FACULTY OF LAW AND CRIMINOLOGY

ISIL terrorists and the use of social media platforms.

Are offensive and proactive cyber-attacks the solution to the online presence of ISIL?

Océane Dieu
Student number: 01905845

Promoter: Prof. Dr Gert Vermeulen
Commissioner: Philipp Martin Dau

Word count: 44.019

A dissertation submitted to Ghent University in partial fulfilment of the requirements for the degree of Master of Laws.

Academic year: 2020-2021

This master's thesis is an exam document that has not been corrected for any errors that may have been identified.

GHENT UNIVERSITY

Abstract

De Islamitische Staat is massaal aanwezig op sociale media platformen waar ze haar trouwe en nieuwe aanhangers voedt met terroristische propaganda. Doorgaans wordt deze propaganda in de vorm van *posts*, foto's of video's neergehaald door de private platformen, vaak als reactie op een notificatie, een zogeheten 'referral', van een gebruiker van het platform of op een verwijderingsbevel uitgevaardigd door een overheid. Deze eerste reactieve tussenkomst, via de zogeheten 'notice-and-takedown' mechanismen, is behelsd door een vaag wettelijk kader dat onvoldoende rechtszekerheid biedt aan zowel de platformen als de gebruikers ervan. De onlangs door het Europees Parlement aangenomen "Verordening inzake het tegengaan van de verspreiding van terroristische online-inhoud" brengt hier kleine veranderingen in. Het tweede reactieve mechanisme, de verwijderingsbevelen, werd eveneens, maar op een ingrijpendere manier aangepast door deze Verordening. Zo werd de reactietijd van platformen om een bevel na te leven gereduceerd tot een uur en kunnen overheden grensoverschrijdende bevelen uitvaardigen. Het valt te betwijfelen of zulke maatregelen wel gerechtvaardigd kunnen worden in een Europa waarin landen minder en minder waarden delen en steeds verder democratisch verwijderd staan. Bovendien heeft er over de afgelopen jaren heen een geleidelijke afwending van het verbod om een algemene toezichtsverplichting op de private dienstverstrekkers te leggen, plaatsgevonden. De Europese autoriteiten moedigen in stijgende lijn de private dienstverstrekkers aan om technologische innovatie in hun werking te incorporeren om zo efficiënter terroristische inhoud op te sporen. Dit staat echter op gespannen voet met het voornoemde verbod. Of deze mechanismen vandaag hun doelstelling nog bereiken, de 'vrijwillige' samenwerking tussen staat en private platformen nog te verantwoorden valt en de verregaande bevelen wel gerechtvaardigd zijn, vormt de eerste centrale vraag van dit werk.

Het toekennen aan de Belgische autoriteiten van de bevoegdheid om proactief offensieve cyberaanvallen uit te voeren op toestellen van terroristen zou een oplossing voor de online aanwezigheid van de Islamitische Staat kunnen zijn. Of dit in het huidige Belgisch wettelijk kader mogelijk en wenselijk is, is de tweede centrale vraag die deze masterproef tracht te beantwoorden. Uit de analyse van de wetgeving op internationaal, Raad van Europa, Europese Unie en Belgisch niveau blijkt dat dit in het huidige Belgisch wettelijk kader niet mogelijk is. De Belgische wet kent de inlichtingen- en veiligheidsdiensten de mogelijkheid toe om defensief cyberaanvallen uit te voeren. In het kader van een gewapend conflict, kunnen de Belgische militaire inlichtingen- en veiligheidsdiensten bovendien offensieve cyberaanvallen orkestreren op terroristen die zich buiten het Belgisch grondgebied bevinden. De bevoegdheid om proactief offensieve cyberaanvallen op terroristische toestellen in België uit te voeren werd echter nog niet toegekend aan deze diensten. Of dit vandaag wenselijk is, werd negatief beantwoord gezien de huidige cybercapaciteit van deze diensten en de lacunes in de wet.

Acknowledgement

Before turning to the core subject of this dissertation, I would like to take the time and space to properly thank several people.

For starters, I would like to thank my promoter Prof. Dr Gert Vermeulen, who endlessly challenged me towards a more critical reflection on the subject, always found time to help me unknot the complexity of this subject and opened doors to other persons who would prove to be valuable sources of information. Thank you, Professor, for your time and effort.

Another person who has been invaluable throughout this year is my mentor Bart D'Hooge. Ever since our paths crossed in September 2020, he has been a reference and a central part of my studies. Bart encouraged and supported me in my choice to pursue an extra Master's degree in Cyber Crime and Terrorism. Moreover, he has been an endless source of new opportunities and insights in both this subject and my general personal development. Bart, thank you for everything.

There are several persons I would like to thank for their input in this work. First, I would like to thank Prof. Dr Marc Cools for having taken the time to put me in contact with Senior Captain Bombeke and Member of Parliament Koen Metsu. Moreover, I would like to thank Prof. Cools for having participated in the discussion I had with Senior Captain Bombeke. Second, I wish to express my gratitude towards Senior Captain Bombeke for his explanation of the current state of affairs of the military intelligence services' cyber capabilities. This information has been invaluable for this dissertation. Third, I wish to express my gratitude towards Commissioner Luypaert, who took the time to answer all the questions I had regarding the Belgian Internet Referral Unit and the operations of November 2019. Fourth, I would like to sincerely thank Member of Parliament Koen Metsu for spontaneously having gone to great lengths to assemble information on my subject. Thank you so much for your input, time, and insights.

Last and most importantly, I wish to thank my parents and friends. I want to thank my friends for having been my rock and infinite resource of laughter, motivation, dinner, and wine. It has been a tough year for everyone, but you made it easier.

I am very privileged to say that both my parents have been an endless source of inspiration and support. Not only for this dissertation but for the entire course of my studies, my mother has inexhaustibly read all my papers. Her knowledge and love for the English, French and Dutch language have allowed me to become (I hope) a better writer. I wish to thank my father for having been a sparring partner over the five years. I know I have (sometimes) exhausted you

with my (legal) opinions and that we didn't always agree, but I have learned to be both more moderated in my thinking and more critical in my opinions. Thank you both for endlessly and unconditionally having provided me with coffee, food, support, and love.

Table of Contents

List of abbreviations

CJEU	Court of Justice of the European Union
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
ECtHR	European Court of Human Rights
EU	European Union
EU IRU	European Union Internet Referral Unit
ICCPR	International Covenant on Civil and Political Rights
ICRC	International Committee of the Red Cross
ICTY	International Criminal Tribunal for Yugoslavia
IRU	Internet Referral Unit
ISIL	Islamic State of Iraq and the Levant
i2-IRU	Belgian Internet Referral Unit
NATO	North Atlantic Treaty Organization
UK	United Kingdom
UN	United Nations
USA	United States of America

Introduction

1. On the 21st and 22nd of November 2019, Europol, together with several Member States of the European Union (hereinafter: "EU"), including Belgium, and private service providers, such as Telegram, coordinated a takedown procedure on online terrorist content of the "Islamic State of Iraq and the Levant" (hereinafter: "ISIL"[1]), which had been published on social media platforms by its news channel 'Amaq'.

2. The ever-growing presence of today's society online has also meant an increase in the online presence of ISIL supporters and their propaganda. As a reaction to this online presence, governments, the EU, civil society and private actors have increasingly developed ways to counter this online presence. One of these methods is taking down content that terrorist supporters have published on online social media platforms.

1. Research questions

3. The events of November 2019 have often been qualified and referred to as 'attacks' or 'cyberattacks' perpetrated by Europol and Member States on ISIL propaganda and Amaq.[2] But can the operation legally be qualified as such? Do public authorities, such as governments or EU institutions, have the power to 'attack' terrorist content or online users by, for example, performing cyber-attacks on ISIL's supporters?

4. If answered positively, can these cyber-attacks be considered an 'online' version of targeted attacks perpetrated in armed conflicts, to which the Law of Armed Conflict would

[1] The choice was made to exclusively use the name Islamic State of Iraq and the Levant, hence leaving similar names such as Daesh, Islamic State (IS) or Islamic State of Iraq and Syria (ISIS) aside. This dissertation will specifically concentrate on ISIL and not on other terrorist groups.

[2] X, "La Belgique à la tête d'une opération pour anéantir Amaq, "l'agence de presse de l'EI"", *RTBF* 25 November 2019, https://www.rtbf.be/info/belgique/detail_amaq-agence-de-presse-de-l-ei-hors-d-etat-de-nuire-grace-a-des-cyberattaques-menees-par-la-police-belge-et-europol?id=10373496; A. DE JAEGERE and S. GROMMEN, "Na geslaagde cyberaanval door Belgische politie: "Terreurgroep IS volledig uitgeschakeld op het internet"", *VRT NWS* 25 November 2019, https://www.vrt.be/vrtnws/nl/2019/11/25/europol/; M. CHINI, "Major Belgian cyberattack eliminates Islamic State's presence on the internet", *The Brussels Times* 26 November 2019, https://www.brusselstimes.com/news/belgium-all-news/80427/major-belgian-cyberattack-eliminates-islamic-states-presence-on-the-internet/; X, "Belgian judiciary and Europol attack ISIS' 'press agency'", *Utrecht University* 29 November 2019, https://www.uu.nl/en/in-the-media/belgian-judiciary-and-europol-attack-isis-press-agency.

apply? Is it then legitimate for states to attack, with the purpose of removing, online information in light of the right to freedom of expression?

5. However, if answered negatively and states do not have the capacity to perpetrate cyber-attacks on online terrorist content, the question arises whether there is a need for such mechanisms to remove terrorist content? Or are the existing instruments, and more specifically the notice-and-takedown mechanism, sufficient to combat the online presence of ISIL? Is it still justifiable for states to shift their responsibility of protecting their citizens against terrorist threats towards private actors who are entrusted with the responsibility of ensuring a terrorist-free online environment? Should the state reclaim its responsibility by, for example, perpetrating cyber-attacks on terrorist supporters? Would such cyber-attacks on terrorist supporters and leaders be a legitimate solution for combatting online terrorist content? If so, how would this be framed in the Belgian legal scene?

6. To tackle online terrorist content, Europol and the Member States have primarily been working reactively. Once terrorist content is published on social media, these public actors intervene through the notice-and-takedown mechanism, often cooperating with private service providers. In a nutshell, this mechanism implies that by making service providers aware of the terrorist content on their platform (by flagging the content), the providers can take that content down or make it unavailable for their users. The intervention of Europol and the Member States is essential in the fight against ISIL's presence online. However, once the content has been uploaded, it is visible to a broad public. The damage has, as to say, already been done. Therefore, it is interesting to examine whether this notice-and-takedown mechanism is a sufficient and efficient instrument to tackle online terrorist content. If answered negatively, the question raises whether public actors can take more offensive and proactive measures. One possible offensive measure would be to target ISIL's online presence by proactively disabling their connection to the online world. Another possibility would be to destroy terrorist propaganda on a terrorist's device before it can be uploaded on social media.

7. The cooperation with private actors is central in the debate on the responsibility of tackling online terrorism. Hence, this dissertation's analysis will be limited to the state's and the private service providers' responsibility and liability for online terrorist content, with the exclusion of the liability of the author of the terrorist content.[3] Furthermore, the analysis of the intervention of private service providers will be limited to social media platforms, with the exclusion of, for example, search engines such as Google.

[3] For more information on the liability of the author of the terrorist content online, see SWISS INSTITUTE OF COMPARATIVE LAW, *Legal instruments for combating racism on the internet*, Council of Europe Publishing, 2009, 175 p; E. ÖZKAYA, "The Use of Social Media for Terrorism", *Defence Against Terrorism Review* 2017, Issue 9, 47-59.

Moreover, since the Belgian involvement in the takedown action of November 2019 was crucial[4], the analysis of proactive and offensive cyber-attacks will specifically be centered on whether the Belgian state is competent to perpetrate such cyber-attacks. If answered negatively, this dissertation will analyse whether Belgium is equipped and ready for such competence and responsibility.

8. These questions will guide the reader of this dissertation through the labyrinth of legal instruments and mechanisms. One preliminary caveat is, however, in order. The purpose of this dissertation is to analyse whether the existing mechanism of notice-and-takedown is sufficient and efficient and whether today cyber-attacks are perpetrated on ISIL supporters to diminish their overall presence online. This latter question is very relevant today because of the possibilities it could offer to eradicate ISIL's presence. However, this is also a topic covered by a veil of secrecy. A state that perpetrates cyber offences on citizens heavily flirts with the border of illegality if solid legal barriers do not contain these operations. Even if provided for by the law, one could question the necessity of such a measure. Hence, governments have an interest in not publicly revealing their cyber capacities and operations. The current secrecy that reigns over this topic has, therefore, complicated the quest towards an exhaustive answer. Consequently, the answers (humbly) presented in this dissertation are based on publicly accessible information. Even though the dissertation includes a discussion with a member of the Belgian military intelligence and security services, the decision was made to only rely on information accessible to the public and exclude activities that the state performs in secrecy.

Therefore, the reader should bear the secrecy that surrounds this topic in mind.

[4] *Cf. infra* n° 13.

2. The problematic presence of ISIL on Telegram

9. Amaq is one of ISIL's news channels that often claims terrorist attacks, such as the London Bridge attack of 2019[5] or the Brussels metro attack of 2016[6]. Arisen from the fresh ashes of Osama Bin Laden, the leader of the terrorist group Al-Qaeda who was killed by the United States of America (hereinafter: "USA"), ISIL with at its head Abu Bakr al-Baghdadi gained ground in Syria and Iraq throughout 2014. During this year, it detached itself from Al-Qaeda to become a more violent and independent terrorist group.[7]

10. In the past, several procedures to take content published by Amaq down have been launched by more prominent social network platforms, such as Facebook and YouTube.[8] Due to the higher visibility on Twitter, some ISIL supporters prefer to publish their propaganda on that particular social network and continue to call on their followers to migrate back to Twitter.[9] However, under heavy public pressure, Twitter decided to toughen its policy on online terrorist content.[10] This sterner policy led ISIL's members to relocate part of their official propaganda, recruitment, and news spreading towards a smaller platform, Telegram.[11] Telegram is a platform created in 2013 by Pavel Durov, who is also the creator of Facebook's Russian competitor VKontacte[12], intended to compete with WhatsApp and evade Russian censorship and control.[13] Telegram was created with the possibility of engaging in end-to-end encrypted conversations[14] ("secret conversations"), which enables the users to share and upload an

---

[5] A. VILLAS-BOAS, "The Islamic State claimed responsibility for the London Bridge knife terror attack", *Business Insider* 30 November 2019, https://www.businessinsider.com/isis-claiming-responsibility-for-london-bridge-knife-terror-attack-2019-11?r=US&IR=T.

[6] X, "Islamic State claims attacks at Brussels airport and metro station", *The Guardian* 22 March 2016, https://www.theguardian.com/world/2016/mar/22/brussels-airport-explosions-heard.

[7] S. SPANGENBERG, "Cyber Jihadism: An Analysis on How the Cyber Sphere Has Altered Islamic Terrorism", *Butler Journal of Undergraduate Research* 2020, Vol. 6, 130; C. GLENN, M. ROWAN, J. CAVES and G. NADA, "Timeline: the Rise, Spread, and Fall of the Islamic State", *Wilson Center* 18 October 2019, https://www.wilsoncenter.org/article/timeline-the-rise-spread-and-fall-the-islamic-state.

[8] X, "ISIS' media mouthpiece Amaq was silenced, but not for long", *CBS News* 2 May 2018, https://www.cbsnews.com/news/isis-amaq-online-propaganda-hit-cyber-takedown-bounces-back-in-just-days/.

[9] A.-L. WATKIN and J. WHITTAKER, "Evolution of terrorists' use of the Internet", *Counterterror Business* 20 October 2017, http://www.counterterrorbusiness.com/features/evolution-terrorists%E2%80%99-use-internet.

[10] *Ibid*.

[11] M. BLOOM, H. TIFLATI and J. HORGAN, "Navigating ISIS's Preferred Platform: Telegram", *Terrorism and Political Violence* July 2017, http://dx.doi.org/10.1080/09546553.2017.1339695, 1; M. CONWAY, M. KHAWAJA, S. LAKHANI, J. REFFIN, A. ROBERTSON, and D. WEIR, "Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts", *Studies in Conflict & Terrorism* 2019, Vol. 42, Issue 1-2, 151.

[12] M. BLOOM, H. TIFLATI and J. HORGAN "Navigating ISIS's Preferred Platform: Telegram", *Terrorism and Political Violence* July 2017, http://dx.doi.org/10.1080/09546553.2017.1339695, 1.

[13] N. ROBBINS-EARLY, "How Telegram became the App of choice of ISIS", *Huffington Post* 24 May 2017, http://www.huffingtonpost.co.uk/entry/isis-telegram-app_us_59259254e4b0ec129d3136d5; POLITICO, "Pavel Durov – The life wire", https://www.politico.eu/list/politico-28-class-of-2021-ranking/pavel-durov/.

[14] R. WILLIAMS, "What Is Telegram? The New WhatsApp?", *Telegraph* (*UK*) 25 February 2014, http://www.telegraph.co.uk/technology/news/10658647/What-is-Telegram-the-new-WhatsApp.html.

unlimited amount of photos, files, videos and other content in hidden messages.[15] It is, therefore, more challenging for online service providers to take down the content. Moreover, the programme allows the users to activate a 'self-destruct' timer, which deletes messages once the addressee has read them.[16]

11. Since the content published by ISIL is not publicly available, their audience is reduced. These private 'chats' can host up to 200 participants. In response to this limited audience, ISIL turned to 'supergroups', which allow up to 1000 participants. To be included in these chats, a person must receive an invitation by a URL.[17] Due to the chats' private character, Telegram and specialised units[18] have encountered more difficulties in taking these chats down compared to the channels. Channels were added as a new feature to Telegram in September 2015. These 'channels' enable the unidirectional and public distribution of content. The spreading of terrorist content on Telegram is thus not limited anymore to the merely private sphere. By subscribing to those channels, ISIL supporters can openly receive information spread by, amongst others, Amaq.[19]

From December 2016 to the end of May 2018, Telegram was able to take down 106.573 elements of terrorist content.[20] Whilst Telegram has actively been taking down ISIL's terrorist content, ISIL's supporters have systematically created new channels and chats to re-upload terrorist content.

12. BLOOM, TIFLATI and HORGAN have demonstrated in their research on the use by ISIL of Telegram that ISIL administrators were able to share the same content simultaneously through several channels, bringing the authors of the research to conclude that these administrators had to be using bots to share significant amounts of content at the exact same

---

[15] J. AMMAR, "Cyber Gremlin: social networking, machine learning and the global war on Al-Qaida and IS-inspired terrorism", *International Journal of Law and Information Technology* 2019, Vol. 27, Issue 3, 252.

[16] M. BLOOM, H. TIFLATI and J. HORGAN "Navigating ISIS's Preferred Platform: Telegram", *Terrorism and Political Violence* July 2017, http://dx.doi.org/10.1080/09546553.2017.1339695, 2.

[17] J. M. BERGER and H. PEREZ, "The Islamic State's diminishing returns on Twitter: how suspensions are limiting the social networks of English-speaking ISIS supporters" (occasional paper), *Program on Extremism at George Washington University* 2016, https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/downloads/JMB%20Diminishing%20Returns.pdf, 19.

[18] These 'specialised units' are referral units. The referral units will be described and discussed at large in Part 2, 1.3.1.5. … made partly possible by the intervention of the European Internet Referral Unit (*Cf. infra* n° 105-109) and 1.4.1. The referral units (*Cf. infra* n° 121).

[19] J. M. BERGER and H. PEREZ, "The Islamic State's diminishing returns on Twitter: how suspensions are limiting the social networks of English-speaking ISIS supporters" (occasional paper), *Program on Extremism at George Washington University* 2016, 18; M. BLOOM, H. TIFLATI and J. HORGAN "Navigating ISIS's Preferred Platform: Telegram", *Terrorism and Political Violence* July 2017, http://dx.doi.org/10.1080/09546553.2017.1339695, 3.

[20] M. CONWAY, M. KHAWAJA, S. LAKHANI, J. REFFIN, A. ROBERTSON, and D. WEIR, "Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts", *Studies in Conflict & Terrorism* 2019, Vol. 42, Issue 1-2, 156.

moment.[21] This recourse to bots allowed ISIL to inflate their numbers of shared content and make their presence seem more prominent than it actually was.

Hence, a joint police and cooperation effort was needed to reduce the online presence of ISIL.

13. The takedown action of November 2019 was managed by Europol (and more precisely the European Union Internet Referral Unit, hereafter: "EU IRU") together with a few EU Member States (one of them being Belgium) and Telegram.[22] The entire takedown procedure was triggered and led by the Belgian Investigating Counter-Terrorism Judge, the Belgian Federal Prosecutor's Office, and the Belgian Federal Judicial Police of East-Flanders.[23] The Belgian involvement was thus crucial.

14. In 2020, the EU IRU issued a report declaring that ISIL has been trying to get hold of the social environment ever again since the takedown action on Telegram at the end of 2019. Accordingly, ISIL supporters and publishers have migrated to other social networking sites or applications, such as TamTam, Hoop Messenger, BCM, RocketChat32 and Riot.[24] Consequently, it is questionable whether this notice-and-takedown action fulfils its aim of diminishing ISIL's online presence.

15. In the following dissertation, Europol's, and the Member States' action to take down ISIL's propaganda will be analysed and an alternative will be proposed.

16. First, some notions used throughout this dissertation will be explained, and preliminary remarks concerning the analysis will be made (Part 1).

Governments often intervene after terrorist content has been uploaded online. They 'react' to the content which is already available to the users of the platform. Therefore, a non-exhaustive overview of the most important reactive measures to tackle online terrorist content will be provided, and their efficiency analysed, with a particular focus on the so-called 'notice-and-takedown' mechanisms and the removal orders (Part 2). This second part will assess whether

---

[21] M. BLOOM, H. TIFLATI and J. HORGAN "Navigating ISIS's Preferred Platform: Telegram", *Terrorism and Political Violence* July 2017, http://dx.doi.org/10.1080/09546553.2017.1339695, 6.

[22] EU INTERNET REFERRAL UNIT, "EU law enforcement and judicial authorities join forces to disrupt terrorist propaganda online" (Press Release), 25 November 2019, https://www.europol.europa.eu/newsroom/news/eu-law-enforcement-and-judicial-authorities-join-forces-to-disrupt-terrorist-propaganda-online.

[23] Email with Commissioner A. LUYPAERT, Commissioner (Head of Unit) DJSOC / Internet Recherche - I2-IRU, 29 October 2020; EU INTERNET REFERRAL UNIT, "EU law enforcement and judicial authorities join forces to disrupt terrorist propaganda online" (Press Release), 25 November 2019, https://www.europol.europa.eu/newsroom/news/eu-law-enforcement-and-judicial-authorities-join-forces-to-disrupt-terrorist-propaganda-online.

[24] EU INTERNET REFERRAL UNIT, *Online jihadist propaganda: 2019 in review*, 28 July 2020, https://www.europol.europa.eu/newsroom/news/online-jihadist-propaganda-2019-in-review, 15-16.

the takedown action on Amaq can legally be qualified as a ‘cyber-attack’ or whether a different legal regime covers this operation.

After reviewing the reactive measures that governments, civil society organisations, and private actors undertake, the possibility of perpetrating proactively ‘offensive’ cyber-attacks will be evaluated. ‘Offensive’ measures or attacks are to be understood as governments’ actions to destabilise ISIL supporters offensively instead of merely defending their citizens and institutions against attacks. By proactively intervening, the state does not merely ‘react’ to the activities of terrorists, but it undertakes offensive operations before any hostile attack occurs to prevent the terrorists from acting. An explanation of these notions and an analysis of the existing offensive actions will be provided, followed by the question of whether offensive operations take place on the Belgian soil or should take place if this question is answered negatively (Part 3).

Part 1. Preliminary notions and remarks

17. Throughout this dissertation, several terms will be used extensively. The notion of 'terrorism', for example, raises many questions. Hence, clearly defining these terms is of utmost importance. Therefore, this work will begin with some preliminary notions and remarks. Many of these notions find their definition in the e-Commerce Directive[25]. This Directive will receive a significant place in this dissertation, first, due to the exemption of liability regime it provides for service providers for content uploaded on their platform and, second, because of the legal basis it constitutes for the regime of removal orders issued by states to these providers to remove certain content of their platform. Moreover, the Regulation on addressing the dissemination of terrorist content online[26] and the Belgian Law regulating the intelligence and security services[27] will regularly reappear in the discussion of the measures that can be taken to counter online terrorism content. In what follows, the notions of 'terrorism' (1.) and 'service provider' (2.) will be analysed. Afterwards, the state's control on online terrorist content will be discussed (3.). Last, the fundamental right to freedom of expression will be addressed (4.).

[25] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), *OJ L* 17 July 2000, n° 178, 1 (hereinafter: "e-Commerce Directive").

[26] Regulation of the European Parliament and of the Council on addressing the dissemination of terrorist content online, 29 April 2021, PE-CONS 19/21 - 2018/0331 (COD) (Unpublished) (hereinafter: "Regulation on addressing the dissemination of terrorist content online").

[27] Belgian Law 30 November 1998 regulating the intelligence and security services, *Belgian Gazette* 18 December 1998, 40.312 (hereinafter: "Belgian Law regulating the intelligence and security services").

1. The notion of terrorism

18. A central notion in this dissertation is 'terrorism'. Easily used to silence political opponents, this notion's delimitation is of utmost importance to counter online terrorist content legitimately. Subsequently, the notion of terrorism in general (1.1.), at the international (1.1.1.), Council of Europe (1.1.2.), European Union (1.1.3.) and Belgian level (1.1.4.), and the notion of cyberterrorism (1.2.) will be discussed.

1.1. The notion of terrorism in general

19. The notion of terrorism does not have a universally accepted definition.[28] This absence allows states to fill in the definition on a discretionary basis. Consequently, a political opponent can be considered a legitimate participant of a democratic debate in a specific country, whereas the same person can be qualified as a terrorist in another country.[29] Therefore, the deprivation of rights that ensues the qualification of being a terrorist is very problematic if the person in question is merely a political opponent.

1.1.1. The notion of terrorism at the international level

20. Despite the absence of an internationally accepted definition of terrorism, the United Nations Security Council adopted Resolution 1566 in 2004 in which it included the following elements to fall under the notion of terrorism:

> "*(a) Acts, including against civilians, committed with the intention of causing death or serious bodily injury, or the taking of hostages; and*
> *(b) Irrespective of whether motivated by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature, also committed for the purpose of provoking a state of terror in the general public or in a group of persons or*

[28] D. M. JONES, P. SCHULTE, C. UNGERER, and M. L. R. SMITH, *Handbook of terrorism and counter terrorism post 9/11*, Northampton, Edward Elgar Publishing, 2019, 28.
[29] S. M. BOYNE, "Free Speech, Terrorism, and European Security: Defining and Defending the Political Community", *Pace Law Review* January 2010, Vol. 30, Issue 2, 467; J. YU, "Regulation of social media platforms to curb ISIS incitement and recruitment: The need for an international framework and its free speech implications", *Journal of Global Justice and Public Policy* 2018, Vol. 4, 2.

particular persons, intimidating a population, or compelling a Government or an international organization to do or to abstain from doing any act; and
(c) Such acts constituting offences within the scope of and as defined in the international conventions and protocols relating to terrorism."[30] (emphasis added)

The notion of terrorism thus covers acts that intentionally cause harm, acts that, regardless of the motivation, provoke a state of terror, intimidate a population or compel authorities to do or abstain from doing a certain act, and acts that have been qualified as relating to terrorism by international conventions and protocols.

1.1.2. The notion of terrorism at the level of the Council of Europe

21. At the Council of Europe level, several instruments have been adopted to regulate the fight against terrorism. Taking as examples the 1977 Convention on the Suppression of Terrorism[31] and the 2005 Convention on the Prevention of Terrorism[32], neither of them provide a definition of terrorism.

However, the Convention of 2005 does provide an obligation for the Member States to qualify the public provocation to commit a terrorist offence as a terrorist offence.[33] 'Public provocation to commit a terrorist offence' is to be understood as the "*distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed*"[34]. When committed unlawfully and intentionally, this offence should be criminalised in national law.

The explanatory Report to the Convention specifies that the distribution or the making available of the message can also occur online.[35] However, Belgium did not ratify the Convention.[36]

---

[30] Resolution 1556 of the Security Council of the United Nations (30 July 2004), *UN Doc.* S/RES/1566 (2004).
[31] Convention of the Council of Europe on the Suppression of Terrorism of 27 January 1977, *ETS*, n° 90.
[32] Convention of the Council of Europe on the Prevention of Terrorism of 16 May 2005, *CETS*, n° 196.
[33] Art. 5.2 Convention of the Council of Europe on the Prevention of Terrorism of 16 May 2005, *CETS*, n° 196.
[34] Art. 5.1 Convention of the Council of Europe on the Prevention of Terrorism of 16 May 2005, *CETS*, n° 196.
[35] COUNCIL OF EUROPE, *Explanatory Report to the Council of Europe Convention on the Prevention of Terrorism*, *CETS* 16 May 2005, n° 196, §104.
[36] COUNCIL OF EUROPE, "Chart of signatures and ratifications of Treaty 196" (Status as of 15 May 2021), https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/196/signatures?p_auth=ACutsH6N.

1.1.3. The notion of terrorism at the level of the European Union

22. At the European Union level, the Directive on combating terrorism[37] (1.1.3.1.) and the Regulation on addressing the dissemination of terrorist content online (1.1.3.2.) are worth discussing on the notion of terrorism.

1.1.3.1. The Directive on combating terrorism

23. The Directive on combating terrorism of 2017 does not explicitly define the notion of 'terrorism' but delineates notions related to the concept of 'terrorism', such as a terrorist group or terrorist offences.

As such, the Directive defines a 'terrorist group' as "*a structured group of more than two persons, established for a period of time and acting in concert to commit terrorist offences*"[38].

A 'structured group' means "*a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure*"[39]. The Directive's penholders decided to keep the criminalisation of directing and participating in a terrorist group[40], as was already provided in the, by the Directive replaced, Council Framework Decision 2002/475/JHA on combating terrorism[41].

24. The Directive then further elaborates the minimum of offences that are to be transposed in national law as terrorist offences, such as attacks upon a person's life that may cause death[42], attacks on a person's physical integrity[43], and kidnapping or hostage-taking[44]. For these acts to be categorised as terrorist offences, one of the following purposes must be at the origin of the perpetration: "*seriously intimidating a population, unduly compelling a government or an international organisation to perform or abstain from performing any act or seriously*

[37] Directive 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* 31 March 2017, n° 88, 6 (hereinafter: "Directive on combating terrorism").
[38] Art. 2.3 Directive on combating terrorism.
[39] Art. 2.3 Directive on combating terrorism.
[40] Art. 4 Directive on combating terrorism.
[41] Art. 2 Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, *OJ L* 22 June 2002, n° 164, 3.
[42] Art. 3.1, a) Directive on combating terrorism.
[43] Art. 3.1, b) Directive on combating terrorism.
[44] Art. 3.1, c) Directive on combating terrorism.

destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation"[45]. This criminalisation largely coincides with the UN Resolution 1566.

Whereas the Council Framework Decision 2002/475/JHA already foresaw the sanctioning of the incitement to commit a terrorist offence[46], the Directive on combating terrorism explicitly provides the prohibition of 'public provocation to commit a terrorist offence'. The Directive requires the Member States to make criminally punishable "*the distribution, or otherwise making available by any means, whether online or offline, of a message to the public, with the intent to incite the commission of one of the offences listed in points (a) to (i) of Article 3(1), where such conduct, directly or indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed*"[47] (emphasis added).

25. Moreover, the Directive imposes the criminalisation of the recruitment[48], the receiving[49] and providing[50] of training.

1.1.3.2. The Regulation on addressing the dissemination of terrorist content online

26. The Regulation defines 'terrorist content' as "*material that*":

> *"(a) incites the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541, where such material, directly or indirectly such as by the glorification of terrorist acts, advocates the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed;*
> *(b) solicits a person or a group of persons to commit or contribute to the commission of one of the offences, referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541;*"[51] (emphasis added)

[45] Art. 3.2 Directive on combating terrorism.
[46] Art. 4.1 Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, *OJ L* 22 June 2002, n° 164, 3.
[47] Art. 5 Directive on combating terrorism.
[48] Art. 6 Directive on combating terrorism.
[49] Art. 7 Directive on combating terrorism.
[50] Art. 8 Directive on combating terrorism.
[51] Art. 2.7, a) – b) Regulation on addressing the dissemination of terrorist content online.

The referred offences in article 3.1 of the Directive on combating terrorism are, for example, the previously cited attacks upon a person's life which may cause death, attacks upon a person's physical integrity and kidnapping or hostage-taking.[52]

Furthermore, terrorist content can be "*material that*":

> "*(c) solicits a person or a group of persons to participate in the activities of a terrorist group, within the meaning of point (b) of Article 4 of Directive (EU) 2017/541;*
> *(d) provides instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques for the purpose of committing or contributing to the commission of one of the terrorist offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541;*
> *(e) constitutes a threat to commit one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541.*"[53] (emphasis added)

If these offences take the form of online content, they fall under the scope of the Regulation.

27. The Regulation also defines 'the dissemination of information to the public', similarly to the Directive. As such, publicly disseminating information is understood as "*the making available of information, at the request of a content provider, to a potentially unlimited number of persons*"[54].

28. The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism encouraged the adoption of a definition in the Regulation in line with the elements that the United Nations Security Council included under the notion of terrorism.[55] This European definition incorporates a broader panel of actions under the notion of terrorism than the Security Council did in the Resolution. However, contrary to the Resolution, the Regulation does not refer to the intent that must underly the act.

29. On the 28th of April 2021, the European Parliament agreed on the Council's position on the Proposal for a Regulation on preventing the dissemination of terrorist content online of the 16th of March 2021. This adopted Regulation will serve as the basis for the ensuing

[52] *Cf. supra* n° 24.
[53] Art. 2.7 c) – e) Regulation on addressing the dissemination of terrorist content online.
[54] Art. 2.3 Regulation on addressing the dissemination of terrorist content online.
[55] SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION AND THE SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS WHILE COUNTERING TERRORISM, *Recommendations on the new draft 'Regulation on preventing the dissemination of Terrorism Content Online'*, 3 November 2020, https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=25661.

dissertation. The Regulation will enter into force 20 days after the Regulation will have been published, which at the time of writing has not occurred yet.[56]

1.1.4. The notion of terrorism at the Belgian level

30. At the Belgian level, the legislator defined the notion of 'terrorism' in, amongst others, the Belgian Law regulating the intelligence and security services.[57] As such, 'terrorism' is to be understood as "*the use of force against persons or material interests for ideological or political reasons with the aim of achieving its objectives through terror, intimidation or threats, including the radicalization process*"[58]. This definition is less extensive than the previous ones. Since neither the instruments at the international nor the European level provide a comprehensive definition of terrorism, the Belgian understanding will be used henceforth.

1.2. The notion of cyberterrorism

31. 'Cyber' and 'terrorism'[59] are notions that will be used extensively in this dissertation. The notion of 'cyber' refers to the 'cyberspace' which MELZER defines as "*a globally interconnected network of digital information and communications infrastructures, including the Internet, telecommunications networks, computer systems and the information resident therein*"[60]. The combined form of these notions, 'cyberterrorism', is sometimes used to describe the use of the internet by terrorists.[61] However, agreeing with several authors such as GILLESPIE or OGULANA, this is a misunderstanding of the term since the mere use of the internet by terrorists for purposes of, amongst others, propaganda spreading, recruitment, incitement, or financing is not to be understood as cyberterrorism.[62]

---

[56] EUROPEAN PARLIAMENT, "New rules adopted for quick and smooth removal of terrorist content online" (Press release), 29 April 2021, https://www.europarl.europa.eu/news/nl/press-room/20210422IPR02621/new-rules-adopted-for-quick-and-smooth-removal-of-terrorist-content-online.

[57] Art. 137-141*ter* Belgian Criminal Code regulate the criminalisation of terrorist offences, such as the public provocation to commit a terrorist act in article 140*bis* Belgian Criminal Code.

[58] Art. 8, 1°, b) Belgian Law regulating the intelligence and security services.

[59] For the definition of terrorism, see '1. The notion of terrorism'.

[60] N. MELZER, *Cyberwarfare and International Law*, *UNIDIR Resources*, 2011, https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf, 4.

[61] S. O. OGUNLANA, "Halting Boko Haram / Islamic State's West Africa Province Propaganda in Cyberspace with Cybersecurity Technologies", *Journal of Strategic Security* 2019, Vol. 12, Issue 1, 79.

[62] S. O. OGUNLANA, "Halting Boko Haram / Islamic State's West Africa Province Propaganda in Cyberspace with Cybersecurity Technologies", *Journal of Strategic Security* 2019, Vol. 12, Issue 1, 78; A. A. GILLESPIE, *Cybercrime: Key Issues and Debates*, 2nd ed., London, Routledge, 2019, 98.

32. Similarly, YAR and STEINMETZ distinguish computer-focused crimes from computer-assisted crimes. The former refers to computer crimes such as hacking, denial of service attacks or cyberterrorism, whereas the latter comprises online propaganda, recruitment, and publicity.[63] Hence, these latter actions are understood as computer-assisted crimes, crimes facilitated by the online environment, and not as cyberterrorism.

33. Following the classification given by YAR and STEINMETZ, this dissertation will not analyse the acts of cyberterrorism since this notion does not cover the use of the internet by terrorists.

2. The notion of service provider

34. The notion of 'service provider' often surfaces in the discussion on combatting online terrorist content. The e-Commerce Directive defines a service provider as "*any natural or legal person providing an information society service*"[64].

35. Three types of service providers exist: the mere conduit service providers[65], such as the Belgian Telenet or Proximus[66], the caching service providers[67], such as Cloudflare[68], and the hosting service providers, such as the social media platforms. Henceforth, only the hosting service providers will be included in the analysis since the mere conduit and caching service providers lie out of the scope of the current assessment of terrorist content shared on social media platforms.

A hosting service provider is to be understood as a provider of "*an information society service (…) that consists of the storage of information provided by a recipient of the service*"[69]. Service providers located outside of the European Union that could potentially evade European law are nevertheless subjected to these provisions if they offer services to the European citizens on European soil.[70] Moreover, the service provider should offer its users a platform that makes

[63] M. YAR and K. F. STEINMETZ, *Cybercrime and Society*, 3rd ed., California, Sage Publications, 2019, 98.
[64] Art. 2, b) e-Commerce Directive.
[65] Art. 12.1 e-Commerce Directive.
[66] Cass. 18 January 2011, *NC* 2011, 84, concl. DE SWAEF.
[67] Art. 13.1 e-Commerce Directive.
[68] C. VAN DE HEYNING, "De strijd tegen de niet-consensuele verspreiding van seksuele beelden opgevoerd", *T.Strafr*. 2020, Issue 3, 180.
[69] Art. 14.1 e-Commerce Directive.
[70] Art. 4, a) European Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, C/2018/1177, *OJ L* 6 March 2018, n° 63 (hereinafter: "Commission Recommendation on measures to effectively tackle illegal content online").

the transmission of content more efficient[71] whilst limiting its intervention to a "*merely technical, automatic and passive*" conduct.[72]

36. A more specific form of hosting service providers are the Social Networking Services, or more commonly known as 'social media'. These services can be defined as "*online communication* platforms *enabling individuals to join or create networks of like-minded users*"[73]. The Court of Justice of the European Union (hereinafter: "CJEU") has recognised that "*the owner of an online social networking platform*", such as Facebook[74], "*stores information provided by the users of that platform, relating to their profile, on its servers, and that it is thus a hosting service provider within the meaning of Article 14 of Directive 2000/31*"[75](emphasis added). Facebook, and by analogy Twitter and Telegram, are hence widely recognised as hosting providers.

Since this dissertation entails the implication of 'hosting service providers', and more specifically, 'social media providers' or 'social media platforms', these three terms will be used intertwiningly.

37. The Regulation on addressing the dissemination of terrorist content online introduces a similar definition for a hosting service provider. As such, the provider's intervention consists of the "*storage of information provided by and at the request of a content provider*"[76].

[71] Recital 42 e-Commerce Directive.
[72] CJEU (Grand Ch.) 12 July 2011, C-324/09, ECLI:EU:C:2011:474, *L'Oréal SA v. eBay International AG*, §113; CJEU (Grand Ch.) 23 March 2010, Joined Cases C-236/08 to C-238/08, ECLI:EU:C:2010:159, *Google France SARL v. Louis Vuitton Malletier SA*, §114.
[73] ARTICLE 29 WORKING PARTY, *Opinion 5/2009 on online social networking*, 12 June 2009, WP 163, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf, 4.
[74] CJEU (3rd Ch.) 3 October 2019, C-18/18, ECLI:EU:C:2019:821, *Eva Glawischnig-Piesczek v. Facebook Ireland Limited*, §22.
[75] CJEU (3rd Ch.) 16 February 2012, C-360/10, ECLI:EU:C:2012:85, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*, §27.
[76] Art. 2, 1) Regulation on addressing the dissemination of terrorist content online; Art. 1, b) Directive 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, *OJ L* 17 September 2015, n° 241, 1 defines 'services' as "*any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*".

3. The state's control on online terrorist content

38. The state intervenes to combat terrorism because it has a legitimate interest in doing so (3.1.). However, sometimes the notion of terrorism is abused to silence and prosecute political opponents (3.2.).

3.1. The state's legitimate interest in combatting terrorism

39. Terrorist fighters have increasingly been using the internet for several purposes. The internet and, more specifically, online platforms such as Telegram have been a valuable and inexpensive tool for communicating with other like-minded individuals. It becomes significantly easier to get into contact with people from a niche community in the online world than it would in the offline world. Users who feel marginalised in the offline world because of their radical ideas now feel empowered because of their connectedness in the online world with like-minded persons.[77] This became apparent after the Brussels attacks, which the perpetrators had been communicating about, preparing, planning and coordinating on Telegram.[78] The World Wide Web can also serve as a universally accessible database for instructions and manuals on building specific weaponry[79] or for recruitment and mobilisation purposes.[80]

Stephen Donald Black, former leader of the Ku Klux Klan and founder of Stormfront, which is a white supremacist and far-right Internet forum, said the following:

> "*As far as recruiting, [the Internet has] been the biggest breakthrough I've seen in the 30 years I've been involved in [white nationalism]*."[81] (emphasis added)

---

[77] J. YU, "Regulation of social media platforms to curb ISIS incitement and recruitment: The need for an international framework and its free speech implications", *Journal of Global Justice and Public Policy* 2018, Vol. 4, 4; UNODC, *The use of the Internet for terrorist purposes*, Austria, United Nations publications, 2012, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf, 5.

[78] M. BLOOM, H. TIFLATI and J. HORGAN "Navigating ISIS's Preferred Platform: Telegram", *Terrorism and Political Violence* July 2017, http://dx.doi.org/10.1080/09546553.2017.1339695, 2; A.-L. WATKIN and J. WHITTAKER, "Evolution of terrorists' use of the Internet", *Counterterror Business* 20 October 2017, http://www.counterterrorbusiness.com/features/evolution-terrorists%E2%80%99-use-internet.

[79] G. WEIMANN, *Terror on the internet: The New Arena, the New Challenges*, Washington, United States Institute of Peace, 2006, 123.

[80] UNODC, *The use of the Internet for terrorist purposes*, Austria, United Nations publications, 2012, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf, 5; EUROPOL, *Changes in Modus Operandi of Islamic State (IS) Revisited*, November 2016, https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited.

[81] Quoted from M. YAR and K. F. STEINMETZ, *Cybercrime and Society*, 3rd ed., California, Sage Publications, 2019, 157.

This statement confirms that the internet is used for recruitment purposes of like-minded persons.

40. To reach this niche community of (potential) ISIL supporters, online propaganda has proven to be a helpful tool. Propaganda *an sich* is not illegal. It is rather the incitement to commit violent acts (such as terrorist acts) through propaganda that is prohibited.[82]

41. Whereas before the internet era, the reach of terrorist networks, organisations and propaganda was limited to the territory they occupied and to some extend further (through traditional paper messages), ISIL's reach today is illimited. As CAMBRON puts it, "*social media serves to magnify ISS's ideology*"[83].

42. Furthermore, as the High Commissioner for Human Rights stated, terrorism "*threatens the dignity and security of human beings everywhere, endangers or takes innocent lives, creates an environment that destroys the freedom from fear of the people, jeopardizes fundamental freedoms, and aims at the destruction of human rights*"[84]. Constituting "*the most serious attacks on democracy and the rule of law*" and one of "*the most serious violations of the universal values of human dignity, freedom, equality and solidarity, and enjoyment of human rights and fundamental freedoms*"[85], it is beyond doubt that the will of public authorities to counter the online presence of terrorists is legitimate.

3.2. The notion of terrorism abused by states to silence opponents

43. As became apparent in the previous analysis[86], there is no universally adopted and agreed-upon definition of the notion of 'terrorism'. Only related notions, such as terrorist offences or terrorist groups, have vaguely been defined. This imprecision creates the danger of arbitrarily qualifying certain persons as 'terrorist'[87], whereas their supporters and sympathisers see them as freedom fighters. On several occasions, the European Court of Human Rights

[82] UNODC, *The use of the Internet for terrorist purposes*, Austria, United Nations publications, 2012, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf, 6.
[83] R. J. CAMBRON, "World War Web: Rethinking "Aiding and Abetting" in the Social Media Age", *Case Western Reserve Journal of international law* 2019, Vol. 51, Issue 1, 301.
[84] HIGH COMMISSIONER FOR HUMAN RIGHTS, *UN Factsheet 32 - Human Rights, Terrorism and Counter-Terrorism*, July 2008, https://www.ohchr.org/documents/publications/factsheet32en.pdf, 8.
[85] Recital 2 Directive on combating terrorism.
[86] *Cf. supra* 1.1. The notion of terrorism in general (n° 19-30).
[87] C. WALKER and M. CONWAY, "Online terrorism and online laws", *Dynamics of Asymmetric Conflict* 2015, Vol. 8, Issue 2, 159; M. YAR and K. F. STEINMETZ, *Cybercrime and Society*, 3rd ed., California, Sage Publications, 2019, 96.

(hereinafter: "ECtHR") has condemned Turkey because of labelling political opponents as terrorists.[88]

44. Wanting to take terrorist content down is, as discussed previously[89], an entirely legitimate interest of states. However, not all online content covering terrorist information or news should be regarded as illegal terrorist content. Civil society organisations, journalists, and experts, for example, have an interest in communicating about terrorist activities. Their reporting and exchange of views on terrorist activities should not be taken down in the way terrorist content uploaded by terrorists or terrorist sympathisers should. There is a thin line between those two very different purposes. 'Raqqa is being slaughtered silently' is a good example of such a civil society organisation that portrays real life under the ISIL regime. The organisation has an obvious and legitimate interest in spreading its message.[90]

45. The vague definition of 'terrorism' only contributes to the blurring line which distinguishes political opponents from terrorists.

The more societies push certain content towards the threshold of 'terrorism', the less included the persons who agree with the content will feel in society. This pushes individuals already open for such discourses to the margins of society. Hence, they end up being qualified as 'terrorists'.

Furthermore, the vagueness of the definition of terrorism allows for censorship creep, which refers to using a particular legal basis for a different purpose than for which it was initially adopted.[91] Hence, the definition of terrorism will be used to suppress freedom of thought, freedom of expression and freedom of assembly.

Consequently, the adoption of a clear, exhaustive, and unequivocal definition of the notion of 'terrorism' is more than needed. The Regulation on addressing the dissemination of terrorist content online could have been the perfect instrument for the European Union to incentivise the other international and European organisations to adopt an internationally unified definition. However, the European penholders missed this opportunity by avoiding to adopt a definition of the notion of 'terrorism'.

[88] ECtHR 10 September 2018, n° 13237/17, *Mehmet Hasan Altan v. Turkey*; ECtHR 20 June 2018, n° 16538/17, *Şahin Alpay v. Turkey*; ECtHR 8 July 1999, n° 26682/95, *Sürek v. Turkey*.
[89] *Cf. supra* 3.1. The state's legitimate interest in combatting terrorism (n° 39-42).
[90] J. ELLERMANN, "Terror won't kill the privacy star – tackling terrorism propaganda online in a data protection compliant manner", *ERA Forum* 2016, Vol. 17, Issue 4, 564.
[91] D. K. CITRON, "Extremist speech, compelled conformity, and censorship creep", *Notre Dame Law Review* 2017-2018, Vol. 93, Issue 3, 1051.

4. The fundamental right to freedom of expression in the discussion of combatting terrorism online

46. All persons enjoy fundamental rights, regardless of their political or religious beliefs. Measures taken against terrorists often infringe these fundamental rights. This restriction is legitimised in the securitarian discourse to protect citizens against any terrorist threat. As such, the terrorist's right to assemble and associate online on social media platforms is restricted when the terrorist's access to the internet is limited. Freezing a person's device to prevent the person from accessing the information stored on the device is a violation of the person's right to property.[92] Limiting a person's access to upload information, such as propaganda, on a social media platform constitutes an infringement on the terrorist's right to freedom of expression. The latter fundamental right (4.1.) will be discussed at the international (4.1.1.), the Council of Europe (4.1.2.), the European Union (4.1.3.) and the Belgian (4.1.4.) level. Afterwards, the restriction to this right (4.2.) will be addressed.

4.1. The right to freedom of expression…

4.1.1. The legal framework at the international level

47. At the international level, the right to freedom of expression is, amongst others, enshrined in article 19 of the International Covenant on Civil and Political Rights (hereinafter: "ICCPR").[93] This provision entails an absolute right to hold opinions, which prohibits the state from restricting this right.[94] Every citizen is thus entitled to have a favourable opinion on the messages spread by terrorist groups. People are allowed to consider ISIL to be a legitimate group of freedom fighters.

48. The provision also contains a qualified right to freedom of expression, including the freedom to seek, receive and impart information and ideas.[95] This right can be restricted for purposes of respecting the rights and reputation of others or for the protection of national security, public order, public health or morals.[96] The Human Rights Committee of the United

[92] Due to the limited scope of this dissertation, the right to assembly and association and the right to property will not be discussed.
[93] International Covenant on Civil and Political Rights of 16 December 1966, *United Nations Treaty Series*, Vol. 999, 1. Due to the limited scope of this dissertation, the choice was made to limit the analysis of the international protection of the right to freedom of expression to the ICCPR, with the exclusion of other relevant international instruments, such as the Universal Declaration of Human Rights of 1948.
[94] Art. 19.1 ICCPR.
[95] Art. 19.2 ICCPR.
[96] Art. 19.3 ICCPR.

Nations recognised in its General Comment No. 34 on Article 19 that these restrictions also apply to the online environment.[97]

49. Article 20.2 of the ICCPR prohibits advocating national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.[98] Terrorist propaganda of ISIL would fall under this provision and is hence not protected under the right to freedom of expression.

4.1.2. The legal framework at the level of the Council of Europe

50. At the level of the Council of Europe, freedom of expression and opinion is protected under article 10 of the European Convention on Human Rights (hereinafter: "ECHR").[99] Since no specific mention is made of the medium through which this right should be exercised, the freedom of expression also applies to the internet.[100] Moreover, the ECtHR recognised that "*user-generated expressive activity on the Internet provides an unprecedented platform for the exercise of freedom of expression*"[101]. This right also covers the right to receive and impart information and ideas.[102]

51. The right to freedom of expression contains both a negative and a positive facet. The negative obligation to respect this human right prohibits the state from interfering with the citizens' right to freedom of expression. This negative obligation rests on the state and not on private actors. The positive obligation for states to respect the right to freedom of expression, on the other hand, implies that states must ensure that whenever a conflict arises between a citizen and a private company, the citizen will still be able to enjoy this right.[103] Hence in this horizontal relationship between consumer and private company, the former's right to freedom of expression is still ensured. This negative obligation will be important in the context of the intervention of private actors in the fight against online terrorist content.

---

[97] HUMAN RIGHTS COMMITTEE, *General Comment No. 34 on Article 19: Freedoms of opinion and expression*, 12 September 2011, *CCPR/C/GC/34* (2011), §43.
[98] Art. 20.2 ICCPR.
[99] Art. 10 European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950, *ETS*, n° 5.
[100] W. BENEDEK and M. C. KETTEMANN, *Freedom of expression and the Internet*, Strasbourg, Council of Europe Publishing, 2013, 24.
[101] ECtHR 10 October 2013, n° 64569/09, *Delfi AS v. Estonia*, §110.
[102] Art. 10.1 ECHR.
[103] ECtHR 28 June 2001, n° 24699/94, *Verein Gegen Tierfabriken v. Switzerland*, §45; R. F. JØRGENSEN and A. M. PEDERSEN, "Chapter 10 - Online Service Providers as Human Rights Arbiters", in M. TADDEO and L. FLORIDI (eds.), *Law, Governance and Technology Series*, Vol. 31, *The Responsibilities of Online Service Providers*, Switzerland, Springer, 2017, 181-182.

52. The right to freedom of expression is the backbone of a democracy. Without freedom of expression, citizens cannot fully enjoy and participate in a democratic regime. Consequently, this right covers a broad range of acts. Already in 1976, the European Court of Human Right recognised that article 10 of the ECHR "*is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no "democratic society"*"[104] (emphasis added). The Court also held in a later case that the right to freedom of expression allows for a certain level of exaggeration or provocation.[105] Therefore, it is not because terrorist content offends, shocks, disturbs or provokes the other social media consumers that the content should immediately be banned.

53. Recognising the responsibilities that accompany this right, article 10.2 of the ECHR allows for restrictions: "*The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary*"[106] (emphasis added).

The right to introduce such restrictions on the freedom of expression lies in the states' margin of appreciation and must be provided by a clear, foreseeable, and accessible law. Moreover, the restriction must be necessary in a democratic society and pursue one of the abovementioned aims. Furthermore, these restrictions cannot be used to silence political opponents. As was discussed previously[107], terrorists can be qualified as such for political reasons. The European Court of Human Rights has held in several judgments that "*there is little scope under Article 10 § 2 of the Convention for restrictions on political speech or on debate on matters of public interest*"[108]. Consequently, a delicate approach is required when limiting a person's right to freedom of expression based on terrorist allegations.

[104] ECtHR 7 December 1976, n° 5493/72, *Handyside v. UK*, §49.
[105] ECtHR 16 July 2009, n° 10883/05, *Willem v. France*, §33.
[106] Art. 10.2 ECHR.
[107] *Cf. supra* 3.2. The notion of terrorism abused by states to silence opponents (n° 43-45).
[108] ECtHR 11 July 2006, n° 71343/01, *Brasilier v. France*, §41; ECtHR 8 July 1999, n° 26682/95, *Sürek v. Turkey*, §61; ECtHR 25 November 1996, n° 14719/90, *Wingrove v. UK*, §58.

4.1.3. The legal framework at the level of the European Union

54. At the European Union level, article 11 of the EU Charter of Fundamental Rights covers the freedom of expression and opinion and the freedom to "*receive and impart information and ideas*"[109]. The "*particular importance*" of the internet "*to freedom of expression and of information*" has also been recognised by the Court of Justice of the European Union.[110]

55. According to article 52.3 of the Charter, all rights provided for in the Charter and the European Convention on Human Rights enjoy the same interpretation. However, this identical interpretation does not prevent the European Union from adopting legislation that grants more extensive protection to its citizens. [111]

Therefore, the limitations that are provided in article 10.2 of the ECHR are also applicable in European Union law.

4.1.4. The legal framework at the Belgian level

56. At the Belgian level, articles 19 and 25 of the Constitution protect the freedom of expression. Contrary to the international and European levels, the Belgian Constitution does not provide an explicit basis for the right to freedom of opinion.

The right to freedom of expression is not absolute since both federal and regional laws restrict this right in the case of, for example, incitement to hatred.[112]

57. The right to freedom of expression and its potential restrictions are also applicable in the online environment.[113]

---

[109] Art. 11 EU Charter of Fundamental Rights, *OJ C* 26 October 2012, n° 326, 391.
[110] CJEU (2nd Ch.) 8 September 2016, C-160/15, ECLI:EU:C:2016:644, *GS Media BV v. Sanoma Media Netherlands BV*, §45; F. WILMAN, *The responsibility of online intermediaries for illegal user content in the EU and the US*, Northampton, Edward Elgar Publishing, 2020, 200.
[111] Art. 52.3 EU Charter of Fundamental Rights.
[112] As such, the Belgian Law 30 July 1981 criminalising certain acts inspired by racism or xenophobia, *Belgian Gazette* 8 August 1981, 9.928 replaced by the Belgian Law of 10 May 2007 modifying the Law of 30 July 1981 criminalising certain acts inspired by racism or xenophobia, *Belgian Gazette* 30 May 2007, 29.046 criminalises certain forms of incitement to hatred against persons because of different nationality, skin colour and other grounds. Other laws have been adopted to restrict the freedom of expression, but these will not be discussed since they fall outside of the scope of this dissertation.
[113] D. VOORHOOF, "Vrijheid van meningsuiting en persvrijheid", in J. VANDE LANOTTE et al (eds.), *Belgisch Publiek Recht*, Vol. 1, Brugge, Die Keure, 2015, 578.

4.2. … can be restricted when amounting to hate speech

58. Once information and ideas amount to the level of 'hate speech', the European Court of Human Rights considers that the information and ideas cross the limit of freedom of expression and do not enjoy the protection offered by the Convention anymore.[114] Hate speech was defined by the Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law as the "*publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin*"[115] (emphasis added).

59. Article 17 of the ECHR proscribes the abuse of the rights provided by the Convention.[116] The use of hate speech to negate the fundamental values of the Convention is consequently prohibited.[117] As such, a person cannot rely on the right to freedom of expression to violate the fundamental values of the Convention by, for example, inciting to commit a terrorist attack.

This abuse of the rights of the Convention was condemned by the ECtHR in the case *Belkasem v. Belgium*. The Court took a firm stance regarding hate speech and the glorification and propagation of the *sharia* on YouTube through a series of videos: "*In the present case, the applicant had published a series of videos on the Youtube platform through which he called on his audience to dominate non-Muslims, to teach them a lesson and to fight them. The Court has no doubt about the highly hateful content of the applicant's opinions and endorses the conclusion of the domestic courts that the applicant sought, through his recordings, to hate, discriminate and be violent towards all persons not of the Muslim faith. In the Court's view, such a general and vehement attack is in contradiction with the values of tolerance, social peace and non-discrimination underlying the Convention*"[118] (emphasis added).

The Court further states that "*the applicant is attempting to divert Article 10 of the Convention from its intended purpose by using his right to freedom of expression for purposes manifestly contrary to the spirit of the Convention*"[119] (emphasis added). The Court then concludes that

[114] H. DUFFY, *The 'war On Terror' and the Framework of International Law*, 2nd ed., Cambridge, Cambridge University Press, 2015, 522.
[115] Art. 1, a) Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, *OJ L* 6 December 2008, n° 328, 55.
[116] Art. 17 ECHR.
[117] ECTHR, *Factsheet – Hate Speech*, September 2020, https://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf, 1.
[118] ECtHR 27 July 2017, n° 34367/14, *Fouad Belkacem v. Belgium*, §33. Own translation.
[119] ECtHR 27 July 2017, n° 34367/14, *Fouad Belkacem v. Belgium*, §36. Own translation.

"*by virtue of Article 17 of the Convention, the applicant cannot enjoy the protection of Article 10*"[120].

60. Consequently, terrorists inciting violence and hatred towards others cannot enjoy the benefits of the Convention and, more specifically, the protection of freedom of expression.

[120] ECtHR 27 July 2017, n° 34367/14, *Fouad Belkacem v. Belgium*, §37. Own translation.

Part 2. Reactive measures to tackle ISIL's online content

61. States intervene when terrorist content has been uploaded online. Public authorities want to remove this content from social media platforms to prevent others, especially people interested in such content, to view the content. In doing so, states 'react' to the content put online by terrorist supporters. Hereinafter follows an overview of the legislative initiatives that have been taken to counter online terrorist content reactively (1.).

One preliminary caveat should be made. Taking down all terrorist content might lead people to assume that no such content exists anymore, thus masking the threat terrorist propaganda constitutes. Taking away the terrorist narrative also undermines the counter-terrorism efforts. By taking terrorist content down, while still promoting counter-terrorist narratives, citizens will not see the necessity to publish counter-narratives anymore. Moreover, preventing terrorists from uploading terrorist content on large social media platforms such as Facebook or Twitter incentivises these terrorists to turn towards less public and controlled platforms. Relocating to smaller platforms with more restricted access or to dark web platforms where the terrorist content can flourish unnoticed can be a consequence of denying their access. This migration might toughen the state's work to eradicate terrorist content online and should be born in mind when addressing the issue.

62. Central to this discussion is the liability regime of service providers for content uploaded on their platform and the exemption of liability when they take down the content. Hence, these legislative initiatives significantly impact the functioning of the social media platforms on which such content has been uploaded. These service providers have increasingly been entrusted with growing responsibility for the content published on their platform. Consequently, a discussion on these service providers' (voluntary) cooperation with public authorities is required (2.).

1. Legal framework of reactive measures taken to tackle ISIL's online content

63. Different measures have been taken over the years to combat the online presence of terrorist groups. In what follows, an analysis of the measures taken at the international level (1.1.), the level of the Council of Europe (1.2.), the European Union level (1.3.) and the Belgian level (1.4.) will be provided.

1.1. Reactive measures taken at the international level

64. At the United Nations (hereinafter: "UN") level, there is no international treaty on terrorism that provides measures states should take to counter terrorism online.[121]

65. The UN General Assembly, however, adopted in 2006 the UN Global Counter-Terrorism Strategy, which requires Member States to work with the UN to explore ways to:

> "*(a) Coordinate efforts at the international and regional levels to counter terrorism in all its forms and manifestations on the Internet;*
> *(b) Use the Internet as a tool for countering the spread of terrorism, while recognizing that States may require assistance in this regard*."[122] (emphasis added)

Hence, the General Assembly recognised the extent of online terrorist activities and encouraged countering the spread of terrorism online. The UN Security Council reiterated this concern on the increased use of the internet by terrorists for purposes of recruitment, incitement, financing, planning and preparation of activities in Resolution 1963.[123]

66. Accordingly, at the international level, there is only a general requirement for the *states* to work together to counter the presence of terrorists on the internet, but there is no specific obligation for *hosting service providers* to take down the terrorist content that appears on their platform.

---

[121] UNODC, *The use of the Internet for terrorist purposes*, Austria, United Nations publications, 2012, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf, 18.
[122] Resolution 60/288 of the General Assembly of the United Nations on The United Nations Global Counter-Terrorism Strategy (8 September 2006), *UN Doc.* A/RES/60/288 (2006).
[123] Resolution 1963 of the Security Council of the United Nations (20 December 2010), *UN Doc.* S/RES/1963 (2010).

1.2. Reactive measures taken at the level of the Council of Europe

67. At the Council of Europe level, the legislative instruments adopted by this institution (1.2.1.) and the intervention by the European Court of Human Rights (1.2.2.) are worth discussing.

1.2.1. The legislative instruments of the Council of Europe[124]

68. No legislation holding social media platforms liable for the content uploaded on their platform has been adopted at the Council of Europe level. Nevertheless, in its Declaration on the freedom of communication on the internet of 28 May 2003, the Committee of Ministers of the Council of Europe recognised a similar liability exemption as provided by the e-Commerce Directive[125].[126] Principle 6 of the Declaration reads as follows:

> "*Member states should not impose on service providers a general obligation to monitor content on the Internet to which they give access, that they transmit or store, nor that of actively seeking facts or circumstances indicating illegal activity.*
> *(…)*
> *In cases where the functions of service providers are wider and they store content emanating from other parties, member states may hold them co-responsible if they do not act expeditiously to remove or disable access to information or services as soon as they become aware, as defined by national law, of their illegal nature or, in the event of a claim for damages, of facts or circumstances revealing the illegality of the activity or information.*"[127] (emphasis added)

This Declaration encourages the Member States to hold accountable hosting service providers whose platforms store content uploaded by third parties if the service provider does not expeditiously remove or disable the illegal content when becoming aware of its presence.

[124] Since the European Convention on the Suppression of Terrorism of 1977 aims to facilitate the extradition of persons having committed acts of terrorism (art. 1) and that the internet or social media platforms were not part of the discussions yet, this instrument will not be discussed.
[125] *Cf. infra* 1.3.1.1.1. The regime of liability exemption for hosting service providers (n° 78-83).
[126] COMMITTEE OF MINISTERS OF THE COUNCIL OF EUROPE, *Declaration on freedom of communication on the Internet*, 28 May 2003, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805dfbd5 (hereinafter: "Declaration on freedom of communication on the Internet of the Ministers of the Council of Europe").
[127] Principle 6, 1st – 3rd indent Declaration on freedom of communication on the Internet of the Ministers of the Council of Europe.

However, as emphasised in the Declaration, Member States should not impose a general monitoring obligation on the service provider for the information it stores.

Moreover, the Declaration states that the service providers' obligations cannot jeopardise the freedom of expression of the users of the service.[128] However, this is not a legally binding instrument since it is a mere declaration.

69. A second instrument worth mentioning is the Convention on the Prevention of Terrorism adopted by the Council of Europe in 2005. As was discussed previously, this Convention requires the Member States to qualify the public provocation to commit a terrorist offence as a terrorist offence, but it does not provide an explicit legal basis for tackling online terrorist content. However, this Convention cannot serve as a legal basis in Belgium.[129]

70. Hence, at the Council of Europe level, no legal instrument provides for a(n) (exemption of) liability regime for the social media platforms on which terrorist content is made public. Moreover, the Convention on the Prevention of Terrorism, which imposes the criminalisation of the online public provocation to commit terrorist offences, is not applicable in Belgium.

1.2.2. The intervention of the European Court of Human Rights

71. Whereas no explicit legislation on the liability of service providers has been adopted at the level of the Council of Europe, the European Court of Human Rights, however, has ruled on the matter. In the cases *Delfi AS v. Estonia*[130] and *MTE v. Hungary*[131], the Court was brought to rule on the relationship between the liability of hosting service providers that offer a platform where users can upload content and the hosting service providers' right to freedom of expression.

72. In *Delfi AS v. Estonia*, the Estonian news portal Delfi was convicted by the ECtHR due to its lack of reactiveness regarding hate speech and incitement to violence uploaded on its platform in the form of comments under news articles by several readers.

[128] Principle 6, 4th indent Declaration on freedom of communication on the Internet of the Ministers of the Council of Europe.
[129] *Cf. supra* n° 21.
[130] ECtHR 10 October 2013, n° 64569/09, *Delfi AS v. Estonia*.
[131] ECtHR 2 May 2016, n° 22947/13, *MTE v. Hungary*.

Considering the context of the comments[132], the liability of the authors of the comments[133], the measures taken by Delfi[134] and the consequences of the domestic proceedings for Delfi[135], the ECtHR held that the Estonian courts had struck a fair balance with the right to freedom of expression. The Court ruled that there had been no violation of Delfi's right to freedom of expression.[136] The Court also held that Delfi could not benefit from the liability exemption since its involvement on the news portal went beyond the role of a "*passive, purely technical service provider*"[137].

The Delfi ruling was met with some very critical reactions. The 'Article 19' organisation, for instance, considered that the Court had disregarded the prohibition of imposing on service providers a general monitoring obligation, pursuant to article 15 of the e-Commerce Directive, by stating that Delfi should have prevented those comments from appearing on its website.[138]

73. Following the *Delfi* case, the ECtHR was brought to rule again on the matter of the liability of service providers in the similar case *MTE v. Hungary*. MTE ('Magyar Tartalomszolgáltatók Egyesülete') is the self-regulatory body of Hungarian internet content providers that allows users of their platform to upload comments under publications on their website.[139] As a reaction to an article regarding an alleged consumer-unfriendly real estate website, readers had published several comments perceived as offensive by this real estate website.[140]

Following a similar structure as used in the *Delfi* case, the Court additionally took the comments' content into account when analysing their context and the consequences of the comments on the injured party.[141] Considering the comments as merely 'offensive' and 'vulgar' and the notice-and-takedown procedures of MTE as sufficient to remove the unlawful comments, the Court concluded to a violation of MTE's right to freedom of expression.[142]

74. Consequently, even if no legal basis exists at the level of the Council of Europe for the notice-and-takedown procedure, the European Court of Human Rights has ruled on the issue. The Court's rulings, however, do not provide consistent case-law.

---

[132] ECtHR 16 June 2015, n° 64569/09, *Delfi AS v. Estonia*, §§144-146.
[133] ECtHR 16 June 2015, n° 64569/09, *Delfi AS v. Estonia*, §§147-151.
[134] ECtHR 16 June 2015, n° 64569/09, *Delfi AS v. Estonia*, §§152-159.
[135] ECtHR 16 June 2015, n° 64569/09, *Delfi AS v. Estonia*, §§160-161.
[136] ECtHR 16 June 2015, n° 64569/09, *Delfi AS v. Estonia*, §162.
[137] ECtHR 16 June 2015, n° 64569/09, *Delfi AS v. Estonia*, §146.
[138] X, "European Court Strikes serious blow to free speech online", *Article 19* 14 October 2013, http://www.article19.org/resources.php/resource/37287/en/european-court-strikes-serious-blow-to-free-speech-online.
[139] ECtHR 2 May 2016, n° 22947/13, *MTE v. Hungary*, §6.
[140] ECtHR 2 May 2016, n° 22947/13, *MTE v. Hungary*, §§11-12.
[141] ECtHR 2 May 2016, n° 22947/13, *MTE v. Hungary*, respectively §§74-77 and §§84-85.
[142] ECtHR 2 May 2016, n° 22947/13, *MTE v. Hungary*, respectively §§64 and 91.

1.3. Reactive measures taken at the level of the European Union

75. The European Union has been quite active in the fight against the online presence of ISIL supporters and terrorists in general. The notice-and-takedown regime, which will be discussed extensively in the e-Commerce Directive's context[143], was not the only European attempt to tackle online terrorist content. Over the years, the EU has launched several sensitisation programmes, such as "Check the Web" or "CleanIT". "Check the Web" was an initiative undertaken in 2007 to enable states to collect data on online terrorist propaganda at the offices of Europol.[144] "CleanIT" was another project of dialogue between the academic, governmental and internet industries to reduce the presence of online terrorist content by voluntarily sharing the burden of monitoring the internet for terrorist content.[145] This dialogue resulted in a report of 2013 on best practices and conditions for actions.[146]

76. Two instruments are worth examining in the discussion on the reactive measures taken to limit the online presence of ISIL: the notice-and-takedown mechanism (1.3.1.) and the removal orders (1.3.2.). This first mechanism was initially introduced by the e-Commerce Directive. This Directive has provided a long-standing liability exemption for service providers that take down illegal content stored on their platforms (1.3.1.1.). This takedown practice of illegal content was reiterated in article 21 of the Directive on combating terrorism, which provides the measures Member States must take against public provocation in content online.[147] Second, the Code of conduct on countering illegal hate speech online created new rules for the Code's signatories to tackle online hate speech and sharpened the existing notice-and-takedown mechanism (1.3.1.2.). Third, the Regulation on addressing the dissemination of terrorist content online reiterated the voluntary notice-and-takedown mechanism (1.3.1.3.). Fourth, the Digital Services Act, together with the Digital Markets Act, would, if adopted, introduce new rules for the online environment (1.3.1.4.). Last, the intervention by the European Union Internet Referral Unit, the European body that specialised in this referral mechanism, will be considered (1.3.1.5.). Before turning to the mechanism of removal orders, the legal regime of the notice-and-takedown will be analysed.

---

[143] *Cf. infra* n° 77-88.

[144] C. WALKER and M. CONWAY, "Online terrorism and online laws", *Dynamics of Asymmetric Conflict* 2015, Vol. 8, Issue 2, 167.

[145] ARTICLE 36 COMMITTEE OF THE COUNCIL OF THE EUROPEAN UNION, *Council Conclusions on cooperation to combat terrorist use of the Internet ("Check the Web")*, 29 May 2007, n° 8457/3/07, https://data.consilium.europa.eu/doc/document/ST%208457%202007%20REV%203/EN/pdf.

[146] C. WALKER and M. CONWAY, "Online terrorism and online laws", *Dynamics of Asymmetric Conflict* 2015, Vol. 8, Issue 2, 167.

[147] Art. 21 Directive on combating terrorism. Since the e-Commerce Directive is the main instrument for the notice-and-takedown mechanism, art. 21 of the Directive on combating terrorism will only briefly be discussed in the context of the procedure of taking down online terrorist content (*Cf. infra* n° 87).

1.3.1. The notice-and-takedown mechanism …

1.3.1.1. …introduced by the e-Commerce Directive

77. The e-Commerce Directive introduced the notice-and-takedown procedure, one of the mechanisms most used to take down online terrorist content.[148] When correctly performed, this mechanism exempts the service provider of the liability for having provided a platform on which the users have uploaded the terrorist content. This regime of liability exemption for the service providers (1.3.1.1.1.) will be analysed. Afterwards, the procedure of taking down the alleged illegal content will be addressed (1.3.1.1.2.).

1.3.1.1.1. The regime of liability exemption for hosting service providers

78. The notice-and-takedown procedure does not have an explicit legal basis in European Union law but is implicitly contained in the 'safe harbour' principle of article 14.1 of the e-Commerce Directive[149], which provides:

> "*14. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:*
> *(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or*
> *(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.*"[150] (emphasis added)

79. This provision states that the Member States will not hold liable hosting service providers for the content stored on their platforms if these service providers either do not have knowledge of the illegal content or act immediately to remove or disable the access to that content upon obtaining knowledge or awareness of the illegal content. The immediate action

[148] A. DE STREEL, E. DEFREYNE, H. JACQUEMIN, M. LEDGER and A. MICHEL, *Online Platforms' Moderation of Illegal Content Online: Law, Practices and Options for Reform*, June 2020, PE 652.718, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL_STU(2020)652718_EN.pdf, 40.
[149] Recital 40 e-Commerce Directive recognises the liability exemption of article 14 as the notice-and-takedown mechanism.
[150] Art. 14.1 e-Commerce Directive.

by the service providers refers to the notice-and-takedown procedure since it exempts them from their responsibility of hosting illegal content if they block or remove the content when becoming aware of its presence.

For the service providers to enjoy this exemption, their intervention must, however, be limited to "*the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored*"[151]. As was explained previously, their intervention must be limited to a "*mere technical, automatic and passive*" conduct.[152]

Applied to the dissemination of online terrorist content by ISIL supporters on Twitter, Telegram or Facebook, these hosting service providers will enjoy an exemption of liability if they remove or disable expeditiously the terrorist content uploaded by ISIL. Worth singling out are the requirements of 'not having knowledge of the illegal content' and 'acting expeditiously', which require a more detailed analysis.

80. Illegal content should be distinguished from harmful content.[153] Whereas illegality of content is defined by both the European and national level[154], the threshold of harmful content is susceptible to differ according to cultural and legal differences and will thus not always be criminalised.[155]

A second distinction lies in the difference between the actual knowledge of the *presence* of the illegal content and of the illegal *character* of the content.[156] According to the Advocate General JÄÄSKINEN in the *L'Oréal* case, the "*mere suspicion or assumption regarding the illegal activity or information*"[157] does not attain the threshold of 'actual knowledge'.[158]

---

[151] Recital 42 e-Commerce Directive.
[152] *Cf. supra* n° 35.
[153] For more information on the difference between illegal and harmful content, see Y. AKDENIZ, "To Block or Not to Block: European Approaches to Content Regulation, and Implications for Freedom of Expression", *Computer Law and Security Review* May 2010, Vol. 26, Issue 3, 260-272.
[154] EUROPEAN COMMISSION, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Tackling illegal content online – Towards an enhanced responsibility of online platforms*, 28 September 2017, COM (2017) 555 final, 4-5 (hereinafter: "Communication from the Commission on Tackling illegal content online – Towards an enhanced responsibility of online platforms").
[155] Y. AKDENIZ, "To Block or Not to Block: European Approaches to Content Regulation, and Implications for Freedom of Expression", *Computer Law and Security Review* May 2010, Vol. 26, Issue 3, 264.
[156] G. J. SVENSØY, *The e-Commerce Directive Article 14: Liability exemptions for hosting third party content*, Master Thesis Law University of Oslo, 2011, https://www.duo.uio.no/bitstream/handle/10852/19450/117618.pdf, 35.
[157] Opinion Advocate General JÄÄSKINEN of 9 December 2010, C-324/09, ECLI:EU:C:2010:757, *L'Oréal SA v. eBay International AG*, §162.
[158] For the difference in understanding of the terms 'actual knowledge' and 'awareness', see F. WILMAN, *The responsibility of online intermediaries for illegal user content in the EU and the US*, Northampton, Edward Elgar Publishing, 2020, 36-39.

Service providers do not have a general monitoring obligation regarding the content their platform offers to the users. Article 15 of the e-Commerce Directive explicitly prohibits the Member States from imposing a general monitoring obligation on service providers for the content they host.[159] Hence, social media platforms do not have an obligation to be aware of illegal content's *presence* on their platform.

The knowledge by service providers of the illegal *character* of online content might prove to be more problematic. According to VERBIEST et al., service providers complain about "*being pressured into the role of an illegitimate judge since they are supposed to assess the unlawfulness of content – sometimes on the basis of a vague private notice – in order to decide whether the information should be removed or access disabled*"[160]. The question arises whether today's society wants to entrust private service providers with the responsibility of assessing the (il)legality of certain content. This responsibility amounts to private law enforcement. The privatisation of law enforcement is not a new phenomenon.[161] However, when private actors are to police a forum where freedom of expression stands central, the private law enforcement can quickly become discretionary.

81. Moreover, service providers must act *expeditiously* when becoming aware of the illegal content's presence on their platform. The reactiveness of a service provider depends on the classification of the content and the context thereof. Child pornography is easily qualified as illegal, whereas establishing the illegality of content with terrorist aspects might prove to be more complicated as the content's context will play a more prominent role. Therefore, the fulfilment of the criterium 'expeditiously' will depend on the context[162], which again opens the door to the discretionary filling of this notion.

82. Consequently, and agreeing with JØRGENSEN and PEDERSEN[163], the notions of 'actual knowledge' and 'expeditiously' make the notice-and-takedown procedure legally uncertain. One way of ensuring that service providers will benefit from the exemption of liability regime is to monitor their platform proactively. The Commission recognised this in its 2018 Communication on online terrorist content. Moreover, it stated that the platform's proactive and voluntary monitoring would not automatically imply the loss of the liability exemption

[159] Art. 15 of the e-Commerce Directive; CJEU (Grand Ch.) 12 July 2011, C-324/09, ECLI:EU:C:2011:474, *L'Oréal SA v. eBay International AG*, §139.
[160] T. VERBIEST et al., *Study on the liability of internet intermediaries – final report,* 2007, https://digital-strategy.ec.europa.eu/en/library/archive-e-commerce-directive-what-happened-and-its-adoption, 37.
[161] E. COCHE, "Privatised enforcement and the right to freedom of expression in a world confronted with terrorism propaganda online", *Internet Policy Review* 2018, Vol. 7, Issue 4, 3.
[162] Communication from the Commission on Tackling illegal content online – Towards an enhanced responsibility of online platforms, 14.
[163] R. F. JØRGENSEN and A. M. PEDERSEN, "Chapter 10 - Online Service Providers as Human Rights Arbiters", in M. TADDEO and L. FLORIDI (eds.), *Law, Governance and Technology Series*, Vol. 31, *The Responsibilities of Online Service Providers*, Switzerland, Springer, 2017, 189.

offered under article 14 of the e-Commerce Directive.[164] However, the proactively and voluntary monitoring of a platform equals a general monitoring of the platform. Obliging providers to have recourse to such monitoring is, as was discussed previously[165], prohibited under article 15 of the e-Commerce Directive. As will be posited hereunder, the European Union has been shifting towards more general monitoring 'incentives'. Hiding behind the qualification of 'incentives', instead of recognising them as 'obligations', which would be a violation of the e-Commerce Directive provisions, is problematic because it, again, creates legal uncertainty.

1.3.1.1.2. The procedure of taking down online terrorist content

83. The notice-and-takedown actions can be broken up into different stages. First, the existence and presence of terrorist content on a social media platform must be signalled to the platform. The procedure of flagging allows for this awareness-raising. Once becoming aware of its presence on the platform, the social media platform will analyse the compatibility of the alleged terrorist content with its Terms and Conditions.

84. ELLERMAN defines the operation of flagging as "*providing a unique Uniform Resource Locator (URL), or a set of unique URLs, relating to suspicious content, for subsequent referral action*"[166]. Any person, EU Member State, third party, or institution can 'flag' to the social media platform content they deem is illegal. Within the Member States, national Internet Referral Units (hereinafter: "IRU"), such as the Belgian i2-IRU, have been set up to flag content deemed illegal.

Since all internet users can flag content, the service providers are often overwhelmed with enormous amounts of data they need to analyse. Therefore, some companies, such as YouTube[167], have decided to grant the quality of 'trusted flagger' to the EU IRU and national IRUs. Because of their "*particular expertise and responsibilities for the purposes of tackling illegal content online*"[168], the EU IRU can upload in batch media profiles or online terrorist videos, tweets, or posts.[169] After this awareness-raising by the EU IRU or national IRUs, the

[164] Communication from the Commission on Tackling illegal content online – Towards an enhanced responsibility of online platforms, 10.
[165] *Cf. supra* n° 80.
[166] J. ELLERMANN, "Terror won't kill the privacy star – tackling terrorism propaganda online in a data protection compliant manner", *ERA Forum* 2016, Vol. 17, Issue 4, 564.
[167] *Ibid.*, 567; B. CHANG, "From Internet Referral Units to international agreements: censorship of the internet by the UK and EU", *Columbia HR Law Review* 2018, Vol. 49, Issue 2, 135.
[168] Art. 4, g) Commission Recommendation on measures to effectively tackle illegal content online.
[169] J. ELLERMANN, "Terror won't kill the privacy star – tackling terrorism propaganda online in a data protection compliant manner", *ERA Forum* 2016, Vol. 17, Issue 4, 567; B. CHANG, "From Internet Referral Units to

service provider assesses whether the alleged illegal content is in breach of its terms and conditions. If so, the service provider takes the illegal content down from its platform.[170]

85. The Terms and Conditions or Terms of Service[171] of a social media platform are the rules the platform's users have to comply with to gain access to the platform. The users accept these Terms and Conditions when they create a profile on these platforms as they then enter into an agreement with the platform. When those Terms and Conditions are not respected, the user is in breach of its 'contractual' obligations towards the platform[172], and the content uploaded by the user can be taken down or made unavailable by the social media platform. Subsequently, the removal of terrorist content online, the blocking of access to the information and the reparation measures for content wrongfully taken down will be discussed.

86. Service providers usually do not assess the uploaded content against their Terms and Conditions before allowing it on their platform. They analyse the compatibility of the content against their Terms and Conditions once they become aware of its presence. The prior control would be too time-consuming. Since Telegram, Facebook and Twitter are platforms used by ISIL, their Terms and Conditions will be analysed hereunder.

The Terms of Service of Telegram require the users to agree to abstain from "*promot*[*ing*] *violence on publicly viewable Telegram channels, bots, etc.*" and "*post*[*ing*] *illegal pornographic content on publicly viewable Telegram channels, bots, etc.*"[173] (sic). Whilst users are prohibited to upload content promoting violence or containing illegal pornographic content, no explicit reference to the prohibition of uploading terrorist content is made.

The Community Standards of Facebook prohibit "*organisations or individuals that proclaim a violent mission or are engaged in violence to have a presence on Facebook*" in order to "*prevent and disrupt real-world harm*"[174]. Organisations and individuals involved in terrorist activities fall under this prohibition.[175] Facebook' Community Standards also provide that the firm will remove content that supports such activities.[176] Furthermore, it details that it does not allow the presence of a non-state actor that: "*engages in, advocates or lends substantial support to purposive and planned acts of violence, which causes or attempts to cause death, injury or*

---

international agreements: censorship of the internet by the UK and EU", *Columbia HR Law Review* 2018, Vol. 49, Issue 2, 135.

[170] A. KUCZERAWY, *Intermediary Liability and Freedom of Expression in the EU: from concepts to safeguards*, Mortsel, Intersentia, 2018, 203.

[171] These notions have the same meaning and will be used intertwiningly.

[172] G. HERMANS, "De toepasselijkheid van algemene voorwaarden bij online contracteren", *HOR* 2018, Issue 128, 78.

[173] TELEGRAM, Terms of Service, https://telegram.org/tos.

[174] FACEBOOK, "Community Standards", https://www.facebook.com/communitystandards/violence_criminal_behavior.

[175] *Ibid.*

[176] *Ibid.*

serious harm to civilians, or any other person not taking direct part in the hostilities in a situation of armed conflict, and/or significant damage to property linked to death, serious injury or serious harm to civilians with the intent to coerce, intimidate and/or influence a civilian population, government or international organisation in order to achieve a political, religious or ideological aim"[177].

The general guidelines and policies of Twitter prohibit the "*threatening with or promotion of terrorism or violent extremism*"[178]. As such, it considers amongst others the following activities as a violation of its terms and conditions: "*engaging in or promoting acts on behalf of a violent organization; recruiting for a violent organization; providing or distributing services (e.g., financial, media/propaganda) to further a violent organization's stated goals; and using the insignia or symbol of violent organizations to promote them or indicate affiliation or support*"[179]. If Twitter finds illegal content on its platform, it will "*immediately and permanently suspend any account*" it considers in violation with its policy.[180] However, an exception is provided for content with an educational, documentary, or artistic purpose. This content will be able to remain on the platform.[181]

Apart from the unquestionably more extensive terms of service of Twitter and Facebook compared to those of Telegram, the Terms of Service of the former platforms are more detailed since they include the prohibition of publishing terrorist content. Telegram's Terms of Service do not include this prohibition. The only reference to 'terrorist' can be found in Telegram's privacy policy: "*If Telegram receives a court order that confirms you're a terror suspect, we may disclose your IP address and phone number to the relevant authorities. So far, this has never happened*"[182]. However, there is no mention of disabling the content. Consequently, Telegram appears to be more appealing for ISIL supporters to share terrorist content than Twitter or Facebook.

87. In some instances, the removal of online terrorist content proves to be impossible. The service provider can, for example, be located in a third country (outside of the EU) that refuses to cooperate and to oblige the service provider to remove the content. Then, access from the European territory to the information can be disabled by public action.[183] Since this mechanism engenders far-reaching consequences, the Directive on combating terrorism requires sufficient

[177] *Ibid.*
[178] TWITTER, "Rules and policies, General guidelines and policies of Twitter", https://help.twitter.com/en/rules-and-policies/violent-groups.
[179] *Ibid.*
[180] *Ibid.*
[181] *Ibid.*
[182] TELEGRAM, "Telegram Privacy Policy – 8.Who Your Personal Data May Be Shared With – 8.3Law Enforcement Authorities", https://telegram.org/privacy.
[183] Art. 21.2 and Recital 22 Directive on combating terrorism.

transparent procedures and adequate safeguards[184] to ensure that the blocking is proportionate and necessary[185] and that the users are informed on why content is being taken down or blocked.[186] According to the Commission's latest report on the Directive's national transposition, Belgium has not included this last notification requirement in its national law.[187]

88. Once content has been taken down, the content's author has two options when considering the takedown to be illegitimate. Either, the author chooses to introduce a counter-notice so that the content can be restored. Wrongfully silenced users can then post the adjudication outcome of the counter-notice on the social media platform.[188] However, this out-of-court settlement has been considered too opaque and potentially infringing on the right to freedom of expression and to an effective judicial remedy.[189] Either, the author decides to introduce a court action to obtain rapid measures to put an end to these infringements pursuant to article 18 of the e-Commerce Directive.[190] Nevertheless, instigating a court action for each wrongful takedown appears to be too burdensome and disproportionate.

The lack of accountability of service providers when wrongfully taking down legitimate content and the absence of judicial oversight before removal or blockade of allegedly illegal content is problematic. The loss of a few wrongfully silenced users will not lead to the loss of public support for the social media platform. Hence this might not appear to be problematic to the service providers. As GAN puts it, accountability is "*vital for effective democracy*"[191].

[184] Art. 21.3 Directive on combating terrorism.
[185] Art. 21.3 Directive on combating terrorism.
[186] Art. 21.3 Directive on combating terrorism.
[187] Art. XII.19 Wetboek 28 February 2013 van economisch recht, *BS* 29 March 2013, 19.975 (hereinafter: "Belgian Code of Economic Law") does not offer this possibility; EUROPEAN COMMISSION, *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*, 30 September 2020, COM (2020) 619 final, 16.
[188] H. Z. GAN, "Corporations: The Regulated or the Regulators - The Role of IT Companies in Tackling Online Hate Speech in the EU", *Columbia Journal of European Law* 2017, Vol. 24, Issue 1, 138.
[189] *Ibid.*, 137; T. QUINTEL and C. ULLRICH, "Self-Regulation of Fundamental Rights? The EU Code of Conduct on Hate Speech, related initiatives and beyond", in B. PETKOVA and T. OJANEN (eds.), *Fundamental Rights Protection Online: The Future Regulation of Intermediaries*, Northampton, Edward Elgar Publishing, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3298719, 8.
[190] Art. 18.1 e-Commerce Directive.
[191] H. Z. GAN, "Corporations: The Regulated or the Regulators - The Role of IT Companies in Tackling Online Hate Speech in the EU", *Columbia Journal of European Law* 2017, Vol. 24, Issue 1, 137.

1.3.1.2. … sharpened by the voluntary Code of conduct on countering illegal hate speech online

89. Due to the increased presence of hate speech and incitement to violence, the European Commission and several IT Companies (Facebook, Microsoft, Twitter and YouTube) decided to draft in 2016 a 'Code of conduct on countering illegal hate speech online'.[192] The Code of Conduct enumerates several rules the IT Companies commit to following. As such, they should have "*clear and effective processes*" to review referrals of alleged illegal speech and clear Community Guidelines that the users have to respect when using their services. Moreover, the IT Companies should review the "*requests against their rules and community guidelines*" and, where necessary, against national law within twenty-four hours from receiving valid notifications. If the content is deemed contrary to the Community Guidelines or national law, then the Companies should "*remove or disable access to such content if necessary*". Last, the Companies should have notice and flagging systems for content that "*promotes incitement to violence and hateful conduct*"[193].

90. The signature and implementation of the Code of Conduct rest on a voluntary basis. Companies cannot be obliged to sign the Code.[194] Nevertheless, the Code does not provide a sanction enforcement mechanism if the signatories do not comply with its provisions.[195] This absence is worrisome in light of the Code's general implementation since it threatens the Code to remain an empty promise. This lacuna is, however, not the only problem with this Code.

91. On a general note, the drafting process of the Code has been criticised due to the lack of transparency regarding the companies involved and the absence of involvement of civil society organisations.[196] The alleged absence of civil society organisations in the discussions seems to be even contrary to article 16.2 of the e-Commerce Directive, which emphasises the

[192] Code of conduct on countering illegal hate speech online of the European Commission and IT Companies, 31 May 2016, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en (hereinafter: "Code of Conduct" or "Code"); Art. 16 e-Commerce Directive provides that the Member States and the Commission should encourage the drafting of Codes of Conduct.
[193] Code of Conduct, 2.
[194] Recital 49 e-Commerce Directive.
[195] J. TROMMEL, *Online jihadi content combat: How serving public interest could ease the privatization of freedom of expression*, Master Thesis Crisis and Security Management (MSc) Leiden University, 2018, https://openaccess.leidenuniv.nl/bitstream/handle/1887/84031/Trommel_CSM_2018.pdf?sequence=1, 36.
[196] A. PORTARU, "Freedom of expression online: The code of conduct on countering illegal hate speech online", *Revista Romana de Drept European* 2017, Vol. 4, 80; M. F. PEREZ, "New documents reveal the truth behind the Hate Speech Code", *EDRi* 7 September 2016, https://edri.org/new-documents-reveal-truth-behind-hate-speech-code; J.-H. JEPPESEN and E. J. LLANSÓ, "Letter to European Commissioner on Code of Conduct for "Illegal" Hate Speech Online", *Center for Democracy and Technology* 3 June 2016, https://cdt.org/insights/letter-to-european-commissioner-on-code-of-conduct-for-illegal-hate-speech-online/.

need to include consumer organisations in the process of drafting Codes of Conduct.[197] Moreover, the Commission allegedly spread the Code of Conduct to the (then) 28 EU Member State only a few days before its adoption, preventing the Member States from thoroughly analysing the Code.[198]

92. More specifically, the Code has been criticised on the necessity for service providers to assess the flagged content first to their Terms of Service, and only *where necessary* to national laws. This requirement entails that social media platforms first assess whether the content can be removed because of its incompatibility with the Terms of Service of the hosting service provider and only at a second stage with the law. The Terms of Service of the social media platform consequently become law for the users of the platform. This assessment implies that these providers will be able to take down content that is contrary to their Terms of Service but not necessarily to the law. Hence, they are in a position to take down content that could be regarded as lawful by the legislator.[199] Consequently, these providers are able to restrict legitimate speech and limit their users' freedom of expression. Furthermore, the Code does not contain explicit safeguards for the users' fundamental rights.[200]

93. The requirement for social media platforms to review and remove, or block if necessary, the referred and alleged illegal content within twenty-four hours seems to be a sufficient timeframe for those platforms to react to referrals. This requirement does not appear to be excessive.

94. The voluntary Code of Conduct was a laudable effort to sharpen and update the notice-and-takedown mechanism. However, the absence of sanction enforcement, transparency and involvement of civil society organisations and the potential restriction of legitimate speech indicate that this Code was a mere reputational effort, empty of genuine engagement.

---

[197] Art. 16.2 e-Commerce Directive.

[198] A. PORTARU, "Freedom of expression online: The code of conduct on countering illegal hate speech online", *Revista Romana de Drept European* 2017, Vol. 4, 80; M. F. PEREZ, "New documents reveal the truth behind the Hate Speech Code", *EDRi* 7 September 2016, https://edri.org/new-documents-reveal-truth-behind-hate-speech-code.

[199] A. PORTARU, "Freedom of expression online: The code of conduct on countering illegal hate speech online", *Revista Romana de Drept European* 2017, Vol. 4, 85.

[200] *Ibid.*, 85; M. F. PEREZ, "New documents reveal the truth behind the Hate Speech Code", *EDRi* 7 September 2016, https://edri.org/new-documents-reveal-truth-behind-hate-speech-code; T. QUINTEL and C. ULLRICH, "Self-Regulation of Fundamental Rights? The EU Code of Conduct on Hate Speech, related initiatives and beyond", in B. PETKOVA and T. OJANEN (eds.), *Fundamental Rights Protection Online: The Future Regulation of Intermediaries*, Northampton, Edward Elgar Publishing, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3298719, 6.

1.3.1.3. … blurred again by the legally binding Regulation on addressing the dissemination of terrorist content online

95. Building on the Code of Conduct's principles, the European Commission published in September 2017 a Communication containing numerous guidelines and principles on how service providers had to prevent, detect and remove illegal online content, such as violence, hatred and terrorist propaganda.[201] Following this Communication, the Commission issued a Recommendation in March 2018 in which it set out several non-binding operational measures.[202] These measures include, amongst others, a general rule according to which service providers have to take down illegal terrorist content within one hour after referral.[203] According to the Commission, this one-hour rule finds its explanation in the observation that terrorist content online is at its most harmful stage during the first hour of publication.[204] The Recommendation also provided guidance on how the flagging operation should be carried out and processed. A few months later, in September 2018, the European Commission published its Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online.[205] This Regulation likewise treats the referral regime. As was mentioned before, the European Parliament agreed on the Council's position on the 28th of April 2021.[206]

96. Whilst recognising that online service providers, such as social media platforms that allow their users to watch videos uploaded by other users[207], have "*particular societal responsibilities to protect their services from misuse by terrorists and to help address terrorist content disseminated through their services online*"[208], this new legislative instrument also acknowledges the importance of granting legal certainty to the service providers.[209] The European drafters also emphasise the importance of the freedom of expression, the freedom to receive and impart information and the freedom and pluralism of the media.[210]

[201] Communication from the Commission on Tackling illegal content online – Towards an enhanced responsibility of online platforms.
[202] Recommendations are not legally binding; Art. 288 Treaty on the Functioning of the European Union, *OJ L* 26 October 2007, n° 326, 1.
[203] Art. 35 Commission Recommendation on measures to effectively tackle illegal content online.
[204] Recital 35 Commission Recommendation on measures to effectively tackle illegal content online.
[205] Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, 12 September 2018, COM (2018) 640 final – 2018/0331 (COD).
[206] *Cf. supra* n° 29.
[207] Recital 14 Regulation on addressing the dissemination of terrorist content online.
[208] Recital 5 Regulation on addressing the dissemination of terrorist content online.
[209] Recital 1 Regulation on addressing the dissemination of terrorist content online.
[210] Recital 1 Regulation on addressing the dissemination of terrorist content online.

97. The voluntary Code of Conduct introduced a twenty-four hour rule within which the service providers are to assess referred content. This timeframe was consequently reduced to the non-legally binding one-hour rule in the Commission's Recommendation of 2018. The Regulation's drafters decided to keep the requirement to respond *expeditiously*[211] to a referral of illegal content and refrain from making the one-hour removal rule mandatory on referrals.[212] However, the Regulation obliges hosting service providers exposed to terrorist content to implement specific measures to safeguard their platform against the dissemination of terrorist content.[213] The choice of the type of measures the social media platforms want to implement is left to those platforms. One of the measures is "*an easily accessible and user-friendly mechanism for users to report or flag to the hosting service provider alleged terrorist content*"[214], being the notice (through flagging)-and-takedown mechanism.

98. The Regulation also details a complaint mechanism according to which a person whose content was allegedly taken down wrongfully can submit a complaint with the service provider to request the reinstatement or access to the information.[215] The service provider has to assess the complaint *expeditiously* and provide the user with the outcome of the complaint within two weeks.[216] A refusal to reinstate the content or grant access has to be accompanied by reasons for the decision.[217] The user has the right to instigate a court case to challenge the platform's decision, even if the content has been reinstated or the access thereto regained.[218]

99. The new Regulation incentivises service providers to notify the content provider of the content's removal.[219] However, if notifying the content provider of the removal would jeopardise public security, for example, because the content provider would quickly re-upload the same information, this obligation disappears, and the competent authority can decide to refrain from notifying the content provider.[220] Since this measure constitutes a severe infringement on one's right to freedom of expression, the Regulation also contains a possibility for the content provider to contest the service provider's decision to remove the content.[221]

This obligation is a laudable safeguard given to the users of the platform. However, as was discussed previously[222], Belgium has not transposed the notification requirement of the

[211] Art. 5.2, 2nd indent, a) Regulation on addressing the dissemination of terrorist content online.
[212] Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, 12 September 2018, COM (2018) 640 final – 2018/0331 (COD), 5.
[213] Art. 5.2, 1st indent Regulation on addressing the dissemination of terrorist content online.
[214] Art. 5.2, 2nd indent, b) Regulation on addressing the dissemination of terrorist content online.
[215] Art. 10.1 Regulation on addressing the dissemination of terrorist content online.
[216] Art. 10.2, 1st indent Regulation on addressing the dissemination of terrorist content online.
[217] Art. 10.2, 2nd indent Regulation on addressing the dissemination of terrorist content online.
[218] Art. 10.2, 3rd indent Regulation on addressing the dissemination of terrorist content online.
[219] Art. 11.1 Regulation on addressing the dissemination of terrorist content online.
[220] Art. 11.3 Regulation on addressing the dissemination of terrorist content online.
[221] Art. 5.1 Regulation on addressing the dissemination of terrorist content online.
[222] *Cf. supra* n° 87.

Directive on combating terrorism. Even though this *Directive*'s nature is different from the *Regulation*, it is questionable whether Belgium will be able (and willing) to comply with this requirement.

100. The Regulation consequently does not add much to the notice-and-takedown regime. It is doubtful whether this instrument will attain its objective of providing more legal certainty to the social media platforms and their users, given that it simply rephrased the existing mechanism. Moreover, it is questionable whether Belgian will comply with the notification requirement.

1.3.1.4. … restated by the Digital Services Act

101. Parallel to the negotiations of the Regulation on addressing the dissemination of terrorist content online, the European penholders introduced a Proposal for a Regulation on a Single Market for Digital Services[223], otherwise known as the Digital Services Act, and a Proposal for a Regulation on contestable and fair markets in the digital sector[224], also known as the Digital Markets Act. Together, these two instruments form the Digital Services Act Package. The Digital Services Act focuses, amongst others, on the protection granted to the platform's users[225] and the increased legal certainty offered to the online service providers.[226] By "*ensuring contestable and fair markets in the digital sector*"[227], the Digital Markets Act aims to redress the existing imbalance between major online platforms (known as the 'gatekeepers') and smaller ones.

102. The Digital Services Act is meant to replace a number of provisions of the e-Commerce Directive. More specifically, the Act would delete articles 12 to 15 of the e-Commerce Directive that constitute the legal basis for the exemption of liability regime of intermediary

[223] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15 December 2020, COM (2020) 825 final - 2020/0361 (COD) (hereinafter: "Proposal for a Digital Services Act"); Even though this instrument is called in abbreviated form the Digital Services Act, the instrument is a Recommendation. Due to the limited scope of this dissertation, the Digital Services Act will only briefly be analysed.
[224] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15 December 2020, COM (2020) 842 final, 2020/0374 (COD) (hereinafter: "Proposal for a Digital Markets Act").
[225] Art. 1.2, b) Proposal for a Digital Services Act.
[226] Art. 1.1, a) Proposal for a Digital Services Act.
[227] Art. 1.1 Proposal for a Digital Markets Act. This instrument does not lie in the scope of this dissertation. Hence, it will not be included in the analysis.

service providers and the prohibition to impose a general monitoring obligation on service providers[228] to replace them with the similar articles 3 to 10.[229]

Hence, the notice-and-takedown mechanism will receive a new legal basis if this Act is adopted.

103. Moreover, this Digital Services Act would introduce stricter rules for the so-called 'Very Large Online Platforms (VLOPs)', which are platforms that reach more than 10% of the 450 million consumers in Europe.[230] Facebook will probably be recognised as a VLOP.[231] This specific category was created out of the conviction that those platforms pose a greater risk to the dissemination of illegal content.[232]

104. The Digital Services Act forms no obstacle to the application of the Regulation on addressing the dissemination of terrorist content online since the Act specifically provides that it complements the existing, more specific, legislation. It consequently recognises the Regulation as *lex specialis*, law which takes precedence on the *lex generalis*, *in casu* being the Digital Services Act.[233] The Act also further builds on the Commission's Recommendation on illegal content online.[234]

Since the Digital Services Act gives precedence to the Regulation on addressing the dissemination of terrorist content online, the latter will serve as the basis for the further analysis of this dissertation.

1.3.1.5. … made partly possible by the intervention of the European Union Internet Referral Unit

105. ISIL's growing online presence confirms that terrorist groups have a broad understanding of social media and have a profound knowledge of the value it brings to their propaganda, recruitment campaigns and glorification of acts. As the presence of online terrorist

[228] *Cf. supra* 1.3.1.1.1. The regime of liability exemption for hosting providers (n° 78-82).
[229] Art. 71.1 Proposal for a Digital Services Act.
[230] Recital 54 Proposal for a Digital Services Act.
[231] Considering that Facebook had, according to Statista, 419 million users in Europe during the last quarter of 2020, Facebook will probably be recognized a VLOP; H. TANKOVSKA, "Facebook's monthly active users (MAU) in Europe from 4th quarter 2012 to 4th quarter 2020", *Statista* 2 February 2021, https://www.statista.com/statistics/745400/facebook-europe-mau-by-quarter.
[232] Recital 53 Proposal for a Digital Services Act.
[233] Art. 1.5, d) and Recital 9 Proposal for a Digital Services Act.
[234] Proposal for a Digital Services Act, 5.

material has only been expanding over the last couple of years, the EU understood the necessity and urgency to create a new specialised department.

106. Established within Europol[235] by the Justice and Home Affairs Council of the EU on the 1st of July 2015 and modelled on the English Counter-Terrorism IRU[236], the European Union Internet Referral Unit[237] is meant to operate as a joint European response to this increased overall presence of terrorist groups on the internet. To fulfil its tasks, the EU IRU works in close collaboration with the EU Internet Forum[238], which was created in 2015 by the European Commission to put a halt to this further abuse by international terrorist groups of the internet. The EU IRU and the EU Internet Forum cooperate to reduce the accessibility to online terrorist content[239] by incentivising the online industry to self-regulation when it comes to online terrorist content.[240]

107. The experts of the EU IRU are, amongst others, trusted to "*support the competent EU authorities by providing strategic and operational analysis*", "*flag terrorist and violent extremist online content and share it with relevant partners*" and "*swiftly carry out and support the referral process, in close cooperation with the industry*"[241] (emphasis added). One of the

[235] Europol is the European Union Agency for Law Enforcement Cooperation established to support and strengthen action taken by national authorities or cooperate with the Member States to prevent and combat, amongst others, terrorism (art. 3.1 Regulation 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, *OJ L* 24 May 2016, n° 135, 53 (hereinafter: "Europol Regulation")).

[236] DIRECTORATE GENERAL FOR INTERNAL POLICIES, POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS, *Countering Terrorist Narratives*, 2017, PE 596.829, https://openaccess.leidenuniv.nl/bitstream/handle/1887/62312/Reed-Ingram-Whittaker-Narratives.pdf?sequence=1.

[237] The EU IRU was set up within Europol's department European Counter Terrorism Centre. Europol is entitled to set up bodies and centres invested with more specific tasks (Art. 23.1 Europol Regulation). This Centre was established in 2016 and is situated in The Hague; EUROPOL, "EU Internet Referral Unit - EU IRU", https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru; EUROPOL, "European Counter Terrorism Centre - ECTC", https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc.

[238] EUROPOL, *European Union Terrorism Situation and Trend Report 2020*, 23 June 2020, TE-SAT 2020, https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020, 92.

[239] The reduction of the accessibility to online terrorist content and the empowerment of civil society partners to increase the volume of effective alternative narratives online are the two objectives for which the EU Internet Forum has been created. The second objective lies too far from the scope of this work to be discussed; EUROPEAN COMMISSION, "EU Internet Forum: progress on removal of terrorist content online" (Press release), 10 March 2017, http://europa.eu/rapid/press-release_IP-17-544_en.htm.

[240] DIRECTORATE GENERAL FOR INTERNAL POLICIES, POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS, *Countering Terrorist Narratives*, 2017, PE 596.829, https://openaccess.leidenuniv.nl/bitstream/handle/1887/62312/Reed-Ingram-Whittaker-Narratives.pdf?Sequence=1; B. CHANG, "From Internet Referral Units to international agreements: censorship of the internet by the UK and EU", *Columbia HR Law Review* 2018, Vol. 49, Issue 2, 138-139.

[241] EUROPOL, "EU Internet Referral Unit – EU IRU", https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru.

EU IRU's core tasks is to flag online content that reaches the threshold of 'terrorism' and 'violent extremism'. Because this content can be the subject of ongoing investigations, the EU IRU functions with 24/7 available national contact points to assess whether the content is being used in ongoing investigations. If this is the case, the EU IRU will refrain from referring that content to the hosting service providers.[242]

108. The flagging and referring operations by the EU IRU have, however, been criticised for their non-transparency.[243] Even though IRUs publish reports on the number of online terrorist content that has been the object of referral to service providers[244], the numbers do not accurately lay out the type of content taken down since these numbers are often cumulative statistics.[245]

109. Moreover, this cooperation between the EU IRU and hosting service providers is allegedly voluntary since the former has no enforceable power over the latter.[246] The service providers decide themselves whether the referred content breaches their Terms and Conditions. The voluntary character of the removal of content is, however, questionable.[247]

1.3.1.6. Conclusion

110. When social media platforms remove terrorist content, upon becoming aware of its presence on their platform through the practice of 'flagging' and the subsequent analysis of the compatibility of the content against their Terms and Conditions, they can enjoy an exemption of liability for having provided a forum for this illegal content. This notice-and-takedown action implicitly shifts the responsibility for disabling terrorist content towards the social media

[242] J. ELLERMANN, "Terror won't kill the privacy star – tackling terrorism propaganda online in a data protection compliant manner", *ERA Forum* 2016, Vol. 17, Issue 4, 571.
[243] F. WARISLOHNER, "Europol: Non-transparent cooperation with IT companies", *EDRi* 18 May 2016, https://edri.org/europol-non-transparent-cooperation-with-it-companies/; X, "Understanding the Human Rights Risks Associated with Internet Referral Units", *Global Network Initiative* 25 February 2019, https://globalnetworkinitiative.org/human-rights-risks-irus-eu/.
[244] For the latest report on the EU IRU, see https://www.europol.europa.eu/publications-documents/eu-iru-transparency-report-2019.
[245] X, "Understanding the Human Rights Risks Associated with Internet Referral Units", *Global Network Initiative* 25 February 2019, https://globalnetworkinitiative.org/human-rights-risks-irus-eu/.
[246] J. ELLERMANN, "Terror won't kill the privacy star – tackling terrorism propaganda online in a data protection compliant manner", *ERA Forum* 2016, Vol. 17, Issue 4, 567.
[247] F. WARISLOHNER, "Europol: Non-transparent cooperation with IT companies", *EDRi* 18 May 2016, https://edri.org/europol-non-transparent-cooperation-with-it-companies/; X, "Understanding the Human Rights Risks Associated with Internet Referral Units", *Global Network Initiative* 25 February 2019, https://globalnetworkinitiative.org/human-rights-risks-irus-eu/; *Cf. infra* 2. The cooperation with social media platforms (n° 126-148).

platforms. This broader responsibility of the service providers is problematic since the interests of those private actors are very different from the interests of public authorities. For private authorities, profit is often the primary goal, whereas public authorities, such as the European Union bodies (for example, the EU IRU), act in their citizens' interest.

1.3.2. The removal orders…

1.3.2.1. … provided in the e-Commerce Directive

111. Pursuant to article 14.3 of the e-Commerce Directive, the liability exemption of a host service provider does not hinder the possibility for court authorities and administrative institutions to order the removal or blocking of illegal online content.[248] Furthermore, article 18.1 of the e-Commerce Directive allows for a court to rapidly adopt measures "*designed to terminate any alleged infringement and to prevent any further impairment of the interests involved*"[249].

112. In the *L'Oréal case*, the Court of Justice of the European Union had the opportunity of ruling on the question of disabling a user's account. As such, the Court ruled that "*the measures required of the online service provider cannot consist in an active monitoring of all the data of each of its customers*"[250]. The Court did recognise that if the service provider would not "*suspend the perpetrator of the infringement of intellectual property rights in order to prevent further infringements of that kind*", the service provider could be ordered to do so by the Courts.[251] Hence, injunctions to service providers aim to end an infringement and prevent similar infringement in the future.[252]

1.3.2.2. … developed in the Regulation on addressing the dissemination of terrorist content online

113. The Regulation on addressing the dissemination of terrorist content also brought some changes to the regime of removal orders. These changes will doubtlessly effectively combat

[248] Art. 14.3 and Recital 45 e-Commerce Directive; CJEU (7th Ch.) 11 September 2014, C-19/13, ECLI:EU:C:2014:2209, *Sotiris Papasavvas v. O Fileleftheros Dimosia Etairia Ltd*, §57.
[249] Art. 18.1 e-Commerce Directive.
[250] CJEU (Grand Ch.) 12 July 2011, C-324/09, ECLI:EU:C:2011:474, *L'Oréal SA v. eBay International AG*, §139.
[251] CJEU (Grand Ch.) 12 July 2011, C-324/09, ECLI:EU:C:2011:474, *L'Oréal SA v. eBay International AG*, §141.
[252] CJEU (Grand Ch.) 12 July 2011, C-324/09, ECLI:EU:C:2011:474, *L'Oréal SA v. eBay International AG*, §144.

and reduce the online presence of terrorist content. The legitimacy and necessity of adopting this Regulation are hence without doubt. The Regulation contains, however, some seriously problematic provisions worth addressing. As such, the regime of cross-border removal orders raises some fundamental questions about freedom of expression and their extraterritorial scope (1.3.2.2.1.). Moreover, the one-hour rule (1.3.2.2.2.) within which service providers must take down content seems insufficient and incentivises those service providers to have recourse to automated means (1.3.2.2.3.). For the notification regime of the content's removal to the content's provider, the same remarks made for the notice-and-takedown regime in the context of the Regulation on addressing the dissemination of terrorist content online can be raised for the removal orders.[253]

1.3.2.2.1. The cross-border removal orders: a threat to freedom of expression?

114. The competence to issue removal orders is enshrined in article 3 of the Regulation:

> "*The competent authority of each Member State shall have the power to issue a removal order requiring hosting service providers to remove terrorist content or to disable access to terrorist content in all Member States.*"[254] (emphasis added)

The Member States have to designate the competent authority that can be administrative, law enforcement or judicial.[255] This authority is competent for both issuing the orders and hearing complaints from content providers whose content was allegedly wrongfully taken down.[256]

115. A substantial novelty this Regulation introduces is the competence of issuing cross-border removal orders. When the service provider is located in a different Member State than the authority that sends the injunction, the injunction has to fulfil complementary conditions pursuant to article 4 of the Regulation. As such, the hosting provider has to comply with the injunction and ensure measures are taken that allow to reinstate or re-access the removed content.[257]

The cross-border dimension of these orders is problematic since all Member States do not share the same level of protection of the right to freedom of expression. Consequently, the reaction by the social media platforms to these orders is not voluntary, and they will be bound to comply with orders that restrict the freedom of expression of their users whilst potentially considering

[253] *Cf. supra* n° 99.
[254] Art. 3.1 Regulation on addressing the dissemination of terrorist content online.
[255] Recital 35 Regulation on addressing the dissemination of terrorist content online.
[256] Art. 9.2 Regulation on addressing the dissemination of terrorist content online.
[257] Art. 4.2 Regulation on addressing the dissemination of terrorist content online.

the content legitimate. These cross-border removal orders will endanger the fundamental rights of the platform's users.

1.3.2.2.2. The one-hour rule to remove content: is the swift removal of content reconcilable with the users' fundamental rights?

116. The new Regulation introduces a binding one-hour rule, according to which competent authorities are allowed to issue removal orders that are to be complied with within the hour.[258] This possibility, the Regulation specifies, is to happen only in emergency cases where a more extended timeframe would cause serious harm, "*such as in a situation of an imminent threat to life or the physical integrity of a person or events depicting ongoing harm to life or physical integrity*"[259]. The Regulation further elaborates that if the service provider would be unable, due to force majeure or *de facto* impossibility, be it technical or operational, to comply with the order, the service provider will have to inform the authorities as soon as possible and comply with the order once the obstacle to its compliance is no longer present.[260] It is questionable whether the difference in time zones will constitute a *de facto* operational impossibility. Complying with this requirement compels the service providers to offer a 24/7 availability to satisfy such an order. Either this requires an enormous investment in personnel, either the companies decide to have recourse to automated tools. These automated tools can immediately delete certain content upon receiving an order or proactively find and delete content with terrorist elements. The unsupervised automatic removals are, however, highly worrisome considering the fundamental rights of the platform's users.

117. Having recourse to automated tools can help social media platforms find online terrorist content faster, easier, and more efficiently. However, the new Regulation provides that there can exist no obligation for such platforms to have recourse to such automated tools.[261] Nevertheless, requiring to remove content within one hour and recognising that there can be no obligation for such platforms to use automated tools seems contradictory. Implicitly, service providers will have to turn towards automated means to comply with their obligation to respond to the orders within one hour. This ambiguity was also recognised by, amongst others, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism[262] and the European Data Protection

[258] Art. 3.3 Regulation on addressing the dissemination of terrorist content online.
[259] Recital 17 Regulation on addressing the dissemination of terrorist content online.
[260] Art. 3.7 and Recital 17 Regulation on addressing the dissemination of terrorist content online.
[261] Art. 5.8, 2nd indent and Recital 25 Regulation on addressing the dissemination of terrorist content online.
[262] SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION AND THE SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF HUMAN RIGHTS AND

Supervisor[263]. The one-hour rule might incentivise service providers to create programmes that automatically ban certain content.

Furthermore, automated tools take away the human control behind the takedown and constitute a grave danger to the right to freedom of expression. As will be discussed hereunder[264], automatic tools do not understand the context of certain online content as well as humans do. Hence, these tools are more inclined to qualify certain content as illegal content, opening the path towards censorship.

118. If service providers systematically fail to comply with removal orders, penalties of "*up to 4% of the platform's global turnover of the preceding business year*"[265] can be imposed on them. Consequently, a social media provider that does not have the human resources to comply with such an order immediately will be fined heavily. The same is true for a social media platform that refuses to comply with cross-border removal orders that persistently target for political reasons a user's legitimate use of their right to freedom of expression. This scenario would not exist if all the Member States of the European Union shared the same protection of this right. This, however, is far from being true.

1.3.2.2.3. Conclusion

119. The adoption of the Regulation on addressing the dissemination of terrorist content online was necessary to transcribe the voluntary rules provided in the Code of Conduct and the Commission's Recommendation in a binding instrument. Even though it is unquestionably necessary to tackle ISIL's presence online, it is debatable whether this instrument will attain this aim without excessively infringing on the European citizens' rights. The Regulation appears particularly worrisome in light of the fundamental rights of the users of the social media platforms. The cross-border removal orders are a threat to the freedom of expression of these users since not all Member States share the same level of protection of this right. Moreover, the Regulation implicitly encourages the service providers to have recourse to such automated tools. The recourse to automated tools opens the path towards censorship since these tools do not understand context and subtleties. Consequently, they will needlessly take down

FUNDAMENTAL FREEDOMS WHILE COUNTERING TERRORISM, *Recommendations on the new draft 'Regulation on preventing the dissemination of Terrorism Content Online'*, 3 November 2020, https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=25661.

[263] EUROPEAN DATA PROTECTION SUPERVISOR, Formal comments on the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, 12 February 2019, https://edps.europa.eu/sites/edp/files/publication/2018-02-13_edps_formal_comments_online_terrorism_regulation_en.pdf, 5.

[264] *Cf infra* n° 141.

[265] Art. 18.3 Regulation on addressing the dissemination of terrorist content online.

legitimate speech. Last, it is questionable whether Belgium will be able and willing to implement the notification regime of the person whose content has been removed since it has not transposed the similar requirement provided in the Directive on combating terrorism. Therefore, it is debatable whether the Regulation attains its objective of providing more legal certainty to the private service providers and ensuring the freedom of expression, the freedom to receive and impart information and the freedom and pluralism of the media.

1.4. Reactive measures taken at the Belgian level

120. At the Belgian level, referral (1.4.1.) and blocking measures (1.4.2.) are provided in the law.

1.4.1. The referral measures

121. The notice-and-takedown regime of article 14 of the e-Commerce Directive was transposed into Belgian law by article XII.19 of the Code of Economic Law.[266] This Belgian provision exempts service providers from any liability of hosting illicit content whenever they do not hold knowledge of hosting such information or immediately delete or block access to the information as soon as becoming aware of hosting such content.[267] Moreover, the Belgian law provides that the service providers do not have an obligation to overlook the information they hold or transmit, nor do they have an obligation of actively searching illegal content.[268] This absence of active intervention, which is the transposition of article 15 of the e-Commerce Directive, ends whenever these providers obtain knowledge, such as through flagging, of illicit content on their platforms. Then, they should as soon as possible inform the Belgian prosecutor.

The Belgian judicial authorities should also be notified whenever there is a Belgian interest at stake concerning certain terrorist content online, such as a public provocation to commit a terrorist act on Belgian soil. Then, the national Internet Referral Unit, the i2-IRU, set up in January 2016, will report the content to the competent judicial authority, which can then

[266] Art. XII.19 Belgian Code of Economic Law.
[267] Art. XII.19, §1 Belgian Code of Economic Law.
[268] Art. XII.20 Belgian Code of Economic Law.

instigate an investigation.[269] This national IRU operates both independently and in close collaboration with its European counterpart, the EU IRU.[270]

1.4.2. The blocking measures

122. The Belgian Code of Criminal Procedure also provides for a regime of blocking access to online content.

A first possibility lies in the Public Prosecutor's competence to order the taking of technical measures to make information that is the object or consequence of a crime and contrary to public order unavailable or delete the information after obtaining a copy of it.[271]

A second possibility for the Public Prosecutor in the context of the investigation and only in case of urgency is to order that certain online terrorist content that incites the perpetration of a terrorist offence is made unavailable. This order must be confirmed as soon as possible in writing.[272]

The investigative judge can, in the context of an inquiry, also order that those measures be taken.[273]

1.5. Conclusion

123. Over the years, the notice-and-takedown regime has developed into a mechanism of combatting online terrorist content. Initially adopted to regulate European electronic commerce, this regime has grown into a mechanism to hold social media providers accountable for terrorist content uploaded on their platforms. The exemption of liability that stems from this regime has also been developing. The legal frameworks that surround this regime have, however, remained a source of vagueness and ambiguity. Social media providers have a growing responsibility for the content stored on their platforms, which seems legitimate

[269] Email with Commissioner A. LUYPAERT, Commissioner (Head of Unit) DJSOC / Internet Recherche - I2-IRU, 29 October 2020.
[270] T. CARLIER (Federal Judicial Police Belgium – Internet investigations, Internet Referral Unit), "How to tackle internet for fighter recruitment process – Part 1: Situation in Belgium", https://www.inach.net/wp-content/uploads/7.Carlier-How-to-tackle-Internet-use-for-fighter-recruitment-process.ppt.pdf.
[271] Art. 39*bis*, §6, 4th indent Belgian Code of Criminal Procedure.
[272] Art. 39*bis*, §6, 6th indent Belgian Code of Criminal Procedure.
[273] Art. 89 Belgian Code of Criminal Procedure.

considering their role in the public debate, but they also require more certainty regarding their legal obligations.

124. Moreover, the possibility to receive cross-border removal orders and the recent reduction of the timeframe within which service providers have to respond to such orders disproportionately burdens them, threatens the platform's users' freedom of expression and incentivises the platforms to use automatic mechanisms, which is prohibited under the e-Commerce Directive.

125. Often portrayed as a 'cyber-attack', the removal of online terrorist content by Europol and the Member States, such as was the case during the action days of November 2019 on ISIL's news channel Amaq, is legally not qualified as such. These were referrals of content to Telegram that took the content down. Hence, these actions were part of the notice-and-takedown regime and cannot be considered cyber-attacks. This mechanism was also confirmed by Commissioner LUYPAERT of the DJSOC/Internet Recherche of the Belgian i2-IRU.[274]

[274] Email with Commissioner A. LUYPAERT, Commissioner (Head of Unit) DJSOC / Internet Recherche - i2-IRU, 29 October 2020.

2. The cooperation with social media platforms

126. The Internet Referral Units, both at the European and Belgian level, cannot achieve much without the private service providers who have the final decisional power on whether to take down the alleged terrorist content. When encountering online terrorist content which it deems contrary to the Terms of Service of the hosting service provider, the EU IRU notifies the provider about this content. Then, the provider has the choice to either remove or leave the content online. Hence, the service provider, and not the EU IRU, has the final decisional power of taking down the content. The extensive power that lies in the service provider's hands can be contrary to their other interests. Furthermore, it can also endanger the interests of the platform's users and the state (2.1.). Moreover, service providers are increasingly incentivised to use artificial intelligence to ensure compliance with their legal obligations. This recourse brings along both positive and negative consequences (2.2.).

2.1. Entrusting private service providers with the task of tackling online terrorist content is a curse for the service providers, the users of the platform and the state

127. Private social media platforms are entrusted today to limit the presence of terrorist content on the online scene. However, the task and responsibility of protecting citizens against any terrorist threat are imposed by several international legal instruments on the state.[275] This shift in responsibility is an effortless way for the state to avoid fulfilling its legal obligations, but it endangers some of the interests of the actors concerned. The privatisation of policing the platform is not entirely a positive shift. In what follows, a non-exhaustive overview of the different interests of the private service providers (2.1.1.), the users of the platform (2.1.2.) and the state (2.1.3.) will be given and discussed.

2.1.1. The interests of the private service providers

128. Service providers enjoy the right to conduct a business and have a legitimate business interest, according to article 16 of the EU Charter of Fundamental Rights. Social media platforms are private businesses that operate on profit. This profit can sometimes hamper the fight against ISIL's presence online.

[275] *Cf. supra* 1.1 The notion of terrorism in general (n° 19-30).

129. To remain financially stable and increase profits, social media providers aim to attract as many users as possible who actively engage on their platform. Hence, taking down content in line with their legal obligation of cooperation might lead to a decrease in user numbers since the users whose content has wrongfully or legitimately been taken down might migrate to other platforms.

130. Increasing the active engagement of the users on the platform is partly based on matching these users with content they find interesting. This content can be uploaded by other users, who are sometimes willing to pay to appear predominantly on the user's newsfeed to increase their visibility.[276] Consequently, the business interest of the social media platforms lies in finding content that interests the users and stimulates them to view similar content.

To use an example: A Dispatches investigation of 2018 revealed a disparity between the internal guidelines of Facebook regarding the moderation of violent content and Facebook's public policy. Facebook's online content moderators were often told that certain violent content (such as punching and stamping a toddler or two girls fighting) did not amount to the violence threshold and was to be kept online. These posts attracted a lot of engagement, which was financially interesting for Facebook. According to one of Mark Zuckerberg's mentors, violent content engages more activity and is part of Facebook's business model since it increases advertisement.[277] Not long after these revelations, Facebooks Terms of Service were adapted.[278]

ISIL supporters often spread information that contains violence. Thus, there is an economic interest for the online social platforms, because of their data-driven business model[279], to allow the spreading of this violent content.[280]

However, this economic interest conflicts with the public role they received of minimising the terrorist content users view.[281] Since service providers have an incentive to avoid crimes and

[276] N. ELKIN-KOREN, "Contesting algorithms: Restoring the public interest in content filtering by artificial intelligence", *Big data & society* July 2020, Vol. 7, Issue 2, 5.
[277] X, "Dispatches investigation reveals how Facebook moderates content", *Channel 4* 17 July 2018, https://www.channel4.com/press/news/dispatches-investigation-reveals-how-facebook-moderates-content; X, "Facebook moderators 'keep child abuse online'", *BBC* 17 July 2018, https://www.bbc.com/news/technology-44859407.
[278] Z. REEVE, "Human Assessment and Crowdsourced Flagging", in B. GANESH and J. BRIGHT (VoxPol) (eds.), *Extreme digital speech contexts, responses and solutions*, 2019 https://www.voxpol.eu/download/vox-pol_publication/DCUJ770-VOX-Extreme-Digital-Speech.pdf#page=56, 76.
[279] E. COCHE, "Privatised enforcement and the right to freedom of expression in a world confronted with terrorism propaganda online", *Internet Policy Review* 2018, Vol. 7, Issue 4, 2.
[280] S. ARAL, "How Lies Spread Online", *N.Y. Times* 8 March 2018, https://www.nytimes.com/2018/03/08/opinion/sunday/truth- lies-spread-online.html.
[281] N. ELKIN-KOREN, "Contesting algorithms: Restoring the public interest in content filtering by artificial intelligence", *Big data & society* July 2020, Vol. 7, Issue 2, 5.

breaches of the law on their platform to prevent litigation and court cases, they will prioritise their legal obligations.[282]

131. Nevertheless, service providers appear not to be shielded from lawsuits. In 2016, Twitter, Google and Facebook were sued in the USA by Mr Gonzalez, father of a victim of the 2015 Paris attacks claimed by ISIL. Mr Gonzalez alleged that Google was co-responsible for his daughter's death since it had offered a platform where ISIL could spread terrorist content. Even though Mr Gonzalez lost against Google before the Court of Appeals of the Northern District of California, the possibility of being sued for being responsible for terrorist content uploaded by a user of the platform is problematic.[283]

132. Apart from avoiding litigation and court cases, reputation also constitutes a significant incentive to comply with the law. According to AMMAR, to avoid negative criticism, "*social media and intermediaries have an economic incentive to voluntarily censor only material that attracts 'universal' condemnation, as opposed to removing all content related to hate speech*"[284]. Since terrorism attracts 'universal condemnation', hosting service providers have an incentive not to be linked to illegal or terrorist activities. The negative connotation that could result from allowing terrorist content to appear on their platforms could be detrimental to their reputation.[285]

133. Lastly, the obligations to which the service providers have to comply, such as those emanating from article 14 of the e-Commerce Directive (exemption of liability for service providers) or the new Regulation on addressing the dissemination of terrorist content online, seem insufficiently clear and precise. More specifically, the obligation for these providers to weigh the referred presumed 'terrorist' content against their Terms and Conditions seems to be opaque.

Rewarding service providers for quickly taking down illegal content by exempting them from any liability obliges them to make a strenuous balancing exercise.[286] On the one hand, service providers either have the choice to look into every referral individually, taking thus more time

[282] Communication from the Commission on Tackling illegal content online – Towards an enhanced responsibility of online platforms, 6.
[283] Court of Appeals (USA), Northern District of California (9th Circuit) 5 May 2019, n° 18-16700, *Reynaldo Gonzalez v. Google LLC.*
[284] J. AMMAR, "Cyber Gremlin: social networking, machine learning and the global war on Al-Qaida and IS-inspired terrorism", *International Journal of Law and Information Technology* 2019, Vol. 27, Issue 3, 248.
[285] UNODC, *The use of the Internet for terrorist purposes*, Austria, United Nations publications, 2012, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf, 124.
[286] E. COCHE, "Privatised enforcement and the right to freedom of expression in a world confronted with terrorism propaganda online", *Internet Policy Review* 2018, Vol. 7, Issue 4, 7; T. QUINTEL and C. ULLRICH, "Self-Regulation of Fundamental Rights? The EU Code of Conduct on Hate Speech, related initiatives and beyond", in B. PETKOVA and T. OJANEN (eds.), *Fundamental Rights Protection Online: The Future Regulation of Intermediaries*, Northampton, Edward Elgar Publishing, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3298719, 8.

to analyse the character of the content, but possibly not reviewing the referral *expeditiously*, hence not respecting the European law obligations. On the other hand, service providers can over-takedown or over-block the access to content that might be considered *a posteriori* as legal to be sure they are not held liable for the uploaded content and respect their European obligations.[287] In doing so, service providers will infringe the fundamental rights of their users.

This balancing puts the service providers in a delicate position, where they are entrusted with numerous obligations without sufficient legal certainty. They operate on the online scene as a sort of proxy for law enforcement agencies of the state.[288] The service providers themselves recognised this difficult balancing and the legal uncertainty of the exemption of liability regime during the public consultation organised by the Commission on the implementation of the e-Commerce Directive.[289]

134. Service providers seem to require more legal certainty regarding the exemption of liability regime. Contrastingly, they are invested with too much power when they have to analyse the non-conformity of online content with their terms of service.

2.1.2. The interests of the users of the platform

135. The practice of blocking social media users' access to content and removing it due to its presumed illegal character is contestable in light of the users' fundamental rights. Service providers have too much power over these practices since their removal policies often lack transparency.[290] The blocking and removal of certain content constitute an infringement on both the freedom of expression of the content's author and the freedom to receive information

[287] COMMISSIONER FOR HUMAN RIGHTS OF THE COUNCIL OF EUROPE, *The rule of law on the internet and in the wider digital world*, Strasbourg, Council of Europe, 2014, 66; R. F. JØRGENSEN and A. M. PEDERSEN, "Chapter 10 - Online Service Providers as Human Rights Arbiters", in M. TADDEO and L. FLORIDI (eds.), *Law, Governance and Technology Series*, Vol. 31, *The Responsibilities of Online Service Providers*, Switzerland, Springer, 2017, 180.

[288] K. PODSTAWA, "Hybrid Governance or… Nothing? The EU Code of Conduct on Combating Illegal Hate Speech Online", in E. CARPANELLI and N. LAZZERINI (eds.), *Use and Misuse of New Technologies*, Switzerland, Springer, 2019, 182.

[289] EUROPEAN COMMISSION, *Staff Working Document on Online Services, Including e-Commerce, in the Single Market, accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A coherent framework to boost confidence in the Digital Single Market of e-commerce and other online services*, 11 January 2011, COM (2011) 942 final, 43-46.

[290] Y. AKDENIZ, "To Block or Not to Block: European Approaches to Content Regulation, and Implications for Freedom of Expression", *Computer Law and Security Review* May 2010, Vol. 26, Issue 3, 263.

of the content's consumer[291] since service providers are to assess first the (in)compatibility of referred content with their terms of service and, only *when necessary,* with the national law. Hence, they can restrict legitimate speech. This restriction is even more problematic because of the inefficient appeals procedure for legitimate content, which was wrongfully taken down.[292]

2.1.3. The interests of the state

136. Entrusting social media platforms with the responsibility and obligation to take down content is an easy way for states to depart from their legal commitments to protect their citizens against terrorist threats. Making private actors responsible for the state's obligations can, however, negatively impact the state as well. Freedom of expression is the cornerstone of a democratic society. The state, therefore, has an interest in the exercise of this right by its citizens. By requiring private service providers to assess content first to their Terms and Conditions and not to the national laws, the contract between the platform and the platform's user becomes law. Hence, the state partly loses control over what constitutes illegal speech and what is to be banned from a democratic forum.

137. Moreover, specific algorithms provide a user's newsfeed with similar content to what has already been seen.[293] This similarity might further radicalise a person receptive to terrorist content. Consequently, counter-narratives that are created and encouraged by the public authorities might lose their effect.

[291] R. F. JØRGENSEN and A. M. PEDERSEN, "Chapter 10 - Online Service Providers as Human Rights Arbiters?", in M. TADDEO and L. FLORIDI (eds.), *The Responsibilities of Online Service Providers*, Vol. 31, *Law, Governance and Technology Series,* Switzerland, Springer, 2017, 180.
[292] *Cf. supra* n° 88.
[293] *Cf. infra* n° 144-145.

2.2. The recourse by service providers to artificial intelligence is both a curse and a cure

138. Considering the legal obligations of social media platforms, such as the one-hour removal rule, and the enormous amount of data shared on their platforms, it would be unrealistic to require them to analyse every flagged content's legality manually. Moreover, the European Commission has been incentivising social media platforms to turn to artificial intelligence (hereinafter: "AI") to filter out content in contravention with the platform's Terms and Conditions:

> "*Online platforms should do their utmost to proactively detect, identify and remove illegal content online. The Commission strongly encourages online platforms to use voluntary, proactive measures aimed at the detection and removal of illegal content and to step up cooperation and investment in, and use of, automatic detection technologies.*"[294] (emphasis added)

Since filtering systems can be very efficient in preventively blocking illegal information from being uploaded on the platform and finding illegal content on the platform, service providers have recourse to a combination of the use of AI and human intervention.[295] Nevertheless, the Court of Justice of the European Union ruled that a general filtering mechanism would equal a general monitoring obligation, which is prohibited by article 15.1 of the e-Commerce Directive, and would be very costly for the service provider.[296] Monitoring all electronic communications, without limitation in time and directed to all future infringements, would constitute, according to the Court, a grave violation of the service provider's right to conduct a business.[297] Consequently, no obligation to install filtering measures can exist.

This was also recognised by the European Court of Human Rights in the *MTE* case. The Court held that requiring the use of filtering mechanisms to filter out potential illegal content would

[294] Communication from the Commission on Tackling illegal content online – Towards an enhanced responsibility of online platforms, 13.
[295] K. HUSZTI-ORBAN, "Internet intermediaries and counter-terrorism: Between self-regulation and outsourcing law enforcement", in T. MINARIK, L. LINDSTROM and R. JAKSCHIS (eds.), *10th International Conference on Cyber Conflict: CyCon X: Maximising Effects*, 2018, 234; E. LLANSÓ, J. VAN HOBOKEN, P. LEERSSEN and J. HARAMBAM (Transatlantic Working Group), "Artificial Intelligence, Content Moderation, and Freedom of Expression", 26 February 2020, https://www.ivir.nl/publicaties/download/AI-Llanso-Van-Hoboken-Feb-2020.pdf, 3.
[296] CJEU (3rd Ch.) 24 November 2011, C- 70/10, ECLI:EU:C:2011:771, *Scarlet v. SABAM*, §§40 and 48; *In casu*, it concerned the injunction imposed on internet service providers (Scarlet), which can also be applied to social media platform by analogy since it concerns the same provision of the e-Commerce Directive.
[297] CJEU (3rd Ch.) 24 November 2011, C- 70/10, ECLI:EU:C:2011:771, *Scarlet v. SABAM*, §48.

amount to "*requiring excessive and impracticable forethought capable of undermining freedom of the right to impart information on the Internet*"[298].

The Regulation also emphasis that no obligation can rest on the hosting service providers to use automated means such as filtering mechanisms.[299]

139. However, requiring the platforms to assess the compatibility of referred content with their Terms and Conditions *expeditiously*, imposing a one-hour rule to take down illegal content and encouraging (not to say pressuring) social media platforms to use such automated tools to comply with that rule, *de facto* obliges the providers that are not able to comply with these rules to utilise these filtering mechanisms. Hence, the EU's position seems to be conflicting with the CJEU's and the ECtHR's.

140. One such filtering method is 'keyword filtering'. This mechanism automatically filters posts out that contain a particular keyword regardless of their context.[300] This mechanism is an example of excessive content filtering since it violates the author's right to freedom of expression by taking legitimate content down. This danger was also recognised by field actors. As such, a workshop report, with contributions of delegates of Google, Centre for Democracy & Technology and Microsoft, indicates that those companies are turning to machine learning, which allows an algorithm to learn from its previous decisions[301], to train their artificial intelligence in understanding the subtleties of particular contexts such as humour or satire.[302]

141. Sometimes, content is not easily qualified as in line or in contravention with the terms of service. Solely relying on AI to address the problem of online terrorist content would be perilous. Consequently, human review is required in such unclear instances to ensure that the content taken down is effectively contrary to the platform's Terms of Service. Algorithms do not have a human eye to interpret the context or subtleties of specific posts.[303] The new Regulation, therefore, provides an exception to the obligation to take down terrorist content when it has an "*educational, journalistic, artistic or research purpose*"[304]. However, this

[298] ECtHR 2 May 2016, n° 22947/13, *MTE v. Hungary*, §82.
[299] Art. 5.8, 2nd indent Regulation on addressing the dissemination of terrorist content online.
[300] E. LLANSÓ, J. VAN HOBOKEN, P. LEERSSEN and J. HARAMBAM (Transatlantic Working Group), "Artificial Intelligence, Content Moderation, and Freedom of Expression", 26 February 2020, https://www.ivir.nl/publicaties/download/AI-Llanso-Van-Hoboken-Feb-2020.pdf, 5.
[301] R. F. JØRGENSEN, *Human rights in the age of platforms*, Cambridge, The MIT Press, 2019, 82.
[302] K. GOLLATZ, F. BEER and C. KATZENBACH, "The Turn to Artificial Intelligence in Governing Communication Online" (HIIG Workshop report), *Big Data & Society* 2018 (special issue), 7.
[303] R. J. CAMBRON, "World War Web: Rethinking "Aiding and Abetting" in the Social Media Age", *Case Western Reserve Journal of International law* 2019, Vol. 51, Issue 1, 306-307; K. HUSZTI-ORBAN, "Internet intermediaries and counter-terrorism: Between self-regulation and outsourcing law enforcement", in T. MINARIK, L. LINDSTROM and R. JAKSCHIS (eds.), *10th International Conference on Cyber Conflict: CyCon X: Maximising Effects,* 2018, 234.
[304] Art. 1.3 Regulation on addressing the dissemination of terrorist content online.

exception will not stand firm against the algorithms that disregard the context of the online content.

Certain information published online with terrorist content could, for example, have an educational purpose. Content shared by public authorities describing the way ISIL operates and illustrating its propaganda techniques contains terrorist elements but has the purpose of educating the viewers. This context would go unnoticed through the algorithmic analysis and automatically be detected as illegal. Taking such information down constitutes a grave error and could be prevented if a human analyses the post. An example of such a takedown that disregarded the context is the YouTube channel of Al-Mutez Billah that was considered the 'digital archive of the Syrian war'. YouTube's automatic takedown procedures do not take the context of the videos into account and allegedly took down the channel's content preventing the legitimate evidence gathering of the ongoing war.[305]

142. Excessive takedowns of legitimate speech are not the only risk related to the use of AI. False positives and false negatives in the filtered contents also endanger the legitimate takedown of terrorist content.[306] In the context of takedowns of illegal content, false positives are results that wrongly qualify certain content as terrorist content, whereas false negatives are posts that contain terrorist content and should be filtered out, but that escape the filtering of the algorithms and wrongly remain on the platform.[307] On a small scale, these errors might not represent a threat. However, once scaled to a much broader amount of content shared on platforms such as Twitter or Facebook, the margin of false positives and negatives becomes enormous. False positives threaten the freedom of expression of the users of the online platform. False negatives, however, allow terrorist content to pursue their purpose of propaganda, recruitment and terror rising.

143. Another risk linked to the use of AI is the inherent biases algorithms can contain.[308] Algorithms are created by humans, who can be biased. If a creator of algorithms considers, for

[305] X, "Activists accuse YouTube of destroying digital evidence of Syria war", *TRTWorld* 8 March 2021, https://www.trtworld.com/life/activists-accuse-youtube-of-destroying-digital-evidence-of-syria-war-44809; X, "Activists in race to save digital trace of Syria war", *Qantara* 8 March 2021, https://en.qantara.de/content/activists-in-race-to-save-digital-trace-of-syria-war.

[306] R. F. JØRGENSEN and A. M. PEDERSEN, "Chapter 10 - Online Service Providers as Human Rights Arbiters", in M. TADDEO and L. FLORIDI (eds.), *Law, Governance and Technology Series*, Vol. 31, *The Responsibilities of Online Service Providers*, Switzerland, Springer, 2017, 183.

[307] M. FERNANDEZ and H. ALANI, "Artificial Intelligence and Online Extremism: Challenges and Opportunities", in J. MCDANIEL and K. PEASE (eds.), *Predictive Policing and Artificial Intelligence*, London, Routledge, 2021, http://oro.open.ac.uk/69799/1/Fernandez_Alani_final_pdf.pdf; E. LLANSÓ, J. VAN HOBOKEN, P. LEERSSEN and J. HARAMBAM (Transatlantic Working Group), "Artificial Intelligence, Content Moderation, and Freedom of Expression", 26 February 2020, https://www.ivir.nl/publicaties/download/AI-Llanso-Van-Hoboken-Feb-2020.pdf, 9.

[308] SECRETARY-GENERAL OF THE UN, *Note by the Secretary-General on the promotion and protection of the right to freedom of opinion and expression* (29 August 2018), *UN Doc.* A/73/348 (2018), 5; K. MCKENDRICK,

example, that all terrorist content is always published by persons practising the Muslim faith, this bias might be transcribed in the algorithms the person creates. Consequently, this would create an algorithm that would disproportionately qualify content published by Muslims as terrorist content. The algorithm would then operate on a discriminatory basis. This bias can be amplified when the technique of machine learning is applied to the algorithms.

144. Online social media platforms rely on automation, which will put content similar to what a user has previously watched, liked or shared on the person's newsfeed. Therefore, the algorithms that analyse the previously watched content play an important role in what the viewer will and will not see next.[309] When a person has been watching several videos of funny animals, the person's newsfeed will contain similar animal videos due to the algorithms that recommend such content. When a person has been viewing posts of a particular political party, his or her newsfeed will contain similar posts. Hence, when a person has been watching terrorist content of ISIL, their newsfeed will contain more similar content. This one-sided perspective is problematic in the view of counter-terrorism.

145. The recommendation system of social media platforms is linked to this automation. The algorithms will recommend certain content to a viewer based on previously watched content. A user's newsfeed is thus not neutral and will magnify the previously seen opinion.[310] This system prevents a person from seeing different opinions regarding a specific topic, except when they specifically look for the opposite opinion.

Because of the further indoctrination this can cause to people (newly) interested in terrorist content, the 'Redirect Method' was offered as a partial answer. This programme was created to ensure that viewers of terrorist content are through microtargeting redirected towards a counter-terrorism narrative.[311]

Another method worth mentioning to ensure that viewers of terrorist content do not see similar content is the practice of downranking, which deprioritises harmful content, such as terrorist

"Artificial Intelligence Prediction and Counterterrorism", August 2019, https://www.chathamhouse.org/sites/default/files/2019-08-07-AICounterterrorism.pdf, 3.

[309] E. LLANSÓ, J. VAN HOBOKEN, P. LEERSSEN and J. HARAMBAM (Transatlantic Working Group), "Artificial Intelligence, Content Moderation, and Freedom of Expression", 26 February 2020, https://www.ivir.nl/publicaties/download/AI-Llanso-Van-Hoboken-Feb-2020.pdf, 14.

[310] *Ibid.*, 19; N. ELKIN-KOREN, "Contesting algorithms: Restoring the public interest in content filtering by artificial intelligence", *Big data & society* July 2020, Vol. 7, Issue 2, 3.

[311] K. MCKENDRICK, "Artificial Intelligence Prediction and Counterterrorism", August 2019, https://www.chathamhouse.org/sites/default/files/2019-08-07-AICounterterrorism.pdf, 8; J. SCHNADER, "The Implementation of Artificial Intelligence in Hard and Soft Counterterrorism Efforts on Social Media", *Santa Clara High Technology Law Journal* December 2019, Vol. 36, Issue 1, 69.

content, and puts the content at the end of the viewer's newsfeed.[312] Hence, the content is less likely to be viewed by the person.

The European Commission addressed this issue of only viewing similar content in the context of disinformation on online platforms. In its 2018 Code of Practice on Disinformation, the Commission and the signatories, such as Facebook and Twitter, recognised the importance to "*dilute the visibility of disinformation by improving the findability of trustworthy content*"[313]. Moreover, the Code provides that the IT companies should "*invest in technological means to prioritize relevant, authentic and authoritative information where appropriate in search, feeds, or other automatically ranked distribution channels*"[314]. In the context of fake news, the Commission and the relevant companies have accepted AI to show a more diverse newsfeed to their users.

146. The process of taking down online terrorist content after it has been flagged only constitutes a reactive and not proactive measure. The banning of online content has thus, rightfully, often been called a game of 'whack-a-mole'.[315] As in the real game, as soon as the content is 'hit down by the hammer' of the service provider, the same content resurfaces on other service providers' platforms or is re-shared by other social media users. This reappearance seems to weaken the referral operations by the IRUs.[316] Once the provider has taken down a social media profile, this user often resurfaces under a different name and is easily and rapidly followed again by the same sympathisers. Having been removed from a social media platform is often also seen by ISIL's sympathisers as some sort of recognition of their content, importance and impact on their receivers. As CONWAY, KHAWAJA et al. put it, removing the account of ISIL supporters only grants them a 'badge of honour'[317]. It also

[312] E. LLANSÓ, J. VAN HOBOKEN, P. LEERSSEN and J. HARAMBAM (Transatlantic Working Group), "Artificial Intelligence, Content Moderation, and Freedom of Expression", 26 February 2020, https://www.ivir.nl/publicaties/download/AI-Llanso-Van-Hoboken-Feb-2020.pdf , 19.
[313] Code of Practice on Disinformation of the European Commission, September 2018, https://ec.europa.eu/digital-single-market/en/code-practice-disinformation, 3.
[314] *Ibid.*, 7.
[315] J. TROMMEL, *Online jihadi content combat: How serving public interest could ease the privatization of freedom of expression*, Master Thesis Crisis and Security Management (MSc) Leiden University, 2018, https://openaccess.leidenuniv.nl/bitstream/handle/1887/84031/Trommel_CSM_2018.pdf?sequence=1, 33-34; B. BUKOVSKÁ, "The European Commission's Code of Conduct for Countering Illegal Hate Speech Online - An analysis of freedom of expression implications", *Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression* 7 May 2019, https://cdn.annenbergpublicpolicycenter.org/wp-content/uploads/2020/06/EC_Code_of_Conduct_TWG_Bukovska_May_2019.pdf, 7.
[316] J. ELLERMANN, "Terror won't kill the privacy star – tackling terrorism propaganda online in a data protection compliant manner", *ERA Forum* 2016, Vol. 17, Issue 4, 572.
[317] M. CONWAY, M. KHAWAJA, S. LAKHANI, J. REFFIN, A. ROBERTSON, and D. WEIR, "Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts", *Studies in Conflict & Terrorism* 2019, Vol. 42, Issue 1-2, 151.

strengthens the user's belief in their legitimacy and often pushes them to a more determined and radical stance.[318] Being destroyed only reaffirms their beliefs.

147. As a reaction to this 'whack-a-mole' figure, several service providers decided to create a "Database of Hashes" in 2017. This database contains posts, videos or pictures that have been qualified as terrorist content and have received a 'fingerprint'. This project enables intermediaries to upload such content in the database so that other intermediaries become aware of its presence on online social media to prevent it from being uploaded again or to take it down as soon as possible.[319]

148. The recourse by service providers to AI is consequently both a cure and a curse. The use of filtering mechanisms to scrutinise the platform for terrorist content is beneficial and efficient for combatting terrorist content online. Moreover, it enables the platforms to fulfil their legal obligations of removing illegal content within the hour of receiving the order and evaluating the compatibility of referred content with their Terms and Conditions expeditiously. Nevertheless, the swift removal of content disregards the context and subtleties of online content and endangers the freedom of expression of the platform's users. However, even though imposing a general monitoring obligation of the platform is prohibited under the e-Commerce Directive, European authorities have increasingly been 'encouraging' service providers to use general filtering mechanisms. False positives, false negatives and inherent biases in AI further endanger this fundamental right to freedom of expression. Automation and recommendation on the user's newsfeed can further intensify the indoctrination and radicalisation of a person interested in the terrorist discourse. This intensification can, however, also be prevented by implementing algorithms that create a more diverse newsfeed. Last, the question can be raised whether the recourse to AI and, more generally, the notice-and-takedown mechanism really help limit terrorist content since it often resurfaces after being taken down.

[318] *Ibid.*, 151.

[319] EUROPEAN COMMISSION, "EU Internet Forum: a major step forward in curbing terrorist content on the internet" (Press release), 8 December 2016, https://ec.europa.eu/commission/presscorner/detail/en/IP_16_4328; F. WILMAN, *The responsibility of online intermediaries for illegal user content in the EU and the US*, Northampton, Edward Elgar Publishing, 2020, 256.

3. Conclusion

149. The increased responsibility given to private social media platforms, the obligations imposed on them and the 'voluntary' cooperation with these private actors seem too opaque to function correctly. Blocking and taking down terrorist content might not be sufficient to counter the online presence of ISIL. Moreover, as the Human Rights Commissioner of the Council of Europe claimed, blocking measures are easy to circumvent.[320]

The special rapporteurs of the United Nations, of the Organisation for Security and Co-operation in Europe, of the Organisation of American States and of the African Commission on Human and Peoples' Rights recommended in their Joint Declaration on freedom of expression and countering violent extremism to refrain from "*pressuring, punishing or rewarding intermediaries with the aim of restricting lawful content*"[321]. Hence, the subsequent adoption of the Code of Conduct on countering illegal hate speech online, the European Commission's Recommendation and the recent Regulation on terrorist content online provide the exact opposite of what the special mandatories recommended.

150. There is some general reticence when giving private actors, such as hosting service providers, power and control over citizens' lives. YANNOPOULOS, however, points out that these private actors can also have a role in the offline world: "*it has been documented that doctors and pharmacists control the dispense of medicines, small shop owners handle the sale of tobacco products, the proprietors of electronic games parlours administrate admittance of minors, while liquor vendors and bartenders control the consumption of alcohol*"[322]. Giving decisional power to private actors has existed for a long time. The difference, however, with content control by social media platforms is that these platforms allow the dissemination of millions of posts a day[323], whereas pharmacists, shop owners, proprietors of electronic games,

---

[320] COMMISSIONER FOR HUMAN RIGHTS OF THE COUNCIL OF EUROPE, *The rule of law on the internet and in the wider digital world*, Strasbourg, Council of Europe, 2014, 68.

[321] UNITED NATIONS (UN) SPECIAL RAPPORTEUR ON FREEDOM OF OPINION AND EXPRESSION, THE ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE (OSCE) REPRESENTATIVE ON FREEDOM OF THE MEDIA, THE ORGANIZATION OF AMERICAN STATES (OAS) SPECIAL RAPPORTEUR ON FREEDOM OF EXPRESSION AND THE AFRICAN COMMISSION ON HUMAN AND PEOPLES' RIGHTS (ACHPR) SPECIAL RAPPORTEUR ON FREEDOM OF EXPRESSION AND ACCESS TO INFORMATION, *Joint Declaration on freedom of expression and countering violent* extremism, 4 May 2016, https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=19915&LangID=E.

[322] G. N. YANNOPOULOS, "Chapter 3 - The Immunity of Internet Intermediaries Reconsidered?", in M. TADDEO and L. FLORIDI (eds.), *Law, Governance and Technology Series*, Vol. 31, *The Responsibilities of Online Service Providers*, Switzerland, Springer, 2017, 53.

[323] Facebook allegedly has 2.8 billion users worldwide, see M. MOHSIN, "10 Facebook statistics every marketer should know in 2021", *Oberlo* 16 February 2021, https://www.oberlo.com/blog/facebook-statistics; H. TANKOVSKA, "Number of monthly active Facebook users worldwide as of 4th quarter 2020", *Statista* 2 February 2021, https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/; M. IQBAL, "Facebook Revenue and Usage Statistics (2021)", *Business of Apps* 6 April 2021,

liquor vendors and bartenders have a limited amount of 'clients' a day. There is a personal interaction with those 'clients' which is missing on an online social media platform.

151. The preceding parts have shown that hosting service providers are increasingly entrusted with responsibility for what is published on their platform. This practice by hosting service providers to fulfil a public role has been qualified as private law enforcement since these private providers are to police their platforms for illegal content. Social media platforms become a proxy for the government to enforce the government's legal obligations to combat terrorism and terrorism propaganda. Private actors hence have to step in where public authorities leap behind.

152. Building on ELLERMAN's proposal to combine reactive measures with proactive measures[324], the proactive measure proposed in this analysis takes the form of cyber-attacks perpetrated by the state on terrorists' online presence. The state could orchestrate a cyber-attack on the devices an ISIL supporter uses to disable the supporter's access to the device or content it stores. Furthermore, this possibility would replace the responsibility and burden of fighting terrorism back where it belongs: with the state.

https://www.businessofapps.com/data/facebook-statistics/. Twitter has allegedly around 190 million users worldwide; H. TANKOVSKA, "Leading countries based on number of Twitter users as of January 2021", *Statista* 9 February 2021, https://www.statista.com/statistics/242606/number-of-active-twitter-users-in-selected-countries/; M. IQBAL, "Twitter Revenue and Usage Statistics (2020)", *Business of Apps* 8 March 2021, https://www.businessofapps.com/data/twitter-statistics/; Y. LIN, "10 Twitter statistics every marketer should know in 2021", *Oberlo* 25 January 2021, https://www.oberlo.com/blog/twitter-statistics.

[324] J. ELLERMANN, "Terror won't kill the privacy star – tackling terrorism propaganda online in a data protection compliant manner", *ERA Forum* 2016, Vol. 17, Issue 4, 573.

Part 3. Proactive and offensive cyber-measures to combat ISIL's online content

153. The first two parts of this dissertation have demonstrated the importance and legitimate interest of the intervention of states to counter online terrorism. It is unquestionably necessary today to reduce ISIL's online presence as much and as fast as possible. The cooperation with the private social media platforms facilitates this task but also partly hinders it. Their intervention is valuable and important since they have the ability and right to take down content deemed illegal and contrary to their Terms and Conditions. The advantageous position they are in also comes with a cost. A human cost because they have to assess the flagged content in part manually, but also an economical cost since they have to invest in their human resources and technological developments, such as algorithms. Large social media platforms might be able to invest in these human resources and technological developments, but this might not be true for smaller platforms. The timeframe in which the social media platforms have to assess the flagged content's compatibility with their Terms and Conditions and comply with removal orders has extensively been criticised. Furthermore, the responsibility and liability that accompanies countering terrorism have been shifted over the years from the state towards private actors. This shift also implies that private social media platforms are regulating the freedom of expression of their users. This privatisation of law enforcement appears problematic since the state writes the law, but its enforcement is left to private actors. It is time the state took back its responsibility. Tackling terrorist content online is not an easy fix. However, the ever-developing cyber capabilities of the military, the police, and the intelligence and security services could allow states to reclaim their responsibility. The following parts will consider whether granting these services the competence to perpetrate cyber-attacks on the devices of terrorists present on Belgian soil would be a legitimate response to tackle online terrorist content. To answer this question, the notion of a proactive and offensive 'cyber-attack' will first be clarified (1.), turning then to the analysis of the existing legal framework regarding proactive and offensive cyber-measures (2.). Last, the possibility to perpetrate proactive and offensive cyber-attacks in Belgium on terrorists on Belgian soil will be analysed (3.).

1. The notion of proactive and offensive cyber-attacks

154. The question of whether proactive and offensive cyber-attacks could be perpetrated on terrorists requires an introductory explanation of these notions. A cyber-attack is "*a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects*"[325].

A cyber-attack is often linked to the operation of hacking, which can be understood as "*the illicit and usually illegal activities associated with unauthorized access to, or interference with, computer systems*"[326]. These attacks fall under the legal branch of cybercrime, which will guide the following analysis.

155. The Cambridge Dictionary defines 'proactive' as "*taking action by causing change and not only reacting to change when it happens*"[327]. Building further on this definition, proactive attacks in the context of the Belgian fight against ISIL terrorists, in contrast with reactive attacks, can be understood as interventions by the state before such a terrorist has perpetrated an attack to neutralise the potential attack. Hence, the state intervenes before an actual attack has occurred.

An 'offensive' action, as opposed to a 'defensive' action, is an easily-understood-difficult-to-define notion. The notion of 'offensive' can be understood as "*a planned military attack*"[328] where the state attacks first, whereas 'defensive' can be understood as "*used to protect someone or something against attack*"[329]. Therefore, when applied to the context of this analysis, 'offensive' will be understood as actively organising actions to eliminate the enemy, whereas 'defensive' will be understood as actions to defend the state against an attack perpetrated by the enemy.

156. In the context of diminishing the online presence of ISIL on social media and the prevention of terrorist attacks, the combination of the notions 'proactive' and 'offensive' allows analysing whether the state can perpetrate offensive attacks, such as a cyber-attack on the device of a terrorist, proactively, before the terrorist has carried out an attack or uploaded propaganda on online social media in order to prevent this from happening.

---

[325] M. N. SCHMITT, *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations*, 2nd ed., Cambridge, Cambridge University Press, 2017, 415, Rule 92 – Definition of cyber-attack.
[326] M. YAR and K. F. STEINMETZ, *Cybercrime and Society*, 3rd ed., California, Sage Publications, 2019, 266.
[327] *Cambridge dictionary*, *v° Proactive*, https://dictionary.cambridge.org/dictionary/english/proactive.
[328] *Cambridge dictionary*, *v° Offensive*, https://dictionary.cambridge.org/dictionary/english/offensive.
[329] *Cambridge dictionary*, *v° Defensive*, https://dictionary.cambridge.org/dictionary/english/defensive.

2. Legal framework of proactive and offensive cyber-measures

2.1. Cyber-measures taken at the international level

157. In what follows, a distinction will be made between the general international level (2.1.1.), such as the instruments adopted at the level of the United Nations, and the Law of Armed Conflict (2.1.2.). At the level of the Law of Armed Conflict, the targeted attacks and their online counterpart, the cyber-attacks, will briefly be examined (2.1.2.1.). Afterwards, the question of whether these cyber-attacks as online form of targeted attacks can be perpetrated on ISIL supporters and propaganda distributors on Belgian soil in the framework of the war against terror will be analysed (2.1.2.2.).

2.1.1. The legal framework at the international level

158. At the United Nations level, no legislation has been adopted that explicitly addresses cybercrime, or more specifically, cyber-attacks.[330] There is an ongoing discussion on creating a Cybercrime Treaty at the UN level, but this has not yet been the object of thorough discussion.[331]

159. At the level of the North Atlantic Treaty Organization (hereinafter: "NATO"), there is an apparent willingness to develop more offensive cyber operations. NATO's Secretary-General J. STOLTENBERG answered in a Press Conference the following to the question of whether he would see NATO having offensive cyber capabilities:

> "*We have integrated national cyber capabilities. (…) We have been able to disrupt the cyber networks of Daesh to reduce their ability to recruit, to fund, to communicate. And these capabilities have been used by NATO Allies against Daesh and these are the same kind of capabilities we now are creating the framework to integrate into NATO missions*

[330] The "International instruments" internet page of the Council of Europe lists several instruments at the level of the Council of Europe, the European Union, the United Nations and Other Regional Organisations. The list with UN instruments does not contain an instrument relating to cybercrime, see COUNCIL OF EUROPE, "International instruments – Cybercrime", https://www.coe.int/en/web/cybercrime/international-instruments; UNODC, *The use of the Internet for terrorist purposes*, Austria, United Nations publications, 2012, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf, 74.

[331] The discussions on the adoption of the Cybercrime Treaty have been postponed due to the COVID-19 outbreak; UNITED NATIONS GENERAL ASSEMBLY, "General Assembly Adopts Decision Postponing Organizational Session of Ad Hoc Committee Elaborating Anti-Cybercrime Convention, Due to COVID-19 Fears" (Meetings Coverage) (15 January 2021), *UN Doc. GA/12309*, https://www.un.org/press/en/2021/ga12309.doc.htm.

and operations. (...) I think it is important that we have those capabilities in NATO missions and operations when needed because it's impossible to imagine any kind of military conflict in the future without a cyber dimension."[332] (emphasis added)

Moreover, NATO's Allied Joint Doctrine for the Conduct of Operations specifies that cyber operations are to be perpetrated by the national members in line with their national legislation. NATO contributes with cyber capabilities and information, but the actual operations are to be carried out by the individual nations.[333] Nevertheless, the Research Division of the NATO Defence College has recommended developing and implementing offensive cyber capabilities.[334]

Hence, some of the NATO members, such as the United States and the United Kingdom[335], already have the operational capability to orchestrate offensive cyber operations.

160. Even though the legal framework necessary at the international and the NATO level is still lacking, there is an opening for discussions and further legislation on cyber operations.

2.1.2. The legal framework of the Law of Armed Conflict

161. The Law of Armed Conflict, also known as International Humanitarian Law[336], is a special branch of international law that applies to armed conflicts. A common practice in armed conflicts is the recourse to targeted killings and attacks. Targeted killings are perpetrated on persons, whereas targeted attacks are aimed at objects. The latter is to be understood as "*acts of violence against the adversary, whether in offence or in defence*".[337] Hence, in conflicts, certain terrorists or terrorist objects are targeted and eliminated. The question at stake is whether targeting a terrorist's device (a computer or cell phone, for example) on which a cyber-attack is perpetrated to disable the person's access to the information stored on the device could constitute the online version of targeted attacks. By destroying data, such as video's, propaganda and other sources of terrorist information, on a terrorist's device, this propaganda

[332] J. STOLTENBERG, *Press conference by NATO Secretary-General Jens Stoltenberg following the meetings of NATO Defence Ministers*, 4 October 2018, https://www.nato.int/cps/en/natohq/opinions_158705.htm?selectedLocale=en.
[333] NORTH ATLANTIC TREATY ORGANIZATION, *Allied Joint Doctrine for the Conduct of Operations of February 2019*, ed. C, Version 1, 1.14.
[334] I. A. IFTIMIE, "NATO's needed offensive cyber capabilities", *NDC POLICY BRIEF* May 2020, Issue 10, 3.
[335] *Cf. infra* n° 201.
[336] Only the notion of the Law of Armed Conflict will be used.
[337] Art. 49.1 Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I) of 8 June 1977, *United Nations Treaty Series*, Vol. 1125, 3.

material would be lost. Consequently, the terrorist supporters and propaganda spreaders would not be able to upload it on social media platforms. Disabling access to a terrorist's device would also prevent them from disseminating that propaganda. This would be a proactive way of eliminating terrorist propaganda and diminishing their presence on social media platforms. The analysis will be limited to the devices of persons located on Belgian soil.

2.1.2.1. Proactive and offensive cyber-attacks: an online version of targeted attacks?

162. Targeted attacks are not limited to those attacks perpetrated by kinetic force.[338] Cyber-attacks also fall under the category of targeted attacks.[339]

163. According to SCHMITT, the majority of the International Group of Experts considered data to be too volatile and intangible to be considered an 'object'.[340] Consequently, the International Group of Experts would not consider the destruction of data on a person's device as a targeted attack. However, disabling access to a terrorist's device by, for example, installing malware on the device that freezes it and makes it useless could be considered an online version of a targeted attack. Nevertheless, the International Committee of the Red Cross (hereinafter: "ICRC") considers that propaganda spreaders cannot be the object of targeted attacks.[341]

2.1.2.2. The global war on terror: a justification for the applicability of the Law of Armed Conflict in Belgium?

164. The Law of Armed Conflict distinguishes international armed conflicts (hereinafter: "IAC") from non-international armed conflicts (hereinafter: "NIAC"). An IAC is a conflict between two or more states.[342] A NIAC occurs "*whenever there is … protracted armed violence between governmental authorities and organised armed groups or between such*

[338] M. N. SCHMITT, *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations*, 2nd ed. Cambridge, Cambridge University Press, 2017, 415.
[339] C. DROEGE, "Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians", *International Review of the Red Cross* 2012, Vol. 94, Issue 886, 557; W. H. BOOTHBY, *The Law of Targeting*, 1st ed., Oxford, Oxford University Press, 2012, 384.
[340] M. N. SCHMITT, *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations*, 2nd ed., Cambridge, Cambridge University Press, 2017, 437.
[341] N. MELZER, *Interpretative guidance on the notion of direct participation in hostilities under international humanitarian law*, Geneva, 2009, 52.
[342] Art. 2 Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of 12 August 1949, *United Nations Treaty Series*, Vol. 75, 31.

groups within a state"[343] (emphasis added). Since the attacks of 11 September 2001 in the USA, an ongoing 'war on terror' has been declared. Initially directed towards Al-Qaeda, the United States' efforts to combat terrorism were soon echoed by the international community to fight ISIL. Following the announcement by ISIL of the 'Islamic Caliphate', former US President OBAMA decided to set up the *Combined Joint Task Force - Operation Inherent Resolve* (CJTF- OIR) through which the USA, joined by 69 institutions and countries (including Belgium), formalised its military actions against ISIL in Syria and Iraq.[344] This military coalition has launched several land and air strikes to defeat ISIL and their facilities in the region.[345]

The 'war on terror' has received an interesting definition by YAR and STEINMETZ: "[The] *rhetorical and political response among Western governments in the wake of the 11 September 2001 (9/11) attacks in New York, which adopts a highly aggressive and 'pro-active' stance in identifying, capturing and disabling actual, suspected and potential terrorists, along with those who are perceived to sympathize with or support their goals*"[346] (sic) (emphasis added). The aspect of 'suspected and potential terrorists, sympathisers and supporters' is particularly appealing in the debate on the restriction of the rights of an alleged terrorist.

165. Even though this qualification of 'war against terror' is widely used, the ICRC has explicitly refused to recognise the ongoing conflict in Syria and Iraq against ISIL as such.[347]

The ICRC qualifies the conflict against ISIL as a non-international armed conflict taking place on different countries' territory. Whilst a NIAC can spill over to another country's territory, the ICRC requires that in order to amount to an armed conflict in all the different territories, a non-state armed group should attain a certain degree of organisation and intensity in each of the territories concerned.[348]

In order to attain the required level of organisation, the International Criminal Tribunal for Yugoslavia (hereinafter: "ICTY") developed in its case-law several criteria, such as "*the fact*

---

[343] ICTY (Appeals Ch.) 2 October 1995, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, n° IT-94-1-AR72, *The Prosecutor v. Dusko Tadić*, §70.
[344] J. R. DA SILVA, "Jihadist Terrorism and EU Responses - Current and Future Challenges", *Austria Institut für Europa - und Sicherheitspolitik*, https://www.aies.at/download/2017/AIES-Fokus--2017-06.pdf; X, "Combined Joint Task Force: Operation Inherent Resolve", APO AE 09306, https://www.inherentresolve.mil/Portals/14/Documents/Mission/HISTORY_17OCT2014-JUL2017.pdf?ver=2017-07-22-095806-793.
[345] J. R. DA SILVA, "Jihadist Terrorism and EU Responses - Current and Future Challenges", *Austria Institut für Europa - und Sicherheitspolitik*, https://www.aies.at/download/2017/AIES-Fokus--2017-06.pdf.
[346] M. YAR and K. F. STEINMETZ, *Cybercrime and Society*, 3rd ed., California, Sage Publications, 2019, 271.
[347] INTERNATIONAL COMMITTEE FOR THE RED CROSS, *Report: International humanitarian law and the challenges of contemporary armed conflicts*, 32nd International Conference of the Red Cross and Red Crescent, Geneva, October 2015, https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts, 18.
[348] *Ibid.*, 19.

that the group controls a certain territory" or "*the ability of the group to gain access to weapons, other military equipment, recruits and military training;*"[349]. ISIL attains this level of organisation in Syria and Iraq[350], but not in Belgium.

Regarding the intensity of the armed conflict, the ICTY stated that there should be a situation of "*protracted armed violence*"[351]. To analyse this level of intensity, the following elements can be taken into account: "*the number, duration and intensity of individual confrontations*", "*the type of weapons and other military equipment used*", "*the number of persons and type of forces partaking in the fighting*" or "*the number of casualties and the number of civilians fleeing combat zones*"[352]. It is beyond doubt that ISIL reaches the required level of intensity in the aforementioned combat zones[353], but not in Belgium.

166. The ongoing conflict involving ISIL and the governments of (primarily) Syria and Iraq consequently amounts to the qualification of a non-international armed conflict. However, the conflict cannot be extended to Belgian soil. For the law of armed conflict to apply to a specific territory, the conflict needs to amount to a NIAC in that territory. This threshold is not reached in Belgium.

2.1.2.3. Conclusion

167. Targeted attacks and their online counterpart are allowed under the Law of Armed Conflict regime in the territory of the ongoing non-international armed conflict against ISIL (primarily Iraq and Syria). However, propaganda spreaders cannot be targeted by attacks. Moreover, since the conflict does not extend to the Belgian territory, attacks cannot be perpetrated on terrorists under the Law of Armed Conflict regime. This Law is consequently not applicable to the current analysis.

[349] ICTY (Trial Ch. I) 3 April 2008, n° IT-04-84-T, *The Prosecutor v. Ramush Haradinaj et al.*, §60.
[350] For a more detailed analysis of the thresholds of 'organisation' regarding the non-international armed conflict involving ISIL, see H. EECHAUTE, *Non-international armed conflict: a trigger for the rules on targeting?*, Master Thesis Law UGent, 2016, https://lib.ugent.be/fulltxt/RUG01/002/272/228/RUG01-002272228_2016_0001_AC.pdf, 15-17.
[351] ICTY (Appeals Ch.) 2 October 1995, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, n° IT-94-1-AR72, *The Prosecutor v. Dusko Tadić*, §70.
[352] ICTY (Trial Ch. I) 3 April 2008, n° IT-04-84-T, *The Prosecutor v. Ramush Haradinaj et al.*, §49.
[353] For a more detailed analysis of the thresholds of 'intensity' regarding the non-international armed conflict involving ISIL, see H. EECHAUTE, *Non-international armed conflict: a trigger for the rules on targeting?*, Master Thesis Law UGent, 2016, https://lib.ugent.be/fulltxt/RUG01/002/272/228/RUG01-002272228_2016_0001_AC.pdf, 17-18.

2.2. Cyber-measures taken at the level of the Council of Europe[354]

168. At the Council of Europe level, the Convention on Cybercrime[355] imposes several measures on the ratifying states to counter cybercrime. For instance, article 5 of the Cybercrime Convention requires the Member States to criminalise the unlawful interfering with a computer system. Under the Convention, a 'computer system' is to be understood as "*any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*"[356].

169. Article 5 of the Convention provides the following:

> "*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.*"[357] (emphasis added)

Hence, intruding into a person's computer or cell phone to then hinder its functioning is to be criminalised in national law. The Cybercrime Convention uses the notion of hindering the computer system 'without right'. This notion is further elaborated in the explanatory note of the Convention. This note states that hindering the functioning of a computer system will not always be considered punishable. A legal basis or justification by consent, necessity or self-defence are reasons this conduct can be considered legitimate.[358]

Consequently, if the law foresees the possibility to perpetrate offensive cyber operations, such as interfering with a computer system, this would not fall under this prohibition.

170. The Council of Europe Convention on the Prevention of Terrorism foresees the possible cooperation with other states to enhance their capacities to prevent the commission of terrorist offences. This cooperation can take the form of 'joint efforts of a preventive character'.[359]

---

[354] Since the European Convention on the Suppression of Terrorism of 1977 aims to facilitate the extradition of persons having committed acts of terrorism (art. 1) and that the internet or cyber-attacks were not part of the discussions yet, this instrument will not be discussed.
[355] Convention on Cybercrime of 23 November 2001, *ETS*, n° 185 (hereinafter: "Cybercrime Convention").
[356] Art. 1, a) Cybercrime Convention.
[357] Art. 5 Cybercrime Convention.
[358] COUNCIL OF EUROPE, *Explanatory Report to the Convention on Cybercrime*, *ETS* 23 November 2001, n° 185, §38.
[359] Art. 4 Convention of the Council of Europe on the Prevention of Terrorism of 16 May 2005, *CETS*, n° 196.

However, the Convention has not been ratified by Belgium.[360] It is therefore not applicable to the current analysis.

2.3. Cyber-measures taken at the level of the European Union

171. At the European Union level, Directive 2013/40/EU on attacks against information systems[361] provides the European legal framework for cyber operations. The Directive provides for a similar definition of a 'computer system', which it qualifies as 'information system'[362], albeit being more extensive: "*a device or group of interconnected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance*"[363].

Hence, telephones, computers, networks and servers fall under the definition of an 'information system'.[364]

172. Similar to the Cybercrime Convention, this Directive also imposes on the Member States the criminalisation of an illegal system interference. The Directive adds, however, two additional grounds for criminalisation. The first ground is the interruption of the functioning of the information system. The second ground is the crime of making data inaccessible.[365]

173. Moreover, the Directive also refers to the notion of 'without right', which, contrary to the Cybercrime Convention, is defined in the Directive. 'Without right' is to be understood as: "*conduct referred to in this Directive, including access, interference, or interception, which is not authorised by the owner or by another right holder of the system or of part of it, or not permitted under national law*"[366] (emphasis added).

Consequently, if the national law foresees the possibility of perpetrating cyber-attacks on an information system of terrorists, this conduct would be 'with right', thus, not to be criminalised by the Member States.

---

[360] *Cf. supra* n° 21.
[361] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, *OJ L* 14 August 2013, n° 218, 8 (hereinafter: "Directive 2013/40/EU on attacks against information systems").
[362] Hereinafter only the notion of 'information service' will be used.
[363] Art. 2, a) Directive 2013/40/EU on attacks against information systems.
[364] L. KLIMEK, "Combating attacks against information systems: EU legislation and its development", *Masaryk University Journal of Law and Technology* 2012, Vol. 6, 91.
[365] Art. 4 Directive on attacks against information systems.
[366] Art. 2, d) Directive on attacks against information systems.

174. The perpetration of proactive and offensive cyber-attacks on ISIL supporters' devices to limit the online presence of ISIL could happen through joint investigation teams[367] at the level of Europol. Europol was entrusted with the task of coordinating, organising and implementing, amongst others, operational actions "*to support and strengthen actions by the competent authorities of the Member States, that are carried out (…) in the context of joint investigation teams in accordance with Article 5*"[368]. Hence, through joint investigation teams, Europol could support combined proactive and offensive cyber actions by several Member States.

2.4. Cyber-measures taken at the Belgian level

175. The previous analysis has shown that proactive and offensive cyber-attacks do not yet have a legal framework to rely on at the international level. At the level of the Council of Europe and the European Union, these proactive and offensive attacks could find their basis in the 'with right' intrusion in computer or information systems, if allowed under national law. Therefore, it is interesting to turn to the national level. Hereafter follows an analysis of the current state of affairs in the Belgian legislative scene (2.4.1), in which the legal frameworks of cyber-attacks (2.4.1.1.), the judicial police and public prosecutors (2.4.1.2.) and the intelligence and security services (2.4.1.3.) will be addressed.

176. During this analysis, it will become apparent whether the Belgian legislation allows the perpetration of proactive and offensive cyber-attacks on devices of terrorists present on Belgian soil.

2.4.1. The current state of affairs in the Belgian legislative scene

2.4.1.1. The legal framework of cyber-attacks

177. The crime of hacking or entering an 'information system'[369] without being authorised to do so is criminalised under article 550*bis* of the Belgian Criminal Code. This unauthorised entry is punished with an imprisonment sentence of six months to two years and with a fine of twenty-six to twenty-five thousand euros, or with one of those penalties. However, if the entry

[367] The entire legal regime of joint investigation teams will not be addressed in this dissertation. For more information on the topic, see EUROPOL, "Joint investigation teams – JITS", https://www.europol.europa.eu/activities-services/joint-investigation-teams.
[368] Art. 4, 1st indent, c), ii) Europol Regulation.
[369] The Belgian legislation uses the notion of 'information system' and not 'computer system'.

is perpetrated with fraudulent intent, the maximum imprisonment sentence is heightened to three years.[370] If the intrusion in the information system leads to damage to the system or data it contains, the sentence is increased to an imprisonment of one to five years and with a fine of twenty-six to fifty thousand euros, or one of these sentences.[371] This last sanction consequently criminalises the destruction of data on a terrorist's device.

178. The crime of sabotaging an information system, by, for example, introducing malware in the system, is also criminalised in Belgian law. As such, article 550*ter* of the Belgian Criminal Code foresees for this crime an imprisonment sentence of six months to three years and a fine of twenty-six to twenty-five thousand euros, or one of these penalties. Here as well, the fraudulent intent heightens the maximum imprisonment sentence to five years.[372] If the intrusion leads to the damage of the data it contains, the sentence provided is an imprisonment of six months to five years and a fine of twenty-six to seventy-five thousand euros, or with one of these sentences.[373] Should the system's intrusion result in the damage or incorrect functioning of the information system, then the imprisonment sentence is brought to a minimum of one year and a maximum of five years, and the fine is raised to twenty-six to one-hundred thousand euros, or with one of these penalties.[374] The sabotage of a terrorist device by, for example, implementing malware to freeze the person's device is thus criminalised by this last sentence.

179. Should the Belgian legislation provide the possibility to perpetrate proactive cyber-attacks on ISIL supporters or terrorists to diminish their online presence, the Belgian legislator will have to provide an exception to this Belgian regime of criminal law.

2.4.1.2. The legal framework of the judicial police and the public prosecutor

180. According to article 8 of the Belgian Code of Criminal Procedure, the "*judicial police investigates crimes, misdemeanours and contraventions, gathers evidence and hands over the perpetrators to the courts to sanction them*"[375]. Article 15 of the Belgian Law on the Police Service of 1992 provides similar tasks.[376] Therefore, the judicial police's role is limited to investigating infringements of the law, gathering evidence of these breaches and handing over

[370] Art. 550*bis*, §1 Belgian Criminal Code.
[371] Art. 550*bis*, §2 Belgian Criminal Code.
[372] Art. 550*ter*, §1 Belgian Criminal Code.
[373] Art. 550*ter*, §2 Belgian Criminal Code.
[374] Art. 550*ter*, §3 Belgian Criminal Code.
[375] Art. 8 Belgian Code of Criminal Procedure.
[376] Art. 15 Belgian Law of 5 August 1992 on the Police Service, *Belgian Gazette* 22 December 1992, 27.124.

the perpetrators to the courts and tribunals. Their competences are restricted to the reaction to a crime, misdemeanour or contravention to help the judicial machine prosecute them.

181. Similarly, the competence of the Belgian public prosecutors is limited to "*investigating and prosecuting offences*"[377].

182. Consequently, orchestrating proactive and offensive cyber-attacks on the device of a terrorist located in Belgium to prevent the person from sharing terrorist content online does not lay in the competences of the police or the public prosecutors.

2.4.1.3. The legal framework of the intelligence and security services

183. Contrary to the police and the public prosecutors, the Belgian intelligence and security services are already entrusted with some offensive cyber-competences.

184. The Belgian scene of intelligence and security services is covered by two different branches (2.4.1.3.1.): one civilian branch, the State Security Service[378] (2.4.1.3.1.1.), and one military branch, the General Intelligence and Security Service[379] (2.4.1.3.1.2.).[380] It is worth analysing whether these branches today have the possibility of perpetrating cyber-attacks on terrorists.

185. The Belgian intelligence and security services are mainly defensive services, where information is gathered and then passed through to other services of the Belgian police to react to that information.[381] This information can both be proactively searched for or gathered as a reaction to a specific terrorist attack. Contrary to the reactive actions or searches, proactive actions occur at an earlier stage, namely before an attack has happened or before certain content has been made available online. As will be discussed hereunder, the defensive intelligence and security services have received over the years more offensive competences. When these offensive competences, such as perpetrating a cyber-attack, are combined with proactive intervention, the intelligence and security services would proactively prevent the terrorists from accessing or uploading certain information.

[377] Art. 22 Belgian Code of Criminal Procedure.
[378] Veiligheid van de Staat (Dutch) – Sureté de l'État (French) (VSSE).
[379] Algemene Dienst Inlichting en Veiligheid (Dutch – ADIV) – Service Général du Renseignement et de la Sécurité (French – SGRS).
[380] D. VAN DAELE and L. MERGAERTS, *Naar een herijking van de Belgische veiligheidsarchitectuur: vaststellingen en aanbevelingen van de parlementaire onderzoekscommissie terroristische aanslagen*, Antwerpen, Intersentia, 2020, 30.
[381] *Ibid.*, 31.

2.4.1.3.1. The bodies of the intelligence and security services

2.4.1.3.1.1. The State Security Service: the civilian branch

186. The civilian branch of the Belgian intelligence services, the State Security Service, has been entrusted, amongst others, with the following tasks:

> "*the collection, analysis and processing of intelligence relating to any activity that threatens or could threaten the internal security of the State and the survival of the democratic and constitutional order, the external security of the State and international relations, scientific or economic potential, as defined by the National Security Council, or any other fundamental interest of the country, as defined by the King on the proposal of the National Security Council.*"[382] (emphasis added)

An 'activity that threatens or could threaten' is understood as:

> "*any individual or collective activity carried out within the country or from abroad which may be related to espionage, interference, terrorism, extremism, proliferation, harmful sectarian organisations, criminal organisations, including the dissemination of propaganda, encouragement or direct or indirect support, including through the provision of financial, technical or logistical resources, the provision of intelligence on possible targets, the development of structures and capacity for action and the achievement of the objectives pursued*."[383] (emphasis added)

Hence, the civilian intelligence services are explicitly competent for intelligence gathering on terrorism, including propaganda dissemination.

2.4.1.3.1.2. The General Intelligence and Security Service: the military branch

187. The military branch of the intelligence services, the General Intelligence and Security Service, has similar competences but limited to the Belgian armed forces. As such, their tasks cover:

> "*the collection, analysis and processing of intelligence relating to factors that affect or may affect national and international security to the extent that the Armed Forces are or*

[382] Art. 7, 1) Belgian Law regulating the intelligence and security services. Own translation.
[383] Art. 8, 1°, 1st indent Belgian Law regulating the intelligence and security services. Own translation.

may become involved in providing intelligence support to their ongoing or possible upcoming operations."[384] (emphasis added)

These intelligence forces are also competent for activities that relate to the "*inviolability of the national territory or population*"[385], "*military defence plans*"[386], or "*the security of Belgian nationals abroad*"[387]. The military intelligence services are not entrusted with a specific task related to terrorism, save for terrorist threats that could jeopardise the aforementioned three specific tasks.[388] The tasks and methods discussed hereunder have to fall within the scope of the limitations mentioned above.

2.4.1.3.2. Competences of the intelligence and security services

188. Even though separate branches cover the intelligence scene in Belgium, these services do not operate isolated from one another. As such, those two services cooperate when gathering intelligence regarding terrorism.[389] Moreover, both the State Security Service and the General Intelligence and Security Service fall under the supervision and control of the 'Committee R/I', which is the Belgian supervisory authority of the intelligence services.[390]

189. In what follows, the special investigative techniques (2.4.1.3.2.1.) and the cyber-capacities (2.4.1.3.2.2.) of the intelligence and security services will be discussed.

2.4.1.3.2.1. Special investigative techniques of the intelligence and security services

190. The Belgian intelligence services' competences can be divided into three levels based on the methods they use and the intrusiveness of these methods on the citizens' rights. As such,

[384] Art. 11, §1, 1° Belgian Law regulating the intelligence and security services. Own translation.
[385] Art. 11, §1, 1°, a) Belgian Law regulating the intelligence and security services. Own translation.
[386] Art. 11, §1, 1°, b) Belgian Law regulating the intelligence and security services. Own translation.
[387] Art. 11, §1, 1°, e) Belgian Law regulating the intelligence and security services. Own translation.
[388] D. VAN DAELE and L. MERGAERTS, *Naar een herijking van de Belgische veiligheidsarchitectuur : vaststellingen en aanbevelingen van de parlementaire onderzoekscommissie terroristische aanslagen*, Antwerpen, Intersentia, 2020, 32.
[389] *Ibid.*, 49.
[390] Art. 3, 7° Belgian Law regulating the intelligence and security services refers to 'intelligence services', as defined by art. 3, 2° Belgian Law 18 July 1991 regulating the supervision of police and intelligence services and the Coordination Unit for Threat Assessment, *Belgian Gazette* 26 July 1991, 16.576.

the effects of ordinary intelligence methods[391] are less intrusive on citizens' rights than the special methods[392] and the exceptional methods[393], which are considered the most intrusive.

191. In order to use the exceptional methods, the prior approval of the Commission is required.[394] This Commission is an administrative organ responsible for the oversight of the use of special and exceptional methods by the intelligence and security services to gather intelligence.[395] This Commission is composed of two judges and one magistrate.[396]

192. One of the exceptional methods the intelligence services can use is, according to article 18/16 of the Belgian Law regulating the intelligence and security services, the possibility for those services to enter into an information system, lift its security, install technical measures to decipher and decode the data of the system and to take this data over.[397] These activities can be undertaken by the intelligence and security services by technical means, false signals, false keys and false capacities.[398] However, this operation is limited to mere intelligence gathering and does not cover the irreversible and offensive destruction or alteration of this data.[399]

193. Surprisingly, the Belgian civilian branch of the intelligence services has been much more active than the military branch in using the exceptional method provided in article 18/16 of the Belgian Law regulating intelligence and security services. To give an example: in 2018, the Belgian State Security Service (civilian) received 40 permissions to make use of this method, whereas the General Intelligence and Security Service (military) received one permission that year.[400] The same trend can be noticed the following year, during which the civilian branch received 48 permissions and the military branch 8.[401] This difference finds its explanation in the different activities those two branches perform.[402] The civilian branch rather uses the special investigative techniques for counter-terrorism in the first place and, to a lower

[391] Art. 14-18 of the Belgian Law regulating the intelligence and security services.
[392] Art. 18/4-18/8 of the Belgian Law regulating the intelligence and security services.
[393] Art. 18/11-18/17 of the Belgian Law regulating the intelligence and security services
[394] Art. 18/9, §2, 2nd indent Belgian Law regulating the intelligence and security services.
[395] Art. 3, 6° Belgian Law regulating the intelligence and security services.
[396] Art. 43/1, §1, 6th indent Belgian Law regulating the intelligence and security services.
[397] Art. 18/16 Belgian Law regulating the intelligence and security services.
[398] Art. 18/16, §1, 1st indent Belgian Law regulating the intelligence and security services.
[399] Art. 18/16, §1, 3rd indent Belgian Law regulating the intelligence and security services.
[400] COMMITTEE I/R, *Activiteitenverslag 2018*, https://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2018.pdf, 48 and 44.
[401] COMMITTEE I/R, *Activiteitenverslag 2019*, https://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2019.pdf, 48 and 44.
[402] J. VANDERBORGHT, "If you torture the data long enough, it will confess – Enkele cijfers over de inzet van bijzondre inlichtingenmethoden", in J. VANDERBORGHT (eds.), *Bijzondere inlichtingenmethoden in de schijnwerpers – Les méthodes particulières de renseignement: de l'ombre à la lumière*, Brussel, Levebvre Sarrut Belgium NV, 2020, 18.

degree, for counter-espionage, whereas the military branch focuses rather on counter-espionage and only later on counter-terrorism.[403]

2.4.1.3.2.2. Cyber capacities of the intelligence and security services

194. In 2010, the Belgian legislator enlarged the cyber-competences of the military branch to include, amongst others, the possibility of reacting to a cyber-attack with a military counter-attack. The military services are competent to protect their systems and infrastructures against a cyber-attack, but they can also immediately react to a cyber-attack by perpetrating such an attack "*in accordance with the laws of armed conflict*".[404] Hence, today, the military intelligence and security services are only competent to perpetrate defensive cyber-attacks and, in the context of the Law of Armed Conflict, offensive cyber-attacks. However, this unique reference to cyber-attacks in this law does not allow the perpetration of a proactive cyber-attack on devices of ISIL supporters and terrorists in Belgium since the Law of Armed Conflict does not apply to the current fight in Belgium against ISIL propaganda.[405]

195. The supervisory Committee R/I recommended in 2016 that the competence to perpetrate such offensive (as provided in article 11, §1, 2° of the Belgian Law regulating the intelligence and security services) cyber-attacks as a reaction to attacks on the military infrastructure would be broadened to all public services and infrastructures.[406]

196. In 2017, the Belgian legislator intervened again to modify the competences of the intelligence and security services.[407] The military intelligence and security service received extra cyber-competences regarding information systems located outside the Belgian territory. As such, it can "*intrude into an information system located abroad, lift its security, install technical facilities in order to decipher, decode, store, and manipulate the data stored, processed, or transmitted by the information system and disrupt and neutralise the information system, (…) within the framework of the missions referred to in Article 11, § 1, 1° to 3° and 5°*"[408] (emphasis added). The military intelligence services have thus received the competence of infiltrating, disrupting and neutralising an information system located abroad. The

[403] K. LASOEN, *Geheim België – Geschiedenis van de inlichtingendiensten 1830-2020,* Tielt, Lannoo, 2020, 323.
[404] Art. 4 Belgian Law 4 February 2010 regarding the methods for the collection of intelligence by the intelligence and security services, *Belgian Gazette* 10 March 2010, 14.916, modifying art. 11, §1, 2° Belgian Law regulating the intelligence and security services.
[405] *Cf. supra* n° 166.
[406] COMMITTEE I/R, *Activiteitenverslag 2017*, https://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2017.pdf, 131.
[407] Belgian Law 30 March 2017 modifying the Law of 30 November 1998 regulating the intelligence and security services and article 259*bis* Criminal Code, *Belgian Gazette* 28 April 2017, 53.768.
[408] Art. 44/1 Belgian Law regulating the intelligence and security services. Own translation.

preparatory works of the Belgian Law of 2017 give the example of the infiltration in a kamikaze's cell phone, located outside of the Belgian territory.

The infiltration is possible if the person in question is part of an organisation, listed as an organisation that can be the object of an interception.[409] The Belgian Minister of Defence has accepted this list. Consequently, the military service is allowed to infiltrate the cell phone to look for any information that could show a terrorist attack is being prepared.[410]

The military intelligence and security services also received the competence of disrupting and neutralising an information system *located abroad*. As was explained earlier, the military and civilian intelligence and security services' competences were, according to article 18/16 of the Belgian Law regulating the intelligence and security, broadened to the intrusion in an information system to intercept its communication. This competence was, however, limited to the mere intelligence gathering. For information systems located *abroad*, these military services have received an enlarged offensive competence.

According to Senior Captain BOMBEKE, the military intelligence services do not perpetrate offensive attacks but only stick to defensive actions.[411] This was also stated by the new head of the military intelligence services, PHILIPPE BOUCKÉ, who emphasised that offensive attacks were not yet perpetrated but that this would be developed in the future.[412]

197. Contrary to their military counterpart, the civilian intelligence and security services have not yet been assigned specific cyber-competences, apart from the previously mentioned exceptional investigative method. This method is, however, limited to mere intelligence gathering. As it currently stands, the civilian intelligence and security services do not have offensive cyber-competences.

198. The legal competence to disrupt and neutralise an information system is thus an exception to the crime of hacking, prohibited under articles 5 of the Cybercrime Convention, 4 of the Directive 2013/40/EU on attacks against information systems and 550*bis* of the Belgian Criminal Code. As explained earlier, these prohibitions exist when the system is intruded without right (at the Council of Europe and European Union level) or without being authorised

[409] Art. 44/3, 1st indent, 1° Belgian Law 8 regulating the intelligence and security services.
[410] Draft Bill 20 September 2016 modifying the Law of 30 November 1998 regulating the intelligence and security services and article 259*bis* Criminal Code, *Parl.St.* Kamer, 2015-2016, n° 54-2043/001, 7; C. VANDEVOORDE, "Les méthodes (particulières) de renseignement mises en oeuvre par le SGRS – De (bijzondere) inlichtingenmethoden ingezet door de ADIV", in J. VANDERBORGHT (eds.), *Bijzondere inlichtingenmethoden in de schijnwerpers – Les méthodes particulières de renseignement: de l'ombre à la lumière*, Brussel, Levebvre Sarrut Belgium NV, 2020, 45.
[411] Interview Senior Captain C. BOMBEKE, Senior Captain ADIV, 23 February 2021.
[412] K. CLERIX, "Militaire veiligheidsdiensten: De nieuwe topman Philippe Boucké zet de ADIV op scherp", *Knack* 24 February 2021 to 2 March 2021, Issue 8, https://www.knack.be/nieuws/belgie/nieuwe-topman-philippe-boucke-zet-adiv-op-scherp-willen-ook-offensieve-cyberoperaties-opzetten/article-longread-1704075.html.

to (at the Belgian level). Having a legal basis for intruding in the system, such as is the case with the Law regulating the intelligence and security services, neutralises this prohibition.

199. The Belgian legislator could go one step further and allow the military and civilian intelligence and security services to perpetrate a proactive and offensive cyber-attack on an in Belgium located terrorist's device to disable the use of that device. Hence, the person would not be able to access the information on the cell phone, which would complicate the perpetration of a terrorist attack or the online presence and propaganda.

2.4.1.4. Conclusion

200. Today, the civilian and military intelligence and security services, respectively the State Security Service and the General Intelligence and Security Service, are competent to intrude into the electronic device of a terrorist located on Belgian soil. Their competence is, nevertheless, limited to the intrusion and mere intelligence gathering. The military Intelligence and Security Service has received additional competences regarding terrorists' devices on foreign soil. The military service is allowed to disrupt and neutralise the information system located abroad. Hence, today, the intelligence and security services do not have the competence to perpetrate a cyber-attack or to disrupt and neutralise the information system of a terrorist's device located on Belgian soil. Consequently, they cannot disable the terrorist's access to the online world or to the information stored on the device, which could be used to perpetrate a terrorist attack or upload propaganda on social media platforms. The opportunity for the Belgian intelligence and security services to receive this competence will be analysed in the following part.

3. Proactive and offensive cyber-attacks on terrorists: a Belgian possibility?

201. Over the years, several countries have developed the capacity to orchestrate offensive cyber actions. The USA has, for example, developed offensive cybercrime capacities in different institutions, such as the army, the NSA, or the Cyber Command.[413] The UK as well has been a strong actor on the offensive cyber scene. UK's GCHQ[414] perpetrated impactful offensive cyber operations against the online recruitment of ISIL.[415] Moreover, the UK created in November 2020 a new cyber department, the National Cyber Force, which is entrusted with perpetrating offensive cyber operations. As such, it can disrupt a terrorist's cell phone to prevent the person from communicating with others.[416] Israel and Russia have also developed similar capabilities.[417] The question arises whether it would be opportune for Belgium to designate a department competent for perpetrating offensive cyber-attacks on devices of terrorists on Belgian soil. This department would be competent to disable access to a device or destroying the information it contains.

202. Now that has been established that the Belgian legislation, as it currently stands, does not provide the possibility of perpetrating proactive and offensive cyber-attacks to disable the access to a terrorist's device or destroy the data it contains to limit ISIL's online presence and propaganda, the legitimacy of perpetrating such cyber-attacks will be analysed (3.1.). Afterwards, several recommendations for a Belgian law authorising the perpetration of cyber-attacks on terrorists located on Belgian soil will be provided (3.2.).

[413] M. YAR and K. F. STEINMETZ, *Cybercrime and Society*, 3rd ed., California, Sage Publications, 2019, 100.
[414] The British Government Communications Headquarters (GCHQ) are the British intelligence services that handle intelligence, cyber and security. For more information about this agency, see GCHQ, "Overview", https://www.gchq.gov.uk/section/mission/overview.
[415] GCHQ, *GCHQ Director Jeremy Fleming's speech at Cyber UK 2018*, 12 April 2018, https://www.gchq.gov.uk/speech/director-cyber-uk-speech-2018; X, "UK launched cyber-attack on Islamic State", *BBC News* 12 April 2018, https://www.bbc.com/news/technology-43738953.
[416] GCHQ, *National Cyber Force transforms country's cyber capabilities to protect the UK*, 19 November 2020, https://www.gchq.gov.uk/news/national-cyber-force.
[417] M. YAR and K. F. STEINMETZ, *Cybercrime and Society*, 3rd ed., California, Sage Publications, 2019, 100.

3.1. Proactive and offensive cyber-attacks in Belgium: a legitimate option?

203. As was discussed in the first part of this dissertation, terrorists' right to freedom of expression can be restricted when amounting to hate speech.[418] Does this, however, mean that perpetrating proactive and offensive cyber-attacks to disable access to devices or information stored on the devices is the correct answer?

204. The absence of a robust Belgian authority capable of launching direct cyber-attacks on ISIL supporters is not only worrisome in the context of their online propaganda. This lacuna will become very apparent in light of potential future cyber-terrorist attacks.

205. The legislator's choice to either invest the judicial police and public prosecutor or the intelligence and security services with the competence of perpetrating proactive and offensive cyber-attacks is consequently essential. Granting the judicial police and the public prosecutor with such a competence would fall outside of the scope of their public role. Allowing the judicial police to perpetrate such cyber-attacks would allocate them competences that transgress the limit of their public purpose of investigating, gathering evidence and handing over criminals to the courts. Legally authorising the public prosecutor to enable such attacks would entail surpassing its competence of investigating and prosecuting. Consequently, the judicial police and public prosecutor cannot be granted this competence in the current state of the law.

The intelligence and security services, and more specifically the military services, are already entrusted with offensive cyber-operations. Hence, these services seem optimal for this competence. It appears opportune for these services to develop, as the Belgian minister of Defence, L. DEDONDER proposed in her Policy Statement of Defence, a fifth component, a cyber-component, co-existing with the land, air, marine and medical component.[419]

206. Over the years, the securitarian discourse, which is to protect the Belgian citizens against terrorist attacks, has increased. Many measures have been adopted which are to protect the Belgian population against such attacks. This increase in securitarian measures has consequently led to a restriction of the fundamental rights of the citizens. Granting this competence to the state could also constitute a grave danger to the right to freedom of expression of the alleged terrorist. As was presented at the beginning of this dissertation, the 'terrorist' label can be allocated to a legitimate political opponent. Can proactive and offensive

[418] *Cf. supra* 4. The fundamental right to freedom of expression in the discussion of combatting terrorism online (n° 46-60).
[419] DEFENSIE, "Over Defensie – Onze Componenten", https://www.mil.be/nl/over-defensie/; DEDONDER, L., Policy Statement of Defence of 4 November 2020, *Parl.St.* Kamer 2020-2021, n° 55-1610/017, 25.

cyber-attacks that destroy a person's cell phone or computer be legitimised in the context of terrorism?[420]

207. The first criterium that has to be fulfilled to be considered a legal restriction on the right to freedom of expression is the existence of a legal basis. Restricting people's right to express their opinion on terrorism, such as by promoting the values of ISIL or sharing videos in which ISIL beheads opponents, should be provided by a clear law. If a law granted the intelligence and security services the power to restrict the terrorist's right to freedom of expression by disabling their access to their device or the information stored on the device, these practices would have a legal basis. The law should be written clearly, be foreseeable and published in the Belgian Gazette to be accessible to the public. Hence, the first criterium of legality would be fulfilled. However, the vagueness surrounding the notion of terrorism could be considered an obstacle to the law being 'sufficiently clear'.

208. The second criterium to be fulfilled is the legitimacy of the measure. The measure taken should pursue one of the legitimate aims enumerated in the limitation clause of article 10.2 of the ECHR. As such, perpetrating offensive cyber operations to disable the access or delete the information stored on a terrorist's device unquestionably fits the legitimate aim of wanting to protect national security, territorial integrity or public safety and the prevention of disorder or crime. Hence, the operation would be legitimate.

209. The third criterium of the analyse is the 'necessity in a democratic society' test, which constitutes a more complex analysis in this context. This test, or also known as the proportionality assessment, will be divided into three parts: the suitability, necessity and proportionality *sensu stricto*.

The suitability of a measure refers to whether the measure taken is appropriate to attain the "*objectives legitimately pursued*"[421]. The measure, which restricts the fundamental rights, must thus be pertinent in light of the aim pursued. Perpetrating such offensive cyber-attacks is a suitable measure to limit the terrorist's access to information stored on the device. However, disabling access of a terrorist to one device will not hinder the person from buying a new device or logging into an account from another device. Hence, this measure might work in the short run, but this might again lead to a 'whack-a-mole' figure in the long run.

This first sub-requirement is linked to the second, the necessity of a measure. This necessity refers to "*a pressing social need*" to employ this specific measure. The measures taken to attain the objective legitimately pursued should be the least restrictive, meaning that if several measures can be taken to achieve the aim pursued, the least intrusive on the rights of the persons

[420] The following analysis is based on the restriction clause of article 10.2 of the ECHR.
[421] S. DE COENSEL, *Counter-Terrorism and Criminal Law. A Normative Legitimacy Test of Terrorism-Related Offences on Expression, Information and Movement*, Antwerp, Maklu, 2020, 125.

concerned should be chosen. However, the necessity of perpetrating proactive and offensive cyber operations that would destroy the person's device or information stored on the device is questionable since less restrictive measures on the freedom of expression of the alleged terrorist exist. As such, the notice-and-takedown or the recourse to counter-narratives exist to diminish the online presence of ISIL. Nevertheless, these measures do not seem to be sufficient since the online presence and content resurfaces quickly. It might thus appear necessary today to take a more aggressive and offensive stance.

Accepting that such a cyber-attack would be necessary, and that no less restrictive measures exist, the proportionality *sensu stricto* of such a technique would be even more questionable. The proportionality *sensu stricto* refers to the idea that "*the means adopted should not impose an excessive burden on the individual*"[422]. This requirement implies that the consequences of the restriction on the person's rights concerned should not be disproportionate regarding the advantages the state has in adopting the measure. The measure seems to be disproportionate in light of the significant efforts the state would currently have to put into perpetrating a cyber-attack on one presumed terrorist fighter and the benefit of having disabled (temporarily) the person's access to the information stored on the device. In order to be capable of performing such cyber-attacks, the state has to invest in personnel, equipment, knowledge and technology. The investment seems disproportionate to the possibility for the terrorist to quickly buy a new cell phone or computer and re-access the information.

210. From the previous analysis, it can be concluded that, keeping in mind that the Belgian offensive cyber capabilities are not sufficiently developed yet[423] and the lacunae in the law, the perpetration of offensive and proactive cyber-attack on a terrorist's device, located in Belgium would be a disproportionate measure. Today, the intelligence and security services might have a more considerable interest in cooperating with other countries with a more robust offensive cyber capacity whilst taking the time to develop their own cyber capacities steadily. Once the Belgian intelligence and security services will have closed the gaps of the defensive cyber-wall, it will be ready for complementary offensive cyber-capacities.

[422] *Ibid.*, 125.

[423] From the discussion conducted with the ADIV, it appeared they are not ready yet to perpetrate offensive attacks. They currently rather want to focus on defensive competences. Moreover, the Belgian Minister of Defence L. DEDONDER expressed her wish to further develop and strengthen the cyber-capacity of the military intelligence and security services in her Policy Statement of Defence of 4 November 2020, *Parl.St.* Kamer 2020-2021, n° 55-1610/017, 25.

3.2. Recommendations for a Belgian law authorising the perpetration of cyber-attacks on terrorists on Belgian soil

211. Once the intelligence and security services will have further developed their cyber-competences, the Belgian law will have to be adapted to include the possibility of perpetrating offensive cyber-attacks. Should the Belgian legislator decide to adopt a new law allowing the proactive and offensive cyber-attacks on alleged terrorist fighters on Belgian soil to limit their access to the online environment or to the information stored on their device, the legislator will have to take into account the European Essential Guarantees for Surveillance Mechanisms. Four European Essential Guarantees have to be taken into account:

(1) "*Processing should be based on clear, precise and accessible rules*
(2) *Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated*
(3) *An independent oversight mechanism should exist*
(4) *Effective remedies need to be available to the individual*"[424]

212. These four principles will be used to guide the recommendations for a Belgian legislative intervention, should the Belgian legislator decide to grant this competence to the intelligence and security services.

3.2.1. Recommendation 1: the need for clear, precise and accessible rules

213. According to J. RAES, the head of the civilian intelligence and security services, the joint memorandum of the State Security Service and the General Intelligence and Security Service as preparation and support for the following federal governmental agreement pleads for a modification of the regime of punishable acts posed by the intelligence and security services. The services request the government to extend the possibility for intelligence services, which already exists for the police and judicial branches, to commit punishable acts in the context of their intelligence work. Taking as an example the further proliferation of propaganda by ISIL in private channels on social media platforms, the memorandum pleads for the adaptation of the Belgian law to extend the possibility of perpetrating punishable acts, such as spreading terrorist content to be invited in such channels. The possibility to do so already exists

[424] EUROPEAN DATA PROTECTION BOARD, *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, 10 November 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_nl, 8.

but under stringent circumstances and is thus very rarely used.[425] Since hacking is a punishable offence, allowing intelligence and security services to commit this punishable offence would be desirable.

214. It is not clear, however, whether the evolving technologies and the proactive and offensive use of these techniques fall under the current legislative framework[426]. Therefore, it seems required to adopt a new law or adapt the existing Belgian Law regulating the intelligence and security services to include these new offensive competences and secure the fundamental rights of alleged terrorists with strong barriers. As such, when performing such a cyber-attack, there can be no doubt about the qualification of the person as a terrorist.

Two possible legislative interventions can be envisaged. First, the Belgian legislator could complement the competences of both the civilian and military intelligence and security services, respectively in articles 7 and 11 of the Belgian Law regulating the intelligence and security services to include the possibility of intruding into an information system of an alleged terrorist present on the Belgian soil and destroying the data it contains, for example by infecting the system with malware. In doing so, the software would be attacked.

The second possibility for the Belgian legislator is to invest the civilian and military intelligence and security branches with the competence, equally provided in articles 7 and 11 of the aforementioned law, of intruding in the information system of the presumed terrorist located on the Belgian soil and freeze its functioning. Hence, the terrorist will not be able to access the information stored on the device, nor will the device have any utility since it will be frozen. Consequently, the hardware would be affected.

215. These two competences would constitute an exception to the crimes of intruding in (art. 550*bis* Belgian Criminal Code) and sabotaging (art. 550*ter* Belgian Criminal Code) an information system. The intelligence and security services would be allowed to commit these punishable offences. Since a legal basis would allow this perpetration, the competence would be in line with the Council of Europe[427] and the European Union[428] 'with right' requirement of cyber-attacks.

[425] J. RAES, "De inzet van bijzondere inlichtingenmethoden door de VSSE: Behaalde resultaten en pistes voor de toekomst", in J. VANDERBORGHT (eds.), *Bijzondere inlichtingenmethoden in de schijnwerpers – Les méthodes particulières de renseignement: de l'ombre à la lumière*, Brussel, Levebvre Sarrut Belgium NV, 2020, 37-38.
[426] T. WETZLING, "Challenges for oversight", in J. VANDERBORGHT (eds.), *Bijzondere inlichtingenmethoden in de schijnwerpers – Les méthodes particulières de renseignement: de l'ombre à la lumière*, Brussel, Levebvre Sarrut Belgium NV, 2020, 94.
[427] *Cf. supra* n° 169.
[428] *Cf. supra* n° 173.

3.2.2. Recommendation 2: the necessity and proportionality regarding the legitimate objectives pursued need to be demonstrated

216. The necessity and proportionality to the legitimate objectives pursued have been discussed previously.[429] Should the Belgian legislator not agree with the analysis and consider the cyber-attacks necessary and proportionate, the following recommendations regarding the need for an independent oversight mechanism and effective remedies can be taken into account.

3.2.3. Recommendation 3: the need for an independent oversight mechanism

217. Since this complementary competence would imply a very severe breach of the person's rights, a strict supervisory mechanism should be provided. The Committee R/I seems optimal for this responsibility since it already is entrusted with the oversight of these two intelligence and security branches.

3.2.4. Recommendation 4: the need for effective remedy mechanisms

218. The Belgian law relating to security and intelligence services already provides a complaint mechanism for every person able to show a personal and legitimate interest in the claim. The Committee R/I can intervene following such a written complaint, containing the specific griefs.[430] If the Committee R/I concludes with the irregularity of the intelligence methods, the Committee will put a halt to its use. The intelligence gathered irregularly can then not be used afterwards.[431] No appeals procedure to the decision of the Committee R/I is possible.[432]

219. This remedy mechanism could be applied to the proposed legislative modification.

[429] *Cf. supra* n° 209.
[430] Art. 43/4, 1st indent Belgian Law regulating the intelligence and security services.
[431] Art. 43/6, §1 Belgian Law regulating the intelligence and security services.
[432] Art. 43/8 Belgian Law regulating the intelligence and security services.

Conclusion

Portrayed as a ‘cyber-attack’, the removal of online terrorist content by Europol and the Member States during the action days of November 2019 on ISIL’s news channel Amaq is legally not qualified as such. This was a referral of terrorist content to social media platforms by, amongst others, the European Union Internet Referral Units, followed by the removal of that content because deemed contrary to the Terms and Conditions of the social media platform. If performed correctly, this notice-and-takedown mechanism exempts the service providers of liability for the content published on their platform.

This mechanism is, however, too vague and unclear. Given their role in the public debate, it seems legitimate that social media providers have a growing responsibility for the content stored on their platforms. The voluntary Code of Conduct and the recent Regulation on addressing the dissemination of terrorist content online were laudable efforts to sharpen and update the notice-and-takedown mechanism. However, the absence of sanction enforcement, transparency and involvement of civil society organisations and the potential restriction of legitimate speech indicate that this Code of Conduct was a mere reputational effort, empty of genuine commitment. The cross-border removal orders, the one-hour removal rule, and the implicitly encouraged recourse to automated tools introduced by the Regulation open the path towards censorship, disproportionately burden the providers, constitute a threat to freedom of expression of these users and flirt with the prohibition to impose a general monitoring obligation on the platforms.

Consequently, it is questionable whether the Regulation attains its objective of providing more legal certainty to the social media platforms and ensuring their users’ freedom of expression. The Regulation could also have been the perfect instrument for the European Union to be a pioneer for adopting a universally accepted definition of the notion of ‘terrorism’. However, the European penholders missed this opportunity to sharpen the line that distinguishes political opponents from terrorists.

It is unquestionably necessary today to reduce ISIL’s online presence as much and as fast as possible. The responsibility and liability that accompanies countering terrorism have slid over the years from the state towards private actors. Social media platforms become a proxy for the government to enforce the government’s legal obligations to combat terrorism and terrorism propaganda. This shift implies that private social media platforms are regulating the freedom of expression of their users. This privatised law enforcement is problematic because, on the one hand, private actors are entrusted with the public role of enforcing the law and, on the other hand, they have to weigh the compliance with their legal obligations against respecting the fundamental rights of their users. Moreover, the private service providers’ interests conflict

with their legal obligations. As such, violent content, such as terrorist content, attracts more views and is thus financially more interesting. Leaving this violent content on the platform to increase profits is, however, contrary to their legal obligations. The incentive to use automated tools because it increases the efficiency of takedowns disregards the context and subtleties of online content. Relying on AI creates a risk of false positives, false negatives and inherent biases in the algorithms and endangers the freedom of expression of the platform's users.

Hence, private actors have to step in where public authorities leap behind. However, these private actors are not in an optimal position to fulfil the state's legal obligations. It is time the state took back its responsibility. The Belgian state could reclaim this responsibility to fight ISIL's online presence by perpetrating offensive and proactive cyber-attacks on the devices of its supporters in Belgium. As such, it could prevent them from sharing terrorist content by disrupting and neutralising the information system. Contrary to the USA or UK, the Belgian authorities cannot yet perpetrate such attacks. Granting the judicial police and public prosecutor this competence would fall outside of the scope of their public role of investigating breaches of the law, gathering evidence, handing over trespassers of the law and prosecuting them. Consequently, the judicial police and public prosecutor do not seem to be the optimal authority for such an offensive competence. The military and civilian intelligence and security services, on the other hand, are competent to intrude in an information system to intercept its communication, which is, nevertheless, limited to mere intelligence gathering. The military intelligence and security services can also perpetrate defensive cyber-attacks, orchestrate offensive cyber-attacks in the context of the Law of Armed Conflict, which does not apply to the current fight in Belgium against ISIL propaganda, or disrupt and neutralise an information system *located abroad*. Hence, these services are not competent to perpetrate offensive and proactive cyber-attacks on devices of its supporters in Belgium to disable their access to information stored on the devices. Nevertheless, granting them this competence does not appear to be legitimate yet. Such cyber-attacks would imply a restriction on the right to freedom of expression of the terrorist concerned since the person would not be able to share the (terrorist) information stored on their device. When amounting to hate speech, this fundamental right can be restricted. Even though the restriction seems legal if provided by a new Belgian law or by an adaptation of the existing Law regulating the intelligence and security services, and the measure appears legitimate, the restriction of the person's freedom of expression seems disproportionate compared to the advantages the state would gain. Especially the proportionality *sensu stricto*, considering the significant efforts the state would have to invest in developing such capacities compared to the temporarily disabled access to the information, do not seem fulfilled.

As the cyber-capacities and the legal framework of the intelligence and security services currently stand, it does not seem desirable to grant this competence to those services yet. It appears more appropriate to first invest in the defensive cyber-capacity of these services and

cooperate with other countries with a more robust offensive cyber capacity to learn from their experience. Once the cyber-capacities of these services will extensively have been developed, it might be opportune for the legislator to grant them this offensive competence.

Should the legislator wish to grant this competence to these services, articles 7 and 11 of the Belgian Law regulating the intelligence and security services should include the competence of intruding into an information system of an alleged terrorist present on the Belgian soil to either destroy the data it contains or freeze the functioning of the device. This competence should be framed as an exception to the Belgian criminalisation of intruding in and sabotaging an information system. Furthermore, the necessity and proportionality regarding the legitimate objectives pursued will have to be demonstrated. Last, the Committee R/I should be designated as the independent oversight body that is also entrusted with hearing complaints.

Are offensive and proactive cyber-attacks the solution to the online presence of ISIL? The current notice-and-takedown procedure seems insufficient to combat ISIL's online presence. Combining this mechanism with offensive and proactive cyber-attacks can be the solution to eradicate the online presence of ISIL. Today, the Belgian authorities, however, do not seem ready yet to orchestrate such cyber-attacks on online terrorist content. Once the intelligence and security services will have acquired extensive cyber-capacities, strengthened their current cyber-competences, deepened their cyber-knowledge and established a fifth military cyber-component, it will be the legislator's task to draw out their sharpest pen to dive into the difficult task of attributing additional cyber-competences to these authorities.

Bibliography

1. Legislation

1.1. International law

International Covenant on Civil and Political Rights of 16 December 1966, *United Nations Treaty Series*, Vol. 999, 1.

Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of 12 August 1949, *United Nations Treaty Series*, Vol. 75, 31.

Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I) of 8 June 1977, *United Nations Treaty Series*, Vol. 1125, 3.

Resolution 1963 of the Security Council of the United Nations (20 December 2010), *UN Doc.* S/RES/1963 (2010).

Resolution 60/288 of the General Assembly of the United Nations on The United Nations Global Counter-Terrorism Strategy (8 September 2006), *UN Doc.* A/RES/60/288 (2006).

Resolution 1556 of the Security Council of the United Nations (30 July 2004), *UN Doc.* S/RES/1566 (2004).

1.2. Council of Europe law

Convention of the Council of Europe on the Prevention of Terrorism of 16 May 2005, *CETS*, n° 196.

Convention on Cybercrime of 23 November 2001, *ETS*, n° 185.

Convention of the Council of Europe on the Suppression of Terrorism of 27 January 1977, *ETS*, n° 90.

European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950, *ETS*, n° 5.

1.3. European Union law

EU Charter of Fundamental Rights, *OJ C* 26 October 2012, n° 326, 391.

Treaty on the Functioning of the European Union, *OJ L* 26 October 2007, n° 326, 1.

Regulation of the European Parliament and of the Council on addressing the dissemination of terrorist content online, 29 April 2021, PE-CONS 19/21 - 2018/0331 (COD) (unpublished).

Regulation 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, *OJ L* 24 May 2016, n° 135, 53.

Directive 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* 31 March 2017, n° 88, 6.

Directive 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, *OJ L* 17 September 2015, n° 241, 1.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, *OJ L* 14 August 2013, n° 218, 8.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), *OJ L* 17 July 2000, n° 178, 1.

Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, *OJ L* 6 December 2008, n° 328, 55.

Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, *OJ L* 22 June 2002, n° 164, 3.

Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15 December 2020, COM (2020) 825 final - 2020/0361 (COD).

Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15 December 2020, COM (2020) 842 final, 2020/0374 (COD).

Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, 12 September 2018, COM (2018) 640 final – 2018/0331 (COD).

European Commission Recommendation 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, C/2018/1177, *OJ L* 6 March 2018, n° 63.

Code of Practice on Disinformation of the European Commission, September 2018, https://ec.europa.eu/digital-single-market/en/code-practice-disinformation.

Code of Conduct on countering illegal hate speech online of the European Commission and IT Companies, 31 May 2016, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en.

1.4. Belgian law

Code of Criminal Law.

Code of Criminal Procedure.

Code of Economic Law.

Belgian Law 30 March 2017 modifying the Law of 30 November 1998 regulating the intelligence and security services and article 259*bis* Criminal Code, *Belgian Gazette* 28 April 2017, 53.768.

Belgian Law 4 February 2010 regarding the methods for the collection of intelligence by the intelligence and security services, *Belgian Gazette* 10 March 2010, 14.916.

Belgian Law 30 November 1998 regulating the intelligence and security services, *Belgian Gazette* 18 December 1998, 40.312.

Belgian Law 30 July 1981 criminalising certain acts inspired by racism or xenophobia, *Belgian Gazette* 8 August 1981, 9.928.

Draft Bill 20 September 2016 modifying the Law of 30 November 1998 regulating the intelligence and security services and article 259bis Criminal Code, *Parl.St.* Kamer, 2015-2016, n° 54-2043/001.

1.5. Other official documents

1.5.1. International official documents

HIGH COMMISSIONER FOR HUMAN RIGHTS, *UN Factsheet 32 - Human Rights, Terrorism and Counter-Terrorism*, July 2008, https://www.ohchr.org/documents/publications/factsheet32en.pdf.

HUMAN RIGHTS COMMITTEE, *General Comment No. 34 on Article 19: Freedoms of opinion and expression*, 12 September 2011, CCPR/C/GC/34 (2011).

INTERNATIONAL COMMITTEE FOR THE RED CROSS, *Report: International humanitarian law and the challenges of contemporary armed conflicts*, 32nd International Conference of the Red Cross and Red Crescent, Geneva, October 2015, https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts.

UNITED NATIONS (UN) SPECIAL RAPPORTEUR ON FREEDOM OF OPINION AND EXPRESSION, THE ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE (OSCE) REPRESENTATIVE ON FREEDOM OF THE MEDIA, THE ORGANIZATION OF AMERICAN STATES (OAS) SPECIAL RAPPORTEUR ON FREEDOM OF EXPRESSION AND THE AFRICAN COMMISSION ON HUMAN AND PEOPLES' RIGHTS (ACHPR) SPECIAL RAPPORTEUR ON FREEDOM OF EXPRESSION AND ACCESS TO INFORMATION, *Joint Declaration on freedom of expression and countering violent extremism*, 4 May 2016, https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=19915&LangID=E.

NORTH ATLANTIC TREATY ORGANIZATION, *Allied Joint Doctrine for the Conduct of Operations of February 2019*, ed. C, Version 1, 1.14.

SECRETARY-GENERAL OF THE UN, *Note by the Secretary-General on the Promotion and protection of the right to freedom of opinion and expression* (29 August 2018), *UN Doc.* A/73/348 (2018).

SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION AND THE SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS WHILE COUNTERING TERRORISM, *Recommendations on the new draft 'Regulation on preventing the dissemination of Terrorism Content Online'*, 3 November 2020, https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=25661.

STOLTENBERG, J., *Press conference by NATO Secretary-General Jens Stoltenberg following the meetings of NATO Defence Ministers*, 4 October 2018, https://www.nato.int/cps/en/natohq/opinions_158705.htm?selectedLocale=en.

UNITED NATIONS GENERAL ASSEMBLY, "General Assembly Adopts Decision Postponing Organizational Session of Ad Hoc Committee Elaborating Anti-Cybercrime Convention, Due to COVID-19 Fears" (Meetings Coverage) (15 January 2021), *UN Doc. GA/12309*, https://www.un.org/press/en/2021/ga12309.doc.htm.

1.5.2. Official documents of the Council of Europe

ARTICLE 36 COMMITTEE OF THE COUNCIL OF THE EUROPEAN UNION, *Council Conclusions on cooperation to combat terrorist use of the Internet ("Check the Web")*, 29 May 2007, n° 8457/3/07, https://data.consilium.europa.eu/doc/document/ST%208457%202007%20REV%203/EN/pdf.

COMMISSIONER FOR HUMAN RIGHTS OF THE COUNCIL OF EUROPE, *The rule of law on the internet and in the wider digital world*, Strasbourg, Council of Europe, 2014.

COMMITTEE OF MINISTERS OF THE COUNCIL OF EUROPE, *Declaration on freedom of communication on the Internet*, 28 May 2003, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805dfbd5.

COUNCIL OF EUROPE, *Explanatory Report to the Convention on Cybercrime*, *ETS* 23 November 2001, n° 185.

ECTHR, *Factsheet – Hate Speech*, September 2020, https://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf.

1.5.3. Official documents of the European Union

ARTICLE 29 WORKING PARTY, *Opinion 5/2009 on online social networking*, 12 June 2009, WP 163, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf.

COUNCIL OF EUROPE, *Explanatory Report to the Council of Europe Convention on the Prevention of Terrorism*, *CETS* 16 May 2005, n° 196.

DE STREEL, A., DEFREYNE, E., JACQUEMIN, H., LEDGER, M. and MICHEL, A., *Online Platforms' Moderation of Illegal Content Online: Law, Practices and Options for Reform,* June 2020, PE 652.718, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL_STU(2020)652718_EN.pdf.

DIRECTORATE GENERAL FOR INTERNAL POLICIES, POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS, *Countering Terrorist Narratives*, 2017, PE 596.829, https://openaccess.leidenuniv.nl/bitstream/handle/1887/62312/Reed-Ingram-Whittaker-Narratives.pdf?sequence=1.

EU INTERNET REFERRAL UNIT, *Online jihadist propaganda: 2019 in review*, 28 July 2020, https://www.europol.europa.eu/newsroom/news/online-jihadist-propaganda-2019-in-review.

EU INTERNET REFERRAL UNIT, "EU law enforcement and judicial authorities join forces to disrupt terrorist propaganda online" (Press Release), 25 November 2019, https://www.europol.europa.eu/newsroom/news/eu-law-enforcement-and-judicial-authorities-join-forces-to-disrupt-terrorist-propaganda-online.

EUROPEAN COMMISSION, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Tackling illegal content online – Towards an enhanced responsibility of online platforms*, 28 September 2017, COM (2017) 555 final.

EUROPEAN COMMISSION, "EU Internet Forum: a major step forward in curbing terrorist content on the internet" (Press release), 8 December 2016, https://ec.europa.eu/commission/presscorner/detail/en/IP_16_4328.

EUROPEAN COMMISSION, "EU Internet Forum: progress on removal of terrorist content online" (Press release), 10 March 2017, http://europa.eu/rapid/press-release_IP-17-544_en.htm.

EUROPEAN COMMISSION, *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*, 30 September 2020, COM (2020) 619 final.

EUROPEAN COMMISSION, *Staff Working Document on Online Services, Including e-Commerce, in the Single Market, accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A coherent framework to boost confidence in the Digital Single Market of e-commerce and other online services*, 11 January 2011, COM (2011) 942 final.

EUROPEAN DATA PROTECTION BOARD, *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, 10 November 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_nl.

EUROPEAN DATA PROTECTION SUPERVISOR, *Formal comments on the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online*, 12 February 2019, https://edps.europa.eu/sites/edp/files/publication/2018-02-13_edps_formal_comments_online_terrorism_regulation_en.pdf.

EUROPEAN PARLIAMENT, "New rules adopted for quick and smooth removal of terrorist content online" (Press release), 29 April 2021, https://www.europarl.europa.eu/news/nl/press-room/20210422IPR02621/new-rules-adopted-for-quick-and-smooth-removal-of-terrorist-content-online.

EUROPOL, *Changes in Modus Operandi of Islamic State (IS) Revisited*, November 2016, https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited.

EUROPOL, *European Union Terrorism Situation and Trend Report 2020*, 23 June 2020, TE-SAT 2020, https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020.

1.5.4. Belgian official documents

Committee I/R, Activiteitenverslag 2019, https://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2019.pdf.

Committee I/R, Activiteitenverslag 2018, https://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2018.pdf.

Committee I/R, Activiteitenverslag 2017, https://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2017.pdf.

DEDONDER, L., Policy Statement of Defense of 4 November 2020, *Parl.St.* Kamer 2020-2021, n° 55-1610/017.

1.5.5. Official documents of other countries

GCHQ, *GCHQ Director Jeremy Fleming's speech at Cyber UK 2018*, 12 April 2018, https://www.gchq.gov.uk/speech/director-cyber-uk-speech-2018.

GCHQ, *National Cyber Force transforms country's cyber capabilities to protect the UK*, 19 November 2020, https://www.gchq.gov.uk/news/national-cyber-force.

2. Case-law

2.1. Case-law of the International Criminal Tribunal for the former Yugoslavia

ICTY (Trial Ch. I) 3 April 2008, n° IT-04-84-T, *The Prosecutor v. Ramush Haradinaj et al.*

ICTY (Appeals Ch.) 2 October 1995, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, n° IT-94-1-AR72, *The Prosecutor v. Dusko Tadić*.

2.2. Case-law of the European Court of Human Rights

ECtHR 10 September 2018, n° 13237/17, *Mehmet Hasan Altan v. Turkey.*

ECtHR 20 June 2018, n° 16538/17, *Şahin Alpay v. Turkey*.

ECtHR 27 July 2017, n° 34367/14, *Fouad Belkacem v. Belgium*.

ECtHR 2 May 2016, n° 22947/13, *MTE v. Hungary*.

ECtHR 10 October 2013, n° 64569/09, *Delfi AS v. Estonia*.

ECtHR 16 July 2009, n° 10883/05, *Willem v. France*.

ECtHR 11 July 2006, n° 71343/01, *Brasilier v. France.*

ECtHR 28 June 2001, n° 24699/94, *Verein Gegen Tierfabriken v. Switzerland*.

ECtHR 8 July 1999, n° 26682/95, *Sürek v. Turkey*.

ECtHR 25 November 1996, n° 14719/90, *Wingrove v. UK.*

ECtHR 7 December 1976, n° 5493/72, *Handyside v. UK.*

2.3. Case-law and Opinions of the Advocate-General of the Court of Justice of the European Union

CJEU (3rd Ch.) 3 October 2019, C-18/18, ECLI:EU:C:2019:821, *Eva Glawischnig-Piesczek v. Facebook Ireland Limited*.

CJEU (2nd Ch.) 8 September 2016, C-160/15, ECLI:EU:C:2016:644, *GS Media BV v. Sanoma Media Netherlands BV.*

CJEU (7th Ch.) 11 September 2014, C-19/13, ECLI:EU:C:2014:2209, *Sotiris Papasavvas v. O Fileleftheros Dimosia Etairia Ltd*.

CJEU (3rd Ch.) 16 February 2012, C-360/10, ECLI:EU:C:2012:85, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*.

CJEU (3rd Ch.) 24 November 2011, C- 70/10, ECLI:EU:C:2011:771, *Scarlet v. SABAM.*

CJEU (Grand Ch.) 12 July 2011, C-324/09, ECLI:EU:C:2011:474, *L'Oréal SA v. eBay International AG*.

CJEU (Grand Ch.) 23 March 2010, Joined Cases C-236/08 to C-238/08, ECLI:EU:C:2010:159, *Google France SARL v. Louis Vuitton Malletier SA.*

Opinion Advocate General JÄÄSKINEN of 9 December 2010, C-324/09, ECLI:EU:C:2010:757, *L'Oréal SA v. eBay International AG.*

2.4. Case-law of the Belgian Courts

Cass. 18 January 2011, *NC* 2011, 84, concl. DE SWAEF.

2.5. Case-law of other countries

Court of Appeals (USA), Northern District of California (9th Circuit), 5 May 2019, n° 18-16700, *Reynaldo Gonzalez v. Google LLC.*

3. Literature

3.1. Books

BENEDEK, W. and KETTEMANN, M. C., *Freedom of expression and the Internet*, Strasbourg, Council of Europe Publishing, 2013, 194 p.

BOOTHBY, W. H., *The Law of Targeting*, 1st ed., Oxford, Oxford University Press, 2012, 652 p.

COMMITTEE I/R, "Bijlage D: De aanbevelingen van het vast Comité I (2006-2016)", *Activiteitenrapport 2017*, Antwerpen, Intersentia, 2018, 152 p.

DE COENSEL, S., *Counter-Terrorism and Criminal Law. A Normative Legitimacy Test of Terrorism-Related Offences on Expression, Information and Movement*, Antwerp, Maklu, 2020, 399 p.

DUFFY, H., *The 'war On Terror' and the Framework of International Law*, 2nd ed., Cambridge, Cambridge University Press, 2015, 993 p.

EECHAUTE, H., *Non-international armed conflict: a trigger for the rules on targeting?*, Master Thesis Law UGent, 2016, https://lib.ugent.be/fulltxt/RUG01/002/272/228/RUG01-002272228_2016_0001_AC.pdf, 129 p.

FERNANDEZ, M. and ALANI, H., "Artificial Intelligence and Online Extremism: Challenges and Opportunities", in J. MCDANIEL and K. PEASE (eds.), *Predictive Policing and Artificial Intelligence*, London, Routledge, 2021, http://oro.open.ac.uk/69799/1/Fernandez_Alani_final_pdf.pdf, 330 p.

GILLESPIE, A. A., *Cybercrime: Key Issues and Debates*, 2nd ed., London, Routledge, 2019, 381 p.

JONES, D. M., SCHULTE, P., UNGERER, C., and SMITH, M. L. R., *Handbook of terrorism and counter terrorism post 9/11*, Northampton, Edward Elgar Publishing, 2019, 447 p.

JØRGENSEN, R. F., *Human rights in the age of platforms*, Cambridge, The MIT Press, 2019, 392 p.

JØRGENSEN, R. F. and PEDERSEN, A. M., "Chapter 10 - Online Service Providers as Human Rights Arbiters", in M. TADDEO and L. FLORIDI (eds.), *Law, Governance and Technology*

Series, Vol. 31, *The Responsibilities of Online Service Providers*, Switzerland, Springer, 2017, 179-199.

KUCZERAWY, A., *Intermediary Liability and Freedom of Expression in the EU: from concepts to safeguards*, Mortsel, Intersentia, 2018, 426 p.

LASOEN, K., *Geheim België – Geschiedenis van de inlichtingendiensten 1830-2020*, Tielt, Lannoo, 2020, 412 p.

MELZER, N., *Cyberwarfare and International Law*, *UNIDIR Resources*, 2011, https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf , 38 p.

MELZER, N., *Interpretative guidance on the notion of direct participation in hostilities under international humanitarian law*, Geneva, 2009, 88 p.

PODSTAWA, K., "Hybrid Governance or… Nothing? The EU Code of Conduct on Combating Illegal Hate Speech Online", in E. CARPANELLI and N. LAZZERINI (eds.), *Use and Misuse of New Technologies*, Switzerland, Springer, 2019, 167-184.

QUINTEL, T. and ULLRICH, C., "Self-Regulation of Fundamental Rights? The EU Code of Conduct on Hate Speech, related initiatives and beyond", in B. PETKOVA and T. OJANEN (eds.), *Fundamental Rights Protection Online: The Future Regulation of Intermediaries*, Northampton, Edward Elgar Publishing, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3298719, 21 p.

SCHMITT, M. N., *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations*, 2nd ed., Cambridge, Cambridge University Press, 2017, 598 p.

SWISS INSTITUTE OF COMPARATIVE LAW, *Legal instruments for combating racism on the internet*, Council of Europe Publishing, 2009, 175 p.

TROMMEL, J., *Online jihadi content combat: How serving public interest could ease the privatization of freedom of expression*, Master Thesis Crisis and Security Management (MSc) Leiden University, 2018, https://openaccess.leidenuniv.nl/bitstream/handle/1887/84031/Trommel_CSM_2018.pdf?sequence=1, 87 p.

UNODC, *The use of the Internet for terrorist purposes*, Austria, United Nations publications, 2012, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf, 142 p.

VAN DAELE, D. and MERGAERTS, L., *Naar een herijking van de Belgische veiligheidsarchitectuur: vaststellingen en aanbevelingen van de parlementaire onderzoekscommissie terroristische aanslagen*, Antwerpen, Intersentia, 2020, 177 p.

VANDERBORGHT, J., *Bijzondere inlichtingenmethoden in de schijnwerpers – Les méthodes particulières de renseignement: de l'ombre à la lumière*, Brussel, Levebvre Sarrut Belgium NV, 2020, 151 p.

VOORHOOF, D., "Vrijheid van meningsuiting en persvrijheid", in J. VANDE LANOTTE et al (eds.), *Belgisch Publiek Recht*, Vol. 1, Brugge, Die Keure, 2015, 577-613.

WEIMANN, G., *Terror on the internet: The New Arena, the New Challenges*, Washington, United States Institute of Peace, 2006, 309 p.

WILMAN, F., *The responsibility of online intermediaries for illegal user content in the EU and the US*, Northampton, Edward Elgar Publishing, 2020, 414 p.

YANNOPOULOS, G. N., "Chapter 3 - The Immunity of Internet Intermediaries Reconsidered?", in M. TADDEO and L. FLORIDI (eds.), *Law, Governance and Technology Series*, Vol. 31, *The Responsibilities of Online Service Providers*, Switzerland, Springer, 2017, 43-59.

YAR, M. and STEINMETZ, K.F., *Cybercrime and Society*, 3rd ed., California, Sage Publications, 2019, 350 p.

3.2. Articles

AKDENIZ, Y., "To Block or Not to Block: European Approaches to Content Regulation, and Implications for Freedom of Expression", *Computer Law and Security Review* May 2010, Vol. 26, Issue 3, 260-272.

AMMAR, J., "Cyber Gremlin: social networking, machine learning and the global war on Al-Qaida and IS-inspired terrorism", *International Journal of Law and Information Technology* 2019, Vol. 27, Issue 3, 238–265.

BERGER, J. M. and PEREZ, H., "The Islamic State's diminishing returns on Twitter: how suspensions are limiting the social networks of English-speaking ISIS supporters", *Program on Extremism at George Washington University* (occasional paper) 2016, https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/downloads/JMB%20Diminishing%20Returns.pdf, 20 p.

BLOOM, M., TIFLATI, H. and HORGAN, J., "Navigating ISIS's Preferred Platform: Telegram", *Terrorism and Political Violence* July 2017, http://dx.doi.org/10.1080/09546553.2017.1339695, 15 p.

BOYNE, S. M., "Free Speech, Terrorism, and European Security: Defining and Defending the Political Community", *Pace Law Review* January 2010, Vol. 30, Issue 2, 417-483.

BUKOVSKÁ, B., "The European Commission's Code of Conduct for Countering Illegal Hate Speech Online - An analysis of freedom of expression implications", *Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression* 7 May 2019, https://cdn.annenbergpublicpolicycenter.org/wp-content/uploads/2020/06/EC_Code_of_Conduct_TWG_Bukovska_May_2019.pdf, 13 p.

CAMBRON, R. J., "World War Web: Rethinking "Aiding and Abetting" in the Social Media Age", *Case Western Reserve Journal of international law* 2019, Vol. 51, Issue 1, 293-325.

CHANG, B., "From Internet Referral Units to international agreements: censorship of the internet by the UK and EU", *Columbia HR Law Review* 2018, Vol. 49, Issue 2, 114-212.

CITRON, D. K., "Extremist speech, compelled conformity, and censorship creep", *Notre Dame Law Review* 2017-2018, Vol. 93, Issue 3, 1035-1072.

COCHE, E., "Privatised enforcement and the right to freedom of expression in a world confronted with terrorism propaganda online", *Internet Policy Review* 2018, Vol. 7, Issue 4, 1-17.

CONWAY, M., KHAWAJA, M., LAKHANI, S., REFFIN, J., ROBERTSON, A., and WEIR, D., "Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts", *Studies in Conflict & Terrorism* 2019, Vol. 42, Issue 1-2, 141-160.

DA SILVA, J. R., "Jihadist Terrorism and EU Responses - Current and Future Challenges", *Austria Institut für Europa - und Sicherheitspolitik*, https://www.aies.at/download/2017/AIES-Fokus--2017-06.pdf, 7 p.

DROEGE, C., "Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians", *International Review of the Red Cross* 2012, Vol. 94, Issue 886, 533-578.

ELKIN-KOREN, N., "Contesting algorithms: Restoring the public interest in content filtering by artificial intelligence", *Big data & society* July 2020, Vol. 7, Issue 2, 1-13.

ELLERMANN, J., "Terror won't kill the privacy star – tackling terrorism propaganda online in a data protection compliant manner", *ERA Forum* 2016, Vol. 17, Issue 4, 555-582.

GAN, H. Z., "Corporations: The Regulated or the Regulators - The Role of IT Companies in Tackling Online Hate Speech in the EU", *Columbia Journal of European Law* 2017, Vol. 24, Issue 1, 111-155.

GLENN, C., ROWAN, M., CAVES, J. and NADA, G., "Timeline: the Rise, Spread, and Fall of the Islamic State", *Wilson Center* 18 October 2019, https://www.wilsoncenter.org/article/timeline-the-rise-spread-and-fall-the-islamic-state.

GOLLATZ, K., BEER, F. and KATZENBACH, C., "The Turn to Artificial Intelligence in Governing Communication Online" (HIIG Workshop report), *Big Data & Society* (special issue) 2018, 22 p.

HERMANS, G., "De toepasselijkheid van algemene voorwaarden bij online contracteren", *HOR* 2018, Issue 128, 73-81.

HUSZTI-ORBAN, K., "Internet intermediaries and counter-terrorism: Between self-regulation and outsourcing law enforcement", in T. MINARIK, L. LINDSTROM and R. JAKSCHIS (eds.), *10th International Conference on Cyber Conflict: CyCon X: Maximising Effects,* 2018, 227-243.

IFTIMIE, I. A., "NATO's needed offensive cyber capabilities", *NDC POLICY BRIEF* May 2020, Issue 10, 4 p.

JEPPESEN, J.-H., and LLANSÓ, E. J., "Letter to European Commissioner on Code of Conduct for "Illegal" Hate Speech Online", *Center for Democracy and Technology* 3 June 2016, https://cdt.org/insights/letter-to-european-commissioner-on-code-of-conduct-for-illegal-hate-speech-online/.

KLIMEK, L., "Combating attacks against information systems: EU legislation and its development", *Masaryk University Journal of Law and Technology* 2012, Vol. 6, 87-100.

LLANSÓ, E., VAN HOBOKEN, J., LEERSSEN, P. and HARAMBAM, J. (Transatlantic Working Group), "Artificial Intelligence, Content Moderation, and Freedom of Expression", 26 February 2020, https://www.ivir.nl/publicaties/download/AI-Llanso-Van-Hoboken-Feb-2020.pdf, 32 p.

MCKENDRICK, K., "Artificial Intelligence Prediction and Counterterrorism", August 2019, https://www.chathamhouse.org/sites/default/files/2019-08-07-AICounterterrorism.pdf, 36 p.

OGUNLANA, S. O., "Halting Boko Haram / Islamic State's West Africa Province Propaganda in Cyberspace with Cybersecurity Technologies", *Journal of Strategic Security* 2019, Vol. 12, Issue 1, 72-106.

ÖZKAYA, E., "The Use of Social Media for Terrorism", *Defence Against Terrorism Review* 2017, Issue 9, 47-59.

PORTARU, A., "Freedom of expression online: The code of conduct on countering illegal hate speech online", *Revista Romana de Drept European* 2017, Vol. 4, 77-91.

REEVE, Z., "Human Assessment and Crowdsourced Flagging", in B. GANESH and J. BRIGHT (VoxPol) (eds.), *Extreme digital speech contexts, responses and solutions,* 2019 https://www.voxpol.eu/download/vox-pol_publication/DCUJ770-VOX-Extreme-Digital-Speech.pdf#page=56, 67-79.

SCHNADER, J., "The Implementation of Artificial Intelligence in Hard and Soft Counterterrorism Efforts on Social Media", *Santa Clara High Technology Law Journal* December 2019, Vol. 36, Issue 1, 42-72.

SPANGENBERG, S., "Cyber Jihadism: An Analysis on How the Cyber Sphere Has Altered Islamic Terrorism", *Butler Journal of Undergraduate Research* 2020, Vol. 6, 128-146.

SVENSØY, G. J., *The e-Commerce Directive Article 14: Liability exemptions for hosting third party content,* Master Thesis Law University of Oslo, 2011, https://www.duo.uio.no/bitstream/handle/10852/19450/117618.pdf, 47 p.

VAN DE HEYNING, C., "De strijd tegen de niet-consensuele verspreiding van seksuele beelden opgevoerd", *T.Strafr*. 2020, Issue 3, 176-183.

VAN DER PERRE, A., VERBIEST, T., SPINDLER, G., RICCIO, G. M. and MONTERO, E., *Study on the liability of internet intermediaries – final report,* 2007, https://digital-strategy.ec.europa.eu/en/library/archive-e-commerce-directive-what-happened-and-its-adoption, 115 p.

WALKER, C. and CONWAY, M., "Online terrorism and online laws", *Dynamics of Asymmetric Conflict* 2015, Vol. 8, Issue 2, 156-175.

WATKIN, A.-L. and WHITTAKER, J., "Evolution of terrorists' use of the Internet", *Counterterror Business* 20 October 2017, http://www.counterterrorbusiness.com/features/evolution-terrorists%E2%80%99-use-internet.

YU, J., "Regulation of social media platforms to curb ISIS incitement and recruitment: The need for an international framework and its free speech implications", *Journal of Global Justice and Public Policy* 2018, Vol. 4, 1-29.

4. Others

4.1. News articles

ARAL, S., "How Lies Spread Online", *N.Y. Times* 8 March 2018, https://www.nytimes.com/2018/03/08/opinion/sunday/truth- lies-spread-online.html.

CHINI, M., "Major Belgian cyberattack eliminates Islamic State's presence on the internet", *The Brussels Times* 26 November 2019, https://www.brusselstimes.com/news/belgium-all-news/80427/major-belgian-cyberattack-eliminates-islamic-states-presence-on-the-internet/.

CLERIX, K., "Militaire veiligheidsdiensten: De nieuwe topman Philippe Boucké zet de ADIV op scherp", *Knack* 24 February 2021 to 2 March 2021, Issue 8, https://www.knack.be/nieuws/belgie/nieuwe-topman-philippe-boucke-zet-adiv-op-scherp-willen-ook-offensieve-cyberoperaties-opzetten/article-longread-1704075.html.

DE JAEGERE, A. and GROMMEN, S., "Na geslaagde cyberaanval door Belgische politie: "Terreurgroep IS volledig uitgeschakeld op het internet"", *VRT NWS* 25 November 2019, https://www.vrt.be/vrtnws/nl/2019/11/25/europol/.

PEREZ, M. F., "New documents reveal the truth behind the Hate Speech Code", *EDRi* 7 September 2016, https://edri.org/new-documents-reveal-truth-behind-hate-speech-code.

ROBBINS-EARLY, N., "How Telegram became the App of choice of ISIS", *Huffington Post* 24 May 2017, http://www.huffingtonpost.co.uk/entry/isis-telegram-app_us_59259254e4b0ec129d3136d5.

VILLAS-BOAS, A., "The Islamic State claimed responsibility for the London Bridge knife terror attack", *Business Insider* 30 November 2019, https://www.businessinsider.com/isis-claiming-responsibility-for-london-bridge-knife-terror-attack-2019-11?r=US&IR=T.

WARISLOHNER, F., "Europol: Non-transparent cooperation with IT companies", *EDRi* 18 May 2016, https://edri.org/europol-non-transparent-cooperation-with-it-companies/.

WILLIAMS, R., "What Is Telegram? The New WhatsApp?", *Telegraph* (*UK*) 25 February 2014, http://www.telegraph.co.uk/technology/news/10658647/What-is-Telegram-the-new-WhatsApp.html.

X, "Activists accuse YouTube of destroying digital evidence of Syria war", *TRTWorld* 8 March 2021, https://www.trtworld.com/life/activists-accuse-youtube-of-destroying-digital-evidence-of-syria-war-44809.

X, “Activists in race to save digital trace of Syria war”, *Qantara* 8 March 2021, https://en.qantara.de/content/activists-in-race-to-save-digital-trace-of-syria-war.

X, “Belgian judiciary and Europol attack ISIS’ ‘press agency’”, *Utrecht University* 29 November 2019, https://www.uu.nl/en/in-the-media/belgian-judiciary-and-europol-attack-isis-press-agency.

X, “Dedonder wil vijfde legercomponent rond cyber”, *Knack* 10 November 2020, https://www.knack.be/nieuws/belgie/dedonder-wil-vijfde-legercomponent-rond-cyber/article-belga-1663989.html.

X, “Dispatches investigation reveals how Facebook moderates content”, *Channel 4* 17 July 2018, https://www.channel4.com/press/news/dispatches-investigation-reveals-how-facebook-moderates-content.

X, “Facebook moderators ‘keep child abuse online’”, *BBC* 17 July 2018, https://www.bbc.com/news/technology-44859407.

X, “ISIS’ media mouthpiece Amaq was silenced, but not for long”, *CBS News* 2 May 2018, https://www.cbsnews.com/news/isis-amaq-online-propaganda-hit-cyber-takedown-bounces-back-in-just-days/.

X, “Islamic State claims attacks at Brussels airport and metro station”, *The Guardian* 22 March 2016, https://www.theguardian.com/world/2016/mar/22/brussels-airport-explosions-heard.

X, “La Belgique à la tête d'une opération pour anéantir Amaq, “l’agence de presse de l’EI””, *RTBF* 25 November 2019, https://www.rtbf.be/info/belgique/detail_amaq-agence-de-presse-de-l-ei-hors-d-etat-de-nuire-grace-a-des-cyberattaques-menees-par-la-police-belge-et-europol?id=10373496.

X, “UK launched cyber-attack on Islamic State”, *BBC News* 12 April 2018, https://www.bbc.com/news/technology-43738953.

X, “Understanding the Human Rights Risks Associated with Internet Referral Units”, *Global Network Initiative* 25 February 2019, https://globalnetworkinitiative.org/human-rights-risks-irus-eu/.

4.2. Webpages

Cambridge dictionary, *v°* *Defensive*, https://dictionary.cambridge.org/dictionary/english/defensive.

Cambridge dictionary, *v°* *Offensive*, https://dictionary.cambridge.org/dictionary/english/offensive.

Cambridge dictionary, *v°* *Proactive*, https://dictionary.cambridge.org/dictionary/english/proactive.

CARLIER, T. (Federal Judicial Police Belgium – Internet investigations, Internet Referral Unit), "How to tackle internet for fighter recruitment process – Part 1: Situation in Belgium", https://www.inach.net/wp-content/uploads/7.Carlier-How-to-tackle-Internet-use-for-fighter-recruitment-process.ppt.pdf.

COUNCIL OF EUROPE, "Chart of signatures and ratifications of Treaty 196" (Status as of 15 May 2021), https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/196/signatures?p_auth=ACutsH6N.

COUNCIL OF EUROPE, "International instruments - Cybercrime", https://www.coe.int/en/web/cybercrime/international-instruments.

EUROPOL, "EU Internet Referral Unit - EU IRU", https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru.

EUROPOL, "European Counter Terrorism Centre - ECTC", https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc.

EUROPOL, "Joint investigation teams – JITS", https://www.europol.europa.eu/activities-services/joint-investigation-teams.

DEFENSIE, "Over Defensie – Onze Componenten", https://www.mil.be/nl/over-defensie/.

FACEBOOK, "Community Standards", https://www.facebook.com/communitystandards/violence_criminal_behavior.

GCHQ, "Overview", https://www.gchq.gov.uk/section/mission/overview.

IQBAL, M., "Facebook Revenue and Usage Statistics (2021)", *Statista* 6 April 2021, https://www.businessofapps.com/data/facebook-statistics/.

IQBAL, M., “Twitter Revenue and Usage Statistics (2020)”, *Business of Apps* 8 March 2021, https://www.businessofapps.com/data/twitter-statistics/.

LIN, Y., “10 Twitter statistics every marketer should know in 2021”, *Oberlo* 25 January 2021, https://www.oberlo.com/blog/twitter-statistics.

MOHSIN, M., “10 Facebook statistics every marketer should know in 2021”, *Oberlo* 16 February 2021, https://www.oberlo.com/blog/facebook-statistics.

POLITICO, “Pavel Durov – The life wire”, https://www.politico.eu/list/politico-28-class-of-2021-ranking/pavel-durov/.

TANKOVSKA, H., “Facebook’s monthly active users (MAU) in Europe from 4th quarter 2012 to 4th quarter 2020”, *Statista* 2 February 2021, https://www.statista.com/statistics/745400/facebook-europe-mau-by-quarter.

TANKOVSKA, H., “Leading countries based on number of Twitter users as of January 2021”, *Statista* 9 February 2021, https://www.statista.com/statistics/242606/number-of-active-twitter-users-in-selected-countries/.

TANKOVSKA, H., “Number of monthly active Facebook users worldwide as of 4th quarter 2020”, *Statista* 2 February 2021, https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ .

TELEGRAM, “Telegram Privacy Policy – 8.Who Your Personal Data May Be Shared With – 8.3.Law Enforcement Authorities”, https://telegram.org/privacy.

TELEGRAM, “Terms of Service”, https://telegram.org/tos.

TWITTER, “Rules and policies – General guidelines and policies”, https://help.twitter.com/en/rules-and-policies/violent-groups.

X, “Combined Joint Task Force: Operation Inherent Resolve”, APO AE 09306, https://www.inherentresolve.mil/Portals/14/Documents/Mission/HISTORY_17OCT2014-JUL2017.pdf?ver=2017-07-22-095806-793.

4.3. Others

Email with Commissioner A. LUYPAERT, Commissioner (Head of Unit) DJSOC / Internet Recherche - I2-IRU, 29 October 2020.

Online Interview Senior Captain C. BOMBEKE, Senior Captain ADIV, 23 February 2021.