



Revista Científica General José María Córdova

(Colombian Journal of Military and Strategic Studies)

Bogotá D.C., Colombia

ISSN 1900-6586 (print), 2500-7645 (online)

Journal homepage: <https://www.revistacientificaesmic.com>

The expansion, intensification, and seduction of Islamist terrorism through the internet: A criminological analysis

Miguel Ángel Cano Paños

<https://orcid.org/0000-0001-5426-7227>

macano@ugr.es

Universidad de Granada, Spain

To cite this article: Cano Paños, M. (2019). The expansion, intensification, and seduction of Islamist terrorism through the internet: A criminological analysis. *Revista Científica General José María Córdova*, 17(26), 271-287. <http://dx.doi.org/10.21830/19006586.431>

Published online: April 1, 2019

The articles published by *Revista Científica General José María Córdova* are Open Access under a Creative Commons license: Attribution - Non Commercial - No Derivatives.



Submit your article to this journal:

<https://www.revistacientificaesmic.com/index.php/esmic/about/submissions>



Miles Doctus



Revista Científica General José María Córdova

(Colombian Journal of Military and Strategic Studies)
Bogotá D.C., Colombia

Volume 17, Number 26, April-June 2019, pp. 271-287

<http://dx.doi.org/10.21830/19006586.431>

The expansion, intensification, and seduction of Islamist terrorism through the internet: A criminological analysis

La expansión, intensificación y seducción del terrorismo islamista a través de internet: análisis criminológico

Miguel Ángel Cano Paños

Universidad de Granada, Spain

ABSTRACT. The presence of Islamist terrorism on the Internet has changed quantitatively and qualitatively in recent years. Never, has it been easier to access all kinds of extremist propaganda through the net, in regular and social networks; in particular, thanks to Web 2.0. The stated objective of organizations such as the Islamic State is to spread an extremist ideology and subculture that justifies violence. This group directs its attention, above all, to young Muslims in the Western Diaspora. In this context, this paper analyzes the evolution of the presence of Islamist terrorism on the Internet for which it focuses on the measures recently approved in Europe to confront this ubiquitous, diffuse, and, at the same time, extremely dangerous threat.

KEYWORDS: extremism; intelligence services; Internet: Islamic State; Islamist terrorism; social media

RESUMEN. La presencia del terrorismo islamista en internet ha cambiado cuantitativa y cualitativamente en los últimos años. Nunca, hasta ahora, había resultado tan fácil acceder a toda clase de propaganda extremista a través de la red, en general, y las redes sociales, en particular, gracias a la web 2.0. El objetivo declarado por parte de organizaciones como Estado Islámico es difundir una ideología y una subcultura de naturaleza extremista que justifica la violencia. Este grupo dirige su atención, sobre todo, a jóvenes musulmanes que habitan en la diáspora occidental. En tal contexto, este trabajo analiza la evolución de la presencia del terrorismo islamista en internet, para lo cual se enfoca en las medidas recientemente aprobadas en Europa para enfrentar esta amenaza de carácter ubicuo, difuso y, a la vez, tremendamente peligroso.

PALABRAS CLAVE: Estado Islámico; extremismo; internet; medios sociales; servicios de inteligencia; terrorismo islamista

Section: SECURITY AND DEFENSE • Scientific and technological research article

Received: February 15, 2019 • Accepted: March 22, 2019

CONTACT: Miguel Ángel Cano Paños ✉ macano@ugr.es

"I say to you: that we are in a battle, and that more than half of this battle is taking place in the battlefield of the media."

—Ayman al-Zawahiri, the leader of al-Qa`ida

Introduction

The jihadist invasion of the Internet has allowed organizations such as Al Qaeda and, above all, the self-proclaimed Islamic State (IS) to open a second front against the West and its allies in countries with a Muslim majority. The progressive radicalization of young Muslims of both sexes in the European diaspora cannot be explained without noting the jihadist propaganda circulated on the web. Furthered by the recruitment of new European subjects, Jihadist terrorism has adapted to the technological evolution of the global internet network with amazing swiftness, which has allowed it, on many occasions, to stay one step ahead of the security forces.

Several reasons could be adduced for this advantage. One of them is that terrorist organizations no longer need to issue their communications and threats through their own websites; instead, there is a broad and, at the same time, decentralized network of thousands of sites and forums publishing and disseminating contents of a radical nature. Meanwhile, in the new technologies, the global jihadist movement has found its greatest ally to carry out wide-ranging activities like indoctrinating, spreading its actions, inciting violence, making itself known, and spreading a message of hatred and terror, for example, through social networks or other online media that is easily accessible globally, free of charge, and of broad diffusion. Differently, counterterrorism has been unable to contend with this evolution effectively. The fact is that the global internet network is a dynamic platform that demands constant adaptation and, what is more, it is difficult to legislate (Tapia, 2016).

Jihadist-inspired terrorism has been an enthusiast of technology, which has allowed it to give the activities outlined new effectiveness, and, at the same time, has opened new possibilities for them to interact and foster a vast network of supporters strewn throughout the planet (Cano, 2011; Torres, 2014).

It should be noted that compared to traditional ethnic-nationalist or social-revolutionary terrorist organizations, Islamist terrorism is characterized by its markedly warlike nature and its global reach, its Pan-Islamic religious ideology, and its far-reaching concept of "enemy," intimately tied with its radical opposition to everything that represents Western civilization. Today, Jihadist-based terrorism is no longer personified in a specific

organization or group, instead, it has become a kind of ideology, that instigates, in those individuals and groups who adopt it, the willingness to carry out the program advocated by organizations, such as the mentioned *supra*, in the form of attacks, regardless of whether they are inserted in the terrorist network as a member or as an autodidact, not affiliated with an organization and not directed by their leaders.

It is indeed ironic that Islamist terrorism uses the most modern means of communication to wage an attack against modernity in the name of a primitive ideology. Albeit, the *corpus online* of jihadism includes writings, videos, and audio files, which are mainly released by collaborators, supporters, and followers of the global jihadist movement. This material provides the jihadist scene, distributed all over the world, with both a coherent system of values and a model of life to emulate (Prucha, 2012).

According to Weimann (2010), terrorists target three types of online audiences: (1) actual and potential supporters; (2) the international community in general and; (3) their enemies. In contrast to the nineties, when Al Qaeda operated only through a website (www.alneda.com), today, this organization is present in hundreds of web pages, chat rooms, and jihadist forums. The same can be said of other organizations, such as the Al Nusra Front and, above all, the IS.

While the successes, over the past few years, in the misnamed “global war on terrorism” has deprived the terrorists of many of the physical sanctuaries they once enjoyed, these have been replaced by this internet-provided virtual sanctuary that offers multiple opportunities for propaganda, radicalization, recruitment, and even training. Undoubtedly, the Internet has become an essential vehicle to inspire, motivate, and encourage both radicalization and violence.

As exposed throughout this work, the jihadist presence on the Internet has played a decisive role in the violent radicalization of young Muslims living in Europe (although not the only triggering factor), especially, because of the countless videos available for download and the massive use of social networks by European jihadists. Moreover, the existence of a jihadi virtual library is, in the long term, a real time bomb. This library includes, from concrete information for the planning and execution of terrorist attacks to a pseudo-religious ideology, which is prepped to be used as a mechanism to justify lethal actions (El Difraoui, 2012a).

There is no doubt that the radical Islamist message, spread through the Internet, has penetrated a sector of the Muslim diaspora that lives in the West. In this sense, there is verified information that indicates that a considerable number of individuals affiliated to the

radical Islamist ideology, living in the West, have recently moved to countries such as Iraq or Syria to become “universal soldiers of Allah” (Hernández & Carrión, 2015). Hence, by mid-2015, the number of young Muslims that moved to these two countries from Germany to fight in the ranks of the IS was about 720. Belgian authorities speak of about 562 subjects. Meanwhile, the French Ministry of the Interior has recorded more than 2,000 young French Muslims who, in recent years, have moved to the first front of Jihad. Similarly, the British authorities have presented a figure of about 760 foreign fighters.

These are mostly young Muslims from Berlin, Paris, London or Brussels, who sometimes travel in groups that include individuals from ex hoodlums from marginal neighborhoods to university students and converts from native European families, not to overlook the recent growing prominence of radicalized Muslim women. Terrorist organizations like the IS focus primarily on the former; their fate illustrates a circumstance of capital importance, that even the “losers” may become something, not in the marginal neighborhoods of Berlin or Brussels but the first front lines of the jihad.

In most cases, the Internet is a vital part of the radicalization process because it intensifies and accelerates this process. The global network can provide the user with the information they are looking for, as well as confirm their beliefs. The videos and images reinforce a particular vision of the world and can be powerful catalysts of radicalization. Notably, social networks play a role in transmitting a bucolic and romantic way of life, where fraternity and adventure reign; this way of life is presented by young people that are already in the front line. The Internet also allows individuals to find others that are ideologically akin –something that is, of course, much more difficult in a physical environment– and create an online community, even a subculture. In doing so, abnormal opinions and behaviors are normalized, such as extremist ideological views that defend, among other things, the use of violence to solve problems and avenge eventual redress (Institute for Strategic Dialogue, 2011).

In short, the development of the Internet has drastically changed the structure and expansion of the threat from global Islamist terrorism. It has provided a new space with two very beneficial, although apparently contradictory, characteristics for these organizations and groups. On the one hand, the global network can be an open and passive source, serving for the mere transmission of information; on the other, it provides high (inter) activity through virtual spaces, such as forums and, above all, social networks, which, as will be seen, have a fundamental role in the processes of recruitment, indoctrination, and recruitment (Hussain & Saltman, 2014).

Based on the previous, this work analyzes, from a theoretical stance, the use of the evolution of the Internet by jihadist terrorist groups, currently personified in the self-styled Islamic State (also known as ISIS or Daesh). To this end, special attention was given to virtual sites currently disseminating the message of hatred and incitement to terrorist violence. The following sections will show that the IS has been, perhaps, the first terrorist organization in history to present terror and violence through the Internet with Hollywood-like magnificence, making them tremendously seductive for much of its audience and bringing about terrible consequences for the Western population, demonstrated in acts like the latest terrorist actions committed in London, Barcelona, and Paris.

Thus, the evolution of the presence of Islamist terrorism on the Internet is analyzed from the nineties to the present time. Then, the set of measures that have been approved in recent years in the European context to address this *virtual* threat from Islamist terrorism is presented.

Phases of the jihadi presence on the internet

In general terms, three phases can be distinguished in the history of the jihadist presence on the Internet. At the same time, these phases reflect, to a certain extent, the evolution of this fundamentalist movement.

(1) The second half of the nineties marks the beginning of the jihadist presence on the Internet. At that time, a series of isolated sites with radical Islamist contents began to appear. These sites barely managed to attract attention. First, because –at that time– the Internet had little implantation in the many layers of global society; and second because Al Qaeda was still immersed in the construction of consolidated physical structures, after its creation in 1997. Therefore, it was basically a group of isolated activists, living in the Western diaspora that assumed the task of disseminating propaganda material to foster this developing jihadist movement.

Created in 1996, www.azzam.com was the most influential website at that time. It published its contents in English and contained photos and information about the war in Chechnya, a conflict that, at the time, constituted the jihadist movement's war scenario par excellence. It was the war in the Caucasus that prompted an unprecedented increase in Islamist propaganda via the Internet. Thus, in 1999, www.kavkazcenter.com was created. This multilingual website offered jihadists around the globe a forum for communication and discussion. In 1998, the site, www.alneda.com, also acquired prominence. Its standing was mainly reached because it published its contents in Arabic and indicated a connection to the Al Qaeda organization.

Prompted by the terrorist attacks of September 11, 2001, in the United States, these and other pages of similar content were closed and its administrators prosecuted to all possible extents. Consequently, since 2001, most of the jihadist organizations have not maintained their own web page but, instead, have carried out their proselytizing and propaganda efforts in a decentralized manner through different means. In the first stage, these means include media producers and radical forums, which will be mentioned later.

(2) From 2002 and 2003, jihadist terrorist organizations created a list of proprietary communications production companies. Because of the increase in the number of internet users and a growing interest in contents of a radical nature, Al Qaeda and other terrorist organizations of the same ideological scope were, so to speak, compelled to professionalize the dissemination of their propaganda content and brand their material. As a result of this, they established a series of media servers primarily aimed at endorsing their products through both formal and content brands.

The first media information distribution site was As-Sahab, which originated from the former Al Qaeda communication office in Afghanistan and, to this day, is in the service of Central Al Qaeda in Pakistan. Later, in 2004, the media Global Islamic Media Front (GIMF) group emerged. This exclusively propagandist organization, in principle, lacked contact or direct relationship with a terrorist network. Its fundamental task was the production and distribution of jihadist material. For many experts, these actions created authenticity, identity, and, above all, cohesion among the jihadists (Holtmann, 2012). To this day, media producers are the connection between terrorist organizations and supporters, and online followers.

At its beginnings, the GIMF's priority was the translation –mostly into English, French or German– and subsequent dissemination of jihadist propaganda originally published in Arabic. With this, the Islamists sought to create a kind of counterweight to the Western media, which they considered mere instruments manipulated by the United States and its allies. Thus, the GIMF was, at the time, merely a propaganda platform, making it a challenging instrument to dismantle for the Western security forces because it lacked physical headquarters (Steinberg, 2012a).

To this day, the activities of the GIMF are mainly focused on distributing propaganda to the Muslim diaspora living in Europe or other Western countries. Activists ascribed to this platform exploit the confusion among security forces, politicians, and jurists concerning the separation of innocuous propaganda and that associated with terrorist activity.

On the other hand, as indicated previously, from 2002 and 2003, the Islamist terrorist organizations forsook their efforts to create their own websites. The constant cy-

ber-attacks on these sites drove their directors to adopt alternative strategies to maintain a more horizontal and diffuse internet presence. Thus, internet forums became the main product of this new stage in which terrorist organizations adapted to the emergence of the so-called web 2.0., a new generation of portals based on virtual social communities and a range of services that promote collaboration and the active exchange of information among users. As a result, radical internet users abandoned the profile of passive consumers of the materials accessible through the web (Web 1.0) and became involved in an online community that also allowed them to become content producers (Torres, 2014).

The most popular jihadi forums of the Islamist community include Qalah, Al-Shamikh, Majahden or Al-Faloja. In these forums, the members use mainly Arabic, although, in recent years, they have opened sub-forums that use European languages. Unlike traditional web pages, these forums allow their users to establish direct contact and interact with other ideologically akin members and to discuss issues related to militant jihadism. It must be said that the vast majority of these forums are managed from the European diaspora or Arab countries. However, these forums have now lost prominence, which has been fundamentally assumed by social networks (the result of the consolidation of the Web 2.0), which begins the third and final phase of the jihadist presence on the Internet.

(3) The main novelty of this third and –until now– the last phase of the jihadist presence on the Internet has been the pervasiveness of audiovisual media (Steinberg, 2012b). Since 2008, technological development has diversified and increased the jihadist presence on the web. This evolution has been reflected especially in the use of social networks such as Facebook and Twitter, and platforms for repositioning videos, such as YouTube. In this sense, the so-called web 2.0 has allowed jihadists to disseminate their propaganda material in a more detailed manner and reach a considerably higher number of potential recipients. Their participation in these new means of virtual interaction offers jihadists the opportunity to address both individuals and groups directly and selectively instead of waiting for internet users to visit pages with radical Islamist content eventually.

In general terms, the current third phase of “cyber jihad” is fundamentally marked by the following three fundamental developments: 1) Jihad propaganda has been expanded to social networks and smartphones, 2) Jihadists have tried to control of a series of very popular Islamist forums in the Islamic world and 3) The global jihadist movement has intensified its activities in the so-called Deep Net and, above all, Darknet (or Dark Web), which can be accessed by downloading software to the computer. This develop-

ment has been driven not only by technical advances but also by the closure or disappearance of some of the most important jihadi websites and radical forums since 2008.

As mentioned, much of the Islamist propaganda is currently transmitted through social networks such as Facebook or Twitter, as well as through audiovisual platforms such as YouTube. On Facebook, for example, groups of friends, supporters of radical Islamism, can conduct interactive and direct exchanges of recent terrorist actions, jihadist publications or the evolution of ideological thinking. At the same time, social networks represent a communication mechanism that greatly facilitates recruitment and recruitment activities.

In short, the inherent interactivity of social networks, blogs, jihadist forums, and video hosting sites blurs the lines that limited previous generations of terrorists and supporters to pamphlets, newspapers, and news bulletins. This possibility encourages active participants in these types of forums to more easily see themselves as part of a broad global jihadist movement and not as mere casual readers or online viewers. In this way, these subjects can eventually become involved in more significant activities, whether active propaganda, indoctrination, financial support, or –what is most concerning– joining a terrorist network (Collins, 2014).

Measures adopted in Europe to counteract the radical message

As pointed out in the previous section, the global internet network is currently being used by Islamist terrorism as a pivotal element to spread propaganda, recruit potential jihadists, radicalize, coordinate terrorist activities, and glorify the atrocities committed by organizations such as the IS. At the same time, the internet has become the primary source of intelligence gathering against terrorism, enabling the disruption of a growing group of terrorist projects that had their starting point in cyberspace. Similarly, many radicals have been detected and neutralized thanks to their “digital traces.” Security forces can use, for instance, jointly produced jihadist propaganda videos disseminated through new internet platforms, to have a window to observe terrorist tactics, their techniques, and procedures and eventually find the place of residence of the producers of these videos.

The fact is that the openness of the new media, the result of the development of Web 2.0, has provided the jihadist world advantages but not without considerable drawbacks. For example, the infiltration of jihadist discussion forums is undoubtedly one of the most effective methods in the fight against radicalization. In these cases, disinformation is one of the different influencing possibilities. Terrorists must restrain from providing operatio-

nal information through the net, as they run the risk of being discovered by intelligence services. Furthermore, groups created in social networks, such as Facebook, which sympathize with the jihadist cause, are easier to identify and dismantle than in closed forums. Unlike in jihadist forums, in social networks, it is relatively easy to detect propaganda, ideology or incitement to violence, which facilitates criminal prosecution.

All these aspects contribute to the security forces being able to easily detect the transversal connections of internet users through groups of friends on Facebook and followers of specific Twitter, Instagram or Telegram accounts, and discover online networks of supporters of radical Islamism, even locate some of its members geographically. Therefore, many jihadists and sympathizers abstain from inciting violence on the net. However, the diffusion and, above all, the quantitative and qualitative increase of web pages with jihadist content greatly hinder the resources available to the security forces (El Difraoui, 2012b).

In Europe, a series of preventive and, mainly, repressive measures have been developed to confront Islamist terrorism using the internet, which can be contained in the following three categories: 1) The promotion of surveillance operations and infiltration of jihadist activity carried out in online and offline environments, if necessary; 2) The use of a strategy to reduce the jihadist offer, resorting to penal measures; and 3) The development of preventive activities to reduce demand by offering the so-called “counter-narratives” and ambitious programs to promote social and labor integration, as well as equal opportunities within the national and foreign collective that are part of the citizenship of a country. In the following paragraphs, we will analyze the first of these three categories.

In 2007, the European Police Office (Europol), in Europe, created an information portal called Check the web to improve the surveillance and analysis of jihadist propaganda on the Internet. Its objective was to promote coordination among the member countries and avoid the squandering of existing resources as a result of overlapping efforts. Currently, this portal holds an electronic reference library of everything related to online jihadist terrorist propaganda. It catalogs original statements, publications, videos, and audios produced by terrorist groups or their supporters. The competent authorities of the Member States of the European Union (EU), as well as third countries, and associated entities can access these materials and analyze their content created directly by Europol.

In June 2011, the European Commission, with the collaboration of Germany, Belgium, Spain, the Netherlands, and the United Kingdom –which were later joined by six other countries– created the Clean IT initiative. The main objective of Clean IT

is to promote an innovative process to facilitate dialogue between organizations of the public and private sectors with the global internet network as a backdrop (Ministerie van Veiligheid en Justitie, 2013). In the course of this dialogue, the terrorist's use of the Internet should be analyzed and the possible ways to reduce its use should be explored.

Another noteworthy measure adopted at the EU headquarters is the Internet Reference Unit (IRU), launched in July 2015 by Europol. The IRU is a key tool of the European Counter Terrorism Center (ECTC). It is a specialized research unit whose primary objective is to flag terrorist content and propaganda online and provide strategic and operational support to both Internet service providers and the EU Member States. Its intention is to, first, effectively detect and then eliminate online terrorist contents and materials. The IRU is constituted by a team of professionals with multiple and diverse knowledge and skills, from experts in terrorism of religious inspiration to translators, computer programmers, and experts in the fight against terrorism from a policing and legal perspective (EU Internet Referral Unit, 2016).

In line with the strategic objectives of Europol, the IRU focuses primarily on three main lines of action: 1) effectively countering terrorist efforts of radicalization and online recruitment by reinforcing an adaptive derivation capacity while carrying out mapping activities and exerting influence on terrorist propaganda networks through the internet; 2) provide a central support capacity for Internet research, based on operational support and strategic analysis; and 3) strive to become a European Center of Excellence, strategically reinforcing cooperation agreements with partners and investing resources in research and development (R & D) coordination and becoming a center of innovation for both Europol and the EU Member States in the field of combating terrorism (EU Internet Referral Unit, 2016).

The United Kingdom has played a leading role in this field; its 2006 and 2009 counter-terrorism strategies called Contest and, especially, Prevent, emphasized the role played by internet forums, social networks, and video platforms as important mechanisms used by Islamist terrorism to recruit, indoctrinate, and even train potential suicide bombers. Fittingly, in 2010, the Association of Chief Police Officers (ACPO) promoted the Counter-Terrorism Internet Referral Unit (CTIRU), a special unit attached to the Metropolitan Police Counter Terrorism Command. The CTIRU is in charge of reporting websites of a radical nature, blocking them, and shutting them down if necessary. The CTIRU works principally with internet service providers, with the joint objective of eliminating extremist and terrorist material. Its activity is mainly focused on analyzing all the terrorist material created and developed in the United Kingdom.

The activities carried out by the police officers assigned to the CTIRU are not limited to searching the internet daily for terrorist material; they also analyze the information received from the general public. The organization has an online system of information and complaints available to citizens. By visiting www.gov.uk/report-terrorism any citizen can, anonymously, fill out a form they encounter the following material on the net: 1) articles, images, speeches or videos promoting terrorism or incitement to violence; 2) content aimed at inciting people to commit acts of terrorism; 3) extremist or terrorist organizations websites; and 4) videos that feature terrorist attacks. When the CTIRU discovers websites with violent radical content, it contacts the internet service providers to request their removal. If the material is of a criminal nature, under the provisions of the British anti-terrorist legislation, the appropriate authorities are informed to initiate the corresponding investigation to establish accountabilities.

Since its creation, and at the request of CTIRU, around 300 companies worldwide have removed materials that include propaganda videos, materials that show executions, and speeches that explicitly call for racial or religious violence from the net. By December 2017, around 300,000 pages containing illegal terrorist material had been removed from the Internet at CTIRU's request.

In 2007, in Germany, the Berlin-based Joint Internet Center (*GIZ, Gemeinsame Internet-Zentrum*) was created. Personnel of the Office of Protection of the Constitution (BfV), the Federal Bureau of Criminal Investigation (BKA), the Military Intelligence Service (MAD), and the State Attorney General's Office (GBA) cooperate in this institution. The work carried out by the GIZ pursue the following three objectives: 1) The early recognition of extremist and terrorist activities on the net, 2) Discovering terrorist attack plans or preparations 3) Understanding and perceiving the new-member recruitment and radicalization efforts of radical Islamists (Bundesamt für Verfassungsschutz, 2019).

The experts working at the GIZ observe the presence and development of the jihadist movement on the internet, and transfer the results of their research to the Ministries of Defense and Interior, as well as to the competent bodies of the *Bund* (Federation) and the different *Länder* (federal states). If one considers that around two-thirds of all internet users and the majority of jihadist page managers do not code their IP addresses through proxy servers, all of them can, in principle, be easily identified and located¹.

1 In 2007, the Austrian police was able to identify Mohammed Mahmoud, manager of the Globale Islamische Medienfront (GIMF) media platform, which is basically the German franchise of this platform that operates worldwide. His arrest possible because he used a computer in the house that he shared with his parents, with-

However, the GIZ not only performs observation tasks, but it also infiltrates the different jihadist networks with an online presence. Thus, GIZ workers converse in forums with jihadist sympathizers, also advising confidants who are active in the network.

Finally, in 2014, the Intelligence Center for Counter-Terrorism and Organized Crime (CITCO) was created, in Spain. This body is dependent on the State Secretariat for Security and which involved the integration of the National Anti-Terrorism Coordination Center (CNCA) and the Center for Intelligence Against Organized Crime (CICO) in the same device (Ministerio del Interior, 2014). The CITCO is made up of members of the National Police Force, the Civil Guard, the Customs Surveillance Service, officials of penitentiary institutions, members of the Armed Forces, and staff of the National Intelligence Center (CNI).

Among other functions, this body is responsible for receiving, integrating, and analyzing all available strategic information related to terrorism, organized crime, and violent radicalisms, for which it draws intelligence and foresight. In this sense, one of its main tasks is to make observations directly and receive information provided by third parties concerning all terrorist activity that takes place on the Internet.

Within the framework of the National Strategic Plan to Combat Violent Radicalization, the Spanish Ministry of the Interior launched, at the beginning of December 2015, a web page whose objective was to use all citizen information to act on the recruitment of future Islamist radicals on the internet and online jihadist narrative. The website www.stop.radicalismos.es allows any citizen to anonymously expose possible situations of radicalized individuals or groups, individuals who have moved to areas of conflict, and radical contents on the internet. This page is available in Spanish and Arabic. There is also a state-of-the-art police application for cell phones called Alertacops, which includes a tab that allows anonymous reporting of extremist and terrorist behaviors in both online and offline environments. All the information obtained goes directly to the CITCO, which is the central receiver of all the information.

The main issue that arises concerning the observation and infiltration measures analyzed in the previous paragraphs is to what extent can an online content be blocked or eliminated if it does not violate the law directly. Documents screened by the European Digital Rights Association (EDRi) on the Clean IT program have shown that a general understanding of what constitutes “illegal content” can lead to forms of censorship be-

out having adopted any security measure to protect his IP address. As a result of this detention in Austria, eight other GIMF members, residing in German territory, were identified. In this respect, see Salloum (2014).

yond what is required by law and undermines fundamental principles supported by the constitution such as ideological freedom or freedom of expression (Ragazzi, 2014). To read further on this matter see European Digital Rights [EDRI] (2012).

Conclusions

The jihadist presence on the internet has changed quantitatively and qualitatively in recent years. Never before has it been so easy to access all kinds of extremist propaganda on the net and the new active social media, resulting from Web 2.0. Recently, the audiovisual propaganda distributed by the IS has expanded considerably. Similarly, it can be observed how, more and more frequently, supporters and followers of radical Islamism take center stage, while the terrorist organizations themselves remain in the background.

The Internet has provided terrorists with a new and wide-ranging virtual realm to carry out their ideological operations. Terrorist organizations are no longer confined to specific physical regional borders. Now, terrorist networks can recruit members anywhere in the world. Instead of waiting for internet users to access their websites and propaganda materials, terrorists, their followers, and supporters can now seize, indoctrinate and, if necessary, mobilize subjects through online platforms such as Facebook or YouTube.

The best way to persuade someone to support a cause is to create an emotional, psychological or intellectual link with the victim. A potential new member must perceive that he or she is part of a community. The proliferation of multimedia materials with a high emotional content through different channels of open, fast, and direct global communication create, among the users of these materials, the feeling of belonging to an international community or a jihadist subculture that exploits the new cyber-media to present this community as egalitarian, at the same level and with almost the same rights as other communities and cultures.

The danger inherent in the “internet and jihadist propaganda” binomial has sparked debates in political, police, and academic spheres concerning the most effective way to counter the presence of Islamist terrorism on the Internet. These discussions have yielded two mindsets. The first approach favors all repressive measures, considering the recent exponential increase and effectiveness of the jihadist movement in disseminating its program of hatred and incitement to violence on the net. Its objective is to assiduously observe the jihadist presence online, close those websites with radical content, and identify and expunge the most active jihadists. The second approach is to adopt progressive measures that require, among other things, combating terrorist propaganda through a

“counter-narrative.” The defenders of this strategy are often skeptical of interventions aimed primarily at censoring jihadists content on the Internet because they consider that the fundamental problem lies in the dissemination of extremist *ideology* and subculture that justifies violence. Therefore, they believe that it is best to counteract this danger through alternative discourses disseminated through the net, as well as through ambitious programs to prevent radicalization and de-radicalization, developed, mainly, in Western countries (Cano, 2018).

After the analysis carried out throughout this work, it can be affirmed that there are solid arguments for the two strategies outlined in the previous paragraph. Undoubtedly, it is necessary to identify and, whenever possible, hold the activists that move continuously between virtual and physical reality accountable for activities typified as terrorist crimes by the Western mainstream criminal legislation; for example, for the glorification of terrorism or the training of future jihad fighters. However, it is unclear whether these proceedings should be maintained at all costs, especially regarding the extremist activities carried out on the Internet, which are merely activities of ideological indoctrination. In Spain, there are currently rulings issued by the Supreme Court (for example, STS 661/2017 of October 10) that have revoked previous rulings by the National Court. For instance, a ruling that condemned the accused of terrorist activities was revoked under the Court of Cassation’s argument that the conducts did not represent a criminal value; therefore, the acts lacked any terrorist connotation (Cano & Castro, 2018).

It must also be borne in mind that the Internet is currently an ideal place where security forces can follow the tactical, strategic, and ideological evolution of the jihadist movement. For this reason, websites of extremist nature are enormously critical for security apparatuses, for whom the possibility of surveillance and analysis of the information circulating there is vital.

As indicated at the beginning of this paper, the topic analyzed here will be presented in two separate articles. This first article analyzed the evolution of the presence of Islamist terrorism on the Internet, as well as the set of measures that have been approved in the European context in recent years to face this *virtual* threat from Islamist terrorism. The second article will deal with what, from criminology, is known as the “environmental element” of crime, circumscribed, in this case, to terrorist behavior in the context of the Internet. To this end, the *online* sites with jihadist propaganda will be analyzed attentively, as well their reaches in a large sector of the Muslim population settled in Europe.

Disclaimer

The author declares that there is no potential conflict of interest related to the article. The work is part of the research project *Criminología, evidencias empíricas y política criminal. Sobre la incorporación de datos científicos para la toma de decisiones en relación con la criminalización de conductas*. State Research Agency (AEI) / Ministry of Science, Innovation, and Universities, and the European Union (Ref. DER2017-86204-R). Principal researcher: Fernando Miró Llinares.

Funding

The research project, from which this article is derived, was financed by the State Research Agency (AEI)/Ministry of Science, Innovation, and Universities, and the European Union, through the European Regional Development Fund –FEDER– (Ref. DER2017-86204-R).

About the author

Miguel Ángel Cano Paños graduated in Law at the Universidad de Barcelona (Spain). He holds a degree in Criminology from the Universidad de Barcelona (Spain). Ll. M. by the Westfälische Wilhelms-Universität Münster (Germany). He holds a Ph.D. in Law from the University of Potsdam (Germany) and Criminology from the Universidad de Murcia (Spain).

<https://orcid.org/0000-0001-5426-7227> - Contact: macano@ugr.es

References

- Bundesamt für Verfassungsschutz. (2019). *Gemeinsames Internet Zentrum (GIZ)*. Recuperado de <https://www.verfassungsschutz.de/print/de/arbeitsfelder/af-islamismus-und-islamistischer-terrorismus/gemeinsames-internetzentrum-giz>.
- Cano, M. A. (2011). El binomio Internet/terrorismo islamista. *Iter Criminis*, 21, 115-161.
- Cano, M. A. (2018). La lucha contra la amenaza yihadista más allá del derecho penal. Análisis de los programas de prevención y des-radicalización a nivel europeo. *Revista de Estudios en Seguridad Internacional (RESI)*, 4(2), 177-205.
- Cano, M. A., & Castro, F. J. (2018). El camino hacia la (ciber)yihad. Un análisis de las fases del proceso de radicalización islamista y su interpretación por parte de los tribunales españoles a partir de los datos suministrados por sentencias judiciales. *Revista Electrónica de Ciencia Penal y Criminología*, 20, 1-36.

- Collins, L. (2014). "Jihad Cool": The young Americans lured to fight for ISIS militants with rap videos, adventurism and first hand accounts of the 'fun' of guerrilla war. *Daily Mail*. Recuperado de www.dailymail.co.uk/news/article-2661727/Jihad-Cool-The-young-Americans-lured-fight-ISIS-militants-rap-videos-adventurism-hand-accounts-fun-guerrilla-war.html.
- El Difraoui, A. (2012a). Jihad.de. Jihadistische Online-Propaganda: Empfehlungen für Gegenmaßnahmen in Deutschland. *SWP Studie*, 5, 5-29.
- El Difraoui, A. (2012b). Web 2.0 – mit einem Klick im Medienjihad. En G. Steinberg (Ed.), *Jihadismus und Internet: Eine deutsche Perspektive* (pp. 67-75). Berlin: Stiftung Wissenschaft und Politik (SWP).
- EU Internet Referral Unit. (2016). *Year one report. Highlights*. Recuperado de <https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-year-one-report-highlights>.
- European Digital Rights (EDRi). (2012). *Clean IT - Leak shows plans for large-scale, undemocratic surveillance of all communications*. Recuperado de <https://edri.org/cleanit/>.
- Hernández, I., & Carrión, F. (2015, marzo 9). Diez mil europeos a la yihad. *El Mundo*. Recuperado de <https://www.elmundo.es/internacional/2015/03/09/54fc9cae268e3ef12b8b4578.html>.
- Holtmann, P. (2012). Virtual leadership: How Jihadists guide each other in cyberspace. En R. Lohlker (Ed.), *New approaches to the analysis of Jihadism. Online and Offline* (pp. 63-124). Viena: Vienna University Press.
- Hussain, G., & Saltman, E. M. (2014). *Jihad trending: A comprehensive analysis of online extremism and how to counter it*. London: Quilliam Foundation.
- Institute for Strategic Dialogue. (2011). *Radicalisation: The role of the internet*. Recuperado de <https://bit.ly/2H9xQkn>.
- Ministerie van Veiligheid en Justitie. (2013). *Reducing terrorist use of the Internet*. Recuperado de <https://bit.ly/2SNI5NI>.
- Ministerio del Interior. (2014). *El Ministerio del Interior crea el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO)*. Recuperado de http://www.interior.gob.es/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/2624738.
- Prucha, N. (2012). Die Vermittlung arabischer Jihadisten-Ideologie: Zur Rolle deutscher Aktivisten. En G. Steinberg (Ed.), *Jihadismus und Internet: Eine deutsche Perspektive* (pp. 45-55). Berlin: Stiftung Wissenschaft und Politik (SWP).
- Ragazzi, F. (2014). Towards "Policed Multiculturalism"? Counterradicalization in France, the Netherlands and the United Kingdom. *Les Etudes du CERJ*, 206, 1-37.
- Salloum, R. (2014). Der Brandstifter aus Wien. *Spiegel Online*, edición de 6 de agosto. Recuperado de <http://www.spiegel.de/politik/ausland/islamischer-staat-mohamed-mahmoud-der-brandstifter-aus-wien-a-1046964.html>.
- Steinberg, G. (2012a). Die Globale Islamische Medienfront (GIMF) und ihre Nachfolger. En Autor (Ed.), *Jihadismus und Internet: Eine deutsche Perspektive* (pp. 23-31). Berlin: Stiftung Wissenschaft und Politik (SWP).
- Steinberg, G. (2012b). Jihadismus und Internet. Eine Einführung. En Autor (Ed.), *Jihadismus und Internet: Eine deutsche Perspektive* (pp. 7-22). Berlin: Stiftung Wissenschaft und Politik (SWP).

- Tapia, M. E. (2016). Análisis de la estrategia comunicativa del terrorismo yihadista: El papel de las redes sociales. *Documento Opinión - Boletín Instituto Español de Estudios Estratégicos*, 1, 370-384.
- Torres, M. R. (2014). *Al Andalus 2.0*. Granada: Biblioteca GESI.
- Weimann, G. (2010). Terrorist Facebook: Terrorists and online social networking. En M. Last, & A. Kandel (Eds.), *Web intelligence and security. Advances in data and text mining techniques for detecting and preventing terrorist activities on the web* (pp. 19-30). Amsterdam: IOS Press.