ISIL TERRORISTS AND THE USE OF SOCIAL MEDIA PLATFORMS

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

Article written: January 2022

Private social media platforms are entrusted today with the task of limiting the presence of terrorist groups, such as the Islamic State, on the online scene. Through mechanisms, such as a 'notice-and-takedown' or a removal order, these platforms are made aware of online terrorist content and consequently remove it from their platforms. However, the responsibility to protect citizens against terrorist threats lies with states and not with private companies. To reclaim this responsibility, states could perpetrate offensive and proactive cyber-attacks on devices of terrorists located in Belgium to disable their access to information to perpetrate attacks or diminish their online presence. This article discusses the legal frameworks of these mechanisms, their advantages and disadvantages and whether the Belgian state can perform such cyber-attacks or whether it would be desirable for the Belgian authorities to receive this competence. Last, several recommendations are presented to adapt the current Belgian framework to allow the perpetration of such cyber-attacks.

Keywords:

Terrorism;
social media platforms;
notice-and-takedown;
cyber-attacks;
Belgian state;
Islamic State of Iraq and the Levant;
Belgian army;
cybercrime.

Océane Dieu *(Faculty of Law and Criminology, University of Ghent)*

On the 21st and 22nd of November 2019, Europol, together with several Member States of the 'European Union' (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' (ISIL) published on social media platforms by its news channel 'Amaq'. These events have often been qualified and referred to as 'cyberattacks'.[1] But can the operation legally be qualified as such? Are the existing instruments, such as the notice-and-takedown mechanism and removal orders, 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? Or should the state reclaim its responsibility by, for example, perpetrating cyber-attacks on terrorist supporters? Would this be a legitimate solution for combatting online terrorist content and how would this be framed in the Belgian legal scene? These questions will guide the reader through the labyrinth of legal instruments and mechanisms, starting with a brief discussion on the notion of terrorism (1.) and the right to freedom of expression in the context of combatting terrorism online (2.). Afterwards, the existing reactive measures to tackle ISIL's online presence (3.) and the existing legal framework of proactive and offensive cyber-attacks (4.) will be analysed. Last, whether such proactive and offensive cyber-attacks would constitute a legitimate Belgian solution will be addressed (5.).

1 "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; Axel De Jaegere and Stefan 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/; Maïté 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/.

1. The notion of terrorism

States have a legitimate interest in combatting terrorism given the online presence of ISIL. However, sometimes, the notion of terrorism is abused by states to silence opponents. The absence of a universally accepted definition of 'terrorism'[2] allows states to arbitrarily qualify certain persons as 'terrorist',[3] whereas their supporters and sympathisers could see them as freedom fighters.

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

At the international and European Union level, the right to freedom of expression grants citizens an absolute right to hold opinions and a qualified right to freedom of expression.[4] The ***absolute*** right to hold opinions prohibits the state from restricting this right. Every citizen is thus entitled to have a favourable opinion on the messages spread by terrorist groups, such as considering ISIL to be a legitimate group of freedom fighters. The ***qualified*** right to freedom of expression includes the right to seek, receive and impart information and ideas. This right can be restricted for the protection of national security, public order, public health or morals. These restrictions also apply to the online environment.[5]

Moreover, advocating national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence is prohibited.[6] Terrorist propaganda of ISIL is hence not protected under the right to freedom of expression.

At the Belgian level, articles 19 and 25 of the Constitution protect the freedom of expression. Whilst the Belgian Constitution does not provide an explicit basis for the right to freedom of opinion, this right is inherently intertwined with the protected right to freedom of expression.

3. Reactive measures to tackle ISIL's online content

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. To remove this content, states require social media platforms to take the content down. This 'voluntary' cooperation mechanism is legally enshrined (3.1.), but significantly impacts the functioning of these platforms, who consequently have recourse to 'artificial intelligence' (AI) to comply with their obligations (3.2.).

2 David Martin Jones et al., *Handbook of terrorism and counter terrorism post 9/11* (Northampton: Edward Elgar Publishing, 2019), 28.

3 Clive Walker and Maura Conway, "Online terrorism and online laws," *Dynamics of Asymmetric Conflict* 8, no. 2 (2015): 159; Majid Yar and Kevin F. Steinmetz, *Cybercrime and Society,* 3rd ed. (California: Sage Publications, 2019), 96.

4 The right to freedom of expression is protected, amongst others, by article 19 of the International Covenant on Civil and Political Rights ('ICCPR'), article 10 of the European Convention on Human Rights ('ECHR') and article 11 of the Charter of Fundamental Rights of the European Union.

5 Human Rights Committee, *General Comment No. 34 on Article 19: Freedoms of opinion and expression*, 12 September 2011, CCPR/C/GC/34, §43; Wolfgang Benedek and Matthias C. Kettemann, *Freedom of expression and the Internet* (Strasbourg: Council of Europe Publishing, 2013), 24.

6 Art. 20.2 ICCPR; Art. 17 ECHR proscribes the abuse of the rights provided by the Convention, such as abusing the right to freedom of expression to negate the fundamental values of the Convention; European Court of Human Rights, *Factsheet – Hate Speech*, September 2020, https://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf, 1.

3.1. Existing reactive measures

At the level of the 'United Nations' (UN), there is no international treaty on terrorism,[7] but only a general requirement for ***states*** to work together to counter the online presence of terrorists.[8] Both at the UN and Council of Europe level there is no specific obligation for ***hosting service providers*** to take down the terrorist content that appears on their platform or hold them liable for the content uploaded on their platform.[9] Whilst the European Court of Human Rights has ruled on the liability of hosting service providers for content uploaded on their platform,[10] the Court's rulings do not provide consistent case-law.

Contrary to the UN and the Council of Europe, the EU has been quite active in adopting legislation to fight terrorists' online presence, amongst others through the notice-and-takedown mechanism (3.1.1.) and the removal orders (3.1.2.).

3.1.1. The notice-and-takedown mechanism

The notice-and-takedown procedure implies that the Member States will not hold hosting service providers liable for the content stored on their platforms if these providers either do not have knowledge of the illegal content or act expeditiously to remove or disable the access to that content upon obtaining knowledge or awareness of the illegal content.[11] Applied to the dissemination of online terrorist content by ISIL supporters on Twitter, Telegram or Facebook, these platforms will enjoy an exemption of liability if they remove or disable expeditiously the terrorist content uploaded by ISIL. Worth singling out is the requirement of 'acting expeditiously'.

Service providers must act ***expeditiously*** when becoming aware of the illegal content's presence on their platform. The voluntary Code of Conduct on countering illegal hate speech online of 2016, drafted by the European Commission and several IT Companies (Facebook, Microsoft, Twitter and YouTube), introduced a twenty-four hour rule within which the service providers are to assess the compatibility of the referred content against their Terms and Conditions.[12] This timeframe was afterwards reduced to the non-legally binding one-hour rule in the Commission's Recommendation of 2018.[13] The recently adopted Regulation on preventing the dissemination of terrorist content online kept the requirement to respond ***expeditiously*** to a referral and refrained from making the one-hour removal rule mandatory on referrals.[14]

7 United Nations Office on Drugs and Crime, *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.

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

9 The Council of Europe's Convention on the Prevention of Terrorism, which imposes the criminalisation of the online public provocation to commit terrorist offences, is not applicable in Belgium.

10 ECtHR, *MTE v. Hungary* (2 May 2016), n° 22947/13; ECtHR, *Delfi AS v. Estonia* (10 October 2013), n° 64569/09.

11 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, which was transposed into Belgian law into article XII.19 of the Code of Economic Law.

12 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 ('Code of Conduct').

13 European Commission Recommendation 2018/334 on measures to effectively tackle illegal content online (1 March 2018), in *Official Journal of the European Union* (6 March 2018), C/2018/1177, n° 63.

14 14 Art. 5.2, 2nd indent, a) Regulation 2021/784 of the European Parliament and of the Council on addressing the dissemination of terrorist content online (29 April 2021), in *Official Journal of the European Union* (17 May 2021), n° 127, 79 ('Regulation on addressing the dissemination of terrorist content online').

The reactiveness of a service provider to referred content 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,[15] which opens the door to the discretionary filling of this notion.

Moreover, rewarding service providers for quickly taking down illegal content by exempting them from any liability obliges them to make a strenuous balancing exercise.[16] On the one hand, service providers either have the choice to look into every referral individually, taking thus more time 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.[17] In doing so, service providers restrict legitimate speech and infringe their users' fundamental rights.

Given that freedom of expression is the cornerstone of a democratic society, the state also has an interest in the exercise of this right by its citizens. Because of this system of liability exemption, the state partly loses control over what constitutes illegal speech and what is to be banned from a democratic forum.
Consequently, and agreeing with Jørgensen and Pedersen, the notice-and-takedown procedure is surrounded by legal uncertainty.[18] One way of ensuring that service providers will benefit from the exemption of liability regime is to monitor their platform proactively. Obliging providers to have recourse to such monitoring is, however, prohibited under article 15 of the e-Commerce Directive.[19]

The recently adopted 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 and shifts the responsibility for disabling terrorist content towards the social media 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.
As such, service providers enjoy the right to conduct a business and have a legitimate business interest.[20] Social media platforms are private businesses that operate on profit, which can sometimes hamper the fight against ISIL's presence online. Increasing the active engagement of the platform's users is partly based on matching these users with content they find interesting. Consequently, the business interest of these platforms lies in finding content that interests the users and

15 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, 14.

16 Eugénie Coche, "Privatised enforcement and the right to freedom of expression in a world confronted with terrorism propaganda online," *Internet Policy Review* 7, no. 4 (2018): 7; Teresa Quintel and Carsten Ullrich, "Self-Regulation of Fundamental Rights? The EU Code of Conduct on Hate Speech, related initiatives and beyond," in *Fundamental Rights Protection Online: The Future Regulation of Intermediaries,* ed. Bilyana Petkova and Tuomas Ojanen (Northampton: Edward Elgar Publishing, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3298719, 8.

17 Commissioner for Human Rights of the Council of Europe, *The rule of law on the internet and in the wider digital world*, 2014, Strasbourg: Council of Europe, 66; Rikke Frank Jørgensen and Anja Moller Pedersen, "Chapter 10 - Online Service Providers as Human Rights Arbiters," in *Law, Governance and Technology Series*, Vol. 31, *The Responsibilities of Online Service Providers*, ed. Mariarosaria Taddeo and Luciano Floridi, (Switzerland: Springer, 2017), 180.

18 Jørgensen and Pedersen, *Chapter 10 - Online Service Providers as Human Rights Arbiters*, 189.

19 Art. 15 of the e-Commerce Directive; CJEU (Grand Ch.), *L'Oréal SA v. eBay International AG* (12 July 2011), C324/09, ECLI:EU:C:2011:474, §139.

20 Art. 16 Charter of Fundamental Rights of the European Union.

stimulates them to view similar content. However, this economic interest conflicts with the public role they received of minimising the terrorist content users view.[21] The social media platforms' interests consequently differ significantly from the public authorities' aim of acting in their citizens' interest.

3.1.2. The removal orders

Court authorities and administrative institutions can also order the removal or blocking of illegal online content.[22] More specifically, a court can rapidly adopt measures "***designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.***"[23] In Belgium, the public prosecutor[24] and investigative judge[25] are competent to order such removal.

This regime of removal orders has also been modified by the newly adopted Regulation, which introduced the competence of issuing ***cross-border*** removal orders. These orders have to fulfil complementary and more stringent conditions,[26] such as measures taken by the platform that allow to reinstate or re-access the removed content.[27] 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, social media platforms will be bound to comply with orders that restrict the freedom of expression of their users whilst potentially considering the content legitimate. These cross-border removal orders will endanger the fundamental rights of the platform's users.

Moreover, the new Regulation introduces a binding one-hour rule within which the removal order has to be complied with.[28] This possibility 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.***"[29] Moreover, if the service provider is 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.[30] 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. Having recourse to automated tools can help social media platforms find online terrorist content more efficiently, given that they 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 that they take away the human control behind the takedown and constitute a grave danger to the right to freedom of expression. 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.

21 Niva Elkin-Koren, "Contesting algorithms: Restoring the public interest in content filtering by artificial intelligence," *Big data & society* 7, no. 2 (July 2020): 5.
22 Art. 14.3 and Recital 45 e-Commerce Directive; CJEU (7th Ch.), *Sotiris Papasavvas v. O Fileleftheros Dimosia Etairia Ltd* (9 September 2014), C-19/13, ECLI:EU:C:2014:2209, §57.
23 Art. 18.1 e-Commerce Directive.
24 Art. 39bis, §6, 4th and 6th indent Belgian Code of Criminal Procedure.
25 Art. 89 Belgian Code of Criminal Procedure.
26 Art. 4 Regulation on addressing the dissemination of terrorist content online.
27 Art. 4.2 Regulation on addressing the dissemination of terrorist content online.
28 Art. 3.3 Regulation on addressing the dissemination of terrorist content online.
29 Recital 17 Regulation on addressing the dissemination of terrorist content online.
30 Art. 3.7 and Recital 17 Regulation on addressing the dissemination of terrorist content online.

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

The combat against online terrorist content increasingly relies on the intervention of private social media platforms. Requiring the platforms to assess the compatibility of referred content ***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 filtering mechanisms that rely on AI.
Sometimes, content is not easily qualified as terrorist material. Solely relying on AI to address the problem of online terrorist content would be perilous. Consequently, human review is required to ensure that the content taken down is effectively terrorist content. Algorithms do not have a human eye to interpret the context or subtleties of specific posts.[31] 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.***"[32] However, this 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.

Excessive takedowns of legitimate speech are not the only risk related to the use of AI. ***False positives***, being the wrongly qualification of legitimate content as terrorist content, threatens the freedom of expression of the platform's users. ***False negatives***, being terrorist content that escapes the filtering of the algorithms and wrongly remains on the platform, allows terrorist content to pursue their purpose of propaganda, recruitment and terror rising.[33]

Another risk linked to the use of AI is the ***inherent biases*** algorithms can contain.[34] Algorithms are created by humans, who can be biased. If a creator of algorithms considers, for example, that all terrorist content is always published by persons following the Islam, 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.

31 Rebecca J. Cambron, "World War Web: Rethinking 'Aiding and Abetting' in the Social Media Age," *Case Western Reserve Journal of International law* 51, no. 1 (2019): 306-307; Krisztina Huszti-Orban, "Internet intermediaries and counter-terrorism: Between self-regulation and outsourcing law enforcement," in *10th International Conference on Cyber Conflict: CyCon X: Maximising Effects,* ed. Tomas Minarik, Lauri Lindstrom and Raik Jakschis (2018): 234.

32 Art. 1.3 Regulation on addressing the dissemination of terrorist content online.

33 Jørgensen and Pedersen, Chapter 10 - *Online Service Providers as Human Rights Arbiters*, 183; Miriam Fernandez and Harith Alani, "Artificial Intelligence and Online Extremism: Challenges and Opportunities," in Predictive Policing and Artificial Intelligence, ed. John McDaniel and Ken Pease (London: Routledge, 2021), http://oro.open.ac.uk/69799/1/Fernandez_Alani_final_pdf.pdf; Emma Llansó, Joris van Hoboken, Paddy Leerssen and Jaron 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.

34 Secretary-General of the United Nations, *Note by the Secretary-General on the promotion and protection of the right to freedom of opinion and expression* (29 August 2018), in UN Doc. A/73/348 (2018), 5; Kathleen McKendrick, "Artificial Intelligence Prediction and Counterterrorism," *Chatham House*, August 2019, https://www.chathamhouse.org/sites/default/files/2019-08-07-AICounterterrorism.pdf, 3.

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.[35] 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 watching terrorist content of ISIL, their newsfeed will equally contain more similar content. 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, which is problematic in the view of counter-terrorism.

3.3. Conclusion

Often portrayed as a 'cyber-attack', the 2019 removal of online terrorist content by Europol, the Member States and their respective Internet Referral Units, is legally not qualified as such. These were referrals of content to Telegram that took the content down according to the notice-and-takedown regime.

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'.[36] As in the real game, as soon as the content is 'hit down by the service provider's hammer', the same content resurfaces on other platforms or is re-shared by other social media users who are easily and rapidly followed again by the same sympathisers, which weakens the referral operations.[37] 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.[38]

Over the years, social media providers have received a growing responsibility for the content stored on their platforms. Whilst this seems legitimate considering their role in the public debate, they also require more certainty regarding their legal obligations. Moreover, this shift is an effortless way for the state to avoid fulfilling its legal obligations. Social media platforms become a proxy for the government to enforce the government's legal obligations. Private actors hence have to step in where public authorities leap behind. Consequently, building on Ellerman's proposal to combine reactive measures with proactive measures,[39] the proactive measure proposed in this analysis takes the form of offensive and proactive cyber-attacks perpetrated by the state on terrorists' online presence. The state could orchestrate a cyber-attack on an ISIL supporter's devices to disable their access to the device or content it stores. 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

35 Emma Llansó, *Artificial Intelligence, Content Moderation, and Freedom of Expression*, 14.

36 Jesse 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; Barbora 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.

37 Jan Ellermann, "Terror won't kill the privacy star – tackling terrorism propaganda online in a data protection compliant manner," *ERA Forum* 17, no. 4 (2016): 572.

38 Maura Conway, Moign Khawaja, Suraj Lakhani, Jeremy Reffin, Andrew Robertson and David Weir, "Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts," *Studies in Conflict & Terrorism* 42, no. 1-2 (2019): 151.

39 Ellermann, "Terror won't kill the privacy star – tackling terrorism propaganda online in a data protection compliant manner," 573.

the online presence and propaganda. Furthermore, this possibility would replace the responsibility and burden of fighting terrorism back where it belongs: with the state. The ever-developing cyber capabilities of the military, the police, and the intelligence and security services could allow states to reclaim their responsibility.

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

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.

In what follows, the cyber-measures to counter online terrorist content taken at the international (4.1.) and the Belgian level (4.2.) will be addressed.

4.1. Cyber-measures taken at the international level

Whilst at the UN level, no legislation has been adopted that explicitly addresses cybercrime or cyber-attacks,[40] there is an ongoing discussion on creating a Cybercrime Treaty.[41] A similar tendency occurs at the level of the 'North Atlantic Treaty Organization' (NATO), where there is an apparent willingness to develop more offensive cyber operations.[42]

At the level of the 'Law of Armed Conflict' (LOAC), proactive and offensive cyber-attacks would constitute the online version of targeted attacks. The majority of the International Group of Experts who drafted the Tallinn Manual 2.0 on the international law applicable to cyber operations, considered data to be too volatile and intangible to be considered an 'object' of a targeted attack.[43] Moreover, the ICRC qualifies the conflict against ISIL as a non-international armed conflict taking place on different countries' territory. Given that in Belgium the conflict against ISIL does not attain the required degree of organisation and intensity,[44] the LOAC does not apply to this analysis.

40 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; United Nations Office on Drugs and Crime, *The use of the Internet for terrorist purposes*, 74.

41 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), in UN Doc. GA/12309, https://www.un.org/press/en/2021/ga12309.doc.htm.

42 Jens 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.

43 Michael Schmitt, *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge: Cambridge University Press, 2017), 437.

44 Schmitt, *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations*, 19; For a more detailed analysis of the thresholds of 'organisation' and 'intensity' regarding the non-international armed conflict involving ISIL, see Hannes 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, 15-18.

The criminalisation of the unlawful interfering with a computer system is provided in article 5 of the Council of Europe Convention on Cybercrime,[45] and article 4 of the European Union Directive 2013/40/EU on attacks against information systems,[46] when the interference occurs 'without right'.[47] The Directive adds, however, two additional grounds for criminalisation: interrupting the functioning of the information system and making data inaccessible.[48] Consequently, if the national law foresees the possibility of perpetrating cyber-attacks on an information system of terrorists, this conduct would be lawful or 'with right', thus, not to be criminalised by the Member States.

4.2. Cyber-measures taken at the Belgian level: current state of affairs

The crime of hacking or entering an information system without being authorised to do so and the crime of sabotaging an information system by, for example, introducing malware in the system, are criminalised in respectively articles 550***bis*** and 550*ter* of the Belgian Criminal Code. 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.

4.2.1. The role of the judicial police and the public prosecutor

The judicial police's role is limited to investigating infringements of the law, gathering evidence of these breaches and handing over 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.[49] Similarly, the competence of the Belgian public prosecutors is limited to investigating and prosecuting offences.[50] Consequently, orchestrating proactive and offensive cyber-attacks does not lay in the competences of the police or the public prosecutors.

4.2.2. The role and competences of the intelligence and security services

The civilian intelligence service in Belgium, the State Security Service,[51] is, amongst others, competent for intelligence gathering on terrorism, including propaganda dissemination.[52] The military branch of the intelligence services in Belgium, the General Intelligence and Security Service,[53] has similar competences but they are limited to the Belgian armed forces.[54]

45 Convention on Cybercrime (23 November 2001). In *European Treaty Series*, n° 185 ('Cybercrime Convention').
46 Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (12 August 2013), in *Official Journal of the European Union* (14 August 2013), n° 218, 8 ('Directive 2013/40/EU on attacks against information systems').
47 'Without right' means that the conduct 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 as, see Council of Europe, *Explanatory Report to the Convention on Cybercrime. In European Treaty Series* (23 November 2001), n° 185, §38; art. 2, d) Directive on attacks against information systems.
48 Art. 4 Directive on attacks against information systems.
49 Art. 8 Belgian Code of Criminal Procedure.
50 Art. 22 Belgian Code of Criminal Procedure.
51 Veiligheid van de Staat (Dutch) – Sureté de l'État (French) (VSSE).
52 Art. 7, 1) Belgian Law regulating the intelligence and security services (30 November 1998), in *Belgian Gazette* (18 December 1998), 40.312 ('Belgian Law regulating the intelligence and security services').
53 Algemene Dienst Inlichting en Veiligheid (Dutch – ADIV) – Service Général du Renseignement et de la Sécurité (French – SGRS).
54 Art. 11, §1, 1° Belgian Law regulating the intelligence and security services.

The Belgian intelligence services' competences can be divided into three levels based on the intrusiveness of the methods used on the citizens' right: the ordinary intelligence methods,[55] the special methods,[56] and the exceptional methods,[57] One exceptional method allows the intelligence 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.[58] However, this operation is limited to mere intelligence gathering and does not cover the irreversible and offensive destruction or alteration of this data.[59]

Moreover, the military branch can also perform defensive cyber-attacks to protect their systems and infrastructures against a cyber-attack,[60] offensive cyber-attacks to immediately react to a cyber-attack in accordance with the LOAC (which is not applicable in Belgium)[61] and infiltrate, disrupt and neutralise an information system located abroad,[62] such as infiltrating in a kamikaze's cell phone located outside of the Belgian territory. However, this unique reference to cyber-attacks in this law does not allow the perpetration of proactive and offensive cyber-attacks on devices of ISIL supporters and terrorists in Belgium.

Contrary to their military counterpart, the civilian intelligence and security service has not yet been assigned specific cyber-competences, apart from the previously mentioned exceptional investigative method, limited, however, to mere intelligence gathering.

The Belgian legislator could go one step further and allow the military and civilian intelligence and security services to perpetrate proactive and offensive cyber-attacks on an in Belgium located terrorist's device to disable the use of that device. The military competence to perpetrate such cyber-attacks could further be developed in the fifth military component, the cyber-component, as was proposed in 2020 by the Belgian minister of Defence L. Dedonder.[63]

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

Given that other countries, such as the USA,[64] the UK,[65] Israel and Russia,[66] have developed the capacity to orchestrate offensive cyber actions, 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.

55 Art. 14-18 of the Belgian Law regulating the intelligence and security services.
56 Art. 18/4-18/8 of the Belgian Law regulating the intelligence and security services.
57 Art. 18/11-18/17 of the Belgian Law regulating the intelligence and security services
58 Art. 18/16 Belgian Law regulating the intelligence and security services.
59 Art. 18/16, §1, 3rd indent Belgian Law regulating the intelligence and security services.
60 Art. 11, §1, 2° Belgian Law regulating the intelligence and security services.
61 Art. 11, §1, 2° Belgian Law regulating the intelligence and security services.
62 Art. 44/1 Belgian Law regulating the intelligence and security services. Own translation.
63 Defensie, *Over Defensie – Onze Componenten*, https://www.mil.be/nl/over-defensie/; Ludivine Dedonder, *Policy Statement of Defence* (4 November 2020), in Parl.St. Kamer 2020-2021, n° 55-1610/017, 25.
64 Yar and Steinmetz, *Cybercrime and Society*, 100.
65 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; "UK launched cyber-attack on Islamic State", *BBC News*, 12 April 2018, https://www.bbc.com/news/technology-43738953.
66 Yar and Steinmetz, *Cybercrime and Society,* 100.

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

As was discussed previously, terrorists' right to freedom of expression can be restricted when amounting to hate speech. However, the 'terrorist' label can also wrongly be allocated to a legitimate political opponent. Can proactive and offensive cyber-attacks to disable access to devices or information stored on the devices be legitimised in the context of terrorism?[67]

First, the restriction of the terrorist's right to freedom of expression should be provided by a clear, foreseeable and accessible (published in the Belgian Gazette) 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. Hence, the first criterium of legality would be fulfilled. However, whilst the Belgian law provides a definition of the notion of 'terrorism',[68] the vagueness surrounding this notion due to the absence of an internationally accepted definition could be considered an obstacle to the law being 'sufficiently clear'.

Secondly, the restriction should pursue one of the legitimate aims enumerated in 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.
Thirdly, the restriction should be 'necessary in a democratic society', which requires a proportionality assessment that is threefold: the restriction has to be suitable, necessary and proportionate ***sensu stricto***.

The suitability of a measure refers to whether the measure taken is appropriate to attain the "***objectives legitimately pursued.***"[69] 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 might again lead to a 'whack-a-mole' figure in the long run.

The necessity refers to "***a pressing social need***" to employ this specific measure.[70] The measures taken to attain the objective legitimately pursued should be the least restrictive and thus the least intrusive on the rights of the persons concerned. Today, less restrictive measures on the alleged terrorist's freedom of expression, such as the notice-and-takedown or the recourse to counter-narratives, exist. Nevertheless, these measures seem insufficient since the online content resurfaces quickly. It might thus appear necessary today to take a more aggressive and offensive stance.

Last, the proportionality ***sensu stricto*** of such cyber-attacks is even more questionable. This requirement refers to the idea that "***the means adopted should not impose an excessive burden on the individual.***"[71] Consequently, the restriction's consequences on the person's rights should not be disproportionate regarding the advantages the state has in adopting the measure. The measure in question seems

67 The following analysis is based on the restriction clause of article 10.2 of the ECHR.
68 Art. 8, 1°, b) Belgian Law regulating the intelligence and security services.
69 Stéphanie De Coensel, *Counter-Terrorism and Criminal Law. A Normative Legitimacy Test of Terrorism-Related Offences on Expression, Information and Movement* (Antwerp: Maklu, 2020), 125.
70 De Coensel, *Counter-Terrorism and Criminal Law. A Normative Legitimacy Test of Terrorism-Related Offences on Expression, Information and Movement*, 125.
71 De Coensel, *Counter-Terrorism and Criminal Law. A Normative Legitimacy Test of Terrorism-Related Offences on Expression, Information and Movement,* 125.

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. Performing such cyber-attacks, requires the state to disproportionately invest in personnel, equipment, knowledge and technology, whilst the terrorist can quickly buy a new cell phone or computer and re-access the information.

From the previous analysis can be concluded that, keeping in mind that the Belgian offensive cyber capabilities are not sufficiently developed yet,[72] 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.

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

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 proactive and offensive cyber-attacks on alleged terrorist fighters on Belgian soil. The following recommendations could be taken into account.[73]

Firstly, there is a need for clear, precise and accessible rules. As the law currently stands, it is not clear whether the evolving technologies and the proactive and offensive use of these techniques fall under the current legislative framework.[74] 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 by enlarging the competences of the civilian and military intelligence and security services after they have intruded an information system of an alleged terrorist present on the Belgian soil.[75] First, the services could be allowed to destroy the data the device contains, for example by infecting the system with malware, in which case the software would be attacked. Second, the services could freeze the device's functioning, disabling the terrorist's access to the information stored on the device and the device in general. Consequently, the hardware would be affected.

72 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 Ludivine 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* (4 November 2020), in *Parl.St.* Kamer 2020-2021, n° 55-1610/017, 25.

73 The following recommendations are based on the European Essential Guarantees for Surveillance Mechanisms, 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.

74 T. Wetzling, "Challenges for oversight," in *Bijzondere inlichtingenmethoden in de schijnwerpers – Les méthodes particulières de renseignement: de l'ombre à la lumière*, ed. Johan Vanderborght (Brussel: Levebvre Sarrut Belgium NV, 2020), 94.

75 The legislator would have to modify respectively articles 7 and 11 of the Belgian Law regulating the intelligence and security services.

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 and consequently be in line with the Council of Europe and the EU's 'with right' requirement of cyber-attacks.

Secondly, the necessity and proportionality to the legitimate objectives pursued have been discussed previously. However, the Belgian legislator could disagree with the analysis and consider the cyber-attacks necessary and proportionate.
Thirdly, since this complementary competence would imply a very severe breach of the person's rights, a strict and independent supervisory mechanism is required. The Committee R/I seems optimal for this responsibility since it already is entrusted with the oversight of these two intelligence and security branches.[76]

Lastly, an effective remedy mechanism should be provided. 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, which could be applied to the proposed legislative modification. The Committee R/I can intervene following such a written complaint.[77] 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.[78] No appeals procedure to the decision of the Committee R/I is possible.[79]

6. Conclusion

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 ISIL's online presence. 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. ●

76 Art. 3, 7° Belgian Law regulating the intelligence and security services refers to 'intelligence services', as defined by art. 3, 2° Belgian Law regulating the supervision of police and intelligence services and the Coordination Unit for Threat Assessment (18 July 1991), in *Belgian Gazette* (26 July 1991), 16.576.
77 Art. 43/4, 1st indent Belgian Law regulating the intelligence and security services.
78 Art. 43/6, §1 Belgian Law regulating the intelligence and security services.
79 Art. 43/8 Belgian Law regulating the intelligence and security services.

BIBLIOGRAPHY

- Belgian Code of Economic Law.
- Benedek, Wolfgang and Matthias C. Kettemann. *Freedom of expression and the Internet*. Strasbourg: Council of Europe Publishing, 2013.
- Bukovská, Barbora. "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.
- CJEU (7th Ch.), *Sotiris Papasavvas v. O Fileleftheros Dimosia Etairia Ltd* (9 September 2014), C-19/13, ECLI:EU:C:2014:2209.
- CJEU (Grand Ch.), *L'Oréal SA v. eBay International AG* (12 July 2011), C324/09, ECLI:EU:C:2011:474.
- Cambron, Rebecca J. "World War Web: Rethinking 'Aiding and Abetting' in the Social Media Age." *Case Western Reserve Journal of International law* 51, no. 1 (2019): 293-325.
- Charter of Fundamental Rights of the European Union. In *Official Journal of the European Union* (26 October 2012), n° 326.
- Chini, Maïté. "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/.
- 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.
- Coche, Eugénie. "Privatised enforcement and the right to freedom of expression in a world confronted with terrorism propaganda online." *Internet Policy Review* 7, no. 4 (2018): 1-17.
- Conway, Maura, Khawaja, Moign Lakhani, Suraj, Reffin, Jeremy, Robertson, Andrew and David Weir. "Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts." *Studies in Conflict & Terrorism* 42, no. 1-2 (2019): 141-160.
- Commissioner for Human Rights of the Council of Europe. *The rule of law on the internet and in the wider digital world.* 2014, Strasbourg: Council of Europe.
- Convention on Cybercrime (23 November 2001). In *European Treaty Series,* n° 185.
- Council of Europe. *Explanatory Report to the Convention on Cybercrime*. In *European Treaty Series* (23 November 2001), n° 185.
- Council of Europe, *International instruments – Cybercrime*, https://www.coe.int/en/web/cybercrime/international-instruments.

— De Coensel, Stéphanie. *Counter-Terrorism and Criminal Law. A Normative Legitimacy Test of Terrorism-Related Offences on Expression, Information and Movement.* Antwerp: Maklu, 2020.

— De Jaegere, Axel and Stefan 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/.

— Dedonder, Ludivine. *Policy Statement of Defence* (4 November 2020). In *Parl.St.* Kamer 2020-2021, n° 55-1610/017.

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

— Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (12 August 2013). In *Official Journal of the European Union* (14 August 2013), n° 218.

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

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

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

— Eechaute, Hannes. *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.

— Eechaute, Hannes. *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.

— Elkin-Koren, Niva. "Contesting algorithms: Restoring the public interest in content filtering by artificial intelligence." *Big data & society 7*, no. 2 (July 2020): 1-13.

— Ellermann, Jan. "Terror won't kill the privacy star – tackling terrorism propaganda online in a data protection compliant manner." *ERA Forum 17*, no. 4 (2016): 555-582.

— 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 Recommendation 2018/334 on measures to effectively tackle illegal content online (1 March 2018). In *Official Journal of the European Union* (6 March 2018), C/2018/1177, n° 63.

— European Convention on Human Rights (4 November 1950). In *European Treaty Series*, n°5 (November 1950).

— European Court of Human Rights. *Factsheet – Hate Speech,* September 2020.

https://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf.

— 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.

— Fernandez, Miriam and Harith Alani. "Artificial Intelligence and Online Extremism: Challenges and Opportunities." In *Predictive Policing and Artificial Intelligence,* edited by John McDaniel and Ken Pease, 132-162. London: Routledge, 2021. http://oro.open.ac.uk/69799/1/Fernandez_Alani_final_pdf.pdf

— 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.

— Human Rights Committee. *General Comment No. 34 on Article 19: Freedoms of opinion and expression.* 12 September 2011, CCPR/C/GC/34.

— Huszti-Orban, Krisztina. "Internet intermediaries and counter-terrorism: Between self-regulation and outsourcing law enforcement." In *10th International Conference on Cyber Conflict: CyCon X: Maximising Effects*, edited by Tomas Minarik, Lauri Lindstrom and Raik Jakschis (2018): 227-243.

— International Covenant on Civil and Political Rights. In *United Nations Treaty Series* 999 (December).

— Jones, David Martin, Schulte, Paul, Ungerer, Carl and Michael L. R. Smith. *Handbook of terrorism and counter terrorism post 9/11.* Northampton: Edward Elgar Publishing, 2019.

— Jørgensen, Rikke Frank and Anja Moller Pedersen. "Chapter 10 - Online Service Providers as Human Rights Arbiters." In *Law, Governance and Technology Series, Vol. 31, The Responsibilities of Online Service Providers,* edited by Mariarosaria Taddeo and Luciano Floridi, 179-199. Switzerland: Springer, 2017.

— "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.

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

— Law regulating the supervision of police and intelligence services and the Coordination Unit for Threat Assessment (18 July 1991). In *Belgian Gazette* (26 July 1991), 16.576.

— Llansó, Emma, van Hoboken, Joris, Leerssen, Paddy and Jaron 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.

— McKendrick, Kathleen. "Artificial Intelligence Prediction and Counterterrorism." *Chatham House.* August 2019. https://www.chathamhouse.org/sites/default/files/2019-08-07-AICounterterrorism.pdf.

— Quintel, Teresa and Carsten Ullrich. "Self-Regulation of Fundamental Rights? The EU Code of Conduct on Hate Speech, related initiatives and beyond." In

Fundamental Rights Protection Online: The Future Regulation of Intermediaries, edited by Bilyana Petkova and Tuomas Ojanen. Northampton: Edward Elgar Publishing, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3298719.

- Regulation 2021/784 of the European Parliament and of the Council on addressing the dissemination of terrorist content online (29 April 2021). In *Official Journal of the European Union* (17 May 2021), n° 127.
- Resolution 60/288 of the General Assembly of the United Nations on The United Nations Global Counter-Terrorism Strategy (8 September 2006). In *UN Doc.* A/RES/60/288.
- Secretary-General of the United Nations. *Note by the Secretary-General on the promotion and protection of the right to freedom of opinion and expression* (29 August 2018). In *UN Doc*. A/73/348 (2018).
- Schmitt, Michael. *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press, 2017.
- Stoltenberg, Jens. *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.
- Trommel, Jesse. 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.
- UK launched cyber-attack on Islamic State." *BBC News*, 12 April 2018, https://www.bbc.com/news/technology-43738953.
- 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). In UN Doc. GA/12309. https://www.un.org/press/en/2021/ga12309.doc.html.
- United Nations Office on Drugs and Crime. *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.
- Vanderborght, Johan. *Bijzondere inlichtingenmethoden in de schijnwerpers – Les méthodes particulières de renseignement: de l'ombre à la lumière.* Brussel: Levebvre Sarrut Belgium NV, 2020.
- Walker, Clive and Maura Conway. "Online terrorism and online laws." *Dynamics of Asymmetric Conflict* 8, no. 2 (2015): 156-175.
- Yar, Majid and Kevin F. Steinmetz. *Cybercrime and Society.* 3rd ed. California: Sage Publications, 2019.