religions

MDPI

Article

Cyberterrorism and Religious Fundamentalism: New Challenges for Europe in the Age of Universal Internet Access

Silvia Baldassarre

Dipartimento di Scienze Giuridiche, Università degli Studi di Firenze, 50127 Firenze, Italy;
silvia.baldassarre@unifi.it

Abstract: Digital technology is now a fundamental and indispensable component of daily life. While the great opportunities offered by cyberspace are undoubted, the growing security challenges and threats it brings should not be overlooked. Cyberspace, by its nature transnational and elusive regarding forms of control, is useful to terrorism because it allows not only the propaganda of fundamentalist doctrines but also the creation and manipulation of information; the apology and dissemination of information instrumental to the processes of radicalisation; the use of devices capable of transversally violating the security of technical and virtual infrastructures that are critical to the security of nations; the operational planning of terrorist activities; and the recruitment, financing, and training of recruits. The so-called "new terrorism", religiously motivated, makes extensive use of the digital tool. After an excursus concerning the use of cyberspace by religious fundamentalist groups and the transformation of religiously motivated terrorism, this paper focuses on the analysis of the European legal response and on the need for global and shared European action.

Keywords: cyberterrorism; religion; religious fundamentalism; European law

check for updates

Citation: Baldassarre, Silvia. 2023. Cyberterrorism and Religious Fundamentalism: New Challenges for Europe in the Age of Universal Internet Access. *Religions* 14: 458. https://doi.org/10.3390/rel14040458

Academic Editors: Francesco Alicino and Roy C. Amore

Received: 16 January 2023
Revised: 26 February 2023
Accepted: 25 March 2023
Published: 29 March 2023

1. Introduction

Digital technology is, in daily life, a fundamental and indispensable component. It acquired this role in very few decades if we consider that its diffusion took place since after World War II when computers became widespread, devices capable of electronically imitating the working mechanisms of the human brain but with a zero margin of error in mathematical operations, with minimal response times, and with the possibility of storing a large amount of data. Automatic information treatment, therefore, appears to be the third major innovation after the invention of writing and the spread of printing. Among the stages that, since the 1960s, in rapid succession have realised the "information technology revolution", there is certainly the invention of the Internet and its spread in the 1990s. "Cyberspace" has become a real possibility. It constitutes an intangible dimension that enables computers—and so the users—around the world to communicate through a single network. By 2022, about 63.1% of the world's population is online (Statista Research Department 2022), although access to the Internet is still almost entirely reserved for economically advanced countries.

The Internet has profoundly affected individual and collective life in a few decades, transforming many aspects, not only of communication, but also of social, political, economic, and cultural life.

In recent experience, cyberspace, "place-non-place", has represented an escape during the forced confinement and numerous restrictions that were imposed in many Countries in the 2020–2021 biennium to face down the COVID-19 pandemic. During this period, there has been a marked increase in Internet browsing, not only for professional and study purposes, but also "the search for meaning," in its multiform expressions, has produced an increase in access to cultural and religious websites. A study by the University of Copenhagen showed that in 95 countries, daily Google searches for the term "prayer" or similar terms, increased by 50 percent compared to the pre-pandemic period (Sinding Bentzen 2020). The support of information technology tools offered humanity, during this period, the opportunity to continue to work, study, communicate, worship, and explore cultural and recreational spaces.

Many religious groups recorded and broadcast the services online (Consorti 2020; Balsamo and Daniela 2020). The evangelical periodical Christianity Today at the toughest time of the pandemic so titled an article: “When God Closes a Church Door, He Opens a Browser Window” (Shellnutt 2020). Already for several years, many religious communities, especially Protestant ones, have offered services through streaming, on social networks, and through the Internet (Bingaman 2023; Jonveaux 2021; Obadia 2017; Dawson and Cowan 2004, pp. 6–7), but what has happened in recent months is unprecedented. The virtual network has not only made it possible to attend liturgies, but also to organise, by religious groups, fundraisers to try to compensate for the financial losses suffered because of the confinements.

While the great opportunities offered by cyberspace are undoubted, the growing securitarian challenges and threats it brings about should not be overlooked. The transnational nature, ease of access, and real-time communication have made cyber space a virtual place suitable, as will be illustrated in the following pages, for the spread of fundamentalist terrorism. The numerous groups that instrumentalise religion, subordinating it to fanatically delineated political, ideological, and identity projects, have spread over the last thirty years and, while previously they were generally rooted in a specific territory, since the 1990s—also thanks to the Internet—they have extended their range of action globally; the evolutionary path that has modified their operational strategies over the years will therefore be outlined. In § 4 some measures adopted by the European Union to fight international terrorism, also in its cyber dimension, will be illustrated, without any claim to exhaustiveness.

2. Cyberspace and Radicalisation

Cyberspace, by its nature transnational and elusive regarding the forms of control, is useful to radicalisation because it allows not only the propaganda of fundamentalist doctrines but also the creation and manipulation of information; the apology and dissemination of information instrumental to the processes of radicalisation; the use of devices capable of transversally violating the security of technical and virtual infrastructures that are critical to the security of nations; the operational planning of terrorist activities; and the recruitment, financing, and training of recruits. For these reasons, some have defined cyberspace as a new “battlefield” and geopolitical competition, the “fifth domain of military defense” after land, water, sky, and space (Azzarone 2014, p. 36). Discussion forums and social networks allow active and immediate participation also in the creation and spreading of terrorist campaigns. The temporal permanence on the Internet of propagandistic material and videos also constitutes an endless source of inspiration, just as video tutorials (e.g., on the handling or design of weapons), manuals, and material circulating online allow a kind of self-education and self-training for the fundamentalist cause (Policy Department External Policies 2009, p. 14). The accounts of terrorist groups and their supporters on social platforms, such as Facebook and Twitter, are often subject to suspension, which is why terrorists prefer to use encrypted platforms such as Telegram or the dark web (Vivian Fiona Guetler 2022, p. 6; Calo and Hartley 2019). The dark web is not indexed by search engines because it is accessible through special, specific software; users remain anonymous because they are not identifiable to the network and their actions also remain anonymous, which encourages the perpetration of illegal activity (Gupta et al. 2019).

The Internet is a useful tool for spreading radical ideologies and creating a feeling of affiliation; for instance, through meta-narratives, which are adapted to the cultural background of each target group. Meta-narratives are “theory that tries to give a totalising, comprehensive account to various historical events, experiences, social, and cultural phenomena based upon the appeal to universal truth or universal values” (Ali and Bwana,

p. 22). Islamist terrorist groups such as Al-Shabaab, Al Qaeda, and ISIS construct meta-narratives from verses of the Koran, Hadiths, or the life of Muhammad reinterpreted to suit their purposes (Roy 2017). Among the most recurrent themes in their propaganda meta-narratives are: the West is hostile to Islam; the only way to address the West is through violence (jihad); the Caliphate will save from Western corruption.

For these reasons, the use of cyberspace has always been massive by fundamentalist terrorist groups, including religious ones. For example, Al Qaeda or, later, Da'esh, have used social networks and the Internet not only to disseminate material instrumental to radicalisation but to co-opt, enlist, and train foreign fighters.

It is interesting, but beyond the purpose of this paper, to understand how the persuasion or brainwashing techniques peculiar to propaganda communication or charismatic religious leaders affect the personality of the terrorist. In fact, radicalism in itself does not imply the perpetration of terrorist acts. Equally useful is the analysis of terrorist activity that has changed form since the attack on the Twin Towers in 2001. One of the objectives of terrorism is to demonstrate the vulnerability of the target; however, in the past, this purpose was pursued primarily through striking actions, attacking symbols of the qualified "hostile" culture in order to undermine its values. Today, the "quantitative" connotation also becomes central, that is the number of victims, often civilians, which allows for undermining even emotionally the stability of the state structure. Hence comes an increasing level of violence in attacks. "Indiscriminate attacks have a very powerful effect on the public in general, which is one of the main goals of terrorism: to seriously intimidate a population. This preference for soft targets means that attacking critical infrastructure such as power grids, nuclear facilities and transportation hubs is currently not a priority" (Europol 2016, p. 7).

Through the use of the digital channel, terrorism, which has always been an omnipresent and unpredictable enemy, becomes even more difficult to fight. The liquidity of the structures of today's terrorist organisations does not make it easier for contemporary states and international organisations to contrast this phenomenon.

3. Religious Motivated Terrorism

"Religio peperit scelerosa atque impia facta": referring to the past, but also a premonition of future history, Lucretius' verse today can be referred to the phenomenon of religiously motivated terrorism. While religions have been and continue to be instrumental in promoting respect for authority, peaceful coexistence, a sense of belonging to a community, solidarity, and other "virtues" necessary for public life, it must be noted that in the name of a god in every age, crimes and serious offenses have been committed. It may be asked, and this is a debated question, whether religion really constitutes the motive for terrorist actions or whether, on the contrary, the religious matrix is instrumentally subordinated to carry out ideological, political, ethnic, nationalist, and even economic strategies that are substantially unrelated to the messages of faith (Ferrari 2004).

There is no universally accepted definition of terrorism and cyberterrorism today. According to some scholars, it is not possible to clearly define the term, because the means and methods that could be defined as terrorist acts are extremely numerous and different. According to Whitbeck, there is no agreed definition of terrorism "since the word is so subjective as to be devoid of any inherent meaning" (Whitbeck 2004; see also Ziyanda 2018; Shanahan 2016; Sinai 2008; Tilly 2004; Weinberg et al. 2004).

The Latin etymological root ("terrere") links terrorism to the action of "frightening, terrorising, intimidating" (Wilkinson 1974). The term "terrorism" was first used to qualify the Reign of Terror in France during the Revolution and was associated with the intimidating acts of the government in power between 1789 and 1794 (Guillame 1989, p. 297; Tilly 2004, p. 8).

Terrorist actions have, however, changed over time; from the second half of the 19th century until the end of the Great War, they were mostly aimed at striking the leadership in power (e.g., the Sarajevo attack of 28 June 1914 against Archduke Franz Ferdinand of

Habsburg and his wife, which triggered the fuse of the First World War). Terrorist actions were framed within the crimes against state sovereignty as acts of "treason" (Polidori 2006, p. 14) and had an "internal", national character.

In the 1970s, on the other hand, "international", or "transnational" terrorism appeared, which, unlike the previous terrorism, made use of cooperation between terrorist groups from different countries, united by ideologies or interests of a strategic nature. This new form of terrorism aims to draw the attention of the international community to domestic affairs by exporting violence outside its borders and striking at countries deemed guilty of a policy opposed to them. The phenomenon, which has become particularly serious in the Middle East, led the Council of Europe to create the European Convention on the Suppression of Terrorism of 27 January 1977, which was followed by the Agreement on the Application of the European Convention on the Suppression of Terrorism between the Member States of the European Communities, adopted in Dublin on 4 December 1979.

In the 1990s, "cyber terrorism" also appeared on the international scene. Even the term "cyber-terrorism" does not have an agreed definition. According to some authors, it should not be confused with "information warfare", as there is a substantial difference between them. "Information warfare" could be defined as an act of penetration of the computer systems or networks of a State, by another State, with the aim of causing damage. Its purpose is to hit enemy infrastructures to make them incapable of carrying out defensive actions. The goal, therefore, is to deny the possibility of using one's own resources (Janczewski and Colarik 2008; Bellamy 2001). Information warfare, which can encapsulate cyber warfare, has certain objectives. Cyber terrorism takes the form of premeditated and politically motivated attacks by sub-national groups; clandestine agents; or individuals against computer systems, programmes, and data—such acts involve violence against non-combatant targets and cause fear and harm to anyone in the vicinity of the target (Murat et al. 2011).

In this context, religious terrorism is a rather recent phenomenon. It has spread over the past 30 years; in the U.S. State Department's list of terrorist organisations in 1980, there was no movement of a religious nature, while in 1998, half of the 30 most dangerous terrorist groups were religious motivated, and in 2004, they accounted for two-thirds (Conesa 2005).

In the text of the fourteenth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of the United Nations' efforts in support of Member States in countering the threat to the 2021 the United Nations Security Council (2022) states that "online terrorist radicalisation and recruitment, especially among young people, and attacks inspired by Da'esh remain a foremost" (Fourteenth Report of the Secretary-General on the Threat Posed by ISIL 2022, 1). The Da'esh (short for Al dawla al islamiya fi al Iraq wal Sham Islamic State of Iraq and the Levant), or ISIS (Islamic State of Iraq and Syria), or IS (Islamic State), an international paramilitary terrorist organisation founded in 2014, publishes *scelerosa atque impia facta* on the web and organises terrorist attacks, particularly in Western countries.

The United Nations Counter-Terrorism Centre, in collaboration with the Counter-Terrorism Committee Executive Directorate, the International Criminal Police Organisation (INTERPOL), and UNODC, provided capacity-building assistance and training to many countries around the world (including Bangladesh, Burkina Faso, Malaysia, and Mongolia) on the use of new technologies in counter-terrorism investigations in full respect of human rights and the rule of law and protecting critical infrastructure from terrorist cyberattacks. In November 2020, the United Nations Counter Terrorism Center, in collaboration with the Centre-INTERPOL, released a handbook for law enforcement on using open-source methods and online information to prevent, investigate, prosecute, and adjudicate terrorist crimes.

Although the idea of the existence of a "terrorist personality" has now faded, the study of the recurring characteristics and experiences among terrorists appears useful and necessary in the analysis of the terrorist phenomenon; often, these are people who do not perceive themselves as terrorists but as instruments to restore the observance of God's will, and for this reason they are rewarded by him in the afterlife, even when they sacrifice the same life given by the god they believe in.

Some authors underline characteristics common to the perpetrators of attacks in Europe: they are generally predominantly young males—even if the female share is growing—of second- or third-generation immigrants; people with identity problems and economic and family hardships, filed by of the police for previous crimes, former prisoners who often became radicalised during their stay in prison, "individuals feeling marginalised, ill-treated, socially excluded and desperately seeking a meaning to life and a sense of belonging", unemployed, with a low level of instruction (Laurano and Anzera 2017).

However, other studies show that religious terrorists are sometimes young people with excellent school records who come from economically solid families (Khosrokhavar 2014), even if there is no doubt that in the West, "young people of the lower class form the most extensive base of European jihadism [. . .] and the banlieues remain a privileged recruitment ground" (Guolo 2015, p. 101). In the investigations carried out by Europol, by the other European police and intelligence authorities, the definition of individual terrorist includes Lone Actor and Small Cell, Foreign Terrorist Fighter, Returnee (foreign terrorist fighters trying to return from war zones, where they have often been trained to fight, to the countries where they reside or of origin), and Relocator (former combatant who travels to a country other than that of residence or origin). The United Nations Security Council has defined the Foreign Terrorist Fighter as individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict (UN Security Council Resolution 2178 on Foreign Terrorist Fighters, 2014).

It should be emphasised that religious terrorism does not only involve the extremist fringes of Islam but also of other religions, including Christianity, Judaism, and other religious movements. History, even recent, does not lack examples: in Japan, the attack by the religious group Aum Shinrikyo (Supreme Truth) with sarin gas in the Tokyo subway (March 1995) caused 12 deaths and thousands of injuries (Lewis 2019); in 1997 and 1988, Eric Robert Rudolph, who described himself as a militant member of the extremist Christian movement Christian Identity, planted bombs in an abortion clinic, an LGBTQ+ bar in Atlanta, and another clinic in Birmingham; the National Liberation Front of Tripura uses terrorist tactics to achieve mass conversions to Christianity. Within Judaism, the Kach and Kahane Chai groups are included by the US government in the list of terrorist groups. Terrorist groups are also present among Sikhs, such as Babbar Kahlsa.

Islamic terrorism is almost a century old; the first movement that theorised the use of violence to restore the fundamentalist and orthodox lifestyle of the first Islamic believers was that of the Muslim Brotherhood founded in 1928 in Egypt. The phenomenon took on a globally relevant dimension only after the Second World War, following decolonisation and globalisation. Various organisations have resorted to tools such as bomb attacks, kidnappings, plane and bus hijackings, assassinations, and suicide bombings. The different groups have strongly related to liberation struggles, such as the Palestinian territorial claims and the Iranian Revolution, but it was following the Russo–Afghan War that the phenomenon acquired a global and anti-West guise. To better understand the roots and threat of Islamist fanaticism, it can be considered how modern terrorism has evolved in the Middle East and South Asia. While in the 1970s groups focused on material damage and limited attacks aimed at killing individuals, the 1980s saw an increase in urban-based attacks with a consequent increase in collateral casualties and a change in targeting methodology: civilians became the target. The conflict between superpowers in Afghanistan became a formative period for the proliferation of weapons and the emergence of militant and fundamentalist Islam. In the 1990s, the end of the Cold War and the creation of new states, the abandonment of some unstable states, gave impetus to the rise of a new set of extremists whose ideology or motivations allow, or even require, indiscriminate targeting.

Particularly since the 1989 Soviet withdrawal, the region of Afghanistan has emerged as a terrorist training ground. Pakistan, struggling to balance its needs for political–economic reform with a domestic religious agenda, provides assistance to terrorist groups both in Afghanistan and Kashmir while acting as a further transit area between the Middle East and South Asia. Volunteers from various parts of the Islamic world fought in Afghanistan, supported by conservative countries such as Saudi Arabia. In Yemen, the Riyadh-backed Islamic Front was established to provide financial, logistical, and training support for Yemeni volunteers. Iraq and Syria were heavily involved in supporting various terrorist groups. (Moore 2001).

Bin Laden ushered in the era of "hyperterrorism": much of online jihad can be traced back to then Al Qaeda leader Osama Bin Laden, in his call for jihadists globalisation launched back in 1998, under the banner of "the international front of jihad against the Jews and the crusaders", accompanied by cross-border digitisation of both ideology, communication, and coordination (Laytouss 2021). On 11 September 2001, 19 militants associated with the Islamic extremist group Al Qaeda hijacked four airplanes and carried out suicide attacks against targets in the United States. Two of the planes were flown into the Twin Towers of the World Trade Center in New York City; a third plane hit the Pentagon in Arlington, Virginia, just outside Washington, D.C.; and the fourth plane crashed in a field in Shanksville, Pennsylvania. Almost 3000 people were killed during the terrorist attacks.

After the attack on the Twin Towers, some authors define terrorism as having a religious origin and it is referred to with the formula "new terrorism" to differentiate it from "traditional". The new terrorism is characterised by the coexistence of autonomous cells as well as organisational hierarchies, transnationality, the purpose of causing maximum destruction, the objective also constituted by civilians, and the religious motivation that replaces the political motivation (Gofas 2012).

Online communication, propaganda, and methods of information, often based on the techniques of coercive psychology, play a decisive role in the "new terrorism". In 2015, terrorist attacks hit freedom of expression (Charlie Hebdo) and the Western lifestyle (Bataclan) in Paris; after 2015, starting with Nice in July 2016, in France, the picture changed. The terrorist acted alone and used makeshift weapons (a truck in Nice)—in most of the cases, a knife. Profiles became more heterogeneous in terms of age, social background, and ethnic or national origin; there were more converts, some women, more recent migrants (like the two attacks in Nice in 2017 and 2020), and more diverse ethnic backgrounds. None of them had any training in foreign jihad, and while some of them paid tribute to ISIS, there is no evidence of a concrete link between them and any terrorist headquarters abroad. The systematic use of knives instead of guns is certainly connected to the absence of a support network, but it also seems to be connected to a different conception of the attack. The aim seems not to make as many victims as possible but to perpetrate a sort of "sacrifice" (hence the knife and beheading) before being killed (Roy 2020).

After the defeat of the Islamic State caliphate in Iraq and Syria in 2019, cyberterrorism has evolved. Under the name of "United Cyber Caliphate", it is trying to take root everywhere in the world, including Europe. Radical Islam has since reinvented itself and adapted a new cyber-terrorism strategy that will dominate much of international security. Cyberterrorism uses the Internet not only to prepare and organise terrorist attacks but also to conduct cyber-attacks (such as DoS attacks and hacking attacks). Concerns related to political cyberterrorism mainly revolve around possible cyber-attacks on the critical infrastructure of society (Critical Infrastructure, Critical Information Infrastructure, and Critical Internet Resources). While it is believed that terrorist organisations do not currently have the capability to stage a large-scale cyber-attack that could endanger critical infrastructure, it is also believed that it is a matter of time before they develop such capabilities (Gavrilović 2019). While these extremely violent religious extremists represent a minority view, their threat is still real today.

4. The Response of the EU

After the 2001 attack, the European Union implemented measures to fight international terrorism by, on the one hand, promoting social policies to prevent radicalisation and, on the other hand, committing states to harmonise criminal law and implement information exchange and judicial cooperation. In this sense, the European institutions adopted the 2002/584/JHA: Council Framework Decision on the European arrest warrant; the 2002/187/JHA: Council Decision setting up Eurojust (amended by Council Decision 2009/426/JHA and later replaced by the Regulation (EU) 2018/1727 of 14 November 2018 setting up the European Union Agency for Criminal Justice Cooperation, operational since 12 December 2019); and the Council Framework Decision 2002/475/JHA on combating terrorism (amended by Council Framework Decision 2008/919/JHA). The latter states that the definition of terrorist offences should be approximated in all Member States, including offences relating to terrorist groups; penalties and sanctions should be provided for natural and legal persons having committed or being liable for such offences, reflecting the seriousness of such offences. The decision also points out that the objectives of the proposed action cannot be sufficiently achieved by the Member States unilaterally and can, therefore, by reason of the need for reciprocity, be better achieved at the level of the Union, which may adopt measures in accordance with the principle of subsidiarity.

Directive (EU) 2017/541 of the European Parliament and of the Council replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA confirms that, taking account of the evolution of terrorist threats to and legal obligations on the Union and Member States under international law, the definition of terrorist offences, offences related to a terrorist group, and offences related to terrorist activities should be further approximated in all Member States, so that it covers conduct related to, in particular, foreign terrorist fighters and terrorist financing more comprehensively. These forms of conduct should also be punishable if committed through the Internet, including social media. The Directive also specified that the criminalisation of receiving training for terrorism complements the existing offence of providing training and specifically addresses the threats resulting from those actively preparing for the commission of terrorist offences, including those ultimately acting alone. Receiving training for terrorism includes obtaining knowledge, documentation, or practical skills. Self-study, including through the Internet or consulting other teaching material, should also be considered to be receiving training for terrorism when resulting from active conduct and done with the intent to commit or contribute to the commission of a terrorist offence. In the context of all the specific circumstances of the case, this intention can, for instance, be inferred from the type of materials and the frequency of reference. Thus, downloading a manual to make explosives for the purpose of committing a terrorist offence could be considered to be receiving training for terrorism. By contrast, merely visiting websites or collecting materials for legitimate purposes, such as academic or research purposes, is not considered to be receiving training for terrorism. The Directive also suggests that an effective means of combating terrorism on the Internet is to remove online content constituting a public provocation to commit a terrorist offence at its source. Member States should make every effort to cooperate with other countries to ensure the removal from servers within their territory of online content that constitutes a public provocation to commit a terrorist offence. However, when the removal of such content at its source is not feasible, mechanisms may also be put in place to block access from Union territory to such content. Measures taken by Member States pursuant to this Directive include removing online content which constitutes public provocation to commit a terrorist offense or, where this is not feasible, blocking access to such content may be based on an action public, such as legislative, non-legislative, or judicial action. In this context, the Directive is without prejudice to voluntary action taken by the Internet industry to prevent misuse of its services or any support for such action by Member States, such as the detection and reporting of terrorist content.

The Council Decision 2005/671/JHA on the exchange of information and cooperation concerning terrorist offences, adopted after the attacks in Madrid (2004) and London

(2005), committed Member States to transmit information on terrorist crimes to Eurojust and Europol and to designate one, or where its legal system so provides more than one authority, as Eurojust national correspondent for terrorism matters.

With Regulation (EU) 2021/784 Of the European Parliament and of the Council of 29 April 2021, on addressing the dissemination of terrorist content online, the fight against the improper use of hosting services for terrorist purposes has been strengthened. Specifically, the Regulation provides the option for Member States to issue service providers with an order to remove terrorist content in all Member States (Art. 3). After receiving that order, hosting providers will have to remove the content as soon as possible, and in any case within one hour of receiving the order. Removed content shall be preserved for six months, except for specific extensions, to allow for administrative or judicial review proceedings. Article 5 of the Regulations states that a hosting service provider exposed to terrorist content shall take specific measures to protect its services against the dissemination to the public of terrorist content, effective and proportionate, based on both automated and human verification mechanisms. For the purposes of judicial protection, when the hosting service provider independently removes the content hosted on its platform, it shall make available to the content provider information on such removal or disabling. If, on the other hand, the terrorist content involves an imminent threat to life or an alleged terrorist offense, as defined by Directive (EU) 2017/541, the hosting service provider will have to promptly notify the competent authorities. However, Article 15 of Directive 2000/31/EC does not allow the imposition of a general obligation on hosting service providers to actively search for terrorist content.

A very important tool in the fight against terrorism is the blacklists, which contain lists of individuals, entities, and other groups linked to organisations classified as terrorist. The criteria for compiling the lists are varied, not always clear, and differ depending on which body (European or UN) is in charge of drawing up the lists. In the second case (UN), the criteria are even more uncertain since inclusion on a UN list may also depend on reports from Member States of the Sanctions Committee and regional organisations, based on the activities of secret services (Pasculli 2012); the secrecy of the latter's activities leads to a decrease in the guarantees of the person on the list. Registration leads to the application of preventive measures that severely restrict the terrorist suspect's freedom of movement and assets, such as the freezing of assets and a ban on transit through EU Member States.

The EU can either transpose the lists drawn up by the UN or draft them independently. In the first case, through the adoption of common positions, the lists drawn up by the UN are incorporated into European law (e.g., 2002/402/CFSP of 27 May 2022, drawn up to combat jihadist terrorism, refers in its entirety, in Article 1, to the lists drawn up by the United Nations in Resolutions 1267 of 15 October 1999 and 1333 of 19 December 2000).

In the second case, however, Common Position 2001/931/CFSP established a special committee whose task is to draw up a draft list to be submitted to the Council for consideration. The committee also carries out the six-monthly review of the lists, which must be submitted to the Council for final approval. The criteria for inclusion on the European lists and the subjects to be included are drawn up independently by the Union. Common Position 2001/931/CFSP states (Article 4) that inclusion may also take place on the basis of investigations by the competent national judicial or police authorities or convictions by national courts for terrorist offences.

The criteria mentioned for inclusion in the European lists appear to be more guaranteed than the parameters used in the UN, but they are not entirely free of problems. As mentioned, in fact, inclusion on the list can also occur as a result of a pending investigation or police investigation, without the guarantee of a judicial review of the merits of the allegations.

The need to prevent future crimes—which explains the immediacy of registration without waiting for the outcome of the judicial proceeding—leaves open some questions concerning the balance between the need to guarantee the security of European citizens on the one hand and the need to guarantee the fundamental rights of the persons listed on the other. The lists drawn up at the European level target "home terrorists", i.e., those who belong to terrorist organisations of the Member States. The sanctions derived from inclusion in the list have a "hybrid" nature; formally, they are administrative but fall within the scope of police and judicial cooperation in criminal matters. In addition, the severity of measures, such as the freezing of assets and the prohibition of transit through states, suggest a criminal qualification. In this sense, the ECtHR (Grand Chamber, judgment of 23 November 1976, Engel and Others v Netherlands), observed that the classification of the classification of the sanction in criminal terms derives from the public nature of the protected interests, the repressive and general-preventive purpose of the sanction imposed, and its severity (Mazzacuva 2017, p. 95; Manes 2017, p. 994; Tebaldi 2018, p. 81).

It should be made clear that lists are an effective tool for combating terrorism and for ensuring the circulation of information and cooperation between states; however, CFSP common positions can profoundly affect an individual's fundamental rights both because of the sanctions they impose and because of the manner and criteria for drawing up the lists (Cha et al. 2012). This is easily understood in the case of a person who has been listed as a suspect but turns out not to be guilty following investigation and a court decision. The person may ask to be removed from the list or may be removed ex officio during the periodic review of the lists. This entails the forfeiture of the sanctions, but the impairment of his personal, relational, and working life is undeniable.

It is interesting to refer in this respect to the Yassin Abdul Kadi case, which also offers interesting insights into the relationship between international, UN, and European legal systems. Council Regulation (EC) No. 467/2001 of 6 March 2001, which implemented the aforementioned Common Position 2001/156/CFSP, merely transposed a list drawn up at UN level by Resolution 1333 of 2000. Kadi had been blacklisted because he was considered to be linked to Al Qaeda and the Taliban; he applied to the General Court of the European Union complaining of infringement of the right of defence recognised by Article 6 ECHR. The Court dismissed the application, relying on Article 27 of the Vienna Convention, which does not allow a party to invoke the provisions of its domestic law to justify the non-execution of a treaty, and on the necessary respect for international obligations (Kadi, Case T-315/01, 21 September 2005).

The Court of Justice overturned the judgment of the General Court, stating that respect for the constraints set by the international community cannot entail the sacrifice of fundamental rights and constitutional principles (European Court of Justice, Yassin A. Kadi, and Al Barakaat International Foundation v Council of the EU and EC Commission, Joined Cases C-402/05 P and C-415/05 P, judgment of 3 September 2008). The Court thus recognised Kadi's right of defence.

The Commission subsequently issued a new regulation (1190 of 28 November 2008), after having summarily heard the applicant's arguments, confirming his listing and the corresponding sanctions. However, the new regulation was also annulled by the General Court as infringing the right of defence (EU General Court, judgment of 30 September 2010, T-85/09, Yassin Abdul Kadi v European Commission). In contrast to what was stated in the Kadi judgment, the new regulation did not provide for any procedure to inform the list of the elements of evidence underlying the decision to freeze his assets or to allow him to comment on these elements: the simple sending to the applicant of a summary of the reasons for the listing does not meet the requirements of a fair procedure. The summary of reasons constitutes a series of generic, vague, and imprecise accusations. Consequently, the appellant is unable to refute, even before the courts, the accusations made against him.

The General Court's decision was confirmed by the Court of Justice in 2013 (CJEU, judgment of 18 July 2013 in Case C-584/10, European Commission and Others v Yassin Abdullah Kadi). The Court recalled that the right of defence of those who are listed must be guaranteed through the communication to the member of the reasons on which his registration is based and the possibility to formulate observations. Furthermore, cooperation between the Court of Justice and the international and European listing authorities must be ensured, both to guarantee the need for transparency in relation to the criteria for creating lists, and to ensure judicial protection.

The Kadi case thus represented a step forward in the protection of the fundamental rights of those listed, establishing the need for correct information, the possibility of opening an effective dialogue between the person concerned and the listing authorities, and the right to judicial protection.

The Segi judgment (CJEU, judgment of 27 February 2007, Segi, and Others v Council, case C-355/04) also constitutes a further step forward. The Court of Justice, ruling on the autonomously elaborated lists elaborated at European level on the basis of the common position 2001/931/CFSP, has elaborated a fundamental general principle, according to which the acts of the common foreign and security policy which affect the fundamental rights of people must be able to be brought under its control.

With the entry into force of the Treaty of Lisbon, important changes were made that affected the matter and improved it. In particular, the second paragraph of Article 275 TFEU provides for the possibility for the Court of Justice to rule on foreign policy acts if they provide for restrictive measures applied against natural or legal persons. Common positions have been replaced by common decisions and new types of implementing regulations have been provided for. However, the pre-2009 common positions remain in force. Protocol 36, Art. 9 provides for the continuing effects of former second (and third) pillar acts even after the Lisbon Treaty. Thus, the entire existing legislation on blacklists is unaffected.

Among the unresolved issues remains the problem of the still hybrid and debated nature of the sanctions imposed on those who are put on the list; moreover, the criteria for inclusion on the blacklists continue to be ambiguous and affected by the aforementioned problems related to the absence of guarantees of protection (Eckert 2016; Pusateri 2013; Ciampi 2011; Bothe 2008). The analysed profiles of this system appear to be incompatible with both the principle of taxation and determinacy proper to criminal law and with the principles of due process, in that the right of defence is severely impaired.

Although the importance of blacklisting legislation is unquestionable, it is important to resolve the problematic knots inherent in the protection of the fundamental rights of those who are registered.

5. Conclusions

Approaching, understanding, and combating the new forms of terrorism cannot be reduced to a simple war on terrorism, based on the traditional regulatory instruments for combating domestic terrorism and organised crime; what is needed is a wide-ranging, global, and coordinated strategy, consistent with the democratic principles and values of freedom that are foundational to the European Union and constitutionally guaranteed in all the Member States (Alicino 2020); terrorist attacks strike not just against the victims, their friends, and families but against the fundamental principles of the European Union. It is therefore fundamental to allocate additional resources, to train expert personnel capable of decrypting the cyber strategies of terrorist groups—especially in the 2020–2030 decade in which Europe's digital transformation is to be implemented—to implement more inclusive migration policies and to foster interculturalism and its dissemination through school systems and the mass media. The role of religious communities is also fundamental, both to identify terrorists, to foster the full social and cultural integration of their faithful, and to contribute with their messages to peaceful coexistence.

The relatively recent historical emergence of the phenomenon under analysis makes its framing within traditional conceptual categories complex, just as it makes the vision of a path leading to the eradication, or at least the effective countering, of a phenomenon that constitutes a real threat to the world's still nebulous geo-political balances.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

References

Ali, Mustafa Yusuf, and Othman Mujahid Bwana. Peace-Building and Conflict Prevention Training Manual and Resource Guide for Building Resilience against Violent Extremism. Available online: https://cscrcenter.org/wp-content/uploads/2019/09/BRAVE-MANUAL-POPULAR-VERSION.pdf (accessed on 15 January 2023).

Alicino, Francesco. 2020. *Terrorismo di Ispirazione Religiosa. Prevenzione e Deradicalizzazione Nello Stato Laico*. Edited by Francesco Alicino. Roma: Apes, ISBN 978-88-72331-61-3.

Azzarone, Raffale. 2014. Cyber vademecum, Part II. *Gnosis* 3: 36–47.

Balsamo, Fabio, and Tarantino Daniela. 2020. Law, Religion and the Spread of COVID-19 Pandemic. Available online: https://diresom.net/2020/11/07/law-religion-and-the-spread-of-covid-19-pandemic-ebook-diresom-papers-2/ (accessed on 15 January 2023).

Bellamy, Christopher. 2001. What is Information Warfare? In *Managing the Revolution in Military Affairs*. Edited by Ron Matthews and John Treddenick. London: Palgrave Macmillan. [CrossRef]

Bingaman, Kirk A. 2023. Religion in the Digital Age: An Irreversible Process. *Religions* 4: 108. [CrossRef]

Bothe, Michael. 2008. Security Council's targeted sanctions against presumed terrorists. The need to comply with human rights standards. *Journal of International Criminal Justice* 6: 541–55. [CrossRef]

Calo, Ben, and Eliza Hartley. 2019. ISIL recruiters as social media influencers: Mechanisms of legitimation by Australian Muslim men. *Contemporary Voices: St Andrews Journal of International Relations* 1: 2. [CrossRef]

Cha, Kiho, Stolz Tilo, and Wammes Maarten. 2012. United Nations security council sanctions and the rule of law: Ensuring fairness in the listing and de-listing process of individuals and entities subject to sanction. *The Whitehead Journal of Diplomacy and International Relations* XIII: 133–51.

Ciampi, Annalisa. 2011. Security Council targeted sanctions and human rights. In *Securing Human Rights? Achievements and Challenges of the UN Security Council*. Edited by Bardo Fassbender. Oxford: Oxford University Press, pp. 98–140, ISBN 9780199641499.

Conesa, Pierre. 2005. La violence au nom de Dieu. *Revue Internationale et Stratégique* 1: 73–82. [CrossRef]

2020. Law, Religion and COVID-19 Emergncy. DiReSom Papers. Available online: https://web.unicz.it/admin/uploads/2020/06/guzzo-law-and-religion.pdf (accessed on 15 January 2023).

Dawson, Lorne L., and Douglas Cowan. 2004. Introduction. In *Religion Online. Finding Faith on the Internet*. Edited by Lorne L. Dawson and Douglas Cowan. New York: Routledge, pp. 1–16.

Eckert, Sue E. 2016. The Role of Sanctions. In *The UN Security Council in the 21st Century*. Edited by Sebastian von Einsiedel, David M. Malone and Bruno Stagno Ugarte. Boulder: Lynne Rienner Publishers, pp. 415–41.

Europol. 2016. Changes in Modus Operandi of Islamic State (IS) Revisited, Europol Public Information. The Hague. January 18. Available online: https://www.europol.europa.eu/cms/sites/default/files/documents/changes_in_modus_operandi_of_is_in_terrorist_attacks.pdf (accessed on 15 January 2023).

Ferrari, Silvio. 2004. Individual Religious Freedom and National Security in Europe After September 11. *Brigham Young University Law Review* 2004: 356–84.

Fourteenth Report of the Secretary-General on the Threat Posed by ISIL (Da'esh) to International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat. Available online: https://digitallibrary.un.org/record/3957700?ln=en (accessed on 15 January 2023).

Gavrilović, Adrijana. 2019. Violent Extremism. Available online: https://dig.watch/topics/violent-extremism (accessed on 15 January 2023).

Gofas, Andreas. 2012. "'Old' vs. 'New' Terrorism: What's in a Name?". *Uluslararası İlişkiler/International Relations* 8: 17–32. Available online: www.jstor.org/stable/43926201 (accessed on 14 January 2023).

Guetler, Vivian Fiona. 2022. Exploring Cyberterrorism, Topic Models and Social Networks of Jihadists Dark Web Forums: A Computational Social Science Approach. Graduate Theses, Dissertations, and Problem Reports. 11253. Available online: https://researchrepository.wvu.edu/etd/11253 (accessed on 15 January 2023).

Guillame, Gilbert. 1989. Terrorisme et droit international. Recueil des cours de l'Académie de droit international, III. *Tome* 215: 287–416.

Guolo, Renzo. 2015. L'ultima utopia. In *Gli jihadisti Europei*. Milano: Guerini e Associati.

Gupta, Abhineet, Sean B. Maynard, and Ahmad Atif. 2019. The Dark Web Phenomenon: A Review and Research Agenda. In Proceedings of the Australasian Conference on Information Systems, Perth, WA, Australia, December 9–11.

Janczewski, Lech, and Andrew M. Colarik. 2008. *Cyber Warfare And Cyber Terrorism, Information Science Reference*. Hershey: IGI Global.

Jonveaux, Isabelle. 2021. To use or not to use the Internet to support Religious and Spiritual Life. In *Religion in the Age of Digitalization. From New Media to Spiritual Machines*. Edited by Giulia Isetti, Elisa Innerhofer, Harald Pechlaner and Michael de Rachewiltz. New York: Routledge, pp. 61–72.

Khosrokhavar, Farhad. 2014. *Radicalisation*. Paris: Maison des Sciences de l'Homme. [CrossRef]

Laurano, Patrizia, and Giuseppe Anzera. 2017. L'analisi sociologica del nuovo terrorismo tra dinamiche di radicalizzazione e programmi di de-radicalizzazione. *Quaderni di Sociologia* 75: 99–115. [CrossRef]

Laytouss, Brahim. 2021. New Terrorism and the Use of Electronic Jihad, Brussels International Center. Available online: www.bic-rhr.com/sites/default/files/inline-files/New%20Terrorism%20and%20the%20Use%20of%20Electronic%20Jihad_1.pdf (accessed on 15 January 2023).

Lewis, James R. 2019. Religion and Terrorism: Introduction to Journal of Religion and Violence. *Journal of Religion and Violence* 7: 1–3. [CrossRef]

Manes, Vittorio. 2017. Profili e confini dell'illecito para-penale. *Rivista Italiana di Diritto e Procedura Penale* 60: 998–1007.

Mazzacuva, Francesco. 2017. *Le Pene Nascoste. Topografia delle Sanzioni Punitive e Modulazione dello Statuto Garantistico*. Torino: Giappichelli, ISBN 8892111663.

Moore, John. 2001. The Evolution of Islamic Terrorism: An Overview. Available online: www.pbs.org/wgbh/pages/frontline/shows/target/etc/modern.html (accessed on 15 January 2023).

Murat, Dogrul, Adil Aslan, and Eyyup Celik. 2011. Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism. In Proceedings of the 3rd International Conference on Cyber Conflict, Tallinn, Estonia, June 7–10; Edited by Christian Czosseck, Enn Tyugu and Thomas Wingfield. Tallinn: CCD COE Publications, pp. 29–43.

Obadia, Lionel. 2017. Cyber-Religion. In *The Wiley Blackwell Encyclopedia of Social Theory*. Edited by Bryan S. Turner. Oxford: Wiley-Blackwell.

Pasculli, Lorenzo. 2012. *Le Misure di Prevenzione del Terrorismo e dei Traffici Criminosi Internazionali*. Padova: Padova University Press, ISBN 8897385508.

Policy Department External Policies. 2009. Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks. Available online: www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede090209wsstudy_/SEDE090209wsstudy_en.pdf (accessed on 15 January 2023).

Polidori, Claudio Maria. 2006. Il Terrorismo Internazionale Negli Ordinamenti Giuridici dei Paesi Occidentali e i Relativi Strumenti di Cooperazione Giudiziaria e di Polizia, Centro Militare di Studi Strategici. Available online: www.difesa.it/SMD_/CASD/IM/CeMISS/Pubblicazioni/Documents/97574_polidori_pdf.pdf (accessed on 15 January 2023).

Pusateri, Verana. 2013. La Corte edu su Contrasto al Terrorismo Internazionale e Rispetto dei Diritti Fondamentali. Diritto Penale Contemporaneo. Available online: https://archiviodpc.dirittopenaleuomo.org/d/1935-la-corte-edu-su-contrasto-al-terrorismo-internazionale-e-rispetto-dei-diritti-fondamentali (accessed on 15 January 2023).

Roy, Olivier. 2017. *Jihad and Death The Global Appeal of Islamic State*. London: C Hurst & Co Publishers Ltd., ISBN 9781849046985.

Roy, Olivier. 2020. How Jihadi Terrorism Has Changed in France Since the 2015 Attacks. Available online: www.ispionline.it/it/bio/olivier-roy (accessed on 15 January 2023).

Shanahan, Timothy. 2016. *The Definition of Terrorism in Jackson, R. Routledge Handbook of Critical Terrorism Studies*. London: Routledge, pp. 103–13.

Shellnutt, Kate. 2020. When God Closes a Church Door, He Opens a Browser Window. *Christianity Today*. Available online: www.christianitytoday.com/news/2020/march/online-church-attendance-covid-19-streaming-video-app.html (accessed on 15 January 2023).

Sinai, Joshua. 2008. How to Define Terrorism. *Perspectives on Terrorism* 4: 9–11.

Sinding Bentzen, Jeanet. 2020. In Crisis, We Pray: Religiosity and the COVID-19 Pandemic, University of Copenhagen, CEPR, CAGE. Available online: www.Economics.ku.dk/research/corona/Bentzen_religiosity_covid.pdf (accessed on 15 January 2023).

Statista Research Department. 2022. Worldwide Digital Population July 2022. Available online: iwww.google.com/search?q=google+traduttore&oq=google+trad&aqs=chrome.0.69i59j69i57j0i512j0i433i512l2j69i60l3.5028j0j7&sourceid=chrome&ie=UTF-8 (accessed on 15 January 2023).

Tebaldi, Marcello. 2018. Le black lists nella lotta al terrorismo. *Diritto Penale Contemporaneo* 7–8: 77–91.

Tilly, Charles. 2004. Terror, Terrorism, Terrorists. *Sociological Theory* 1: 5–13. [CrossRef]

United Nations Security Council. 2022. Fourteenth Report of the Secretary-General on the Threat Posed by ISIL (Da'esh) to International Peace and Security and the Range of United Nations Efforts in Support of Member States in Countering the Threat. Available online: www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2022_63_E.pdf (accessed on 15 January 2023).

Weinberg, Leonard, Ami Pedahzur, and Sivan Hirsch-Hoefler. 2004. The Challenges of Conceptualising Terrorism. *Terrorism and Political Violence* 4: 777–94. [CrossRef]

Whitbeck, John V. 2004. 'Terrorism': A World Ensnared by a Word By, International Herald Tribune. Available online: www.nytimes.com/2004/02/18/opinion/terrorism-a-world-ensnared-by-a-word.html (accessed on 15 January 2023).

Wilkinson, Paul. 1974. *Political Terrorism*. London: Red Globe Press.

Ziyanda, Stuurman. 2018. Terrorism as Controversy. The Shifting Definition of Terrorism in State Politics. *E-International Relations*, 1–9. Available online: https://www.e-ir.info/pdf/80101 (accessed on 15 January 2023).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.