most important forms of deception that affect this integrity are fraud and plagiarism. Plagiarism is the copying of another person's work without proper acknowledgement, and it is a form of fraud. The following is a detailed explanation of what is considered to be fraud and plagiarism, with a few concrete examples. Please note that this is not a comprehensive list!

If fraud or plagiarism is detected, the study programme's Examination Committee may decide to impose sanctions. The most serious sanction that the committee can impose is to submit a request to the Executive Board of the University to expel the student from the study programme.

## Plagiarism

Plagiarism is the copying of another person's documents, ideas or lines of thought and presenting it as one's own work. You must always accurately indicate from whom you obtained ideas and insights, and you must constantly be aware of the difference between citing, paraphrasing and plagiarising. Students and staff must be very careful in citing sources; this concerns not only printed sources, but also information obtained from the Internet.

The following issues will always be considered to be plagiarism:

- cutting and pasting text from digital sources, such as an encyclopaedia or digital periodicals, without quotation marks and footnotes;
- cutting and pasting text from the Internet without quotation marks and footnotes;
- copying printed materials, such as books, magazines or encyclopaedias, without quotation marks or footnotes;
- including a translation of one of the sources named above without quotation marks or footnotes;
- paraphrasing (parts of) the texts listed above without proper references: paraphrasing must be marked as such, by expressly mentioning the original author in the text or in a footnote, so that you do not give the impression that it is your own idea;
- copying sound, video or test materials from others without references, and presenting it as one's own work;
- submitting work done previously by the student without reference to the original paper, and presenting it as original work done in the context of the course, without the express permission of the course lecturer;
- copying the work of another student and presenting it as one's own work. If this is done with the consent of the other student, then he or she is also complicit in the plagiarism;
- when one of the authors of a group paper commits plagiarism, then the other co-authors are also complicit in plagiarism if they could or should have known that the person was committing plagiarism;
- submitting papers acquired from a commercial institution, such as an Internet site with
- summaries or papers, that were written by another person, whether or not that other person received payment for the work.

The rules for plagiarism also apply to rough drafts of papers or (parts of) theses sent to a lecturer for feedback, to the extent that submitting rough drafts for feedback is mentioned in the course handbook or the thesis regulations.
The Education and Examination Regulations (Article 5.15) describe the formal procedure in case of suspicion of fraud and/or plagiarism, and the sanctions that can be imposed.

Ignorance of these rules is not an excuse. Each individual is responsible for their own behaviour. Utrecht University assumes that each student or staff member knows what fraud and plagiarism entail. For its part, Utrecht University works to ensure that students are informed of the principles of scientific practice, which are taught as early as possible in the curriculum, and that students are informed of the institution's criteria for fraud and plagiarism, so that every student knows which norms they must abide by.

I hereby declare that I have read and understood the above.

Name: Matthijs Koch

Student number: 5996198

Date and signature: June 15, 2020

Submit this form to your supervisor when you begin writing your Bachelor's final paper or your Master's thesis.

Failure to submit or sign this form does not mean that no sanctions can be imposed if it appears that plagiarism has been committed in the paper.