International Comparative Jurisprudence 2020 Volume 6 Issue 2
ISSN 2351-6674 (online) DOI: http://dx.doi.org/10.13165/j.icj.2020.12.005

JIHADIST, FAR-RIGHT AND FAR-LEFT TERRORISM IN CYBERSPACE – SAME THREAT AND SAME COUNTERMEASURES?

Milena Ingelevič-Citak[1]

Jagiellonian University, Poland
E-mail: milena.ingelevic-citak@uj.edu.pl

Zuzanna Przyszlak[2]

Jagiellonian University, Poland
E-mail: zuanna.przyszlak@student.uj.edu.pl

Received: 1 December 2020; accepted: 23 December 2020
DOI: http://dx.doi.org/10.13165/j.icj.2020.12.005

Abstract. This paper investigates whether the counter-terrorism measures developed and implemented within the European Union have a universal character and are equally effective in the context of various types of terrorism. The authors focus on the strategies applicable to the terrorist activities online, since information and communication technology is perceived as the fastest growing and continually changing field of the terrorist threat. So far, most of the counteractions and security strategies have been subordinated to the jihadism combating. However, in recent years, the significant growth of threats coming from far-right and far-left terrorist activities has been observed. It raises questions about the capability of instruments to prevent and combat other types of terrorism as well as jihadism.
The research was conducted in particular, on the basis of international organizations' reports, the authors' observations, and practitioners' remarks. As follows from its results, there are significant differences in the phenomenon, current trends, and modus operandi of the perpetrators in the jihadi, far-right, and far-left terrorism. Consequently, it is possible to conclude that the effectiveness of chosen countermeasures, subordinated - as a rule – to the fighting of the jihadi extremists, is doubtful in preventing and combating far-right and far-left terrorism.

Keywords: counter-terrorism, cyberspace, far-right, far-left, jihadi terrorism

Introduction

Since the terrorist attack on the WTC on 11 September 2001 through all the attacks committed by perpetrators associated with Al-Qaida and ISIS that took place in the last two decades, jihadist terrorism has been considered as the biggest threat for western democratic societies. Therefore, it has been the center point for constructing counter-terrorism policies, strengthening the capacity of national law enforcement and justice systems, and implementing new legal instruments. Unfortunately, the major drawback of such an approach is the distorted perception of the threat sources. It cannot be forgotten that "terrorism" is a much broader concept than just jihadism-motivated extremism. The phenomenon of terrorism is very complex, multi-threaded and constantly changing. It takes many forms and can involve the activities of very diverse groups, including right-wing and left-wing extremists, nationalist-separatist organizations, political and religious networks, or perpetrators who

[1] Assistant Professor, Chair of Public International Law, Faculty of Law and Administration, Jagiellonian University, Cracow, Poland.
[2] 5th year Law Student, Head of The Public International Law Research Circle at Jagiellonian University, Cracow, Poland.

carry out terrorist acts based on other ideologies or motivations[3]. In the face of all this diversity, it is beyond comprehension that efforts in the field of broadly understood counteraction are, as a rule, focused on the threat arising from jihadists. Building security strategies based on the assumption that jihadism is the biggest headache of the international community, while other types of terrorism do not require such increased attention, and are left without proper control and counteraction, has presumably contributed to a significant development of the activity of far-right and far-left groups in recent years.

Referring to the terrorism counteraction strategies, they include comprehensive activities of various entities, i.e., not only political and legal instruments developed by states and international organizations, but also initiatives developed in cooperation with the private sector, in particular with tech-companies. For the purposes of this study, the authors decided to narrow the research down to the counter-terrorism instruments and methods developed within the EU and collaborating institutions. Such a choice has been required to ensure the clarity of disquisition. It is also legitimate because the EU is very active in this field and therefore often sets trends and continually contributes a lot to counteracting terrorism at the global level. Therefore, it will be possible to draw more general conclusions from the specific analysis.

The data presented by Europol in the TE-SAT 2020 report clearly demonstrates the changing picture of the terrorist threat in Europe. Due to the strengthening of efforts and, consequently, also the increased effectiveness of EU counteraction strategies, the number of jihadist activity in recent years shows a downward trend – less than 18% of 119 completed, failed, and foiled terrorist attacks in 2019 were jihadism-motivated, while far-right and far-left radicals carried out 34 attacks[4], which makes 29% of all attacks. With 20 far-right and far-left terrorist acts reported in the year 2018, this is a significant increase.

In light of such statistics and trends, the following question arises, namely, why do we emphasize jihadist attacks? Hitherto, it was assumed that they cause both most tremendous human losses, as well as the most extensive material damages and at the same time have severe political and socio-psychological consequences. However, now it becomes clear that for two decades of the 21st century, we have been focusing our attention on combating jihadist terrorism while ignoring or overlooking the fact that the threat from far-right and far-left extremists is dangerously growing. This observation leads us to a further question - if our actions were subordinated to the jihadism combating, will the developed and implemented solutions be equally effective in countering far-right and far-left radicals' activities? It is precisely the question that we are looking to answer in this study.

The main objectives of the paper are to present the considerable distinction between chosen types of terrorism, demonstrate differences in the profiles of attacks perpetrators, and explore methods of exploiting cyberspace for terrorist purposes and subsequently assess whether developed countermeasures share universal character, i.e., are just as effective in combating any type of terrorism.

Following such goals, the considerations aim to confirm or disprove the put-forward thesis that the developed legal solutions and other counteraction methods do not take into account the specificity of far-right and far-left extremists, which makes the effectiveness of such measures questionable. Consequently, another hypothesis emerging from this assumption is that underestimating the recently escalating problem of far-right and far-left terrorism may lead to a situation where the international community will be unable to counteract this threat effectively due to the lack of dedicated countermeasures.

[3]Terrorist groups and organizations are usually classified on the basis of the motivation and ideology of their members. Relatively often, however, we are dealing with a mixture of motives, goals, and beliefs, which makes the proper classification much more problematic. Europol's report TE-SAT 2020 mentions such types of terrorism as jihadist, right-wing, left-wing and anarchist, ethno-nationalist, separatist and single issue. Security experts and scholars mention as well state-terrorism, racial terrorism, gender-selective or criminal terrorism, however, such typological classification is somewhat debatable.

[4] Including two attacks not classified as terrorist but carried out by far-right extremists.

It is worth stating at this point, that one of the complexities of the analyzed issue is the lack of the universally accepted, legal definition of terrorism. This circumstance may sometimes cause difficulties in classifying whether a specific act is a terrorist act or an action that does not meet the criteria of terrorism. Since this paper is not aimed at terminological considerations, we will only briefly refer to the issue of understanding the concepts of jihadist, far-right and far-left terrorism. For the purposes of this study, the term "terrorism" is used in a broad sense, referring to both terrorist offenses and other deliberate violent acts by extremists. Such an approach is justified, especially as we broadly describe counteracting the terrorist activities online - at this stage, there are no grounds for differentiation.

Due to the limited scope of this study, the analysis will focus on the specificity of terrorist activities in cyberspace and the assessment of the adopted counteraction measures in a given field. In order to further narrow the area covered by the study, we analyzed groups that, objectively speaking, should raise the greatest concerns of states, namely jihadists, far-right and far-left groups.

The seeking of a remedy for the problem of terrorism has gained continued popularity and remains of interest not only to governments and international organizations but also to experts of the academic community. The constantly evolving threat has been noticed in every aspect, including particularly activity in cyberspace. However, to the authors' best knowledge, very few researches that address the issue of the effectiveness of countermeasures in the context of the far-right and far-left terrorist online activities have been published so far. Furthermore, there are practitioners' voices claiming that in the legal doctrine, there is a lack of "the comparative research of far-right/left and Islamist narratives in order to establish whether there is a case for commonalities and thus common elements to counter-narratives" (RAN, 2016). Taking all of the aforementioned into consideration, the subject of this study all the more appears to be legitimate and desirable.

The study concerns the scrutiny of the counter-terrorism instruments created in the frames of the European Union and cooperating organizations. The authors focus on their efficiency in preventing and combating the spread of terrorist content online in the context of various types of terrorism. Observations and conclusions have been devised based on the conscientious analysis of statistics and comparison of data published in several subsequent reports of well-established organizations and institutions - such as TE-SAT or Global Terrorism Index, as well as on authors' remarks on the current affairs and opinions of practitioners experienced in preventing and combating radicalism in the cyberspace.

The paper is organized as follows. Section I analyzes the current trends, distinguishing features and the *modus operandi* of jihadists, far-right and far-left terrorists, emphasizing their activities in cyberspace as it became the main operational field for them. In Section II the selected countermeasures developed within the UE for preventing and countering terrorism online are discussed. Finally, Section III refers to the previously formulated hypotheses, as assessment of the countermeasures' effectiveness is made. Within the end of this paper, thoughts summarizing the results of research and drawing conclusions are presented.

1. The Comparative Analysis of the Distinguishing Features and the *Modus Operandi* of the Selected Terrorist Types: Jihadists, Far-Right and Far-Left Terrorists

The study of the features that distinguish particular types of terrorism and the presentation of their methods of operation is outstandingly important in light of the discussed issue, as there is a clear correlation between the above-mentioned elements and the effectiveness of the counteracting and combating policies. This interdependence is even bigger than one might expect because the specificity of terrorist activities in cyberspace determines anti-terrorist strategies, and the effectiveness of these strategies can affect, in turn, the possible change of the tools terrorists use and the ways they act. Bearing this in mind, it is particularly alarming that over the past two decades, fear of jihadist terrorism has obscured the threat of far-right and far-left extremism, allowing them to develop, specifically to improve and expand online activity.

1.1. Jihadist terrorism

1.1.1. Understanding the concept of jihad

Jihadist or Jihadi terrorism is difficult to define, even though it has been a much-discussed term. There is not just one single set of motivational factors, but the multiplicity of incentives and at the same time, considerable uncertainty about the genuine motivations of jihadists as they take full advantage of all circumstances to justify their acts of violence.

The ideology of jihadism is built on the concept of jihad. While the comprehensive analysis of it is beyond the scope of this study, it should only be mentioned that there is a lack of consensus about the definition of jihad. Moreover, one can observe that jihad is often considered as the synonym for religious extremism aimed at sowing fear, uncertainty and distrust of the authorities, and being used to relate to the fight against Western democracies. Furthermore, jihad is stereotypically translated as "a holy war" of Muslims against non-believers. However, it is worth noting that terrorists are often misrepresenting the religious sources they cite, therefore the modern perception of the meaning of jihad they have disseminated contradicts the linguistic and contextual meaning of this word which can be found in the Quranic text[5].

Despite the authors' approach that armed struggle does not reflect the full essence of jihad, adapting to the terminology used by Interpol, the narrow sense of the term "jihadist terrorism" will be used in this paper to describe a radical movement aimed at confrontation with everyone whom they consider to be enemy to carry out particular sociological and political changes (TE-SAT, 2020, 35)[6].

1.1.2. Characteristics and current trends

In order to provide a comprehensive picture of the contemporary jihadist terrorism, first of all, we should emphasize that currently, we are dealing with a new generation of terrorists, who are unpredictable and much more challenging in terms of developing countermeasures than their predecessors. Intending to explain why, let us continue with the demonstration of the significant changes that have occurred in their functioning along with the presentation of how the profile of the perpetrator of jihadist attacks evolved.

The description of the jihadist's profile is complex, as it consists of several features. First of all, it should be noted that most attacks in Europe in recent years have been carried out by home-grown, independently acting jihadists – so-called "lone wolves". These are individuals usually born on the territory of European states or living there for many years, identifying themselves with the jihadist ideology and - as a rule – being radicalized through information and communication technologies (ICT). In the majority, they are not listed as belonging to terrorist organizations. Unlike them, individuals explicitly involved in terrorist activities are closely monitored and strictly controlled by special units of EU institutions and law enforcement agencies of the Member States. In contrast, lone actors are hard to detect, as they have no history of radical activity and sometimes do not even express their radical views publicly or do it anonymously with extreme caution, e.g., using encryption software. As a result, the application of countermeasures and implementing prevention mechanisms regarding individuals acting alone is highly complex and challenging.

The threat posed by lone actors is reflected particularly in the statistics published by Europol. According to the report TE-SAT 2020, the perpetrators of 6 out of 7 jihadist attacks completed and failed in 2019 were "lone wolves". It is noticeable that all 14 thwarted attacks were prepared by multiple perpetrators, and the majority of

[5] The word "jihad" literally means in Arabic "struggle" or "effort" and does not mean "war" (war in Arabic is "harb"). Hence, "jihad" embedded in the context of Islamic texts, means a moral or ethical struggle to live in accord with faith, as well as striving to build a good Muslim society or efforts to defend Islam, wherein armed struggle is not a key understanding of the concept.
[6] See also Sedgwick, 2015, 34-41.

the attacks that States failed to contain were carried out by single persons, which clearly shows the problem with the detection of lone actors' activities (TE-SAT, 2020, 14).

Other elements that make up the profile of the jihadism-motivated perpetrator include the proficient use of ICT, the young age – approx. 70% of attackers in 2019 were people aged 20-28 and in overwhelming majority male – comprising 85% (TE-SAT, 2020, 15). Furthermore, mental disorders are considered to have played a role in motivating individuals to commit violent jihadism-inspired attacks. The latest Europol report notes the link between the psychological instability of the individual and the vulnerability to radicalization. According to the report, people with mental health issues are easier to influence through hate speech, fake news and other propaganda tools in the Internet (TE-SAT, 2020, 36).

Europe's jihadist structures are based on loosely connected networks, particularly online communities, acting without a joint strategy, conducting certain activities through relatives and friends, thus increasing effectiveness and reducing the risk of betrayal or information leakage (TE-SAT, 2020, 41).

Referring to the current trends in the discussed area, the impact of the pandemic should be mentioned. Namely, in the first months of the pandemic, with many countries entering a lockdown, an atmosphere conducive to radicalization had developed. The pandemic and the lockdown, in particular, had both economic and social consequences. Some individuals locked in their homes, restricted in the freedom of movement, sometimes in a worse-off financial situation, pursuing their social activity limited to the Internet and social media, are becoming easy targets for propaganda and radicalization. Radicals involved in various types of terrorism, including jihadists, attempt to seize this opportunity to pursue their goals further. Worth mentioning is also the fact that both Al-Qaeda and ISIS claim that COVID-19 is a "divine" retribution for the moral and intellectual degradation of the West and call followers to conduct attacks when authorities are distracted by fighting the pandemic.

One of the recent tendencies in the last few years is also the problem of radicalization in prisons and detention centers. It is a serious security threat that requires active counter-efforts by states, as convicts and detainees are susceptible to engage in criminal behavior and thus are prone to radicalization, violence promotion, and pose a threat both during the imprisonment or detention and after their release (TE-SAT, 2020, 5, 13).

Finally, a noticeable shift in the very concept of jihadist terrorism can be observed. While their predecessors pursued clearly defined ideological and political goals through attacks, the main objective of the new generation of terrorists is to intimidate the European community, destroy the existing order and democracy in EU countries. Jihadist acts are characterized by the efforts of the perpetrators to inflict mass casualties and a tremendous material loss, whereas, in the past, an attack was often an end in itself. Jihadist attacks in Europe are aimed at "soft targets", i.e. facilities or places with large groups of people (e.g. theatres, museums, shopping malls, hotels, restaurants), as well as against "hard targets", i.e. essential facilities and so-called critical infrastructure, the destruction or damage of which may disrupt the functioning of the state, its organs, and institutions or cause other long-term harmful effects, e.g. in the sphere of economy, trade or tourism.

1.1.3. Jihadists' use of the Internet

Referring to jihadists' *modus operandi*, particular attention should be paid to the way online tools are used, as they have become one of the fundamental elements of terrorists' activities. Jihadists exploit Internet tools very skillfully and to a considerable extent. If anyone is wondering why cyberspace is so attractive to jihadists, the answer is simple. The Internet enables cost-free communication regardless of the location of the interlocutors, facilitates spreading propaganda, conducting radicalization and recruitment with the possibility of reaching a very wide audience, planning, controlling and carrying out attacks with a lower risk of detection due to maintaining a high level of anonymity of Internet users, huge possibilities of obtaining and sharing information, as well as fundraising from various sources. To sum up, the advantages of the Internet are colossal: 1) almost cost-free, 2) far-reaching, 3) ensuring anonymity, 4) an excellent source of information and funds, and 5) giving

worldwide audience. Accordingly, with the absence of appropriate, precise and effective countermeasures cyberspace could become an ideal place for terrorist activity.

When classifying jihadists' activities in cyberspace, we can distinguish the following categories of their online activity: a) terrorist acts carried out in cyberspace, e.g. cyber-attacks against key state infrastructures and private entities; b) planning and organization of attacks in the real world; c) organization of terrorist network's functioning - communication, management and control over terrorist cells and individual members; d) propaganda and radicalization - uploading and disseminating terrorist content, including materials depicting extremist ideology, as well as content intended to intimidate, spread anxiety and demonstrate force; e) recruitment and training of new members, f) financing terrorist activities, e.g. fundraising, illicit trade in drugs, weapons and other illegal goods, financial frauds in the digital space.

Let us start a brief overview with a few general remarks on platforms and websites most frequently used by jihadists. Initially, extremists intensively exploited the high popularity and wide audience of such social media giants as Facebook, Twitter, or Instagram. The ability to distribute propaganda on these platforms is perceived as an essential factor that contributed to the initial success of cyber-jihad[7]. However, after the platforms have intensified their efforts to eliminate and prevent terrorist-linked content and launched various countering initiatives[8], the reduction of extremist online activity was expected, but did not happen. Though, according to Facebook's transparency reporting, 99% of terrorism-related content is detected and removed before being reported, research clearly shows that the platform remains an essential place for terrorist activities, through means such as exploiting the weaknesses of security protocols and the hijacking of accounts and hashtags later used for propaganda dissemination, content masking (visual modification as overlaying jihadist videos with the iconography of popular news outlet like BBC and others, allowing to bypass the detection algorithms), gaming text analysis ("broken text" tactics, the use of specialized fonts or misleading, offensive content descriptions – methods to deceive moderators and avoid takedowns), link sharing or coordinated raids on such Facebook pages like US army page or US government pages (Ayad, 2020, 2-4).

As confirmed by the Institute for Strategic Dialogue (ISD) research, social media platforms remain an essential tool in the hands of terrorists. Extremist groups not only can easily be found on social media, but they were able to game the algorithms and keep conducting terrorist activity in a very active and expanded way. For instance, recently the ISD revealed the incredibly high activity of the Fuouaris Upload group – pro-ISIS account network on Facebook, consisting of several hundred accounts and reaching the audience of tens of thousands recipients. As emphasized by the ISD, "the Fuouaris Upload network is not just a case study into the tactics and strategies of a new generation of ISIS supporters online, but it highlights an integrated, multilingual and multiplatform approach to seeding official and do-it-yourself terrorist content on platforms such as Facebook, Twitter and SoundCloud" (Ayad, 2020, 6). The Fuouaris Upload network was brought to life when the world faced pandemic and lockdown, and consequently, people have turned to online communication more than before. Furthermore, currently, the network is quite successfully deceiving both automated and manual content moderation on Facebook.

In addition to the opportunities offered by social media, jihadists take the full advantage of photo, audio and video hosting websites, such as YouTube and LiveLeak, communication applications, e.g. Telegram, Snapchat, WhatsApp and Skype, as well as microblogging platforms such as Tumblr. Their popularity makes the dissemination of ISIS videos, photos, and other propaganda material more successful and far-reaching (Lakomy, 2017).

[7] Cyber-jihad was initiated by the Islamic State at the turn of 2013 and 2014 with the creation of a propaganda machine consisting of specialized cells, including al-Hayat Media Center, Amaq News Agency, al-Himmah Library, Furqan Media Foundation, and al-I'tisam Media Foundation. It was considered the most advanced and probably also the most effective mass terrorist propaganda campaign of this type in history. Currently the network no longer poses a significant threat, as it has lost its effectiveness and influence (Lakomy, 2017).

[8] E.g. the creation of a digital "fingerprints" database for identification of terrorist content initiated by Facebook, Twitter, Google and Microsoft.

It is worth mentioning that messaging and communication app Telegram was the key platform for dissemination of jihadist propaganda online, but due to counter-terrorism actions, it lost its popularity among extremists. Although their presence on the platform is still noticeable, they began to look for new areas for their activity, moving to TamTam or Hoop Messenger, as well as to such marginal apps like BCM or Riot (TE-SAT, 2020, 43). Attempts have been made to use blockchain or peer-to-peer technologies, e.g. Rocket.Chat and ZeroNet (King, 2019). Although these efforts have proved underperforming, however, they show the willingness of terrorists to change and improve their *modus operandi*, while following the latest technological trends.

The above-mentioned online jihadists ecosystem serves them not only for communication, planning, organizing and disseminating propaganda, but also is an excellent set of tools for radicalization, acquiring followers and recruitment of new members of a terrorist network.

Referring to cyber-attacks, we must notice that - according to Europol's research - the probability of them is very low. Furthermore, jihad-inspired hackers so far have not developed their own effective tools and techniques to carry out cyber-attacks. Instead, they only rely on the available instruments offered by the cybercrime market, including the purchase of web-hosting services, download of ready-made software, and rental of botnets to launch DDoS attacks.

An essential element of the jihadists' activity in cyberspace is searching for financial resources. The basic methods in this area include direct fundraising, raising funds through online payment tools, raising funds through pseudo-charity or non-profit organizations (e.g. fundraising allegedly to support the families and orphans of killed militants, to build mosques or wells), money laundering, and online brokering (Cohen-Almagor, 2016). Among other methods we can mention as well are the Hawala money transfer system the use of cryptocurrencies (mainly Bitcoin), and receiving online donations via the Dark Web, which remain important tools for raising funds by jihadist networks. One of the recent trends is the use of cryptojacking technologies.

Summarizing the above, the Internet for jihadists is both a target and a weapon, as they use cyberspace for operational, defensive, and offensive purposes. In operational terms, communication, propaganda, and recruitment are vital for jihadists' online success. Recently we have noticed a renewed expansion of jihadist propaganda to many websites, platforms, and online applications. The methods of spreading propaganda, beside the above-mentioned ones (i.e. overlaying terrorist-related materials with permitted content, "broken text" method, content dissemination through hijacked accounts), include as well: posting links to ISIS-linked websites in the comments section of social media accounts, graphically overlaying such links into videos, publishing propaganda e-books, press[9] and newsletters, audio-video files, cartoons, radio broadcasting[10], composing music with religious and propaganda content (nasheeds), and creation of radicalizing and training computer games[11].

Referring to the defensive sphere, the main point for undetected extremist functioning is the dissemination of the instructions and training on security and anonymity measures, secure and encrypted communication, safe use of mobile phones, and others. Finally, among the offensive capabilities we can notice hacking social media accounts, planting malware, or an opportunity to launch a cyber-attack.

[9], E.g. "Istok" and "Rumiyah" magazines; for more see Matusitz, Madrazo, Udani 2019.
[10], E.g. Al Bayan Radio, renamed later to Radio Al-Tawheed.
[11] The effectiveness of the ISIS strategy and the ability to reach millions of Internet users, even those who are not really interested in terrorist content, rely in particular on the so-called "snowball effect". Namely, after posting of a shocking content (e.g. decapitation, torture) it is instantly transmitted both by news services and shared by ordinary social media users and therefore reaches further recipients from trusted sources, to which they reach more willingly. As a result, the content reaches millions of people with only a small effort of terrorists.

1.2. Right-wing terrorism

1.2.1. Right-wing terrorism phenomenon

Right-wing terrorism does not create a coherent and easy to define movement. The right-wing scene is perceived as extremely heterogeneous in its structure and ideology (TE-SAT, 2020, 67). One can describe the right-wing phenomenon as the ambiance of individuals and small groups united in their rejection of diversity and minority rights and a strong belief in the supremacism of particular groups of people who share some common features – nationality, race, tradition, or culture. It is connected with a variety of sub-currents, which are based on different preconceptions and hatred and includes movements such as, for example, neo-Nazi, racists, anti-Muslimism and anti-Jewish or hooligans groups. Therefore, right-wing ideology is firmly combined with the following political and social beliefs: extreme nationalism, racism, antisemitism, anti-immigration, xenophobia, anti-feminism, and others. The common feature of right-wing terrorists is that they challenge the existing political, economic, and social system and aspire to change it on the radical right model. Following the commonly adopted terminology (ex. used by EUROPOL in TE-SAT and other papers), the authors decided that in this study, the term "right-wing terrorism" will cover all terrorist groups and individual perpetrators sympathetic to the above-mentioned ideas and sharing those characteristics. However, it is worth noting that it does not mean that every far-right group is automatically a terrorist or a violent one (GTI, 2020, 61).

The characteristic feature of right-wing ideological motivated offenses is that they often have "fluid boundaries between hate crime and organized terrorism" (CTED, 2), therefore the same act may sometimes constitute a terrorist crime, while in other cases being perceived as a crime motivated by hate or even an ordinary crime.

1.2.2. Characteristics and current trends

To provide a complex description of the contemporary far-right terrorism that also enables comparison of this phenomenon with jihadist terrorism, we need to address the issue of the perpetrator's characteristic. The noticeable and current trend in the far-right terrorism activity is that most perpetrators of violent radical acts may be qualified as "lone wolves," (TE-SAT, 2020, 19) like the above-mentioned characteristic of jihadi terrorism. It is additionally justified by the "leaderless resistance" doctrine (TE-SAT, 2020, 70), which is popular among right-wing radicals and provides justification for radicalized perpetrators to commit an attack without any guidance, direction, or previous cooperation in planning. The "lone actors" tactic is entwined with online activity because, without having to participate in the big and structured organizations, cyberspace ensures the best way to communicate, share information, and maintain international relations. Therefore, the far-right radicals are considered to be unpredictable and hard to detect. Furthermore, another emerging development of the far-right phenomenon is the increasing number of individuals taking part in extremist activities that have not had any previously detected contact with the radical environment (Weimann, Masri, 2020, 3).

The notable trend is also that far-right terrorists and extremists currently show increasing interest in using explosives and the knowledge about which is mostly facilitated online (TE-SAT, 2020, 20). It is a gradually arising phenomenon that needs to be a subject of concern because traditionally far-right perpetrators were mostly associated with shootings.

Similar to the case of jihadi-motivated perpetrators, a predominant number of far-right-wing radicals that committed, planned, or prepared the violent attack were men. The predominant group consisted of people of young age – between 22 and 30, however, their number in the case of right-wing offenders reached just 40% (TE-SAT, 2020, 18). It is worth emphasizing that, according to some research, far-right activists have a significantly higher previous criminal record than has been noted within jihadists (Ronen, 2020, 8). Despite maintaining international relations, predominant right-wing perpetrators are citizens of the country of attack (TE-SAT, 2020, 18). However, contrary to home-grown jihadi terrorists, in most cases, they not only have

citizenship but also strongly identify with the nation and perceive themself as members of the only ethnically and culturally clean group that has a right to exist in the country.

Like in the case of jihadi terrorism, one can also observe the impact of the ongoing pandemic situation on the far-right functioning. For right-wing terrorists, it creates an unprecedented opportunity "to spread hate, fear, panic and chaos" (Weimann, Masri, 2020, 12). As the pandemic began, it has become the central topic of discussions of right-wing radicals. Like jihadists, right-wing movements have benefited from the above-described consequences of emerging atmospheres conducive to radicalization. However, they also have seized the opportunity to create and disseminate conspiracy such as theories pondering the roles of "the Jewish global elite" and Chinese government or migrants in the creation and spreading of coronavirus (Weimann, Masri, 2020, 12). Radical content, fake news, and conspiracy theories are not the only means used by far-rights according to the pandemic. They also appeal to use the SARS-CoV-2 as a biological weapon to conduct real-world attacks and, for this purpose, launch online campaigns encouraging to spread the virus among the "enemies" and providing tips on how to avoid detection (Weimann, Masri 2020, 12).

Referring to the current trends among far-right terrorism, it is required to discuss briefly the problem's scale. TE-SAT 2020 provides that in 2019, six right-wing terrorist attacks were reported (compare to one in 2018). Moreover, several EU Member States reported the detection of other forms of right-wing activities motivated by anti-immigrant, anti-Jewish, or anti-Muslim ideology that have not met the criteria of terrorist offenses. However, in the same period, the number of arrested decreased more than twice - from 44 to just 21 (TE-SAT, 2020, 18), suggesting that the detecting mechanisms do not work correctly.

Although official data indicates that the number of right-wing terrorist incidents is still relatively low, the factual social hunch of threat remains relatively high. Such an observation has found its manifestation in the words of the German Justice Minister, who claimed that "far-right terror is the biggest threat to democracy right now" (Eddy, 2020). Such a thesis is also supported by practitioners' observations about "an unprecedented influence from violent right-wing extremist groups has developed throughout Europe over recent years" (RAN Network, 2020, 5).

1.2.3. Far-rights use of the Internet

Like the jihadi ones, Far-right extremists actively use the Internet and online tools as one of the fundamental elements of their activities. Moreover, it should be emphasized that they are often considered "the earliest adopters of Internet technology for extremist purposes" (Conway, Scrivens, Macnair, 2019, 2). Therefore, their online activity's intensification has been a natural and fluent process coming from technological development, and policymakers and law enforcement organs should have predicted such. The Institute for Economics & Peace (IEP) analyzed 32 far-right terrorist attacks that occurred between 2011 and 2018 and found out that less than a quarter of perpetrators had significant personal contacts with other right-wing radicals, while over a third were radicalized online. Nevertheless, legislators, policymakers, and academics' closer attention to the widespread use of the Internet by right-wing terrorists and extremists are relatively recent (Conway, Scrivens, Macnair, 2019, 2). Under greater scrutiny, far-right online activity has truly landed only after the Christchurch terrorist attack on 15 March 2019, in which 51 people died. This attack has brutally shown the power and wide range of the use of the Internet. Sometimes, it is even called an "Internet-centric attack" (Conway, Scrivens, Macnair, 2019, 2) because it was both - pre-planned online and live-streamed[12]. Thousands of users had watched the broadcast of Tarrant's attack before Facebook removed it. What is even more terrifying, within the subsequent 24 hours, the clip was copied and posted around 1.5 million times, counting just Facebook (Hoffman, Ware, 2019)[13]. The attack and

[12] Live streaming may be considered nowadays as an arising trend in far-right attacks. Not only the Christchurch attack was live streamed, but also, for example, the attack in Halle on 9 October 2019.

[13] Other social media platforms also were "infected" by the mass posting of the video of the Christchurch attack. The amount of it spreading on YouTube and the fact that users were able to omit its automated flagging system by for example posting modified copies or

the Internet's role made it clear that both – governments and tech companies need to multiply their efforts in the fight against terrorism and violent radical content online.

To emphasize the need for reaction on far-right activity online, we can cite TE-SAT 2020, which states that "despite a recent pushback from major social media platforms, right-wing extremists continued to enjoy much greater freedom to act online in 2019 than, for example, jihadi" (TE-SAT, 2020, 72). It may be caused by the nexus between right-wing political activity, which is socially acceptable and legitimate, and far-right terrorism. That makes it hard to distinguish which content should be removed and to which extent we can treat far-right ideology as being in the frame of the freedom of speech[14].

Let us take a closer look at the far-right extremists' presence online. Right-wing extremists are aware of and, in their online activity, often inspired by methods and tactics of propaganda developed by jihadist factions. They are present on major social media platforms, which is especially important because it gives them a chance to reach millions of people. According to the research, online extreme-right activity has the kind of traction and reach that IS's (Islamic State) and its supporters' content did not have even at the highest point of their social media presence (Conway, 2020). Hence, many far-right extremists, including perpetrators of violent offenses, had their first contact with right-wing ideology there, which makes it justified to claim that the early stage of radicalization often occurs on the popular social media platforms. For many future offenders, content spread there was like "taking the red-pill"[15] - an eye-opening event that let them into a radical ideology (Weimann, Masri, 2020, 5). "Manifestos" distributed online by far-right extremists, often perpetrators of violent attacks, who perform the function of leaders and mentors for many new recruits and "lone wolves", play a crucial role in the radicalization process (Ronen, 2020). They are posted simultaneously on many web platforms and blogs, from the most popular like Facebook or YouTube to those smaller, famous for their weak moderation and high level of users' anonymity - for example, 4Chan or 8Chan[16]. However, contrary to those observations, until recently, some researchers observed an emerging trend among far-right perpetrators of the lack of public communications regarding carried attacks (e.g. publicly claiming responsibility, threats about future acts). It was associated with the "tension strategy", which means raising political and ideological capital on the chaos and social insecurity after the incident (Koehler, 2016).

The characteristic of far-right extremists' activity in social media is the adaptation of the Internet troll-culture with its use of sarcasm and innuendo, (TE-SAT, 2020, 72) and the heavy adaptation of meme culture (Conway, 2020, 2). Both forms let them avoid personal responsibility for their hate speech, incitement of violence, labels, or other content at risk of criminal liability. The memes, jokes, and specialized jargon that dominate far-right online communication channels, while taken separately, cannot be interpreted as terrorist content. However, it does not change the fact that they create "a constant stream of highly distilled ideological thought," and for this reason, pose a significant risk of radicalization (Conway, 2020, 2). Another practice representative for far-right Internet trolls is "doxxing". It is an accumulation of information about their opponents gained from open sources or via hackers' attacks. The purpose of gathering personal, often sensitive, data is intimidation and victimization of persons or groups of people perceived as their enemies (ICT, 2020). Popular and effective right-wing extremists' strategy also uses disinformation and spreading fake news (Weimann, Masri, 2020).

---

recordings forced YouTube to some rapid reaction, such as temporally blocking of some search functions, primarily the "recent uploads" section (Conway, Scrivens, Macnair, 8). YouTube algorithm was also a subject of Global Network on Extremism & Technology report, which confirmed that the recommender system of YouTube prioritizes extreme right-wing material after interaction with similar content, supporting the findings of a previous study (see: Reed, A. et al. (2020). *Radical Filter Bubbles. Social Media Personalisation Algorithms and Extremist Content* [in:] Global Research Network on Terrorism and Technology: Paper No. 8.

[14] It is related to the concept called "the Overton window".

[15] "Red pill - beliefs, choices, or information that allow you to see the world as it really is, even though you would feel safer or happier if you did not. This refers to a scene in the film "The Matrix" where a character is offered a choice between a red pill, which reveals the true world, and a blue pill, which keeps it hidden", https://dictionary.cambridge.org/pl/dictionary/english/red-pill, (accessed: 1.12.2020)

[16] The particular problem is radical content, which apparently has a peaceful character, however, consists of core ideological elements and indirectly encourages hatred. Often, they are perceived as the inspiration for perpetrators of attacks and therefore should also be subject to legal debate.

Among all major social media, special attention should be put on YouTube since a study on radicalization provides "strong evidence for radicalization among YouTube users" (Riberto et al., 2020, 10). Extremists use it to propagate their views, spread hate and even live stream. YouTube uses the algorithm that determines which videos appear as recommended for users. Far-right YouTubers have learned how to utilize it to put their radical violent videos high on the recommendation list for viewers of less extreme content (Weimann, Masri, 2020). In 2019 YouTube itself was subject to accusations stemming from concerns that abusive and violent content posted by YouTubers with broad reach was moderated less harshly because it could bring more financial gains for the company (Conway, 2020)[17].

Another feature of far-right extremists' activity on the Internet is also their use of gaming subculture. They use video gaming platforms to recruit new members[18]. Games often brutal and nested in war scenery, where the player is engaged to combat virtual enemies, create a conducive environment for radicalization. Moreover, this method guarantees straight access to targeted groups – mostly young males – especially vulnerable to radicalization. Online gaming sites are used to communicate via chat features among video gamers and as a platform to broadcast violent materials (e.g. video of terrorist attacks). Gamers on such platforms enjoy much greater freedom than users of traditional social media (Ronen, 2020).

Restrictions emerging on the major social media platforms that continuously develop their policy and methods of eliminating terrorist content motivate radicals to move to so-called "fringe platforms". The most popular among right-wing extremists are *Reddit*, *4Chan*, *8Chan*, *Voat*, and *Gab*. Many researchers have identified the last one as "a safe haven for extreme right-wing movements" (TE-SAT, 2020, 73). Nowadays, it is also observed that the Russian-based platform *VKontakte* is gaining far-right activist interest and is becoming widely used, especially among radical young people (TE-SAT, 2020, 73).

Another separate issue that needs to be addressed in the context of far-right terrorist use of the Internet is the phenomenon of financing terrorist activity. According to TE-SAT 2020, right-wing groups use traditional as well as innovative methods of financing their activities. They collect fees from its members and donations from sympathizers. The characteristic feature is that some of them also gain funds via online merchandising. They produce and distribute the propaganda materials – such as clothes and gadgets with far-right pictures and slogans (often based on the memes' culture mentioned above). Online donations in bitcoin or other cryptocurrencies via various websites have also been detected (TE-SAT, 2020, 23).

1.3. Left-wing terrorism

1.3.1. Left-wing terrorism phenomenon

Left-wing terrorism is a phenomenon frequently nearly omitted in the studies and research. Therefore, due to the lack of data, the authors could not provide as broad or similar a comprehensive analysis for this subject as was done with respect to both previously characterized types of terrorism. Even the look at the TE-SAT 2020 (as well as previous editions) support such observations – for the description of far-left terrorism dedicated twice less space than for far-right and four times less than for jihadi. Such a statement is meaningful and proves that adequate attention is not drawn to this issue, making it questionable if countermeasures meet this phenomenon.
Providing some definitional remarks, we need to note that left-wing terrorism is often combined with anarchist terrorism. For this article, whenever it is not literally distinguished, we will treat those phenomena together. Left-wing terrorism is a term to describe radicals whose primary motivation for activity is triggering revolution

[17] YouTube has recently expanded its hate speech and anti-harassment policy, however, there is no data and research to verify the effects of its new policy.
[18] A separate, but equally important and interesting issue is the use of video games as a tool for radicalization. About the most recent far-right produced games read: https://www.counterextremism.com/blog/emerging-threat-extremist-made-video-games.

that can lead eventually to establish a classless, communist society (TE-SAT, 2020). At the same time, anarchist terrorism is an umbrella term referred to acts committed by people supporting different anarchist ideologies. They are united in the negation of capitalism and authoritarian agenda (TE-SAT, 2020). Their enemies are represented in institutions and people associated with the political, economic, and social system– such as MPs, police and other officials. Therefore, a significant amount of attacks is targeted.

What distinguishes the threat of far-left terrorism from other types is that so far in Europe, it has been polarized on three states – Greece, Italy, and Spain – with only a few occasional, individual attacks in other states. Last year EU Member States reported 26 left-wing and anarchist terrorist attacks, which means that except for a slight decrease in 2018 (19 reported attacks), the total number of attacks perpetrated by far-left radicals has been since 2016, on a stable, but relatively high level. As it can be seen, the number of far-left attacks is much higher than those perpetrated by the far-right. However, it needs to be mentioned that left-wing terrorist attacks are around seven times less lethal than far-right attacks and over 30 times less deadly than jihadi terrorism in average deaths per incident[19] (GTI, 2020).

1.3.2. Characteristics and current trends

Even if associated with organizations, Far-left extremists mostly commit leaderless attacks and often may be described as lone actors. In most cases, perpetrators and organizations claimed responsibility for their actions and published proclamations (the equivalent of far-right "manifestos"). Research shows that most published materials are written in native languages and posted on like-minded online platforms and only occasionally translated into English to reach an international audience (TE-SAT, 2020). It contrasts the far-right publications, where regardless of a country, English plays lingua franca.

When discussing the far-left activities and modus operandi, we should highlight that it is often strictly associated to right-wing terrorism. Far-right sympathizers represent the most natural enemies for them because of their belief and support for opposite values. Therefore, they engage in violent confrontations with them that occasionally take the form of a violent, targeted attack on representatives of far-right organizations or political parties (TE-SAT, 2020, 61).

One of the characteristic features of far-left terrorists and violent offenders in the EU is their strong support of the Kurdish population, especially in Turkey and Syria. Some well-grounded rationales believe that radicalized far-left have travelled to join Kurdish militias in Syria (TE-SAT, 2020). The danger connected with their return from the war places has been raised in public discourse a few years ago and remains a matter of concern for the EU authorities. The activity in the EU Member States of The Turkish Marxist-Leninist terrorist organization (DHKP-C) should be treated as a separate, but not least, issue. The threat of attacks by the DHKP-C on the territory of the EU is relatively low. However, there is strong evidence that European states are a safe logistic base, ensuring finances and military equipment for violent operations aimed at Turkey (TE-SAT, 2020). Therefore, while combating terrorist danger, the EU should take this danger seriously because a tacit approval of radical organizations functioning may easily backfire on those who have let them peacefully grow.

1.3.3. Far-lefts use of the Internet

In detailing the far-left terrorists and radicals' activity in cyberspace, it is justified to claim that they operate in the same way as far-right or jihadi offenders in many areas. What is significant, their online activity has not been a subject of studies or detailed analysis by law enforcement so far (authors have not found at least such reports), as it was in the case of the far-right. The probable reason is that left-wing attacks are often less harmful despite being committed in larger numbers and almost often with no fatalities. From our standpoint, proper and specific research on left-wing content online (on major social media platforms, as well as on fringe ones) should be done.

[19] The average based on data gathered from 1970 to 2018.

The remark needs to be recognized that some groups of far-left extremism consciously resign from using the Internet or restrict it to a minimum, ensuring that the tools used are well-encrypted and do not include GPS or other tracking facilities (TE-SAT, 2020, 62). In relation to this, remains the observation that they display "a high level of security awareness". To communicate, they use mostly encrypted applications and "clean" mobile phones (to lower the risk of tracking their personalities, localization). They also developed their own communicational infrastructure, a specific set of examples being *Riseup.net* (platform for communication that also provides links to other "radical services" – both public and private – with detailed information on how to gain access), *Espiv.net* (platform in the Greek language, that was blocked for some time this year, but in June 2020 its servers have been switched back on), and *Noblogs* (blog mostly in Italian, that promotes itself with a slogan "Connecting radical people. Noncommercial, antifascist, antisexist, privacy-orientated blog platform"[20]).

Therefore, we can summarize that the Internet among left-wing terrorists remains a preferred tool for awareness-raising, propaganda, and recruitments of new sympathizers (TE-SAT, 2020, 62). To spread ideological content, they mostly use websites or weblogs that gather like-minded individuals. It makes it easier to radicalize those most vulnerable because the left-wing rhetoric is close. As mentioned before, they also mostly use native languages, which allow them more transparent and more persuasive communication with supporters from a particular state.

Concerning financing, there have been many similarities between far-left and far-right terrorism. Left-wing organizations also use traditional funding sources, such as members' fees and donations, and what was remarked in TE-SAT 2020 also as coordinating to – collect funds in cryptocurrencies via different online platforms (TE-SAT, 2020, 23).

2. Selected EU Countermeasures Aimed at Preventing and Combating the Terrorist Use of Cyberspace

The European Union is very active in the field of counter-terrorism measures. It is supported by the view that "Member States cannot address those (the most serious and urgent - authors) threats effectively acting on their own" (European Commission EU Security Strategy, 2020). Therefore, there is a necessity to create the tools, infrastructure, and environment for broader collaboration among governments that can help to strengthen their chances of effectively tackling security challenges. The EU competencies in this field are based on Article 83 TFEU (OJ C 326, 26.10.2012), according to which, the European Parliament and the Council have competencies to establish minimum rules concerning severe crimes, among which terrorism is explicitly mentioned. The basis for all of the EU's counter-terrorism responses constitutes the European Union Counter-Terrorism Strategy adopted in 2005. The strategy is grounded on four pillars, that are: prevention, protection, pursuit, and response. Further works on this issue comprise the more concrete elaboration of particular interests generally framed in the strategy.

For the purposes of this article, we can divide recent EU activities on the counter-terrorism field into three major groups:

1) developing and facilitating EU collective cooperation and capability. That means establishing and evaluating common legal mechanisms among others acting on terrorist activity in cyberspace, as well as formulating and developing security strategies and methods for internal EU security in the future years, in which preventing and combating the phenomenon of using cyberspace for terrorists' purposes is one of the priorities;
2) strengthening the internal capabilities of EU Member States, with the aid of studies and research providing them with highly professional, up-to-date, and practical information. This objective is strictly connected with the creation of specialized agencies and other institutional structures gathering politicians, law-enforcement professionals, and non-governmental experts;

[20]See https://noblogs.org/

3) promoting external partnership and cooperation with non-state entities, such as IT Companies. It is an answer to diagnosed danger connected with a borderless character of the terrorist threat.

Counter-terrorism measures require a complex and specific approach. In this article, the authors focus on a matter of terrorist activity in cyberspace and, therefore, analyzes instruments and mechanisms most important for combating this sphere of terrorist activity. Terrorism and radicalization have been isolated as one of the EU Security Union Strategy (2020-2025) priorities. Due to the evolving character of means and patterns of radicalization and terrorism, mechanisms used to prevent, detect, and fight them also need to be continuously revised and updated. The limited extent of the paper makes it impossible to discuss all of the counter-terrorism measures created under the auspices of EU institutions, in collaboration with them or with their support. Therefore, the authors have made a subjective, individual choice of instruments that draw on two grounds: 1) practical importance and adequacy to counter terrorist activity online and 2) representativeness for each of the above-distinguished categories. The chosen instruments and initiatives are the European Union Internet Forum (EUIF) and Radicalization Awareness Network (RAN), Christchurch Call, Directive (EU) 2017/541 on combating terrorism, and the proposed European Council regulation on Preventing the Dissemination of Terrorist Content Online.

2.1. European Union Internet Forum and Radicalization Awareness Network

Terrorism has been appointed in the European Agenda of Security (2015-2020) to be one of the priority threats for the EU's security due to its powerful cross-border and multi-sectorial dimension; a coordinated action plan at the European level is needed. The changing methods of radicalization and strong evidence for the connection between terrorist and violent extremist content online with recent real-world incidents in the EU Member States highlighted the need for closer and more complex cooperation in this field. It was considered that effective counter-terrorism policy demands both - legislative initiatives and legally binding acts, as well as soft law instruments and mechanisms with more voluntary character, which can engage a broader range of entities. For this reason, the European Commission Agenda committed to launching an EU-level Forum to bring together the Commission, EU Member States, and IT companies. Therefore, the EU Internet Forum has been established and gathered a wide range of participants/collaborators, including Europol, academic society and separate EU networks, such as Radicalization Awareness Network (RAN).

The EU Internet Forum (EUIF) has two main objectives: to reduce the accessibility of terrorist content online and empower civil society with effective counter-narratives. Its activity is a subject of the ministerial meeting's annual evaluation that also provides guidance and steers further actions. On 17 July, 2017, the members of EUIF adopted the Action Plan, which includes measures to improve the capabilities of automatic-based detection and removal of terrorist content online. It also contains the commitment to share the technology and tools with other entities, with particular emphasis on smaller IT platforms, which creates a crucial element of building a coherent and stable system.

Considering the task of detecting and quickly removing the terrorist and violent extremist content from the Internet, the authors will discuss two significant EUIF achievements. The first one to mention is "the Database of Hashes"[21], which was announced during the 2nd EUIF meeting in 2016 and launched a few months later. This instrument aims primarily at preventing material from reappearing from one platform to another. Using such a method makes the removal permanent and irreversible. Forasmuch terrorist and violent extremist misuse of the Internet is a subject of continuous and fast changes, and the database also needs to be regularly revised and extended. At the end of 2019, the database has gathered over 300 000 hashes (GIFCT Transparency, 2020) and was perceived as an instrument that significantly helped Internet platforms in quick removal of the terrorist content (European Commission 2029, October 7 Press release). Nowadays, shaping of the database is complemented by the Global Internet Forum to Counter Terrorism (GIFCT) and its Hash-Sharing Consortium

[21] "Hashes" are unique digital "fingerprints" of every known terrorist imaginary or video that had been removed from online service.

based on and connected with the EUIF database. Currently, the Hash-Sharing Consortium consists of 13 companies with access to the database. The system is voluntary, and the members have the freedom to decide how to use it within the frame of terms of services and technical capabilities.

The second instrument that needs to be mentioned in the context of the EUIF is the European Union Crisis Protocol which gained its endorsement at the 5th annual EU Internet Forum meeting on 7 October, 2019. It is the voluntary and subsidiary mechanism helping coordinate the response to the viral spread of terrorist and violent extremist content online in an emergency, when national procedures turned out insufficient. Primary functions of the Protocol are 1) facilitation of a coordinated and rapid reaction to the spread of terrorist or violent extremism content by the EUIF, authorities of Member States, Europol, and the GIFTC; 2) empowerment of public and private sector cooperation through encouraging those entities and supporting voluntary sharing of relevant information (e. g. URLs, metadata) as well as developed technological solutions. The crisis response mechanism consists of four stages – detection, notification, coordination and information sharing, and post-crisis report[22]. The adoption of the Protocol was the EU's response to the far-right extremism incident that occurred in March 2020 in the New Zealand city of Christchurch. This brutal attack betrayed the gap of past mechanisms that were not empowered to efficiently prevent live stream posting and sharing of incidents on a wide range of online platforms. Therefore, it is legitimate to consider the EU Crisis Protocol to contribute to efforts undertaken at the global level, such as the UNGA Crisis Response Protocol or the Christchurch Call (European Commission, 2019, July Fact sheet).

In the field of the development of alternative and counter-narratives strategies, the EUIF works within the frame of the Civil Society Empowerment Programme (CSEP). It is based on the view that violent terrorist and extremist narration online needs a positive counterbalance. Developed in 2015 CSEP, works with civil society organizations and cooperates with them to launch and support "campaigns designed to reach vulnerable individuals and those at risk of radicalization and recruitment by extremists" (CSEP website). CSEP not only establishes campaigns, prepares strategies, and organizes workshops, but also creates a network for European organizations engaged in the field of counter-terrorism. In its database, there are 616 organizations interested in campaigning against radicalization and open for cooperation. CSEP in its last ex-post paper, has also raised the distinction between the online presence of jihadist and far-right extremism. The problem of "the mainstreaming of the extremist language and narratives of far-right extremism (RAN Centre for Excellence, 2019 December)" was noticed and diagnosed as to why countering it is challenging.

Before the EUIF had been launched, in 2011 European Commission founded the RAN. This unique entity brings together first-line practitioners from all Member States engaged in the work with those who have already been radicalized, as well as those diagnosed as vulnerable to radicalization. The RAN – a part of supporting activities of the Member States, other institutions, and programs – consists of a platform for knowledge sharing. It creates a dozen working groups for practitioners from different fields (such as psychologists, IT engineers, law-enforcement organs employees and others) to share experiences and approaches, as well as to review each other's work. Though the meetings are dedicated to professionals, their cooperation's effects and conclusions are shared with the public in a series of publications. Especially important in this article's context is that recently, RAN puts a substantial emphasis on the differences between various kinds of terrorism and points out the need for comprehensive research and appropriate, conscious counter-terrorism measures.

2.2. Christchurch Call

In the fight against terrorist and violent extremist content online, European Union institutions have spotted the need to get involved in actions that range across the EU's borders. As a reaction, they acceded to the Christchurch Call – the action plan announced on 15 May 2019 at the Paris summit to extend cooperation among the wide range of actors involved in the cybersecurity issue. Initiators of the Call appreciated significant steps

[22] There is no information provided if and how many times the Protocol was used (state on 1 December 2020).

that had been already taken by international actors – among other EU institutions. However, they noticed that there is still an area for enhanced actions. Currently (state on 1 December 2020), this initiative gathers 48 countries, the European Committee, two international organizations (Council of Europe, UNESCO), and ten of the largest high-tech corporations – among others Microsoft, Google and Facebook (christchurchcall.com). The Call focuses on a few significant aspects, which are in particular: 1) the development of tools to prevent downloading of terrorist and violent extremism content; 2) combating the causes of violent extremism, 3) the review of the operation of algorithms and modification of them to prevent direction users towards violent extremist content.

It is too soon for general evaluation of the Christchurch Call. Still, after one year of functioning, we can draw some initial conclusions and measure the Call's progress so far, emphasizing its efficiency in combating different types of terrorism and extremism. One of the Call's most significant achievements is the restructuring of the Global Internet Forum to Counter Terrorism (GIFCT). The GIFTC was launched by Facebook, Microsoft, Twitter, and YouTube in 2017. The Call reformed it into an independent organization with dedicated resources capable of wide-range collaboration across multiple entities. The most significant partnerships are those with Tech Against Terrorism[23] and Global Network on Extremism & Technology (GNET)[24]. A significant achievement in combating terrorism content online has been the development and distribution of technological solutions: Hash-sharing consortium, Content Incident Protocol (CIP)[25] and URL-Sharing[26]. Those tech-industrial developed mechanisms are integrated with Christchurch Call Shared Crisis Response Protocol and collectively has been arranged to allow for the far-quicker, more efficient, and better-coordinated response to the online impacts of the attack (European Commission, 2019, October 30 press release). So far, most efforts have been focused on dealing with the problem of livestreams of real-world acts. This activity reaches a broad consensus among governments, tech companies, and civil society, which agree on what content should be removed. Its crisis response protocol has been used twice – in October 2019 and February 2020 (both in case of far-right attacks) - and demonstrated a more efficient and far-quicker response mechanism to the online posting content about attacks, preventing it from turning into a significant online crisis (Arden, Macron, 2020).

2.3. Directive (EU) 2017/541 on combating terrorism

Despite the increasingly extensive set of tools aimed at combating terrorism being developed in the second decade of the XXI century, there were still legal gaps to be filled and the need to address and penalize various forms of actions supporting terrorist activities.

Therefore, in March 2017, the EU took a step towards intensification of the legal struggle against terrorism and adopted the Directive (EU) 2017/541 on combating terrorism. The Directive was supposed to strengthen and extend the scope of already binding EU legislation and among its essential goals were, in particular; to set out a legal framework for judicial harmonization; to improve the exchange of information; to develop investigation tools; to enhance cooperation in the field of preventing, countering, and penalization of terrorist offenses; the enlargement of the list of such offenses that underlie terrorist activity in European countries and extending the protection of terrorism victims. The Directive penalizes such actions as 1) travelling within or outside the EU for terrorist purposes (e.g. aiming to join a terrorist group or to carry out an attack); 2) providing logistical and material support for such trips (e.g. purchase of a ticket, route planning); 3) conducting terrorist training or

[23] The initiative of an interdisciplinary team of counter-terrorism experts supported by the United Nations Counter-Terrorism Executive Directorate (UN CTED) that works with the global tech industry to combat terrorist content online with the maintenance of human rights.
[24] Academic research background of GIFCT that aims to understand better how terrorists use the technology.
[25] The Protocol is based on the online existence of content related to the real-world terrorist or violent extremist attacks, and it aims to prevent the potential distribution of it. By declaring a CIT all hashes are immediately shared in the database with other GIFCT members (GIFCT.org).
[26] Only the tech-company has the jurisdiction to remove the content from their service. This cooperative project guarantees a safe mechanism to share the URL links with the industry partner to whose servers the link direct. Since its launch, it has shared near 24,000 URLs (GIFCT.org).

consciously undergoing it (e.g. training on the production or use of explosives, firearms, harmful and dangerous substances); 4) providing and raising funds with the intention or knowledge that they would be used to commit or finance terrorist offenses.

Referring to the problem of the Internet use for terrorist purposes, it was essential to extend the concept of terrorist offenses not only to new categories of activities considered illegal but to broaden the scope especially to those carried out via the Internet, including the exploitation of social media. The Directive penalizes online incitement of terrorist acts and the online dissemination of terrorist content, such as texts and images supporting the ideas of extremism or serving to intimidate the population. Moreover, the Directive considers it a crime, both providing online training in carrying out terrorist acts, and consciously undergoing such training. The Directive also highlights that simply downloading training material for the purpose of committing a terrorist offense may be considered as undergoing terrorist training and may therefore be subject to criminal liability.

The Directive places particular emphasis on operational and legislative measures to counteract the dissemination of online content inciting commitment of terrorist acts. For the effectiveness of counteractions, it is considered particularly important to remove the source of terrorist content promptly or at least to block access to it. At the same time, the Directive highlights that the means and methods used to combat terrorist content on the Internet should guarantee an appropriate level of legal certainty and foreseeability to Internet users and service providers, as well as accessibility to remedies in domestic procedures.

It should be pointed out that the Directive is not aimed at increasing the accountability of Digital Service Providers (hereinafter DSP) and imposing on them a general obligation to monitor transmitted and stored data or to seek out actively illegal content[27]. Moreover, the Directive stipulates that hosting service providers cannot be held liable for illicit Internet content unless they had a knowledge of it.

The Member States had a duty to transpose the Directive's provisions into domestic law by 8 September, 2018. After the deadline has expired, the European Commission began assessing notifications received from the Member States regarding implementation. It is noteworthy that 16 states have failed to communicate the transposition of the Directive and, therefore, the Commission launched infringement procedures against them. By the end of July of this year, 15 of them have notified completing the implementation (European Commission, 2020, September 30, Report).

The Directive has raised many concerns and criticism. Firstly, it posed a challenge for national legislators, law enforcement authorities, and practitioners, mainly due to indeterminacy of some provisions and doubts as to their consistency with the rule of law and human rights. Secondly, some of the offenses enshrined in the Directive's provisions were perceived incompatible with the principle; that prosecuting and punishing individuals has to be based on their culpable conduct and intent. Thirdly, chosen modes of liability, i.e. facilitating, aiding and inciting, has raised serious concerns as to their limits and implications after the transposition to domestic law. Finally, judges and prosecutors were left with a challenge of applying vague or non-existent definitions.

2.4. Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (TCO-Regulation)

[27] It is the role of the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, so-called NIS Directive. The Directive does not directly address the online safety and security of EU citizens and does not authorize them to act on the reporting of cyber incidents. The NIS Directive is addressed to two categories of recipients: Digital Service Providers (DSP) and Operators of Essential Services (OES). Since the provisions of the NIS Directive do not apply to most of the terrorist activities in cyberspace discussed here, its presentation is beyond the scope of this study.

Further steps by the EU legislator in the field of combating terrorism activities in cyberspace were directed towards intensifying efforts to eliminate the problem of disseminating terrorist content on websites and Internet platforms. Such a step was forced, among others, by the awareness that the jihadists' online propaganda is technologically advanced, well-thought-out and undoubtedly poses a severe challenge to the EU's anti-terrorism strategies. At the same time, combating terrorist content is extremely important, bearing in mind the dangers of disseminating it online and the role it played in carrying out attacks on the territory of EU countries in recent years. The general legal framework for removing illegal content from the Internet was established in 2000 by the so-called E-commerce Directive, however, there was a need for a more effective and up-to-date legal tool.

The European Commission, in its Communication of 28 September 2017 on Tackling Illegal Content Online, emphasized: "What is illegal offline is also illegal online", and unquestionably incitement of terrorist activity, hatred and violence, and racist and xenophobic speech should be considered inadmissible content. The Commission called on Internet platforms to step up their efforts to eliminate illegal content, and opted for an extension of their liability for posted materials, as well as encouraged the dissemination of good practices for prevention, detection, and effective removal of illegal content and implementation of appropriate monitoring mechanisms. The Commission underlined that it expects online platforms to take immediate actions and announced that it will monitor progress and take further measures, including the development of legislative initiatives to complement the existing legal framework. The end of works on the legal instruments for combating illegal content online was then announced for May 2018.

After that first announcement of the new legal initiative aiming to tackle terrorist content, many NGO's expressed their concerns (e.g. Human Rights Watch). They mainly have argued that such a step was neither necessary nor justified and considered the draft regulation very flawed.

Following the recommendations of the European Commission, the largest IT companies, such as Facebook, Instagram, Twitter, YouTube, Microsoft, Google+, Snapchat and Dailymotion, obliged themselves to conduct analyses and, if necessary, remove xenophobic and racist content as quickly as possible (mostly within 24 hours).

On 1 March 2018 the European Commission, considering the necessity to take further action, issued the Recommendation on measures to effectively tackle illegal content online, which changed the rules of liability of DSPs, at the same time postulating an increase in speed and effectiveness of their response to reporting of suspicious content and implying to take proactive actions by them. The "notice and takedown" procedure in the case of terrorist content should be completed within one hour after receiving the notification from the competent state authorities.

In addition to the above-mentioned, the European Commission initiated legislative work on the draft regulation for preventing the dissemination of terrorist content online and consequently presented its TCO-Regulation proposal on 12 September, 2018. The proposed provisions cover hosting service providers who offer their services within the territory of the European Union, regardless of whether their headquarters are in the EU or outside it. The draft regulation obliges them to remove terrorist content from the Internet or block access to it within one hour of receiving an order from state authorities. In case of failure to comply with this obligation, the provider may face a severe financial penalty (up to 4% of its annual turnover).

However, the imposition of sanctions was left to the discretion of the Member States.

In addition to the path of removing illegal content on the order of competent authorities, the proposal of TCO-Regulation also provides for a parallel procedure whereby a state authority sends a non-binding notification of suspicious material. In such a situation, the assessment and decision to remove or block the indicated content will be entirely up to the portal administrator.

The proposal defines the concept of terrorist content as "encouraging participation in terrorist offences", "promoting the activities of a terrorist group", "inciting to commit terrorist offences" and "instructing on methods or techniques for the commission of terrorist offences".

The proposed provisions require DSPs to develop appropriate mechanisms to allow users to challenge actions taken against them, as well as maintain a certain level of diligence and apply proactive measures to prevent the reappearance of removed terrorist content, while state authorities have the right to force providers to apply "specific" measures[28].

Work on the legislative proposal presented by the Commission is still ongoing, as there have been significant divergences of opinion among EU bodies regarding its provisions. The European Parliament has called for strengthening the protection of fundamental rights, in particular freedom of expression, and upon that, has advocated removing the obligation for providers to generally monitor Internet content in line with the E-commerce Directive, and excluding the possibility of forcing them to use proactive measures. Parliament has commented negatively on algorithms and re-upload filters, which compare disseminated content with that already removed and stored as illegal. Parliament has underlined that these mechanisms are not suitable for a complex analysis of the legality of online content as they do not understand the context which was posted. Moreover, such "databases" of illegal content are not transparent and are generally not based on court rulings, and therefore are not subject to control, which may result in abuse and removal of legal content, but constitute polemics or controversial views on specific sensitive political issues.

On 17 April 2019, the European Parliament presented the modified proposal of the TCO-Regulation and consequently, the European Parliament, the Council of the EU, and the European Commission, started trialogue aimed at reaching an agreement on the final shape of the Regulation. On 29 September 2020 the most recent text – Presidency package proposal - was presented (JHD 2020, Presidency). It is a compromise solution between the proposals of the European Parliament, the Council, and the Commission. The Presidency proposal highlights that the main objective of the TCO-Regulation is to establish an institutionalized mechanism ensuring the cross-border cooperation aimed at fast and effective removal of terrorist content online. The developed measures should be harmonized, proportionate, and based on "a clear scope and a targeted definition of terrorist content". Particular emphasis is put on adopting a uniform, targeted definition of terrorist content online throughout the EU, aligned to the Directive (EU) 2017/541. The definition should be based on the assumption that combating is aimed at prohibited, illegal content, while ensuring the protection of fundamental rights, including freedom of expression, thus protecting the publication of materials for educational, journalistic, artistic or research purposes.

The EU's proposed legislation to combat the dissemination of terrorist content online has been the subject of severe criticism not only from NGO's and tech-companies but also from the Member States. It is mainly accused of posing a serious risk to freedom of expression, media pluralism and access to information. The proposed legal solution presents a broad understanding of the concept of "terrorist content", which may lead to the so-called "over-blocking", i.e. excessive restriction of the content distributed, arbitrary removal, and censorship of legal statements with no real threat. According to the assumptions of the proposal, online platforms are to act as arbitrators assessing the legitimacy of the notification, and in case of receiving an order to remove content from the competent state authorities, they are obliged to verify the materials within one hour. In practice, carrying out an in-depth assessment in such a short period of time is unattainable and, as a result, would likely result in the automatic removal of such content as portal moderators would not dare to challenge government orders. The initial proposal to introduce the requirement to apply proactive measures by hosting service providers was also strongly criticized, as it means the use of automated solutions that do not guarantee adequate access to the appeal mechanisms.

[28] In the initial version of the Regulation proposal the term "proactive measures" was used, however, as a result of the European Parliament's protest and the compromise reached, it was replaced with the term "specific measures".

3. The Assessment of the Effectiveness of the Countermeasures

Unambiguous assessment of the EU counter-terrorism efforts is a comprehensive and very complicated issue. In this paper, the authors decided to point out its applicability and efficiency in different types of terrorism and leave beyond the study's scope, occasionally rising in literature, more general concerns and doubts about the nature, adequacy, and functioning of the whole EU counter-terrorism system.

The authors have made general remarks on the jihadi, far-right, and far-left terrorism characteristics, emphasizing their differentiated features. In the authors' opinion, those diagnosed differences are the main reason for the weaknesses in the adequacy of the measures targeted on jihadi terrorism to combat the remaining two and make the possibility of creating a universal tool doubtable.

The first observation refers to a terminological issue and is common to jihadists, far-right, and far-left extremists - namely, the issue concerning the currently dominant "lone wolf" tactics. Some Member States' domestic law recognizes as terrorist offenses only those committed by a terrorist group or individuals acting as members of such a group[29]. As a consequence, the offense committed by a person acting alone, even if it factually constitutes a terrorist act, is not qualified as such. This means that lone perpetrators are not the target of anti-terrorist strategies. Given that the "lone wolf" method is currently dominating in Europe, such tactics by national authorities undermine the effectiveness of the entire EU terrorism counteraction system.

The problem with the lack of definitive boundaries between hate crimes, terrorism, and ordinary crimes is even more visible in the context of far-right and far-left terrorism than with jihadism. The lack of a universal definition of terrorism and terrorist acts among the EU Member States leads to situations where the same act may constitute a terrorist crime in one state while being perceived as a crime motivated by hate or even an ordinary crime in another. That enforces the thesis about probable underestimation of the number of terrorist attacks in some statistics and reports (e.g., TE-SAT) based on classifications prepared according to state law. The definitional difficulties seem to relate to all kinds of terrorism equally. However, they are particularly evident in the far-right and far-left context because of their nature and strong connections with legal movements[30].

There are well-grounded opinions that right-wing terrorists in Europe, in many cases, intentionally and strategically "blend in with the surrounding societies" (EU CTC, 2019) to minimalize the risk of detection and repressions that would meet them in case of adopting the counter-terrorism measures. Far-right extremists often devote themselves to broader ideological, political, or quasi-political organizations and support like-minded protests and initiatives. They can thereby remain in the shadow while simultaneously strengthening and radicalizing their own beliefs and preparing attacks that outwardly may seem to be unprepared and spontaneous. Those remarks apply to far-left perpetrators as well. Therefore, the general observation on the efficiency of the EU counter-terrorism measures in the context of far-right and far-left terrorism is that without a precise and - equally important - unified definition of terrorism, it will be difficult to assess if they work correctly. Forasmuch every instrument only finds the use of the limited amount of acts and behaviors[31].

Except for the difficulties connected with notably different characteristics of every type of terrorism, their diverse fundaments also present a challenge for counter-terrorism measures. Far-right and far-left ideologies are stronger culturally adopted in Europe. The language and some postulates used by the radical wings have also become part of ongoing political debate, especially in areas of so-called political correctness, minority rights, or

[29] E.g. The German Penal Code.

[30] As the authors mentioned in the II section, not many studies concern the far-left terrorism in the EU. Therefore, the defining problem has not been so clearly raised in the literature. However, based on observation of the scene of NGO's, political entities and other movements, the authors conclude that the situation is analogical as with the far-right wing.

[31] It is worth stating at this point, that the TCO-Regulation proposal is an attempt to fill the definition gap, however, as already mentioned, it is so far a largely imperfect project.

gender equality (Kfir, 2019). Such an atmosphere creates an opportunity for far-right and far-left radicals to share their views and recruit like-minded without consequences. Jihadi radicals do not have as much space for the public sharing their content in the early stage of activity.

It is also connected with the problem of algorithmizing of the Internet. Internet platforms suggest its users content that - according to the algorithm – potentially will interest and delight them. So far, only GFCT explicitly declared to carry out the work to modify algorithms to avoid directing users for extremist content. However, the authors believed that this issue demands not only voluntary cooperation of tech-companies, but also legislative countermeasures.

Another issue related to the popularization of the use of algorithms concerns their effectiveness in detecting extremist content online. Europol's report appears to be very optimistic about the effects of automated and manual content moderation strategies, stating that terrorists' online position has been significantly weakened: "The measures taken by social media platforms to counter the spread of terrorist propaganda led some groups, including al-Qaeda and its affiliates, to return to more 'traditional' ways of online communication" (TE-SAT, 2020, 43). Meanwhile, the ISD revealed recently the terrorist accounts network, which was (is?) quite successful in disseminating extremist content on Facebook. This means, that intensified and coordinated actions tackling terrorists' presence in cyberspace, launched by Internet service providers, website owners, and law enforcement authorities of the Member States slightly hinder terrorist activity in cyberspace, but so far have not been able to eliminate it. Moreover, the ISD highlights that "automated and manual moderation practices need to be coupled with real "street-level" understanding of these users' tactics and behaviors" (Ayad, 2020, 5). The aggressive attitude in online content control is not the solution, as it causes more damage than brings benefits.

Another observed issue addressed to counter-terrorism measures is the use of an AI detection and removal system along with concern for far-right and jihadi online activity. Right-wing extremists adopted a meme culture, often using jokes or seemingly neutral symbols with entirely different meanings among like-minded people. For this reason, spread content encroaches into the sphere that is protected by the freedom of speech and freedom of political beliefs. It is then complicated to distinguish right-wing supporters' ordinary and legal content from unlawful hate speech and terrorism. In this context, it is crucial to emphasize that the measures for detection and removal of terrorist content online can be made efficient only if adopted practically on the morrow of that content appearing on the worldwide web. However, that demands a database and code of conducts that are sensible for every characteristic of extremist content and have the capability of contextual analysis that allow distinguishing, non-harmful content; all the while given a high potential of hatred and radicalization being spread.

Conclusions

When answering the question about the universal nature of the developed strategies and countermeasures, as well as the assessment of their effectiveness in fighting the activity of both jihadists and far-left, far-right extremists, we should first consider whether the differences they reveal - in terms of the perpetrator's profile and methods of action - enable the development of effective, universal instruments. The European Union, when proposing legal solutions, has repeatedly emphasized that for the effectiveness of actions and the achievement of the assumed goals of counteraction, a very precise tool is necessary, a tool aimed at the specifics of terrorists' modus operandi and their distinguishing characteristics. Bearing in mind that the methods of operation of jihadists, as well as far-right and far-left extremists have far-reaching differences; the possibility of adopting a universal, highly effective method is somewhat questionable.

Worth noting is the lack of full awareness of the threat posed by far-right and far-left extremists. Primarily there is insufficient available data on the scale, used methods, perpetrators’ profiles, and other far-left terrorism phenomenon characteristics. Quite recently we have turned our attention towards far-right extremism, and it was only due to bloody attacks they have carried out. On the basis of the conducted research, we can see, that far-left

groups are barely-examined, whereas far-right extremists have not shown their full face at all. We can say with high probability, they may still "surprise" us, as they have been gathering their strength standing in the shadow over the last two decades, i.e. since 9/11, while we have been focusing our efforts on fighting jihadists.

From the outcome of this research, we can conclude that it may be impossible to develop a universal counteraction mechanism, especially with regard to terrorist activities online. There is a need for a clear legal framework ensuring compliance with fundamental human rights, defining the limits of states' responsibility in countering terrorism online, and enabling the prosecution and punishment of attacks' perpetrators, including extremists motivated with far-right and far-left ideology. If it is not possible to create one universal legal tool, as long as it ensures effectiveness, we should focus on developing self-contained solutions – created separately for each type of terrorism. Suppose it is not possible to create one universal legal tool, if it is expected to be effective and precise. In that case, we should focus on developing self-contained solutions – created separately for each type of terrorism.

Undoubtedly, technical capabilities to counter the terrorist threat in cyberspace are also indispensable. Social media and other platforms desperately need effective algorithms, that would be capable of removing most of the terrorist content disseminated by both jihadists and far-right, far-left extremists. So far, unfortunately, we haven't found a golden mean in developing such an algorithm. On one hand, if we set too strict boundaries in such algorithms, there is a risk that even neutral, non-threatening content would also be removed. On the other hand, if we develop measures with broader acceptance boundaries, eliminating the above-mentioned "side effects", they could be so imprecise that it would be hard to target particular terrorist activities in cyberspace. Hence, their effectiveness could be compared to the effects of trying to catch a fly with a fishing net.

While looking for a satisfactory solution eliminating the terrorist threat in cyberspace, we should keep in mind the words of Maj. Gen. Yair Golan he said during the ICT's 18th World Summit on Counter-Terrorism in 2018: "The terrorist threats today are not the same terrorist threats from long ago. There's no bearded guy holding a Kalashnikov in the streets anymore. The threat is much more sophisticated".

References

Ardern J., Macron E. (2020). *Christchurch Call: One year Anniversary – Joint statement by Emmanuel Macron and Jacinda Arden. Retrieved from:* https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/christchurch-call-one-year-anniversary-joint-statement-by-emmanuel-macron-and.

Ayad, M. (2020). *The Propaganda Pipeline: The ISIS Fuouaris Upload Network on Facebook*. ISD Briefing. Retrieved from: https://www.isdglobal.org/isd-publications/the-propaganda-pipeline-the-isis-fuouaris-upload-network-on-facebook/.

Civil Society Empowerment Programme. CSEP website. Retrieved from: https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network/civil-society-empowerment-programme_en.

Cohen-Almagor, R. (2016). Jihad Online: How Do Terrorists Use the Internet?, in: Campos Freire F., Rúas Araújo X., Martínez Fernández V. A., López García X. (Eds.). *Media and Metamedia Management*. Springer.

Conway, M. (2020). Routing The Extrime Rights. Challenges for Social Media Platforms. *The RUSI Journal*, 165(1), 108-113. Retrieved from: https://www.tandfonline.com/doi/abs/10.1080/03071847.2020.1727157.

Conway, M., Scrivens, R., Macnair L. (2019). *Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends.* Retrieved from: https://icct.nl/publication/right-wing-extremists-persistent-online-presence-history-and-contemporary-trends/.

Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, *OJ L 88, 31.3.2017.*

Eddy, M. (2020). Far-Right Terrorism Is No. 1 Threat, Germany Is Told After Attack. *The New York Times. Retrieved from:* https://www.nytimes.com/2020/02/21/world/europe/germany-shooting-terrorism.html.

EU Counter-Terrorism Coordinator (2019, August 30). Right-wing violent extremism and terrorism in the European Union: discussion paper, 11756/19.

European Commission (2015, April 28). The European Agenda on Security, Communication From the Commission to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions, COM(2015) 185 final. Retrieved from: https://ec.europa.eu/anti-trafficking/eu-policy/european-agenda-security_en.

European Commission (2017, September 7). Tenth progress report towards an effective and genuine Security Union, Communication From the Commission to the European Parliament, The European Council and The Council, COM/2017/0466 final. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2017%3A0466%3AFIN.

European Commission (2019, July). Security Union. A Europe that protects [Fact sheet]. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/fs_19_4571.
European Commission (2019, October 30). Security Union: Significant progress and tangible results over past years but efforts must continue [Press release]. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6171.
European Commission (2019, October 30). *Twentieth Progress Report towards an effective and genuine Security Union*. Communication From the Commission to the European Parliament, The European Council and The Council, COM/2019/552 final. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0552.
European Commission (2019, October 7). Fighting Terrorism Online: EU Internet Forum committed to an EU-wide Crisis Protocol [Press Release]. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6009.
European Commission (2019, October). A Europe that protects: Countering terrorist content online. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/FS_19_6197.
European Commission (2020, July 24). The EU Security Strategy, Communication From the Commission to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions, COM/2020/605 final. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605.
European Commission (2020, September 30). Report from The Commission to the European Parliament and the Council based on Article 29(1) of Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, COM(2020) 619 final. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A0619%3AFIN.
European Commission (2020, September 30). Report from the Commission to the European Parliament and the Council based on Article 29(1) of Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, COM(2020) 619 final. Retrieved from: https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=COM%3A2020%3A0619%3AFIN.
EUROPOL (2020). European Union Terrorist Situation and Trend Report (TE-SAT). Retrieved from: https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020.
Global Internet Forum to Counter Terrorism (2020, July). Transparency Report. Retrieved from: https://gifct.org/transparency/ .
The Art of Counter-Terrorism (2018). Conference Summary. ICT's 18th World Summit on Counter-Terrorism. Retrieved from: https://www.ict.org.il/images/2018%20Conference%20Summary%20New.pdf.
Hoffman B., Ware J. (2019). *Are We Enternig a New Era of Far-Right Terrorism?* Commentary. Retrieved from: https://warontherocks.com/2019/11/are-we-entering-a-new-era-of-far-right-terrorism/.
Institute for Economics & Peace (2020). Global Terrorism Index 2020: Measuring the Impact of Terrorism. Retrieved from: http://visionofhumanity.org/report.
International Institute for Counter-Terrorism Cyber (ICT) (January-March 2020). Cyber-Desk Review: Report#33. Retrieved from: https://www.ict.org.il/Articles.aspx?WordID=26#gsc.tab=0.
JHA Counsellors (2020, September 29). Terrorist content online. Presidency proposals on various Articles WK 10137/2020.
Kfir, I. (2019). How should the world tackle far-right extremism? Asia & The Pacific Policy Society - Policy Forum. Retrieved from: https://www.policyforum.net/how-should-the-world-tackle-far-right-extremism/.
King, P. (2019, April 9-10). Islamic State group's experiments with the decentralised web. Conference Paper. Hague: Europol. Retrieved from: https://www.europol.europa.eu/publications-documents/islamic-state-group's-experiments-decentralised-web.
Koehler, D. (2016). Right-Wing Extremism and Terrorism in Europe: Current Developments and Issue for the Future. *PRISM*, 6(2), 84-105.
Lakomy, M. (2017). Cracks in the Online "Caliphate": How the Islamic State is Losing Ground in the Battle for Cyberspace. *Perspectives on Terrorism*, 11(3), 40-53. Retrieved from: https://www.jstor.org/stable/26297840.
Martin, G. (2017). Types of terrorism, in Dawson M. et al. (2017). Develo*ping Next Generation Countermeasures for Homeland Security Threat Prevention*. Retrieved from: https://www.researchgate.net/publication/316220694_Types_of_Terrorism.
Matusitz, J., Madrazo, A. and Udani, C. (2019). Online Jihadist Magazines to Promote the Caliphate. Communicative Perspectives. New York: Peter Lang.
RAN Centre for Excellence (2016). Radicalization Research – Gap Analysis. Retrieved from: https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network/ran-papers_en.
RAN Centre For Excellence (2019). Far-right extremism. A practical introduction. Retrieved from: https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network/ran-papers/factbook-far-right-extremism-december-2019_en .
RAN Network (2020). Spotlight. Violent Right Wing Extremism in Focus. Retrieved from: https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network/ran-news/violent-right-wing-extremism-focus_en.
Riberto, M. H. et al. (2019). *Auditing Radicalization Pathways on YouTube*. Retrieved from: https://arxiv.org/abs/1908.08313.
Ronen, H. (2020). F*ar Right Terrorism Similarities and Differences vs. Islamic Terrorism*. ICTs Publication. Retrieved from: https://www.ict.org.il/Article/2534/Far_Right_Terrorism_Eng#gsc.tab=0.
Sedgwick, M. (2015). Jihadism, Narrow and Wide: The Dangers of Loose Use of an Important Term. *Perspectives on Terrorism*, 9(2), 34-41. Retrieved from: https://www.jstor.org/stable/26297358.
Treaty on the Functioning of the European Union, Consolidated version, *OJ C* 326, 26.10.2012.
United Nations Security Council Counter-Terrorism Committee Executive Director Trends Alert (2020). *Member States Concerned by the Growing and Increasingly Transnational Threat of Extreme Right-Wing Terrorism*. Retrieved from: https://www.un.org/sc/ctc/news/2020/04/01/cted-launches-trends-alert-extreme-right-wing-terrorism/.

Weimann, G., Masri, N. (2020). *The Virus of Hate: Far-Right Terrorism in Cyberspace*. ICT. Retrieved from: https://www.ict.org.il/Article/2528/The_Virus_of_Hate#gsc.tab=0.