DIGITAL JIHAD

Online Communication and Violent Extremism

edited by **Francesco Marone**
introduction by **Paolo Magri**

ISPI

DIGITAL JIHAD

Online Communication and Violent extremism

edited by Francesco Marone

ISPI

Via Alamanni, 11 – 20141 Milano – Italy
www.ledizioni.it
info@ledizioni.it

Digital Jihad. Online Communication and Violent Extremism
Edited by Francesco Marone
First edition: November 2019

This report is published with the support of the Italian Ministry of Foreign Affairs and International Cooperation, in accordance with Article 23- bis of the Decree of the President of the Italian Republic 18/1967. The opinions expressed are those of the authors. They do not reflect the opinions or views of the Italian Ministry of Foreign Affairs and International Cooperation.

Print ISBN 9788855261357
ePub ISBN 9788855261364
Pdf ISBN 9788855261371
DOI 10.14672/55261357

ISPI. Via Clerici, 5
20121, Milan
www.ispionline.it

Catalogue and reprints information: www.ledizioni.it

Table of Contents

Introduction

Paolo Magri

Throughout history, violent political groups have exploited available means of communications to promote their cause, engage with their audiences and oppose their adversaries.

Clearly, in our age the internet offers tremendous opportunities for violent extremists across the ideological spectrum and at a global level. In addition to propaganda, digital technologies have transformed the dynamics of radical mobilisation, recruitment and participation. At least in the West, few cases of jihadist radicalisation completely lack a web component, including occasional viewing of extremist propaganda.

The study of the dynamics and trends of violent extremism on the internet are particularly relevant to the current evolution of the jihadist threat. While at first sight the collapse of the "caliphate" in Syria and Iraq, the death of Abu Bakr al-Baghdadi in 2019, and the decrease in the number of jihadist attacks in the West since 2017 could suggest violent extremism has entered a phase of relative decline, the web remains a crucial means for radical propaganda, mobilisation, planning attacks and financing.

Even though the jihadist threat has seemingly declined, the danger exists of the internet being an environment where radical messages can survive and even prosper. Online militants and sympathisers are still difficult to counter and continue to represent a critical part of the extremist threat. The vast availability of diverse digital platforms and the continuous development of technology have allowed extremists to rapidly adapt and employ

new communication techniques. However, this does not imply the virtual sphere can replace the real world; rather, online and offline dynamics can complement one another.

Against this background, this ISPI report aims to investigate the current landscape of jihadist online communication, including original empirical analysis. In doing so, the volume does not interpret the internet as a shapeless monolith but tries to highlight the opportunities and limitations of different digital platforms. It also explores the current Italian-language jihadist scenario, thus filling a gap in the analysis of this phenomenon. Specific attention is also placed on potential measures and initiatives to address the threat of online violent extremism.

In the opening chapter Francesco Marone examines the relationship between violent extremism and the tools made available by digital communication technologies. Clearly, this relationship is anything but new. Back in the 1980s, U.S. far-right militants were the first to grasp the potential of the internet, but its use has increased dramatically since then. Traditional "static" websites were initially replaced by forums and chat rooms, then by social media and finally by encrypted messaging applications. In particular, this chapter covers six areas of application for violent extremism: cyberattacks; dissemination of operational instructions; hacking and "doxing"; recruitment and terrorist "virtual entrepreneurship"; propaganda; and financing.

Torres Soriano puts the spotlight on seven "premises" for how jihadist activism has materialised on the internet and what to expect in the coming years. The author highlights not only the strengths of the web, but also its less evident dilemmas and vulnerabilities: the influence of the medium on the key features of online activism; the complex relationship between web presence and engagement in armed jihad in the real world; the inclination of terrorists to become "early adopters" of internet innovations; the dynamics of "Darwinian negative selection" on the web that favour the most sophisticated extremists; and the consequences of the fact the number of people in terrorist organisations in charge of propaganda tasks is usually small.

Terrorist groups such as so-called Islamic State (IS) quickly understood the potential of social media to broadcast their propaganda and gain support. The chapter by Colombo provides an original empirical analysis of Arab-speaking users' discourse about IS on Twitter with a view to identifying the most recurrent arguments for and against this organisation. There is also an exploration of the issue of political and religious leadership in the Muslim world, a crucial aspect for IS given that, since the proclamation of its "caliphate" in 2014, this organisation, unlike other terrorist groups, has presented itself as the political and religious authority of the entire Sunni community.

As Fisher and Prucha emphasise in their chapter, for jihadist groups the online material in Arabic is particularly important because it tends to carry greater authority and is also more extensive than for other languages. Their contribution provides an evidence-based analysis of what jihadist networks share on Telegram (arguably the favoured online platform for jihadists over the last few years) through a content analysis of an Arabic-language IS core channel which collectively has over 111,000 pages. The authors show the jihadist movement thrives on lengthy documents that set out the movement's theology, beliefs and strategy. They further highlight why examining this content matters in order to understand persistent online presence of jihadists and the outlook for their real-world survival.

Mazzoni presents an original in-depth analysis of the Italian-language jihadist scene on Telegram, a topic that has received little attention so far. In particular, the author analyses one of the main Italian-language propaganda channels affiliated with the Islamic State and compares its activity to that of its more developed counterparts in French and English. The chapter also tries to outline the possible development of the Italian-language channels that translate the material produced by IS and its affiliates, taking into account the organisation's recent territorial defeats and the simultaneous decrease in its propaganda material.

As Lombardi and Plebani emphasise in their chapter, IS has been showing signs of profound transformation since 2017,

through an evident change in strategies and communication practices. This contribution explores this interesting period of change, which may be read through the "caliphate's" communication products, in the belief that this change has led to a "legacy of Islamic State" that defines the ongoing, enduring threat of jihadist terrorism.

The last chapter by Bishop and Macdonald focuses on the response to the threat of online extremist content. It is well-known that in the past few years regulatory measures have been imposed that require social media companies to do more to remove terrorist content from their platforms. The chapter examines what form these measures should take, under the premise that there is no one-size-fits-all measure. In particular, the authors argue that efforts to remove online terrorist content should target the whole of the social media ecosystem, not just the social media giants.

Recognising the salience of this ever-changing environment, this ISPI report intends to provide an original, in-depth and updated analysis of online violent extremism, with the aim of presenting important points for reflection on the phenomenon in the West (including Italy) and beyond.

Digital communication technologies can offer ample opportunities for violent extremists, but at the same time they provide formidable instruments to confront the threat and even to promote alternative visions.

Paolo Magri
ISPI Executive Vice President and Director

1. Violent Extremism and the Internet, Between Foreign Fighters and Terrorist Financing

Francesco Marone

This introductory chapter aims to concisely examine the current relationship between violent extremism and the tools offered by digital communication technologies[1], particularly the Web.

As is well-known, the internet has become a crucial environment for violent extremism and for terrorism across the ideological spectrum. It is worth recalling that US far-right militants were the first to grasp the potential of the internet back in the 1980s. Since then its use has increased dramatically. Over time, traditional extremist websites have been replaced by forums and chat rooms[2], then social media and finally encrypted messaging applications ("apps"). In the future the so-called dark web[3] could represent a new frontier.

With regard to jihadist extremism, in recent years online propaganda and communication has moved to a large extent

[1] A. Meleagrou-Hitchens, A. Alexander and N. Kaderbhai, "The impact of digital communications technology on radicalization and recruitment", *International Affairs*, vol. 93, no. 5, 2017, pp. 1233-1249.

[2] A. Zelin, *The State of Global Jihad Online: A Qualitative, Quantitative, and Cross Lingual Analysis*, New America Foundation, 2013. See also Torres Soriano's chapter in this volume.

[3] See G. Weimann, "Going Dark: Terrorism on the Dark Web", *Studies in Conflict & Terrorism*, vol. 39, no., 3, 2016, pp. 195-206.

from open social media such as Twitter[4] to more protected applications such as Telegram[5]. However, the role of non-encrypted social networks remains salient for the debate on violent extremism[6].

The continuous search for new online platforms and services is not surprising. In general, it is evident that the Web offers huge opportunities to pursue various causes, including radical ones. In general, compared to more traditional communication channels, it presents various benefits, including: high level of anonymity; ease of use; economic convenience; widespread availability; interactivity (so-called "Web 2.0" and beyond); difficult control by public authorities; and the possibility to circumvent the constraints of mainstream media.

For instance, various empirical analyses showed how at the height of the self-proclaimed "Caliphate" the Web – and, in particular, social network platforms – had a key role in informing, inspiring and connecting jihadist foreign fighters headed for Syria and Iraq[7].

On the other hand, the internet is not without problems even for extremist activism, ranging from the dissonance among

---

[4] J.M. Berger and J. Morgan, *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter*, Analysis Paper, Brookings Institution, 2015; A. Alexander, *Digital Decay? Tracing Change over Time among English-Language Islamic State Sympathizers on Twitter*, Report, Program on Extremism at George Washington University, 2017.

[5] N. Prucha, "IS and the Jihadist Information Highway – Projecting Influence and Religious Identity via Telegram", *Perspectives on Terrorism*, vol. 10, no. 6, 2016, pp. 48-58; M. Bloom, H. Tiflati and J. Horgan, "Navigating ISIS's preferred platform: Telegram", *Terrorism and Political Violence*, vol. 31, no. 6, 2019, pp. 1242-1254. See also chapter 3 by Ali Fisher and Nico Prucha, and chapter 5 by Valerio Mazzoni in this volume.

[6] See chapter 4 by Matteo Colombo in this volume.

[7] In particular, J.A. Carter, S. Maher and P.R. Neumann, *#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks*, Report, International Centre for the Study of Radicalisation and Political Violence (ICSR), 2014; J. Klausen, "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq", *Studies in Conflict and Terrorism*, vol. 38, no. 1, 2015, pp. 1-22.

"keyboard warriors" who promote action in the real world without putting it into practice to difficulties in maintaining control and discipline for terrorist organisations[8].

Clearly, the Web can perform different functions for extremists and terrorists. This chapter will present and discuss six areas of application, in decreasing order of proximity to the actual use of violence: 1) cyberattacks; 2) dissemination of operational instructions; 3) hacking and "doxing"; 4) recruitment and terrorist "virtual entrepreneurship"; 5) propaganda; 6) financing.

Cyberattacks

When one thinks about terrorism and cyberspace in our time, it is perhaps natural to consider the possibility that terrorist groups such as the so-called Islamic State (IS) or al-Qaeda could launch attacks, even on a large scale, directly through the Web. Outside of the world of terrorism, destructive cyberattacks, such as those on Iran in the late 2000s or on Ukraine in June 2017, have already indicated the seriousness that certain operations can have in the real world[9]. Furthermore, there may also be the risk of a connection between violent extremism and transnational organised criminal networks[10].

Although there has not yet been anything which can vaguely resemble a "cyber 9/11", it is clear that extremist groups could be interested in taking advantage of the internet for offensive actions. Of particular importance would be the case of the so-called Islamic State or Daesh, which has already demonstrated on several occasions its skills in conducting relevant activities on the internet.

---

[8] See chapter 2 by Manuel R. Torres Soriano in this volume.

[9] Cf. F. Rugge (ed.), *Confronting an "Axis of Cyber"?: China, Iran, North Korea, Russia in Cyberspace*, Milan, Ledizioni-ISPI, 2018.

[10] F. Bosco and M. Becker, *Transnational organized crime and violent extremist organisations: Which links?*, Commentary, ISPI, 16 July 2018.

However, compared to reality, today the effects of "cyber-terrorism" appear to be inflated in many respects. In fact, so far terrorist groups have shown neither the intention nor the capability to launch destructive cyberattacks. On the one hand, the intention to use these methods is not well-documented: few groups appear to have genuinely expressed the intent to target critical networks or national infrastructure using cyberattacks. On the other hand, the undeniable experiences and skills of terrorist groups such as IS in the sphere of online propaganda and communication do not necessarily transfer to the ability to launch destructive cyberattacks[11].

Additionally, in general, claims of responsibility for targeted efforts in the virtual arena are not always identifiable. In the real world, a group can "lie about terrorism"[12] in different ways: by taking credit for an attack it did not commit, by disclaiming an attack it actually committed and also by falsely blaming an attack (regardless of whether it actually committed it) on another actor.

As is well-known, the "attribution problem" is even more serious in cyberspace[13]. For example, cyber groups that appear associated with an extremist or terrorist organisation are not necessarily connected to that organisation[14]. On the one hand, an actor could make some malicious online activities appear to be by other actors, including extremist organisations, *to their detriment* (or at the very least not in their interest), in the context of false flag operations. For example, in October 2018 British authorities claimed that the virtual group called

---

[11] R. Bernard, "These are not the terrorist groups you're looking for: An assessment of the cyber capabilities of Islamic State", *Journal of Cyber Policy*, vol. 2, no. 2, 2017, pp. 255-265.

[12] E.M. Kearns, B. Conlon, and J.K. Young, "Lying about terrorism", *Studies in Conflict & Terrorism*, vol. 37, no. 5, 2014, pp. 422-439.

[13] See, among others, T. Rid and B. Buchanan, "Attributing cyber attacks", *Journal of Strategic Studies*, vol. 38, no. 1-2, 2015, pp. 4-37.

[14] A. Alexander and B. Clifford, "Doxing and Defacements: Examining the Islamic State's Hacking Capabilities", *CTC Sentinel*, vol. 12, no. 4, April 2019, pp. 22-28 (p. 24).

"CyberCaliphate" was actually associated with the Russian military intelligence service[15].

On the other hand, especially since extremist groups are able to inspire other actors from a distance without direct contacts, even white lies "for the good" are possible: for example, cyber groups that appear associated with a terrorist organisation, such as IS, are not necessarily connected with that organisation even if they conduct campaigns that (should) *benefit* that organisation and its leadership. These lies "for the good" may not always be appreciated: for example, the "caliphate" already formally disassociated itself from *pro-IS* cyber collectives[16].

Dissemination of Operational Instructions

The use of the internet for terrorism also includes the provision of operational instructions: information for carrying out attacks with explosive devices or with other weapons or tools (including everyday objects, such as knives), but also instructions about operational security (in particular, on how to avoid detection offline and above all online)[17].

In general, with the exception of simple low-tech actions, the preparation and execution of terrorist attacks requires not only, to use the language of organisational studies, a formal "explicit knowledge", but also a "tacit knowledge", which is not codified and difficult to express and transfer[18]. Michael Kenney[19]

---

[15] Government of the United Kingdom, "UK exposes Russian cyber attacks", Press release, 4 October 2019.

[16] R. Bernard (2017), p. 258.

[17] B. Clifford, "'Trucks, Knives, Bombs, Whatever': Exploring Pro-Islamic State Instructional Material on Telegram", *CTC Sentinel*, vol. 11, no. 5, 2018, pp. 23-29 (p. 26).

[18] B.A. Jackson, "Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption", *Studies in Conflict and Terrorism*, vol. 24, no. 3, 2001, pp. 183-213.

[19] M. Kenney, "Beyond the Internet: Mētis, Techne, and the Limitations of Online Artifacts for Islamist Terrorists", *Terrorism and Political Violence*, vol. 22,

adopted a similar distinction between two types of knowledge: the abstract and universal *techne* and the practical and specific *mētis* which adheres to different local contexts. *Mētis* is a type of knowledge that is gradually acquired with experience. Jihadist and other extremist militants operating in hostile environments, such as Western societies after 9/11, have to resort to a range of precautions and restrictions that can have the effect of reducing opportunities for the accumulation of such practical knowledge. For instance, suicide attacks – acts of violence that, if successful, by definition can only be carried out once – prevent learning from trial and error, at least in the case of lone actors or at least autonomous cells with a low level of labor division[20].

In this context, the internet may not be a reliable source of operational knowledge for terrorists; it offers general information in terms of abstract *techne*, but it can hardly convey that practical knowledge in terms of *mētis* that one learns with training and practice in the real world.

Overall, the practical information available on the Web is frequently introductory and generic, in part because the authors and users of the various platforms know that they may be monitored by intelligence services and law enforcement agencies[21]. In many cases the instructions actually available are only useful if the would-be terrorists already have technical skills. Online indications for carrying out terrorist attacks are not infrequently flawed, when not spoiled by errors, including egregious ones[22].

---

no. 2, 2010, pp. 177-197; Idem, "'Dumb' Yet Deadly: Local Knowledge and Poor Tradecraft Among Islamist Militants in Britain and Spain", *Studies in Conflict and Terrorism*, vol. 33, no. 10, 2010, pp. 911-932.

[20] F. Marone, *La politica del terrorismo suicida*, Soveria Mannelli, Rubbettino, 2013.

[21] See M.R. Torres Soriano, "The Vulnerabilities of Online Terrorism", *Studies in Conflict and Terrorism*, vol. 35, no. 4, 2012, pp. 263-277.

[22] See A. Stenersen, "The Internet: A Virtual Training Camp?", *Terrorism and Political Violence*, vol. 20, no. 2, 2008, pp. 215-233; M. Kenney, *Beyond the Internet*, cit., pp. 188-191.

For example, even today, plotters without relevant offline contacts may find difficult and dangerous to synthesise explosive compounds such as TATP (triacetone triperoxide) and then to construct a bomb that really works: the Parsons Green training bombing in London on 15 September 2017, which provoked no fatal casualties, can be considered a good example in this respect[23].

In this field, Telegram has played a major role in recent years. On this free platform, unlike in other messaging services, users can benefit from encrypted messages, remarkable file-sharing capabilities, and the opportunity to publish material in various file formats and house it internally on the platform. Furthermore, Telegram has been generally criticised for its reluctance to regulate extremist content. Thus, it is not surprising that, in addition to purposes linked with propaganda and recruitment, Telegram has been extensively used to disseminate operational instructions as well[24].

In relation to English-language material, mainly directed at a Western audience, as a recent work noted[25], the so-called Islamic State has rarely released official attack-planning material, except for low-tech attacks (stabbings, vehicular assaults, etc.). Thus, a large proportion of instructional manuals distributed by IS supporters on Telegram are actually replicas of instructions developed by al-Qaeda (in particular, *Inspire*, the notorious English-language magazine published by al-Qaeda in the Arabian Peninsula, AQAP) or other jihadist groups, or even sources external to the broader jihadist movement. In fact, these operational materials can of course be used in order to pursue different militant causes, regardless of their original authors and creators.

[23] B. Clifford (2018), p. 26.
[24] Ibid.
[25] Ibid.

Hacking and Doxing

Another significant threat is represented by hacking and so-called "doxing" (or "doxxing"), that is the practice of gathering and disclosing an individual's personally identifiable information (PII) online for different purposes, particularly with the intent of inflicting harm.

To mention one salient example, beginning in April 2015, Ardit Ferizi[26], a Kosovar hacker who studied computer science in Malaysia, acquired direct contacts with Islamic State militants in Syria, including Junaid Hussain, the notorious British online propagandist and influencer (killed by a US drone strike in late August 2015). Ferizi provided support to the jihadist organisation by transmitting PII of US and Western European citizens he had obtained by illegally accessing customer records databases of a US company. This list was published by Hussain on 11 August 2015. Ferizi was finally arrested in Kuala Lumpur in September 2015 and extradited to the United States where he was sentenced to 20 years in prison in September 2016. Ferizi's hacking efforts resulted in "the publication of one of the best-known 'kill lists' released by Islamic State sympathizers, and to date, it remains one of the more sophisticated computer network operations on behalf of the group"[27].

Another, less sophisticated example of doxing comes from Italy. In 2015, several jihadist-inspired Twitter accounts called for the targeting of ten Italian law enforcement officers, indicating personal data, phone numbers and addresses; this information was presumably retrieved from open sources and it was in many cases partial and/or incorrect. In addition, a document calling for the "conquest of Rome", a slogan widely used by jihadist groups[28], was also circulated from one of these accounts. Meriem Rehaily, a young woman of Moroccan origin, living

[26] A. Alexander and B. Clifford (2019), pp. 22-28 (pp. 23-24).
[27] Ibid., p. 24.
[28] F. Marone and M. Olimpio, *"Conquisteremo la vostra Roma". I riferimenti all'Italia e al Vaticano nella propaganda dello Stato Islamico*, Working Paper, ISPI, 2018.

in the province of Padua (North-Eastern Italy), was behind these accounts. In July 2015, Rehaily left for Syria to join IS[29], thanks to online contacts. In the territory of the self-proclaimed "Caliphate" she reportedly deployed her good computer skills, carrying out propaganda and proselytising activities for the jihadist organisation. In December 2017 she was sentenced in absentia to 4 years in prison for terrorist association.

The different experiences of Ferizi and Rehaily clearly show that the level of sophistication in doxing efforts can be highly variable: while Faridi was able to breach the servers of a private company, Rehaily presumably collected open-source information.

The degree of connection with a terrorist organisation is also variable. Rehaily had probably no direct links with relevant IS members in the Levant before she left Italy in 2015. For his part, Faridi was not a full member of the organisation but acquired contacts with prominent Islamic State militants in Syria. By contrast, towards the other extreme of this continuum, the aforementioned Junaid Hussain (aka Abu Hussain al-Britani)[30], after joining IS, supported hacking-related efforts under the banner of the "Islamic State Hacking Division", ISHD (a hacking collective that however has not been officially recognised by IS). In particular, in March 2015, Hussain posted a kill list including US military personnel.

In general, doxing efforts and the dissemination of hit lists may be attractive to aspiring online operatives because they are relatively feasible, even without expert-level hacking skills, and can instigate fear. In addition to promoters of these doxing

---

[29] F. Marone, *Italy's Jihadists in the Syrian Civil War*, Research Paper, The International Centre for Counter-Terrorism – The Hague (ICCT), 2016. See also F. Marone and L. Vidino, *Destination Jihad: Italy's Foreign Fighters*, The International Centre for Counter-Terrorism – The Hague (ICCT) in partnership with ISPI and the Program on Extremism at George Washington University, 2019.

[30] N. Hamid, "The British Hacker Who Became the Islamic State's Chief Terror Cybercoach: A Profile of Junaid Hussain", *CTC Sentinel*, vol. 11, no. 4, April 2018, pp. 30-39.

efforts, extremist sympathizers can also offer their contribution by reposting these hit lists and by providing additional information and instructions. This type of contribution usually requires even less skills and resources[31].

It is worth recalling that the use of online hit lists is not limited to jihadist extremism. Back in the 1990s US extremist anti-abortion activists secured abortion providers' PII and published them as an alleged hit list on the Web. On the other hand, to mention a recent example, the name of Walter Lübcke, the German local politician who was assassinated at his home by a neo-Nazi activist on 2 June 2019, appeared on an online neo-Nazi hit list and his private address was published on a far-right blog[32].

Recruitment and Terrorist "Virtual Entrepreneurship"

The Web can also play a key role in the recruitment of extremists and terrorists. In particular, the interesting and worrying practice of terrorist "cybercoaching" deserves particular attention. We know in fact that extremist "virtual planners" (also known as "virtual entrepreneurs") can target and guide unaffiliated radical sympathizers remotely, only via the Web, in particular through the use of encrypted applications.

One of IS's best-known virtual planners was Rachid Kassim, a former rapper from the French city of Roanne, who was reportedly killed in July 2017 in Mosul, Iraq. His Telegram channel helped guide several recruits in carrying out attacks in France. Another European foreign fighter, the aforementioned Junaid Hussain, enabled at least six terrorist operations in Europe and the United States.

---

[31] A. Alexander and B. Clifford (2019), pp. 24-26.

[32] K. Bennhold, "A Political Murder and Far-Right Terrorism: Germany's New Hateful Reality", *The New York Times*, 7 July 2019.

In fact the phenomenon of "virtual entrepreneurship" was also exported to the other side of the Atlantic. According to an article published in 2017 by Hughes and Meleagrou-Hitchens, out of a total of 38 IS-inspired domestic plots and attacks in the United States between 1 March 2014, and 1 March 2017, at least eight (21%) involved some form of digital communication with virtual entrepreneurs. In addition, they were also involved in at least six other terrorism-related cases, including assisting with logistics related to traveling to join the Islamic State[33]. In America the most sustained efforts came from a group based in Raqqa, Syria, which the FBI has nicknamed "the Legion". The most prominent member of the group was Junaid Hussain.

As the same authors remarked, "to some extent, the emergence of virtual entrepreneurs represents a hybrid between what are commonly seen as the two previous manifestations of the jihadist terrorist threat to the West: networked and inspired lone-attacker plots"[34], combining some advantages of both. In general terms, virtual entrepreneurship can be effective, does not require extensive resources and reduces the risk of being identified and stopped by the authorities.

In general, today the role of the Web for extremist radicalisation and recruitment is crucial. However, it is important to keep in mind that offline interactions in physical networks are often still essential, especially in the most advanced stages of the processes of radicalisation[35].

---

[33] Hughes and A. Meleagrou-Hitchens, "The Threat to the United States from the Islamic State's Virtual Entrepreneurs", *CTC Sentinel*, vol. 10, no. 3, March 2017, pp. 1-8 (p. 1).

[34] Ibid.

[35] See L. Vidino, F. Marone and E. Entenmann, *Fear Thy Neighbor: Radicalization and Jihadist Attacks in the West*, Forwords by B. Hoffman and M. Ranstorp, Report, ISPI in partnership with the International Centre for Counter-Terrorism – The Hague (ICCT) and the Program on Extremism at George Washington University, 2017.

Propaganda

As is well-known, the use of the Web has played a crucial role in the communication strategy of different extremist groups, including terrorist organisations, and several pages in this volume are devoted to this subject.

Understandably, in recent years much attention has been paid to the so-called Islamic State. IS is of course not the first armed group to have made strategic use of modern media, but its level of sophistication has proven unprecedented. Thanks to the technological and communication skills of some of his militants, it has built and institutionalised a vast and complex propaganda machine capable of attracting at least spectators, if not active sympathizers and militants, all over the world[36].

IS's propaganda campaign combines official publications with unofficial, self-produced content. In fact, on the one hand, in order to create and disseminate its propaganda products (videos, audio, images, magazines, songs, even videogames, etc.), the organisation has made use of highly professional communication structures. On the other hand, it can also count on a large number of sympathizers who independently produce and spread messages in support of the self-proclaimed "Caliphate", usually via the Web.

Overall, extremists have proved to be able to adapt changing circumstances and new constraints. In particular, over time, jihadists have progressively moved to encrypted messaging platforms. As has been noted[37], from 2013 to 2015-2016

---

[36] The literature on IS's propaganda is vast. See, among others, A.Y. Zelin, "Picture or it didn't happen: A snapshot of the Islamic State's official media output", *Perspectives on Terrorism*, vol. 9, no. 4, 2015, pp. 85-97; C. Winter, *The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy*, Quilliam Foundation, 2015; H. Ingram, "An analysis of Islamic State's Dabiq magazine", *Australian Journal of Political Science*, vol. 51, no. 3, 2016, pp. 458-477; C. Winter, "Apocalypse, later: a longitudinal study of the Islamic State brand", *Critical Studies in Media Communication*, vol. 35, no. 1, 2018, pp. 103-121

[37] In particular, C. Winter, *Researching Jihadist Propaganda: Access, Interpretation, and Trauma*, Resolve Network Researching Violent Extremism Series, May 2019,

their propaganda was easily accessible to potentially anyone on mainstream platforms, especially Twitter, with a view to maximising their visibility. However, since mid-2015, in front of the reaction of governments and technology corporations, jihadists started to favor other, lesser-known, and less-accessible platforms, particularly Telegram.

In turn, from the summer of 2016 onwards, Telegram started to become less hospitable to jihadist groups and their supporters: dissemination channels that were once public started to become private, and their accessibility has decreased almost exponentially since[38]. However, the platform has not been abandoned[39].

In general terms, building on social movement theory, it can be argued that propaganda and rhetoric of extremist groups, too, is associated with three "framing" stategies (so-called "core framing tasks")[40]: 1) "diagnostic" framing deals with the identification of the problem and its source; 2) "prognostic" framing promotes the solution to the problem; 3) "motivational framing" presents the rationale for action, including the call to arms[41].

Propaganda by extremists is often based on narratives[42], or systems of stories, which together provide an apparently

---

pp. 2-3.

[38] Ibid., p. 7.

[39] The original contributions by Ali Fischer and Nico Prucha (chapter 3) and Valerio Mazzoni (chapter 5) in this volume provide empirical analysis precisely on IS-linked propaganda on Telegram, respectively in Arabic and in Italian.

[40] D.A. Snow et al., "Frame alignment processes, micromobilization, and movement participation", *American Sociological Review*, vol. 51, no. 4, 1986, pp. 464-481; R.D. Benford and D.A. Snow, "Framing processes and social movements: An overview and assessment", *Annual Review of Sociology*, vol. 26, 2000, pp. 611-639.

[41] See, among others, F. Marone, "Examining the Narratives of Radical Islamists and Other Extremely Violent Groups: The Case of the 'Islamic State'", in M. Martellini and J. Rao (eds), *The Risk of Skilled Scientist Radicalization and Emerging Biological Warfare Threats*, Amsterdam, IOS Press, 2017, pp. 64-73.

[42] In particular, K. Braddock and J. Horgan, "Towards a Guide for Constructing and Disseminating Counternarratives to Reduce Support for Terrorism", *Studies in Conflict & Terrorism*, vol. 39, no. 5, 2016, pp. 381-404.

coherent view of the world. Extremist narratives, often endowed with a strong emotional charge, can portray and convey in a concrete and vivid way ideas and values, even abstract ones, making the radical message more incisive and effective. Some extremist narratives can be invented from scratch, but many others represent selective and creative re-interpretations of events, stories and motifs that already exist in a given cultural environment (for example, within a religious tradition)[43].

In general, extremist propaganda has found fertile ground in the Web. First of all, online radical content can be consumed with ease, for free (or at low cost), and potentially at any time. Moreover, as has been noted, the anonymity on the Web tends to create a disinhibition effect that can, in turn, foster increased hostility and polarisation. Additionally, the attendance of online extremist channels can facilitate the isolation of the user from the surrounding context and the inclusion in closed "echo chambers" of like-minded people in which radical interests and beliefs can be further reinforced and amplified, also due to possible (inadvertent) effects of web algorithms[44].

Financing

A further problem is the financing of terrorism and other extremist activities via the Web. It is evident that, much like legal organisations, terrorist groups need economic resources to survive and to conduct their activities, including the preparation and execution of attacks. In this respect, it is important to note that in recent years several terrorist actions, at least in Europe[45],

---

[43] In particular, see J. R. Halverson, H. L. Goodall, Jr. and S. R. Corman, *Master Narratives of Islamist Extremism*, New York. Palgrave Macmillan, 2011; S. Mahood and H. Rane, *Islamist narratives in ISIS recruitment propaganda*, in «The Journal of International Communication», Vol. 23, No. 1, 2017, pp. 15-35.

[44] In particular, A. Meleagrou-Hitchens, A. Alexander and N. Kaderbhai (2017), pp. 1238-1241.

[45] P. Nesser, A. Stenersen and E. Oftedal, "Jihadi Terrorism in Europe: The IS-Effect", *Perspectives on Terrorism*, vol. 10, no. 6, 2016, pp. 3-24 (pp. 15-18).

did not require significant economic resources: in particular, most low-tech attacks (e.g., stabbings) by lone actors or small cells are relatively inexpensive.

Terrorist groups can use various sources and methods for self-financing, from apparently legitimate activities (businesses, donations, etc.) to illegitimate actions such as crimes, to state sponsorship.

In these efforts, the internet can play a significant role, mainly thanks to its relatively high level of anonymity and ease of use. Extremist or terrorist groups can solicit funds directly from their supporters through electronic transfers of money. On-line fundraising activities can also be based on the participation of non-profit organisations and charities (that may be either deceptively abused by the extremist group or consciously complicit with it) or the creation and management of genuine front organisations, also using social media[46].

On the other hand, other methods of online financing do not imply the consent of the source provider (whether it is informed or based on deception)[47]. Cybercrime can be a relevant method in this respect. For example, part of the funding for the devastating jihadist attacks in London on 7 July 2005 derived from credit card fraud[48].

As for money transfer modes, the use of open-loop prepaid card and internet-based payment systems can be particularly troubling[49]. Moreover, cybercurrencies, associated with an even higher level of anonymity and with a decentralised structure, could represent a new frontier for online terrorist financing. Overall, this option can present limitations and risks, such as the rapid and unpredictable fluctuation of virtual currencies.

---

[46] B.U. Başaranel, "Online Terrorist Financing", in M. Conway, L. Jarvis, O. Lehane, S. Macdonald and L. Nouri (eds.), *Terrorists' Use of the Internet: Assessment and Response*, Amsterdam, IOS Press, 2017, pp. 95-108 (pp. 95-96).

[47] Ibid.

[48] M. Jacobson, "Terrorist financing and the Internet", *Studies in Conflict & Terrorism*, vol. 33, no. 4, 2010, pp. 353-363 (p. 357).

[49] B.U. Başaranel (2017).

However, it is worth mentioning that the Izz ad-Din al-Qassam Brigades, the armed wing of Hamas, has already developed a sophisticated campaign to raise funds using Bitcoin, through its website, available in several languages[50].

Conclusion

Despite the collapse of the self-proclaimed Caliphate in Syria and Iraq, the "legacy" of the so-called Islamic State is still relevant[51]. Overall, the jihadist cause remains very present on the Web.

Moreover, serious terrorist attacks such as the massacre in New Zealand on Friday 15 March 2019 strongly remind us that terrorism is not only jihadist. In the far-right attacks at two mosques in Christchurch, the internet (has) had a major role in publicizing violence, with even a livestream on a social network website[52]. Thus, other forms of radical causes, including far-right or anarchist violent extremism[53], rely heavily on the Web.

In the face of these dangers and challenges, public authorities, companies and civil society organisations are stepping up their efforts. This struggle against online violent extremism is complex and demanding and requires targeted initiatives[54]. On the other hand, for the reasons outlined above, it is increasingly relevant.

---

[50] N. Popper, "Terrorists Turn to Bitcoin for Funding, and They're Learning Fast", *The New York Times*, 18 August 2019.

[51] As chapter 6 by Marco Lombardi and Daniele Plebani argues in this volume.

[52] G. Macklin, "The Christchurch Attacks: Livestream Terror in the Viral Video Age", *CTC Sentinel*, vol. 12, no. 6, July 2019, pp. 18-29.

[53] See F. Marone, "The Rise of Insurrectionary Anarchist Terrorism in Italy", *Dynamics of Asymmetric Conflict*, vol. 8, no. 3, 2015, pp. 194-214.

[54] As chapter 7 in this volume by Patrick Bishop and Stuart Macdonald carefully notes.