# Governing Online Terrorist Propaganda: A societal security issue

Victoria A. Jangada Correia[1], Moufida Sadok[1]

[1] *School of Criminology and Criminal Justice, University of Portsmouth, University House, Winston Churchill Avenue, Portsmouth, PO1 2UP, United Kingdom*

**Abstract**

There is an increasing threat posed by terrorism in modern day, and with the internet enabling new ways of disseminating online terrorist propaganda, audiences and support for terrorist groups are growing. The complex linkage between society and technology is become ever more critical as the world continues to shift more day-to-day life online, and this notion has increased greatly during the coronavirus global pandemic where online platforms have become an essential aspect for communicating. The spread of online terrorist propaganda has sparked concerns about the governance of Internet. However, Internet governance is multifaceted, complex and can be examined through various lenses. This paper argues that there is a need for a socio-technical perspective, exploring the inextricable linkages between societies and technology, on Internet governance. Focusing on the UK's approach to governing terrorist propaganda, the paper highlights the strengths and limitations of the model of national law and regulation.

**Keywords**

Online Terrorist Propaganda, Socio-technical perspective, Internet Governance, Cyber Terrorism

## 1. Introduction

It was stated by Lord Hope [1] that "it is first the responsibility of government in a democratic society to protect and safeguard the lives of its citizens". As terrorist group capabilities continue to expand within cyber environments, so must the regulations and laws held to prosecute individuals in order to ensure the security of societies and its citizens. In order to do this, establishing measures of internet governance which prevent and detect cyber-criminal activity generally is pertinent [2, 3]. Exploring the way in which technology is enabling terrorist activity in modern day will further enable a greater understanding of how societal dimensions are being influenced and impacted by technology, in turn aiding stakeholders involved in combatting the overarching threat of cyber terrorism.

This research paper questions what the most effective way of governing online terrorist propaganda is. To address this question, this paper will firstly provide an overview of the nature and scale of online terrorist propaganda. The following section critically discusses the relevance of the national regulation and law model suggested by [2] in addressing the threats posed by online terrorist content. In this section, the significance of a national model will be applied directly to the UK, considering the recent release of the Online Safety Bill [4] and the way in which this will address online terrorist propaganda in the UK. Ultimately, the paper will reflect and make conclusions on how online terrorist propaganda can be tackled through internet governance to reduce the current risk to societies security.

The discussions and the reflections in this paper are based on reviews of currently available literature regarding cyber terrorism, online terrorist propaganda, and internet governance as well as further reviews of UK laws and regulations in relation to online terrorist propaganda. Further, the paper explores the relevance of a sociotechnical approach to tackle online terrorist propaganda.

7th International Workshop on Socio-Technical Perspective in IS development (STPIS 2021) 11-12 October 2021, Trento, Italy
EMAIL: vickyalexc@icloud.com ; moufida.sadok@port.ac.uk
ORCID: 0000-0002-0305-3381 (A. 1); 0000-0003-2981-6516 (A.2)

## 2. Nature and Scale of Online Terrorist Propaganda

Online terrorist propaganda falls under the umbrella term of cyber terrorism. The UK currently faces a severe threat level from terrorism, and as technology has developed, so are the characteristics of traditional terrorist methods [5, 6]. There is thus far no universally accepted definition of cyber terrorism amongst academics and governments [7, 8]. This is arguably problematic and highlights a lack of unanimity in approaching the threat of cyber terrorism. The Terrorism Act 2006 [9] defines terrorism as an act of violence, or threat of act of violence, against the public and/or property, intimidating the public and/or property, or advancing political or religious ideologies. However, there is no attempt at defining cyber terrorism, a term in which online terrorist propaganda falls under.

Nonetheless, based on the plethora of definitions currently available [10, 11, 12], this paper proposes that cyber terrorism encapsulates cyber enabled activity which intends to advance political, social, or religious ideologies against the public, and cyber dependent activity which further intends to threaten or facilitate damage against the public, properties, and/or systems. As there has been discourse about the distinction between extremism and terrorism [13], this definition merges both concepts by implying that there does not always have to be a physical impact of an action to be categorised as an act of cyberterrorism. In light of the above definition, online terrorist propaganda classifies as a cyber terrorist act, and includes the use of the internet for communications with an audience to increase support and keep followers informed [14, 15]. The relationship between online terrorist propaganda and cyber capabilities can be better understood through McGuire and Dowling's cybercrime classification approach [16]. An enabled cybercrime refers to a crime which could still occur without cyber capabilities whereas a dependent cybercrime refers to a crime which can only be carried out utilising cyber capabilities. Although it could be argued that online terrorist propaganda would fall under the enabled cybercrime, this paper argues that due to the dependence on online platforms for sharing terrorist propaganda, this would more suitably be categorised as a 'cyber dependent' act.

According to the United Nations Office on Drugs and Crime [15], sharing propaganda is a primary use of the internet by terrorist groups and tends to include communications regarding instructions, explanations, justifications or promotions of their terrorist beliefs and activities. Although many of these terrorist online activities are not necessarily prohibited, it is important that these communications are regulated and/or collected as data in order to inform multiple stakeholders involved in the detection, investigation, prevention, and prosecution of terrorist and cyber terrorist crimes in the UK.

According to the Crown Prosecution Service [17], terrorist groups have distinct ethnic, religious, political and racial identities and they all hold varying beliefs, aims and purposes. Some examples of terrorist groups which currently pose a threat across the world include Hamas, Al-Qaeda, Islamic State and right-wing extremist groups. Although not all these groups inflict physical harms against a nation or group of people, they nonetheless pose a threat through their online presence. It has been postulated that terrorist organisations use cyber capabilities for the main aims of recruitment, incitement, and radicalisation [15, 18]. This is in turn a financially beneficial way of growing an audience and fits Jaishankar's Space Transition Theorisation that traditional crimes transition into cyber environments due to financially advantageous characteristics and being able to reach wider audiences [19]. Although terrorism-related arrests have reduced by 37% since 2020 [20, 21], this is merely reflective of the global pandemic which has prompted terrorist groups to alter their methods of disseminating propaganda and spreading misinformation to continue growing support for their beliefs [22]. This potentially has been having effects on the security of societies as there has been greater ease in accessing and engaging with terrorist propaganda, resulting in an unobserved and hidden growing audience. It is however important to highlight that terrorism is merely a social construct of which the meaning is shaped by the views held by the person categorizing what it means to them as an individual [23, 24]. In light of this, although online terrorist propaganda promotes thoughts and beliefs which may be seen as incorrect by one group of people, to another these may be held close to their core norms and values. This makes cyber terrorism and online terrorist propaganda difficult to define and understand due to its alternating nature, in turn

impacting the effectiveness of attempting to govern a concept which holds inter-changing meanings to different groups of people.

A recent case study which was carried out regarding Islamic States' use of online terrorist propaganda can be used to better understand the scale of terrorist online propaganda. This study accessed, archived, and carried out analysis into one of the largest known Islamic State online repositories holding just under 100,000 folders and files [25]– this has been nicknamed "Cloud Caliphate". This studies research highlighted that, in contrast to older Islamic State repositories which would use the likes of Google Drive and Dropbox to share and store their propaganda [26], they have increasingly been utilising standalone websites and social media platforms to resurge support for their group, which is a notion further supported by Weimann [27]. It was also found that thousands of individuals visited the repository each month, and when this is paired with the fact that the "Cloud Caliphate" cache is only a small part of a complex online eco-system, the expanding numbers of support for Islamic State are alluded to [25]. This one case study example puts into perspective the large amount of online terrorist propaganda which can be found online from a variety of terrorist groups. Another significant aspect exemplified in this case study is how terrorists disseminating propaganda are able to make it accessible in different spoken languages for a large scale of viewers [28, 29]. This alludes to the globality of terrorist activity and further emphasizes the way in which technology is affecting the societal security.

A more recent example which explores the scale of online terrorist propaganda is the Plymouth shooting in which Jake Davison murdered five innocent individuals [30, 31]. Davison had an online presence on YouTube in which he actively practiced hate speech against women, encouraged violent acts, and further promoted his Incel (involuntary celibate) alignment. Although Incel is not a proscribed terrorist organisation in the UK, Davison's atrocious actions were classed as a terrorist attack, which suggests that his online actions leading up to the attack were also classed as terrorist behaviour [32], further highlighting the scale of online terrorist propaganda. Davison's online presence was not detected by YouTube or authorities in the UK. Davison had just short of 100 subscribers to his YouTube channel who he shared Incel ideology with and incited violence to, and these were perhaps all missed opportunities to detect present and future terrorist behaviour and prevent the attack from happening. Furthermore, Davison was part of a large YouTube platform called IncelTV with 18,000 subscribers, which encourages Incel ideology [30]. The support which Davison had, let alone the support which IncelTV has, emphasises the scale of undetected online terrorist propaganda in the UK and internationally. Both examples presented in this paper highlight the impact which technology has had on the dissemination of online terrorist propaganda, subsequently impinging on the security of society.

## 3. Internet Governance

Establishing a universally accepted definition of internet governance has long been deliberated by academics and policy makers [33, 34, 35]. However, in order to reach a unanimous understanding of internet governance it is essential that the words making up the term are clearly understood. The internet can be best understood as an umbrella term which categorises hardware and software infrastructures, applications, and content which is used to generate or communicate through these technological means [2, 36]. Amongst academics, it has been generally agreed that governance can be best understood through the term 'regulation' [37, 38] which relates to operations intending influences on any given states' government affairs [35]. In light of these definitional breakdowns, this paper proposes that the following definition can be used to best understand the term 'internet governance' - "the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures and programmes that shape the evolution and use of the internet" [39].

Within internet governance there are five categorisations of parties who could be responsible for governing. Solum [2] coherently breaks this down into: the model of cyberspace and spontaneous ordering; the model of transnational institutions and international organisations; the model of code and

internet architecture; the model of national governments and law; and the model of market regulation. This paper will specifically focus on the model of national governments and law in comparison to the model of transnational and international organisations as these are potentially the most pertinent to online terrorist propaganda.

## 3.1. Model of National Regulation

The model of national governments and law refers to the concept that the internet should be governed in the same way that any other human activity is governed [2]. With regards to the UK, this refers to UK laws and policies such as: The Computer Misuse Act 1990 [40]; The Digital Economy Act 2017 [41]; and most recently drafted, the Online Safety Bill [4]. Contrarily, the international and transnational model of governing proposes that a national governing approach is not suitable due to the global characteristic of cyberspace [2]. This model refers to institutions including The Internet Corporation for Assigned Names and Numbers [42], and The Internet Engineering Task Force [43] who govern the technical infrastructure and architecture of the Internet through a multi-stakeholder approach. Although the international model can be relevant to online terrorist propaganda due to the globality of the cyber environment, the national model has been deemed most suitable to explore the governing of online terrorist propaganda as the terrestrial and cyber effects of terrorism are mostly aimed at an individual nation state/social group, and therefore national regulation of online terrorist propaganda is key for deterrence and prevention.

National governing can be effective in determining the conditions for internet-based markets and enabling background conditions for further development of internet governance ensuring that anything criminal is regulated [2]. These are important aspects in ensuring the internet is governed effectively, enabling stakeholders such as law enforcement and policy makers, to continue developing their approaches to prevent, detect and investigate online terrorist propaganda. Perhaps if conditions were not regulated and developed on a national level, this could result in a nation's government falling behind the evolving nature of the cyber environments impacting the effectiveness of their laws and policies. This could have an undeniable impact on the various stakeholders involved in the direct and indirect regulation of the internet, and additionally on providing security for societies being impacted by technological advancements relating to the dissemination of terrorist content. Arguably, enabling a national government to govern the internet would be more desirable than an international or transnational institution due to the fact that each nation across the globe has differing views of what is classified as criminal, deviant and normal based on their societal, religious and traditional norms [44, 45, 46]. Perhaps attempting to govern various nations under the same policy would disturb the norms and values which make up a country and each nations' individualistic sovereignty.

The model of national governing imposes a potential issue of disabling open-access content for internet users in that nation, which can be better understood through China and Russia who both censor the content which their civilians can view and interact with [47, 48]. Looking specifically at China, for example, their politics typically align with more left wing, communist practices, which would indicate that their governance of the internet would lean more towards the censorship of content which civilians can access as so to control what their perspectives towards an array of topics are [49, 50, 51]. Inevitably, this impacts society, especially the concept of 'self-educating' where individuals are controlled and deterred from exploring outside of what is already known to them [52, 53]. However, this limitation poses less risk to the UK due to its fairly central political standpoint, and furthermore, unlike China the UK does not intend to stop freedom of expression through internet governance, rather the crimes imposing a threat to societal security.

Overall, the discussed limitations could encourage the use of an international or transnational governing model due to the internet's lack of geographic borders and the risk of censorship which national governance poses, however, the discussed national governing limitations arguably still pose the same risks in an international governing approach. Therefore, nationally governing the internet

would be more effective as this approach would work in tandem with the instilled laws and policies of other crimes in a nation.

## 3.2. UK's Approach

Key national bodies and institutions involved in the regulation of online terrorist propaganda include: The UK Internet Referral Unit; The Department for Digital, Culture, Media and Sport; The Home Office; Ofcom; and The Independent Reviewer of Terrorism Legislation. All these national bodies and institutions play differing roles from the detection and referral of terrorist propaganda to the development and scrutinisation of legislation, with the overall aim of safeguarding citizens from terrorism. In the UK, Table 1 presents the current regulatory frameworks and policies regarding online terrorist activity include:

**Table 1**
Regulatory Frameworks in the UK Regarding Online Terrorist Activity.

| Regulatory Framework in the UK | Explanation |
|---|---|
| Draft Online Safety Bill [4] | Published in May 2021, this draft Bill is a direct development of The Online Harms White Paper [54]. It outlines the key principles for the online regulation of terrorist activity and applies a duty of care to tech companies in protecting its users. This will be directly regulated by Ofcom. This Bill highlights the importance of human review in the regulation of the internet. |
| The Terrorism Act 2000 [55] | This is a foundation of UK Legislation for Terrorism in general. An example of the way in which it applies to Online Terrorist Propaganda is in Section 58 where it specifies an offence of having online information which is of use to the terrorist. |
| The Terrorism Act 2006 [9] | The 2006 Act develops new terrorist offences based off the 2000 Act. Most specifically in Section 2, this Act makes it an offence to distribute terrorist propaganda which may aid a terrorist groups aims. |
| The Counter-Terrorism and Border Security Act 2019 [56] | This Act criminalises viewing or acquiring terrorist content online. For example, it amends Section 52 of the Terrorism Act 2000 stating that the viewing of terrorist content could result in up to 15 years in prison dependable on the intent and excuse for viewing the content. |

Earlier this year it was highlighted that not all online terrorist propaganda can be criminalised as a large amount of terrorist material is produced with a 'legal' mindset in order to bypass UK regulations [57]. Although there is not a great deal of readily available literature regarding the effectiveness of the UK government's approach to online terrorist propaganda, instances from the news can aid in discussion. The first instance is a group of three men who were found sharing terrorist propaganda online in chat rooms and on social media in support of Islamic State [58]. All these individuals were sent to jail for a minimum of four years, in turn, mitigating the risk posed on the communities which these individuals were from. In another instance, an individual from a neo-Nazi group, was sharing propaganda and stirring up a 'race war' against ethnic minorities [59]. This individual was found guilty on 12 charges related to terrorism and sentenced to five years in jail. Overall, in both these cases, it can be seen that the regulations in place to govern these internet crimes were effective and further dissemination of online terrorist propaganda from these individuals has at least been halted for a certain

amount of time. This paper nonetheless proposes that the effectiveness of governing online terrorist propaganda should not plateau but rather aim to continue on an upward trend as so to ensure that societies are being kept safe from the posed threats.

As discussed, one of the strengths of national governing is the notion that governments can enable background conditions to be able to continue ensuring the internet is regulated and safe from terrorist propaganda. As explored, the UK, through its regulatory bodies and policies, can ensure that individuals and/or groups disseminating terrorist propaganda online are identified and charged (depending on the nature and severity of the propaganda in question). By ensuring the nation's regulatory control of the internet, stakeholders directly involved in the detection, investigation, prevention and prosecution of online terrorist propaganda can all work in tandem with the overall goal of decreasing the rate of terrorist activity in the UK as outlined in the CONTEST strategy [60, 61]. Were a solely international/transnational approach to be taken, this could affect the effectiveness of UK policing and regulatory bodies in detecting the victims of online terrorist propaganda and providing prompt support.

A strength regarding the future use of the Online Safety Bill [4], is that this enables the UK government to work specifically in tandem with the actual providers of communication services. This will not only enable the investigation of online terrorist crimes which come to surface from public reports but will also enable communication servers to regulate terrorist online activity. More specifically, the online safety bill outlines duties of care, risk assessments, safety duties, freedom of speech, user reporting and record keeping principles which should be followed by a range of providers such as user-to-user and search services. In addition, this bill also highlights specific policies regarding terrorist activity online and the way in which this should be dealt with by service providers. For example, it highlights that Ofcom will have the right to give technology warning notices to service providers if there is evidence of online terrorist activity on their services [4]. Although the draft Online Safety Bill has succumbed to much criticism regarding freedom of expression, privacy and regulating threats to public safety, this is potentially a positive step forward in attempting to regulate online terrorist propaganda and is undergoing pre-legislative scrutiny to ensure these criticisms are investigated [62, 63]. Nonetheless, once the online safety bill has been amended and is paired with the terrorism laws in the UK, this should see success as Ofcom's regulatory position will enable investigative and prosecuting services the evidence needed to charge criminals in line with the Criminal Justice Act 2003 [64] and the Police and Criminal Evidence Act 1984 [65].

On the other hand, there are some limitations in applying the model of national governing to the regulation of online terrorist propaganda, however this paper posits that these limitations could be overcome. One of the limitations discussed outlines the risk of censorship which comes with restricting one's freedom of expression [2]. Where an average person may look at terrorist activity and practice their basic human rights in deciding to not follow it, terrorists also practice their basic human rights by deciding to follow it, as they believe that what they are fighting for is important [61]. Fletcher stated that "those who opt for terror always believe their cause is just" [66], therefore, the censorship of online terrorist propaganda arguably takes away freedom of speech from the terrorist groups. This is an especially interesting stance better understood through YouTube's Community Guidelines which state that terrorist organisations are not permitted to use their services to share terrorist related content [67]. Problematically, these guidelines lack in defining what 'terrorism' and 'terrorist content' actually means, additionally, there is no specific guideline on what is 'just' and 'unjust'. This unclear approach further enables terrorist organisations to continue using these services by circumventing the guidelines as they believe what they are doing is just. In light of this issue, the Draft Online Safety Bill [4] will ensure that service providers such as YouTube, will need to determine definitions of terrorism and put their regulatory principles in the terms of service so that individuals can practice their basic human rights by making an informed decision to use that service or not.

Another limitation of the national governance model is the notion that the internet has no borders and therefore it should not be confined to being regulated in one nation state. Although online terrorist propaganda is affecting all countries globally, and more times than not, the internet platforms which terrorists use to disseminate propaganda are not limited to one nation [25], terrorist propaganda is

directed at individuals who are part of a community within a nation state, and therefore the direct physical results will be seen in a given nation state. Just as national laws dictate legal and illegal activities, the internet should be regulated reflecting on these laws. In light of this, nations should be the primary governance approach to online terrorist propaganda. However, this research paper posits that a multistakeholder approach may be the most suitable way as so to ensure both national governing bodies and institutions, alongside international regulatory bodies, all work in tandem to deter and prevent terrorism. With a multistakeholder approach, the individual nation would practice autonomy in deciding the process of dealing with the online terrorist activity directly affecting them, and the international nations would act as supporting bodies to aid in detecting and preventing further terrorist activity. This multi-stakeholder approach could result in improved approaches for protecting victims of terrorist activity and prosecuting those responsible, as it would mean that despite the cross-border characteristic of cyber terrorism, the threat of terrorism could be better understood and prevented in a more undisputed manner.

## 4. Discussion and Conclusion

This research paper has discussed the relevance and importance of internet governance in contemporary society specifically relating to the dissemination of online terrorist propaganda. The paper suggests that a model of national governing and law would be the most suitable approach to govern and regulate online terrorist propaganda in the UK. Although there are limitations for this approach including the risk of censorship, this paper highlighted mitigation strategies which will be introduced in the UK once the Draft Online Safety Bill has been established [4]. However, it is possibly important to acknowledge that with a multicultural British society, issues regarding the disruption of cultural norms and values may still be apparent, and further limitations of nationally governing the dissemination of online terrorist propaganda may become apparent. In addition, the use of online terrorist propaganda is on an incline, more so over the past year with the global pandemic. As discussed, this increased use of technology for terrorist activity has a direct impact on society and its communities in which individuals who align with terrorist organisations pose threats. Therefore, it is important to consider online propaganda as a sociotechnical phenomena as it requires meaningful communication and interactions between social groups that are supported by the Internet. In turn, the socio-technical aspects of online terrorist propaganda and cyber terrorism can be better understood, and cyber terrorist threats can be reduced.

Overall, this paper has argued that a multi-stakeholder approach would be desirable in order to have nation states and international bodies working in tandem to increase the effectiveness of internet governance, however the primary governor of what is right and wrong should always be the nation in line with their laws. This paper suggests that further research needs to be conducted into the effectiveness of utilising a national governing model for online terrorist propaganda. In addition, further research should be carried out to develop on the “Cloud Caliphate” case study [25] as this will aid key stakeholders in the detection, investigation, prevention and prosecution of online terrorist propaganda. Yet most importantly, is the need for clear definitions and distinctions of cyber terrorism and online terrorist propaganda so that stakeholders can have a more unanimous understanding, in turn ensuring societies are kept secure from the risk posed by terrorism.

## 5. References


[1] House of Lords. (2004). Judgements – A (FC) and others (FC) (Appellants) v. Secretary of State for the Home Department (Respondent). (UKHL 56). https://publications.parliament.uk/pa/ld200405/ldjudgmt/jd041216/a&oth-6.htm

[2] Solum, L. B. (2009). Models of Internet Governance. In L. A. Bygrave & J. Bing (Eds.), Internet Governance: Infrastructure and Institutions (pp. 48-91). Oxford University Press.

[3] Glen, C. M. (2018). Controlling Cyberspace: The Politics of Internet Governance and Regulation. Praeger.

[4] Department for Digital, Culture, Media & Sport. (2021). Draft Online Safety Bill (CP405). London. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf
[5] GCHQ. (2019). The cyber threat. https://www.gchq.gov.uk/information/cyber-threat
[6] Sabbagh, d., & Grierson, J. (2020, November 3). UK terror threat upgraded to sever after France and Austria attacks. The Guardian. https://www.theguardian.com/uknews/2020/nov/03/uk-terror-threat-upgraded-to-severe-after-france-and-austria-attacks
[7] Plotnek, J. J., & Slay, J. (2021). Cyber terrorism: A homogenized taxonomy and definition. Computers & Security, 102, 1-9. https://doi.org/10.1016/j.cose.2020.102145
[8] Yunos, Z., & Sulaman, S. (2017). Understanding Cyber Terrorism from Motivational Perspectives. Journal of Information Welfare, 16(4), 1-13. https://www.jstor.org/stable/26504114
[9] Terrorism Act 2006, c.11. https://www.legislation.gov.uk/ukpga/2006/11/contents
[10] Conway, M. (2014). Reality Check: Assessing the (Un)likelihood of Cyberterrorism. In T. M. Chen, L. Jarvis & S. Macdonald (Eds.), Cyberterrorism: Understanding, Assessment, and Response (pp. 103-121). Springer.
[11] Foltz, B. C. (2004). Cyberterrorism, computer crime, and reality. Information Management & Computer Security, 12(2), 154-166. https://doi.org/10.1108/09685220410530799
[12] Holt, T. J. (2012). Exploring the Intersections of Technology, Crime, and Terror. Terrorism and Political Violence, 24(2), 337-354. https://doi.org/10.1080/09546553.2011.648350
[13] Onursal, R., & Kirkpatrick, D. (2019). Is Extremism the 'New' Terrorism? The convergence of 'Extremism' and 'Terrorism' in British Parliamentary Discourse. Terrorism and Political Violence, 1-23. https://doi.org/10.1080/09546553.2019.1598391
[14] Aly, A., Macdonald, S., Jarvis, L., & Chen, T. M. (2016). Introduction to the special issue: terrorist online propaganda and radicalisation. Studies in Conflict and Terrorism, 40(1), 1-9. https://doi.org/10.1080/1057610X.2016.1157402
[15] United Nations Office on Drugs and Crime. (2012). The Use of the Internet for Terrorist Purposed. United Nations. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf
[16] McGuire, M., & Dowling, S. (2013). Cybercrime: A review of the evidence: Summary of key findings and implications. Home Office Research Report 75. London: Home Office, October. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf
[17] Crown Prosecution Service. (2017). Terrorism. https://www.cps.gov.uk/crime-info/terrorism
[18] Baugut, P., & Neumann, K. (2019). Online Propaganda use during Islamist radicalisation. Information, Communication & Society, 23(11), 1570-1592. https://doi.org/10.1080/1369118X.2019.1594333
[19] Jaishankar, K. (2007). Establishing a Theory of Cyber Crimes. International Journal of Cyber Criminology, 1(2), 7-9. https://doi.org/10.5281/ZENODO.18792
[20] Home Office. (2020). Operation of police powers under the Terrorism Act 2000 and subsequent legislation: Arrests, outcomes and stop and search Great Britain, financial year ending March 2020. Home Office National Statistics. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/891341/police-powers-terrorism-mar2020-hosb1520.pdf
[21] Home Office. (2021). Operation of police powers under the Terrorism Act 2000 and subsequent legislation: Arrests, outcomes, and stop and search Great Britain, year ending March 2021. https://www.gov.uk/government/statistics/operation-of-police-powers-under-the-terrorism-act-2000-financial-year-ending-march-2021/operation-of-police-powers-under-the-terrorism-act-2000-and-subsequent-legislation-arrests-outcomes-and-stop-and-search-great-britain-year-ending#arrests-and-outcomes
[22] Tony Blair Institute for Global Change. (2020). Snapshot: How Extremist groups are responding to Covid-19. Tony Blair Institute for Global Change. https://institute.global/sites/default/files/2020-05/Snapshot%203%20COVID19%20V02.pdf

[23] Anderson, D. (2013). Shielding the Compass: How to Fight Terrorism Without Defeating the Law. SSRN Electronic Journals. 1-19. https://doi.org/10.2139/ssrn.2292950
[24] Greene, A. (2017). Defining Terrorism: One Size Fits All? International and Comparative Law Quarterly, 66(2), 411-440. https://doi.org/10.1017/S0020589317000070
[25] Ayad, M., Amarasingam, A., & Alexander, A. (2021). The Cloud Caliphate: Archiving the Islamic State in Real Time. Institute for Strategic Dialogue. https://www.isdglobal.org/wp-content/uploads/2021/05/Cloud-Caliphate.pdf
[26] Lakomy, M. (2020). Mapping the online presence and activities of the Islamic State's unofficial propaganda cell: Ahlut-Tawhid Publications. Security Journal, 34, 358-384. https://doi.org/10.1057/s41284-020-00229-3
[27] Weimann, G. (2016). The emerging role of social media in recruitment of foreign fighters. In A. de Guttry, F. Capone, & C. Paulussen (Eds.), Foreign fighters under international law and beyond (pp.77-95). T.M.C. Asser Press.
[28] Ozeren, S., Hekim, H., Elmas, M. S., & Canbegi, H. I. (2018). An analysis of ISIS Propaganda and Recruitment Activities Targeting the Turkish Speaking Population. International Annals of Criminology, 56(1-2), 105-121. https://doi.org/10.1017/cri.2018.14
[29] Pashentsev, E. N., & Bazarkina, D. Y. (2021). ISIS Propaganda on the Internet, and Effective Counteraction. Journal of Political Marketing, 20(1), 17-33. https://doi.org/10.1080/15377857.2020.1869812
[30] Bancroft, H., Mathers, M., & Tidman, Z. (2021, August 14). Jake Davison named as Plymouth shooter: What we know so far. The Independent. https://www.independent.co.uk/news/uk/home-news/jake-davison-plymouth-shooting-b1901948.html
[31] Hardy, J., Gardner, B., & Lyons, I. (2021, August 14). 'I am a terminator' boasted Plymouth gunman Jake Davison in final YouTube video before rampage. The Telegraph. https://www.telegraph.co.uk/news/2021/08/14/plymouth-shooting-gunman-said-terminator-final-youtube-video/?li_source=LI&li_medium=liftigniter-onward-journey
[32] Casciani, D., & De Simone, D. (2021, August 13). Incels: A new terror threat to the UK?. BBC News. https://www.bbc.co.uk/news/uk-58207064
[33] World Summit on the Information Society. (2005). WSIS-05/TUNIS/DOC/6(Rev. 1)-E Tunis Agenda for the Information Society. Tunis: World Summit on the Information Society. Retrieved from: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html
[34] DeNardis, L. (2014). The Global War for Internet Governance. Yale University Press.
[35] Hoffman, J., Katzenbach, C., & Gollatz, K. (2016). Between coordination and regulation: Finding the governance in Internet governance. New Media & Society, 19(9), 1406-1423. https://doi.org/10.1177%2F1461444816639975
[36] Abbate, J. (2017). What and where is the internet? (Re)defining Internet histories. Internet Histories: Digital Technology, Culture and Society, 1(1-2), 8-14. https://doi.org/10.1080/24701475.2017.1305836
[37] Feick, J., & Werle, R. (2010). Regulation of cyberspace. In R. Baldwin., M, Cave., & M. Lodge (Eds), The Oxford Handbook of Regulation (pp. 523-547). Oxford University Press.
[38] Mueller, M. (2017). Is cybersecurity eating internet governance? Causes and consequences of alternative framings. Digital Policy, Regulation and Governance, 19(6), 415-428. https://doi.org/10.1108/DPRG-05-2017-0025
[39] Working Group on Internet Governance. (2005, June). Report of the Working group on Internet Governance. https://www.wgig.org/docs/WGIGREPORT.pdf
[40] Computer Misuse Act 1990, c.18. https://www.icann.org/policy/implementation
[41] Digital Economy Act 2017, c.30. https://www.legislation.gov.uk/ukpga/2017/30/part/6/crossheading/internet-filters/enacted
[42] Internet Corporation for Assigned Names and Numbers. (n.d.). Implementing Policy at ICANN. ICANN. https://www.icann.org/policy/implementation
[43] Internet Engineering Task Force. (n.d.). Internet Standards. IETF. https://www.ietf.org/standards/
[44] Epstein, D. (2013). The making of institutions of information governance: The case of the internet governance forum. Journal of Information Technology, 28(2), 137-149. https://doi.org/10.1057%2Fjit.2013.8

[45] Licht, A. N. (2008). Social Norms and the Law: Why Peoples Obey the Law. Review of Law and Economics, 4(3), 715-750. https://doi.org/10.2202/1555-5879.1232
[46] World Health Organisation. (2009). Changing cultural and social norms supportive of violent behavior. Geneva: World Health Organisation. https://www.who.int/violence_injury_prevention/violence/norms.pdf
[47] Ermoshina, K., Loveluck, B., & Musiani, F. (2021). A market of black boxes: The political economy of internet surveillance and censorship in Russia. Journal of Information Technology and Politics, 1-16. https://doi.org/10.1080/19331681.2021.1905972
[48] Zhu, Y., & Fu, K. (2020). Speaking up or staying silent? Examining the influences of censorship and behavioral contagion on opinion (non-) expression in China. New Media and Society, 1-22. https://doi.org/10.1177%2F1461444820959016
[49] Dowell, W. (2006). The internet, censorship, and China. Georgetown Journal of International Affairs, 7(2), 111-120. https://heinonline.org/HOL/P?h=hein.journals/geojaf7&i=289
[50] Shen, H. (2016). China and global internet governance: toward an alternative analytical framework. Chinese Journal of Communication, 9(3), 304-324. https://doi.org/10.1080/17544750.2016.1206028
[51] Yang, F., & Mueller, M. L. (2014). Internet governance in China: a content analysis. Chinese Journal of Communication, 7(4), 446-465. https://doi.org/10.1080/17544750.2014.936954
[52] Bai, Y., & Li, Y. (2020). Good bye Chiang Kai-shek? The long-lasting effects of education under the authoritarian regime in Taiwan. Economics of Education Review, 78, 1-17. https://doi.org/10.1016/j.econedurev.2020.102044
[53] Chen, Y., & Yang, D. Y. (2019). The impact of media censorship: 1984 or brave new world?. American Economic Review, 109(6), 2294-2332. https://doi.org/10.1257/aer.20171765
[54] Department for Digital, Culture, Media & Sport., & Home Office. (2020). Online Harms White Paper. https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper
[55] Terrorism Act 2000, c.11. https://www.legislation.gov.uk/ukpga/2000/11/contents
[56] Counter-Terrorism and Border Security Act 2019, c.3. https://www.legislation.gov.uk/ukpga/2019/3/contents/enacted
[57] Dearden, L. (2021, January 7). Online extremism 'cannot be policed', says head of UK counter-terror police. The Independent. https://www.independent.co.uk/news/uk/home-news/extremism-online-police-definition-freedom-expression-basu-b1779631.html
[58] Reaidi, J. (2021, May 21). Man from Harrow Jailed for terrorism material. Harrow Times. https://www.harrowtimes.co.uk/news/19319843.terrorist-harrow-among-three-men-jailed/
[59] Gordon, A. (2021, May 6). Politics student, 23, accused of 12 terror offences joined neo-Nazi group to stir up 'race war' against ethnic minorities after posting 'virulently racist, anti-Semitic and homophobic propaganda' online, court hears. Mail Online. https://www.dailymail.co.uk/news/article-9549183/Politics-student-joined-neo-Nazi-groups-used-social-media-stir-race-war.html
[60] HM Government. (2018). CONTEST: The United Kingdoms Strategy for Countering Terrorism. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf
[61] Macdonald, S., Correia, S. G., & Watkin, A. (2019). Regulating terrorist content on social media: automation and the rule of law. International Journal of Law in Context, 15(2), 183-197. https://doi.org/10.1017/S1744552319000119
[62] Wingfield, R. (2021, 18 May). First thoughts on the UK's Draft Online Safety Bill. Global Partners Digital. https://www.gp-digital.org/first-thoughts-on-the-uks-draft-online-safety-bill/
[63] Woods, L., & Perrin, W. (2021, 15 June). The Draft Online Safety Bill: Carnegie UK Trust initial analysis. Carnegie UK Trust. https://www.carnegieuktrust.org.uk/blog/the-draft-online-safety-bill-carnegie-uk-trust-initial-analysis/
[64] Criminal Justice Act 2003, c.44. https://www.legislation.gov.uk/ukpga/2003/44/contents
[65] Police and Criminal Evidence Act 1984, c.60. https://www.legislation.gov.uk/ukpga/1984/60/contents
[66] Fletcher, G. P. (2006). The indefinable concept of terrorism. Journal of International Criminal Justice, 4(5), 894-911. https://doi.org/10.1093/jicj/mql060

[67] YouTube. (2018). Community Guidelines Strike Basics. YouTube Help. https://support.google.com/youtube/answer/2802032?hl=en-GB