CYTREC
CYBER THREATS RESEARCH CENTRE

Swansea University
Prifysgol Abertawe
Hillary Rodham Clinton
School of Law | Ysgol y Gyfraith

Response to the Online Harms White Paper

Executive Summary and Recommendations

- We broadly support the nature and scope of the proposed regulatory regime. Whilst we welcome the Government's stated commitment to tackling online harms, we recommend a focus on key priorities, including terrorist content and child sexual exploitation and abuse. The range of stated harms may be too broad to ensure the most serious online harms get the regulatory attention they deserve. Additional investment in specialist enforcement skills and capability within the Government's Serious and Organised Crime Strategy will also be necessary, particularly in mitigating any displacement effects;
- We support the commitment to annual transparency reporting (question 1);
- We advocate the use of super complaints, using as a template the policing system provided by the Police Reform Act 2002, ss.29A-C and associated secondary legislation (question 2);
- We do not believe that the government should consider other measures of user redress (question 3);
- We advocate the creation of a specific parliamentary committee to scrutinise the work of the regulator and the general operation of the regulatory framework (question 4);
- We are supportive of the proposals for defining online platforms and services, as long as a responsive approach to regulation is adopted (question 5);
- We welcome the recognition of the importance of privacy and the differentiated approach for private communications. We recommend any definition of "private communications" distinguishes between privacy on the one hand, and secrecy and covertness on the other (questions 6 and 7);
- We believe that a proportionate regulatory regime would have regard to the degree of company engagement with the regulator and the extent to which the conduct of companies enhances or undermines the overall rationale of the framework, as well

as the capacity of companies, the reach of their platforms and the severity of the harms (question 8);

- We recommend the creation of a new, bespoke regulator (questions 10 and 11);
- We believe that a range of enforcement tools is necessary in order to facilitate responsive regulation. This includes ISP blocking. However, ISP blocking should be regarded as being towards the top of the pyramid of available tools in order to encourage greater engagement with less severe interventions (question 12);
- We believe that companies based outside the UK and EEA should be incentivized, but not required, to appoint a nominated representative in the UK or EEA (question 13);
- We recommend the adoption of a statutory review mechanism. In addition to the regime mentioned in the White Paper (Communications Act 2003, ss.192-196), another possible model for an appeal mechanism is the Data Protection Act 2018, ss.162-164 (question 14);
- We recommend that membership of the current Global Internet Forum to Counter Terrorism (GIFCT) is increased and greater knowledge-sharing amongst GIFCT members to counter terrorism online and further industry collaboration (questions 15 and 16); and,
- Efforts should be taken to involve social media companies in education campaigns which encompass a broad age range of internet users (question 18).

1 Introduction: Online Harms, Terrorism, Extremism and the Evidence Base

1.1 The internet is no longer a distinct space, and notions of 'online' and 'offline' create a false dichotomy. The Internet is embedded in our lives, and should be understood as such.[1]

1.2 Evidence is vital. The White Paper at times blurs notions of correlation and causation, with an assumption that the online milieu causes specific harms. This is not supported by evidence. In many instances, the Internet is merely a facilitative tool for activities happening offline.[2]

[1] Chih-Ping Chen, 'Playing with Digital Gender Identity and Cultural Value', *Gender, Place & Culture* 23, no. 4 (2 April 2016): 521–36, https://doi.org/10.1080/0966369X.2015.1013455; Mia Lövheim, 'Young People and the Use of the Internet as Transitional Space', 2005, https://doi.org/DOI:10.11588/heidok.00005826; Denise Carter, 'Living in Virtual Communities: An Ethnography of Human Relationships in Cyberspace', *Information, Communication & Society* 8, no. 2 (1 June 2005): 148–67, https://doi.org/10.1080/13691180500146235.

[2] Brigitte L. Nacos, 'The Role of Traditional Media in Violent Online Political Extremism' (September 2015); Brigitte L. Nacos, 'Tactics of Terrorism', in *Exchanging Terrorism Oxygen for Media Airwaves: The Age of Terroredia: The Age of Terroredia*, ed. Eid Mahmoud (IGI Global, 2014), 110–23; a. N. Awan, 'Virtual Jihadist

1.3 In relation to the harms in scope provided by the White Paper, the range of alleged harms is ambitiously broad. In this context, the distinct focus on terrorist content and child sexual exploitation and abuse is appropriate but the list of harms in scope presents the risk that the resources of the new regulator will be so stretched that the most serious online harms cannot be provided with the regulatory attention they deserve.

1.4 While the listed harms in scope are broad, they do not include misogyny, a key omission given the emphasis throughout the White Paper on the specific targeting of women and girls online.

Terrorism versus Extremism

1.5 Existing evidence shows that while terrorists use the Internet for a number of purposes, this does not replace the importance of offline interactions.[3]

1.6 This is important for two reasons: first, policy may overemphasise the role of the internet and look for harms in the wrong places, and secondly, Internet usage for activities deemed "harmful" may actually be in the public good. For example, terrorists' use of the Internet has been shown to decrease their opportunities to conduct a successful attack and increase the likelihood of being apprehended.[4]

1.7 It is important to disaggregate terrorist activities online. Rather than broadly considering 'online terrorism', behaviours such as recruitment, attack planning, and propagandising for instance, follow different patterns and should be understood separately. It is important to recognise distinctions in the behaviours of different groups, ideologies, and actors (e.g. leaders vs followers).[5]

Media: Function, Legitimacy and Radicalizing Efficacy', *European Journal of Cultural Studies* 10, no. 3 (August 2007): 389–408, https://doi.org/10.1177/1367549407079713.

[3] For example, see: Ines von Behr et al., 'Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism', *Rand*, 2013, https://doi.org/10.1214/07-EJS057; Paul Gill, 'Online Behaviours of Convicted Terrorists', 2016; Paul Gill and Emily Corner, 'There and Back Again There and Back Again: The Study of Mental Disorder and Terrorist Involvement', *American Psychologist*, 2017, 1–35; Sean C. Reynolds and Mohammed M. Hafez, 'Social Network Analysis of German Foreign Fighters in Syria and Iraq', *Terrorism and Political Violence*, no. April (2017), https://doi.org/10.1080/09546553.2016.1272456.

[4] Paul Gill and Emily Corner, 'Lone Actor Terrorist Use of the Internet and Behavioural Correlates', in *Terrorism Online: Politics Law and Technology*, ed. Lee Jarvis, Stuart Macdonald, and Thomas M. Chen (Abingdon, Oxon: Routledge, 2015), 35–53; PIRUS, 'The Use of Social Media by United States Extremists', *START*, 2018.

[5] Paul Gill et al., 'What Are the Roles of the Internet in Terrorism?' (VOX-Pol, November 2015), http://voxpol.eu/wp-content/uploads/2015/11/DCUJ3518_VOX_Lone_Actors_report_02.11.15_WEB.pdf.

1.8 As suggested in the Online Harms White Paper, while terrorist groups are often easy to recognise, with clearly flaggable content, extremist content is hard to recognise and define.

1.9 The appropriate identification of what constitutes extremist material is crucial. Identity issues are recognised as an important driver in radicalisation.[6] Perceptions that regulation and removal targets particular social groups and identities, especially those who already feel silenced or marginalised, might exacerbate existing grievances. For instance, supporters of the right to offend, working-class white men, and the radical right, have protested the removal of actors including the English Defence League founder Tommy Robinson and, rightly or wrongly, perceive this removal as class-based, rather than content-based.[7]

1.10 Not all of these supporters were part of the UK 'radical right'. This suggests that any impacts of regulation, such as removal or mass suspension, are likely to be negatively perceived by a wider milieu than the individuals removed from social media and their immediate base alone.

1.11 In particular, for some in the UK who feel excluded and marginalised from institutions of political power, social media sites such as Facebook and Twitter can be regarded as sites of genuine participatory democracy, while institutions such as Parliament and the electoral system are not.[8]

1.12 When assessing the impacts of far right, radical right and populist actors, the situation is not directly analogous with the past removal of supporters of Daesh. The boundaries between extreme actors on the political right and general populations are more blurred.[9]

1.13 It is important that rules applied are consistent and not reactive. While a range of extreme ideologies should be addressed online, each must be considered in relation to the harms it poses, not as a way of 'balancing' actions. For instance, far right extremism should be addressed for the risks it poses to society; this should include the impacts on minority groups, but must not simply be a case of acting to appease such groups.

[6] See among others Home Office, 'CONTEST: The United Kingdom's Strategy for Countering Terrorism' (London: The Home Office, June 2018), 40; Quintan Wiktorowicz, *Radical Islam Rising: Muslim Extremism in the West* (Lanham, Md: Rowman & Littlefield Publishers, Inc., 2005); Anja Dalgaard-Nielsen, 'Violent Radicalization in Europe: What We Know and What We Do Not Know', *Studies in Conflict & Terrorism* 33, no. 9 (16 August 2010): 797–814, https://doi.org/10.1080/1057610X.2010.501423.

[7] Elizabeth Pearson, 'To What Extent Does Gender Matter in UK Extremism?' (King's College London, 2019).

[8] Pearson, ibid.

[9] Ongoing research by Professor Maura Conway, Dublin City University.

1.14 It is therefore important that in fostering rules and norms that discourage harmful behaviours, the regulatory framework should not aim to sanitise or gentrify the online space. Cyberspace provides an important forum for the expression of dissenting opinions and no matter how disagreeable these opinions may be to some, they should not be curtailed in the absence of demonstrable evidence of harm.

Displacement

1.15 Removal through regulation raises the possibility of a displacement effect, as extreme actors leave platforms that are willing to participate with both law enforcement and regulators – such as the large social media companies – and migrate towards platforms that do not cooperate.

1.16 Displacement effects were seen when key social media sites including Twitter began to suspend and remove accounts supporting Daesh in a systematic and widespread manner, which led to a mass migration to smaller, more secure platforms, particularly Telegram.[10]

1.17 This undoubtedly had positive effects,[11] but also involved a trade-off. More secure platforms are more difficult to police effectively. As a rule, "hard" interventions such as suspensions and removal tend to inspire innovation in deviant behaviour; there are many lessons here from the study of online drug markets.[12]

1.18 Given we are entering an online environment in which the knowledge barrier for using technologies such as VPNs and TOR has never been lower, this is a trade-off that Government should take seriously.

1.19 Technology is developing all the time, for instance, new social media platforms are emerging that operate using a blockchain, such as Twister.[13] If these become widespread, they offer a home for each and every harm listed in the white paper with relatively little regulatory oversight.

---

[10] Mia Bloom, Hicham Tiflati, and John Horgan, 'Navigating ISIS's Preferred Platform: Telegram', *Terrorism and Political Violence*, 2017, 1–13, https://doi.org/10.1080/09546553.2017.1339695.

[11] J.M. Berger and Heather Perez, 'The Islamic State's Diminishing Returns on Twitter: How Suspensions Are Limiting the Social Networks of English-Speaking ISIS Supporters', *Occasional Paper*, no. February (2016): 1–20.

[12] Martin Horton-Eddison and Matteo Di Cristofaro, 'Hard Interventions and Innovation in Crypto-Drug Markets: The Escrow Example', *Global Drug Policy Observatory*, no.11 Policy Brief (2017).

[13] Gareth Mott, 'A Storm on the Horizon? "Twister" and the Implications of the Blockchain and Peer-to-Peer Social Networks for Online Violent Extremism', *Studies in Conflict and Terrorism* 42, no. 1–2 (2018): 206–27, https://doi.org/10.1080/1057610X.2018.1513986.

1.20 A notable feature of the proposed regime is the desire to avoid the problem of displacement to alternative online platforms not adequately regulated, hence the expansive definition of companies in scope of the regulatory framework and possibility of enforcement options beyond civil fines, such as ISP blocking. However, the proposed regime is limited to sites, platforms etc available on the open internet.

1.21 The justification for such an approach is that a law enforcement response is the most effective option in relation to the threats posed by the dark web. In light of this, an effective regulatory regime restricted to the open internet might conceivably lead to migration to the dark web.

1.22 No regulatory framework operates in a vacuum, so the success of the proposed regime will be partly dependent on the effectiveness of the Government's Serious and Organised Crime Strategy. To this end, we welcome the assertion that the government continues to invest in specialist enforcement skills and capability.

Harms and Benefits: Finding a Balance

1.23 While it is often postulated that "echo chambers" offer a potentially damaging effect on social cohesion, it is rarely considered that having homogenous online communities may in some respects be conducive to the public good. It is possible that the creation of virtual communities can increase solidarity between communities that have often suffered discrimination.

1.24 For example, while it is right to be concerned that users may be influenced to self-harm after being exposed to such content online, there are also a number of cases in which those that may commit self-harm find solace in contacting and interacting with other sufferers online. [14]

[14] Christiane Eichenberg and Markus Schott, 'An Empirical Analysis of Internet Message Boards for Self-Harming Behavior', *Archives of Suicide Research* 21, no. 4 (2017): 672–86, https://doi.org/10.1080/13811118.2016.1259597; Craig D. Murray and Jezz Fox, 'Do Internet Self-Harm Discussion Groups Alleviate or Exacerbate Self-Harming Behaviour?', *Australian E-Journal for the Advancement of Mental Health* 5, no. 3 (2006): 225–33, https://doi.org/10.5172/jamh.5.3.225.

2 Specific Responses to the Consultation Questions[15]

2.1 **Question 1:** We support the commitment to annual transparency reporting; our responses to questions 4, 8 and 14 below highlight how certain features of the regulatory regime might enhance trust and accountability across industry.

2.2 **Question 2**: We advocate the use of super complaints. The regulator's role in user redress will be largely limited to the setting of minimum standards for internal company complaints procedures and will not involve the adjudication of individual complaints. While it is envisioned that individuals will be able to report dissatisfaction to the regulator, a super complaints procedure will facilitate an oversight role and help reveal systemic failures on the part of companies that might otherwise be missed if reliance is placed solely on the contingencies of individual reporting. A useful model which could be adopted for this purpose is the super complaint system utilised for policing as provided by the Police Reform Act 2002, ss.29A-C and associated secondary legislation.

2.3 **Question 3**: We do not believe that the government should consider other measures of user redress. We are supportive of the potential to utilise the regulator's findings, including a determination that a company has breached the statutory duty of care, in any private legal action against a company in scope.

2.4 **Question 4**: We advocate the creation of a specific parliamentary committee to scrutinise the work of the regulator and the general operation of the regulatory framework, including the power to call and question witnesses. In the absence of a bespoke committee, the existing select committee system might be capable of fulfilling this role. However, the regulator's remit cuts across the responsibility of more than one government department, most obviously the Home Office and Department for Digital, Culture, Media and Sport. A designated parliamentary committee would benefit from enhanced visibility and could help foster public and industry confidence in the regulatory framework.

2.5 **Question 5:** Providing a responsive approach to regulation is adopted (see response to question 8 below), we are supportive of the proposals for defining online platforms and services. Please see our general comments above for the concerns we have expressed regarding a possible displacement effect.

2.6 **Questions 6 and 7:** We welcome the recognition of the importance of privacy and the differentiated approach for private communications. We also agree that defining public

[15] We do not address questions 9 and 17.

and private in this context is complex, particularly given that harmful activity online often involves a combination of public and more covert activity. For example, since Twitter became a more hostile environment for supporters of the so-called Islamic State (IS), much of the group's community-building activity migrated to other platforms, primarily Telegram.[16] Telegram chat rooms allow the sharing of content with the opportunity for members to comment or engage with others in the room. Chat rooms may include a membership list and indication of who is online. This enables administrators to monitor and police the network and allows member to engage in secret chat.[17] Daesh use of Twitter is now largely restricted to the use of throwaway accounts to signpost users to content hosted on other platforms.[18]

2.6.1 In developing a definition for private communications, it is important to distinguish between privacy on the one hand and secrecy and covertness on the other. A secret chat room on Telegram may possess some features that give an appearance of privacy, such as membership lists and monitoring of presence. Yet if the aim of the chat room is to recruit sympathetic individuals, it is better understood as being a covert setting not involving private communications. This is particularly true when individuals have been signposted there by recruiters operating on open platforms.

2.6.2 More generally, this example shows that the number of parties to a conversation is not, in itself, conclusive of whether the conversation is private. Perhaps the secret Telegram chat room has only two or three members. Yet if one of those members actively sought out the others as part of a wider recruitment effort conducted on open platforms, the communications within the chat room should not be designated as private.

2.7 **Question 8**: There is ample evidence in the academic literature of the benefits of a responsive regulation approach.[19] The promotion of a risk based and proportionate approach in the White Paper refers specifically to the capacity of companies, the reach of their platforms and the severity of the harms. A successful regulatory regime should not only be responsive to these considerations but also to the degree of company engagement with the regulator and the extent to which the conduct of companies enhances or undermines the overall rationale of the framework.

2.8 **Questions 10 and 11:** Our preference is the creation of a new public body; the creation of a bespoke regulator would produce some obvious benefits. First, a new body would have a positive symbolic effect; it would clearly reinforce the government's commitment

[16] Conway M, Khawaja M, Lakhani S, Reffin J, Robertson A & Weir D (2017) *Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts*. Dublin: VOX-Pol Network of Excellence.
[17] Bloom M, Tiflati H & Horgan J (2017) Navigating ISIS's Preferred Platform: Telegram. *Terrorism and Political Violence*, https://doi.org/10.1080/09546553.2017.1339695
[18] Macdonald, S, Grinnell, D, Kinzel, A & Lorenzo-Dus, N. (2019) *Is Twitter a Gateway to Terrorist Propaganda? A Study of Outlinks Contained in Tweets Mentioning Rumiyah*. GRNTT policy brief. London: RUSI.
[19] Ayres, I, & Braithwaite, J. (1992) *Responsive Regulation: Transcending the Deregulation Debate* (1992). OUP, Oxford; Braithwaite, J. (2002) *Restorative Justice and Responsive Regulation*. OUP, New York.

to tackling online harms. Second, particularly from the public's perspective, a dedicated regulator would benefit from high visibility and would represent an obvious source of guidance for anyone concerned about online harms. If the government elects to add the responsibility to an existing body (e.g. Ofcom or the Information Commission), the new regulatory framework will nevertheless require considerable investment and we would urge the government to ensure that those tasked with the operation of the framework are provided with sufficient resource in order to fulfil their role in a timely and efficacious manner.

2.9 **Question 12:** In order to facilitate responsive regulation, a range of enforcement tools is necessary. This includes ISP blocking. However, ISP blocking should be regarded as being towards the top of the pyramid of available tools in order to encourage greater engagement with less severe interventions. Such an approach would require ISPs to take responsibility for companies that use their services, which is consistent with the responsibility of companies such as Facebook for users of their platform. This would encourage ISPs to self-regulate. For example, the social media platform Gab was forced to find another ISP after domain provider GoDaddy refused to be further associated with it following the October 2018 Pittsburgh Synagogue shooting.

2.10 **Question 13:** Companies based outside the UK and EEA should be incentivized, but not required, to appoint a nominated representative in the UK or EEA. The presence of such a representative would allow for a greater range of resolutions to complaints. In situations involving companies without such a representative, it may be necessary to resort to ISP blocking as the only option. In situations involving companies with a representative in the UK or EEA other measures may be considered, such as civil fines.

2.11 **Question 14:** It is our view that there should be a statutory review mechanism. Judicial review is a relatively limited mechanism and (the concept of perversity notwithstanding) is limited to the decision-making process as opposed to the merits of the decision. A meaningful appeal process will facilitate buy in from the regulated sector by providing an official outlet to challenge any decisions which they consider to be unjustified or unfair. In order to avoid potential frivolous or vexatious appeals, we would suggest that those appeals which are deemed to be without merit are subjected to a costs order to reimburse the regulator for any expenditure incurred responding to the appeal. In addition to the regime mentioned in the White Paper (Communications Act 2003, ss.192-196), another possible model for an appeal mechanism is the Data Protection Act 2018, ss.162-164.

2.12 **Questions 15 and 16:** The White Paper mentions the hackathon that the Home Secretary co-hosted in November 2018, at which technology companies worked to develop a new AI product to detect online grooming of children. In the context of

counterterrorism, the Global Internet Forum to Counter Terrorism (GIFCT) was established in 2017 by Facebook, Twitter, Google and Microsoft to disrupt terrorists' ability to use member companies' platforms to promote terrorism. One GIFCT initiative is the shared industry hash database, which allows members to create "digital fingerprints" for terrorist content, remove matching content and, in some cases, block terrorist content before it is even posted. The database now contains more than 200,000 hashes.

2.13 There is a pressing need to expand membership of the GIFCT. At present the GIFCT has fourteen members, a small number in comparison to the number of platforms on which terrorist content has been discovered.[20] Many smaller technology companies lack the capacity needed to meet the standards imposed by the GIFCT eligibility criteria. Some lack the willingness to abide by these criteria. Here policymakers have an important role to play, providing the support required by the former and offering appropriate incentives to the latter.

2.14 An expansion of the GIFCT's activities should also be encouraged, including the following:

2.14.1 Specialist knowledge is required to understand the nuances of much extremist (and borderline) content. Such knowledge may not always be in place, especially within smaller companies, meaning false positives and false negatives are more likely. Collaboration between large- and small-scale technology companies is therefore essential. Knowledge-sharing will improve the ability of companies with fewer resources to counter terrorist and extremist presence on their platforms effectively. To this end, the GIFCT shared database of hashes – which focuses on 'the most extreme and egregious terrorist images and videos'[21] – should be expanded to include this more borderline content.[22]

2.14.2 Larger social media companies have automated means that employ behavioural cues to block content (e.g. abnormal posting volume or using trending hashtags to gain attention). This is valuable in the context of counterterrorism, given the role that botnet activity plays in efforts to disseminate terrorist propaganda. By contrast, many smaller companies rely exclusively on humans to use content-based cues to identify and remove terrorist content. Where possible, GIFCT members should

[20] For example, from its establishment in 2015 to the end of 2017 the EU's Internet Referral Unit made a total of 44,807 referrals, to over 170 different platforms, with 92 percent of the referred items subsequently removed: Europol (2018). *EU Internet Referral Unit: Transparency Report 2017* https://www.europol.europa.eu/sites/default/files/documents/eu_iru_transparency_report.pdf (accessed 31 January 2019).

[21] Facebook (2016) 'Partnering to Help Curb Spread of Online Terrorist Content,' *Facebook News*, 5 December 2016 https://newsroom.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content/

[22] Macdonald, S., Grinnell, D., Kinzel, A. & Lorenzo-Dus, N. (in press) *Is Twitter a Gateway to Terrorist Propaganda? A Study of Outlinks Contained in Tweets Mentioning Rumiyah*, GRNTT policy brief.

develop shared automated systems that use behavioural cues to block terrorist content.[23]

2.15 **Question 18**: Education on the real and extreme harm that online behaviours cause is important. In particular, we advocate a focus on the online space as part of our lives, as embedded and not separate. In this way, behaviour on social media cannot be simply excused as 'online'. Schools provide an obvious means of educating youth and children. However, education should not be limited to the young. On the issue of extremism, while Jihadist groups may attract youth, older as well as young people can be drawn into the far and extreme right, including online.[24] Efforts should therefore be taken to involve social media companies in education campaigns that encompass a broad age range of internet users.

2.15.1 On the question of education on disinformation, it should be noted that for those who do not trust the mainstream media and do not see their identity groups represented in ways that they recognise, education aimed at promoting 'trusted' sites is likely to backfire.

2.15.2 A 2019 report by the Sutton Trust suggested key professions including politics, the law, business and the media do not represent British people, and social inequality is growing.[25]

2.15.3 If British people do not see themselves represented, and indeed are not represented in elite institutions, they are less likely to trust the recommendations of those institutions on the issue of information and disinformation. People trust their own, often local and everyday experiences, and mistrust official institutions that produce a conflicting narrative.[26]

2.15.4 Rather than directing people on what to trust, a process of dialogue, empathy and engagement is more likely to produce results.

3 Concluding Remarks

This consultation response is drawn from a research team with expertise in law, regulation, criminology, terrorist and extremist behaviours online, and extreme actors offline. Collectively, we broadly welcome the proposals. The devil, of course, is in the detail, with

[23] van der Vegt, I., Gill, P., Macdonald, S. & Kleinberg, B. (in press) *Shedding light on terrorist and extremist content removal*, GRNTT policy brief.

[24] Joel Busher, *The Making of Anti-Muslim Protest: Grassroots Activism in the English Defence League* (London ; New York, NY: Routledge, 2015); Hilary Pilkington, *Loud and Proud: Passion and Politics in the English Defence League* (Manchester University Press, 2016), http://www.oapen.org/search?identifier=607920; Pearson, 'To What Extent Does Gender Matter in UK Extremism?'

[25] The Sutton Trust, 'Elitist Britain 2019: The Educational Backgrounds of Britain's Leading People' (The Sutton Trust, 2019), https://www.suttontrust.com/research-paper/elitist-britain-2019/.

[26] Pearson, 'To What Extent Does Gender Matter in UK Extremism?'

the white paper leaving many aspects of the regulatory framework to be further worked out. In addressing these, we conclude by reiterating our observation at para. 1.14 above concerning the importance of free speech, particularly for dissenting voices, and ensuring that regulation is not used as a tool to sanitise online spaces.

This response was prepared by the following members of CYTREC, the Cyber Threats Research Centre at the Hillary Rodham Clinton School of Law, Swansea University.

Dr Patrick Bishop

Seàn Looney

Professor Stuart Macdonald

Dr Elizabeth Pearson

Joe Whittaker

You can contact us at cytrec@swansea.ac.uk