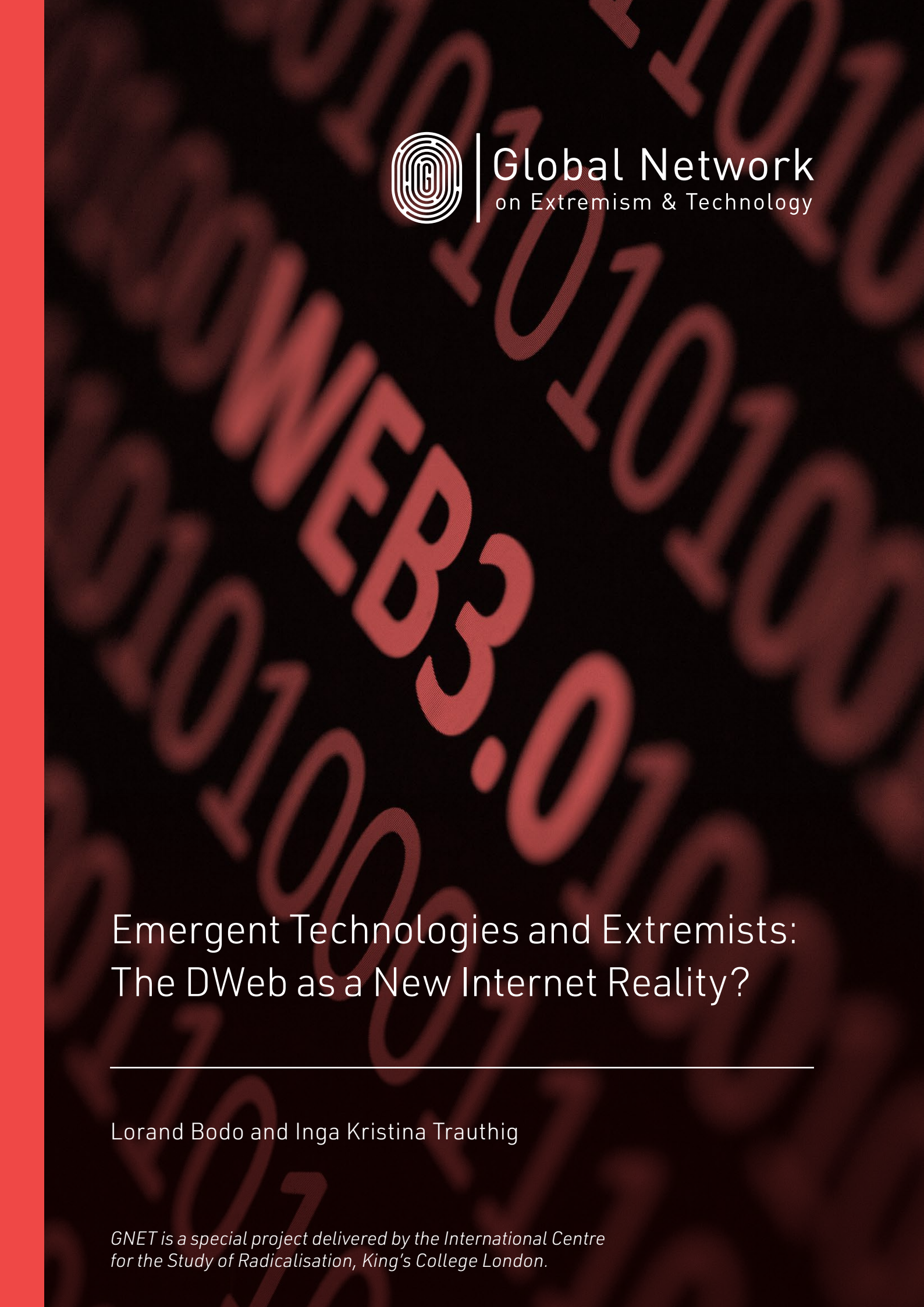


Global Network
on Extremism & Technology

Emergent Technologies and Extremists: The DWeb as a New Internet Reality?

Lorand Bodo and Inga Kristina Trauthig

GNET is a special project delivered by the International Centre for the Study of Radicalisation, King's College London.

The authors of this report are Lorand Bodo and Inga Kristina Trauthig

The Global Network on Extremism and Technology (GNET) is an academic research initiative backed by the Global Internet Forum to Counter Terrorism (GIFCT), an independent but industry-funded initiative for better understanding, and counteracting, terrorist use of technology. GNET is convened and led by the International Centre for the Study of Radicalisation (ICSR), an academic research centre based within the Department of War Studies at King's College London. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing those, either expressed or implied, of GIFCT, GNET or ICSR.

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.

Executive Summary

The World Wide Web, since its development by Sir Tim Berners-Lee in 1989, has steadily evolved into an ecosystem in which billions of users have become dependent on relatively few but large corporations. Using a search engine, posting on social media, communicating with others, or storing data in the cloud, for example, these companies have benefited billions of users positively. However, as the user base has grown over the years, so too has their power. Shifting the power from these few, large corporations back into the hands of users is critical to adherents of the Decentralised Web (DWeb). This 're-decentralisation' should also give the user more control over their data. As extremist actors try to innovate and find inventive ways to spread their propaganda and be more resistant to account and content removals, the DWeb is on their radar.
This report gives a brief overview of the current status of the DWeb and ties it to existing and possible future exploitation of the DWeb by extremists. We focus on right-wing extremist (RWE) and the so-called Islamic State (IS) as these two strands of extremists are accredited with the highest threat potential in many parts of the world. We analyse a sample of thirty Telegram channels that fulfil our categorical features as being attached to the RWE spectrum. The second dataset, which was provided by UN-supported Public-Private Partnership Tech Against Terrorism (TAT), subjects the so-called Islamic State's exploitation of the DWeb to critical scrutiny.

Based on the literature review, conducted interviews and data analysis, we assess:

- Since extremists consider exploiting any technology, the DWeb is also on their radar. One major reason for its attraction is that any content hosted 'on the DWeb' cannot be removed as it is not controlled by a central authority and thus not easily removable.

- However, the analysis shows that other existing technologies are still preferred by those actors.

- Overall, DWeb services are at medium risk of being exploited by RWE and IS entities.

- Furthermore, the DWeb is not necessarily needed to enable extremist entities to host, distribute, and control their content, as required services to achieve this already exist.

- Finally, DWeb services can mitigate the risks of being exploited and thus, it does not necessarily constitute a safe haven for extremists.

Overview

Terms floating around with regard to the decentralised web (DWeb) such as Web3 or bitcoin have become a catchall for anything having to do with blockchains and cryptocurrency. Overall, the major questions related to a decentralised web are coalescing around two themes: (1) Is a decentralised web viable and attractive enough for enough people? and (2) What is the nature of this 'new internet' – in other words, will the decentralised web avoid pitfalls of the current web? The latter is regularly charged for online radicalisation or for enabling authoritarian strengthening. Instead, could the DWeb foster positive aspects such as its potential for activists who could organise out of sight of regime censors using this technology.

This report contributes to both by asking how extremists are already exploiting and how they could exploit it in the future. Why is the decentralised web 'good' or 'bad'? Why do people use it? Is a small percentage that abuses it jeopardising this version of the internet already? What could developers factor into their consideration given existing evidence? What do policymakers need to keep in mind when working on legislating tech? The possible angles researchers and journalists have been exploring with regard to the DWeb are plentiful and range from questions addressing political economy issues to normative ramifications of an ethical underpinning among Web3 developers that 'Big Tech' cannot be trusted. For this report, the focus is on the implications for extremist actors with corresponding security implications for societies as a whole.

A three-pronged strategy guided our research approach. To start with, we undertook a systematic literature review of existing material about the DWeb, focusing especially on content moderation as well as extremism. Second, we collected and collated evidence of right-wing extremists and Islamic State entities experimenting with the DWeb. Finally, we conducted semi-structured interviews with DWeb advocates, critics and developers to inform our understanding of this evolving topic. Underpinning this report is its exploratory nature which is directly linked to the fact that the DWeb currently is more of an idea than a reality for most people around the world.

A major risk in the context of online violent extremism and terrorism is that DWeb technology could be exploited for data storage and retrieval purposes. In that case, "[…] decentralized methods of data storage could make it difficult, if not practically impossible, for a single entity to censor content".[1] As a result, extremist content cannot easily be removed and will thus be accessible to anyone who knows where to find it.

1 Barabas, Chelsea, Neha Narula, and Ethan Zuckerman. 'Defending Internet Freedom through Decentralization: Back to the Future?' The Center for Civic Media & The Digital Currency Initiative MIT Media Lab, August 2017. https://static1.squarespace.com/static/59aae5e9a803bb10bedeb03e/t/59ae908a46c3c480db42326f/1504612494894/decentralized_web.pdf.

Our literature review concluded that DWeb technologies have been on the radar of extremist entities for quite some time, but the limiting features and related limitations of audience reach have been restraining their exploitation by such groups. However, the pressing concern is that the general expansion of the DWeb could go hand-in-hand with an increased exploitation by extremist actors.

The four main findings for our RWE data are:

(1) DWeb services are not significantly represented.

(2) The majority of outgoing links lead to two major social media platforms.

(3) The right-wing extremist sample shared more links to unreliable news and blogs than more reliable news sources.

(4) Archiving Services are used just as much as DWeb services.

The three main findings for our IS data are:

(1) Decentralised services are exploited but not to the same extent as centralised ones.

(2) File hosting and sharing services are prime targets.

(3) There is more verified terrorist content on file hosting and sharing, archiving as well as pasting services than on social media.

Contents

Executive Summary 1

Overview 3

1 Introduction 7

2 What is the DWeb? 9
- 2.1 Historical and Ideological Background 9
- 2.2 Key Terms 13
- 2.3 DWeb Services 14

3 Literature Review 17
- 3.1 Content Moderation and the DWeb 17
- 3.2 Online Extremism and the DWeb 19

4 How Do Extremists Exploit the DWeb? 23
- 4.1 Methodology 23
- 4.2 Overview of the Data 26

5 How Could Extremists Exploit the DWeb? 31

6 Risk Assessment & Discussion 33

Policy Section 37

1 Introduction

While the crash of cryptocurrencies has been dominating technology news headlines throughout the spring of 2022, there is a broader, parallel trend ongoing that may change our individual relations to technology as we know it. The Internet seems to be undergoing a slow but radical transformation that could significantly change the way we interact and handle our data online.[2] This next paradigm shift in Internet applications would be a move away from large and centralised networks and platforms to decentralised ones. One possible outcome of this move would be that users might no longer rely on (big) social media platforms and tech companies to communicate with each other.[3] This would be because the servers in the middle that enable these communications are no longer needed; in fact, people would be able to share data and communicate with whomever whenever they wished, which might give them full, or at least fuller, control over their data and privacy.[4] While this emerging trend is welcomed by privacy advocates, little is known about how these technological revolutions might be exploited. The avenues of exploitation include extremist entities. Another relevant implication for the trust and safety aspects would be that current content moderation efforts would no longer work due to, in simplified terms, the absence of servers in the middle.

Terms floating around with regard to the decentralised web, such as Web3 or bitcoin have become a catchall for anything having to do with blockchains and cryptocurrency.[5] Overall, the major questions related to a decentralised web coalesce around two themes: (1) Is a DWeb viable and attractive enough for enough people? and (2) What is the nature of this 'new internet'? In other words, will the DWeb avoid the pitfalls of the current web, which is regularly accused of facilitating online radicalisation and enabling the strengthening of authoritarianism around the world. Would the DWeb instead foster positive aspects, such as the Internet's potential for activists, who could organise out of sight of regime censors using this technology?[6] This report contributes to both themes by asking how extremists are already exploiting the DWeb and how they could exploit it in the future. Why is the decentralised web 'good' or 'bad'? Why do people use it? Is the small percentage who abuses it jeopardising this version of the Internet already? What could developers factor into their considerations given existing evidence? What do policymakers need to keep in mind when working on legislating tech? The possible angles researchers and journalists have been exploring with regard to the decentralised web are plentiful and range from questions addressing political economy

2 Esber, Jad, and Scott Duke Kominers. 'Why Build in Web3'. Harvard Business Review, 16 May 2022. https://hbr.org/2022/05/why-build-in-web3.
3 Fuller, E.'Web3 Will Change The World. Here's How It Can Change Yours'. 2021. https://medium.com/@ezrawithacamera/web3-will-change-the-world-d724b4ea19d0.
4 Iyer, Sitaram, Antony Rowstron, and Peter Druschel. 'Squirrel: A Decentralized Peer-to-Peer Web Cache'. in Proceedings of the Twenty-First Annual Symposium on Principles of Distributed Computing, 213–22. https://doi.org/10.1145/571825.571861.
5 Wood, Gavin. 'The Father of Web3 Wants You to Trust Less'. Interview done by Edelman, Gilad, in: Wired, 2021. Accessed 3 June 2022. https://www.wired.com/story/web3-gavin-wood-interview/.
6 Krishnan, Armin. 'Blockchain Empowers Social Resistance and Terrorism Through Decentralized Autonomous Organizations'. Journal of Strategic Security 13, no. 1 (2020): 41–58.

issues to normative ramifications of an ethical underpinning felt by Web3 developers that 'Big Tech' cannot be trusted.[7] For this report, the focus is on the implications for extremist actors with corresponding security implications for societies as a whole.

To this end, there is a gap in the current literature that aims to better understand this new technology and assess the risk of it being exploited for extremist purposes. Therefore, this report aims to contribute to filling this gap by providing: first, an analytical overview and explanation of technological developments related to the advent of the DWeb; second, some conceptual clarifications on terms; and, third, an assessment of right-wing extremists and Islamic State advocates exploiting this technology. The ultimate objective of this report is to provide an evidence-based assessment of a potential future threat to inform policy making.

A three-pronged strategy guided our research approach. To start with, we undertook a systematic literature review of existing material about the DWeb, focusing especially on content moderation as well as extremism. Second, we collected and collated evidence of right-wing extremists and Islamic State supporters experimenting with the DWeb. Finally, we conducted semi-structured interviews with DWeb advocates, critics, and developers to inform our understanding of this evolving topic. Underpinning this report is its exploratory nature, which is directly linked to the fact that the DWeb currently is more of an idea than a reality for most people around the world.[8]

In short, there are immense hopes connecting many Internet researchers and activists who expect the DWeb, based on the notion of decentralising everything, will become a version of the Internet that builds on lessons learned from past mistakes of Internet technology and how it was rolled out.[9] However, our research contributes to existing sceptical notions of a centralisation in Web 3.0. With regard to extremist actors, they prove adaptive in the sense that they use DWeb services. However, the scale of the existing reliance on DWeb services is marginal. This is likely tied to broader dynamics that stand in the way of the DWeb being used by more people generally – such as existing affordances of the Web 2.0. Instead of abandoning the idea of building something better, however, we argue that we live in an imperfect world – offline and online – and hence need to work on understanding societal impacts of technological changes. Ideally, this aspiration would also be shared by advocates of the DWeb.

7 Edelman, Gilad. 'The Father of Web3 Wants You to Trust Less' in: Wired, 2021. Accessed 3 June 2022. https://www.wired.com/story/web3-gavin-wood-interview/.
8 Hendrix, Justin. 'Is Web3 the Answer? A Conversation with Gilad Edelman'. Tech Policy Press, 22 May 2022. https://techpolicy.press/is-web3-the-answer-a-conversation-with-gilad-edelman/.
9 Halaburda, Hanna, Miklos Sarvary, and Guillaume Haeringer. Beyond Bitcoin. Wiesbaden: Springer International Publishing, 2022. https://link.springer.com/book/10.1007/978-3-030-88931-9.

2 What is the DWeb?

In order to provide analytical clarity for the next parts of the report, this section gives a systematic overview of the DWeb, which includes (a) its historical and ideological background, (b) an explanation of key terms and (c) a listing of some existing DWeb services.

We conclude that the DWeb is a movement the members of which share ideals but differ in their approaches of how to achieve them.[10] Some parts of this movement, however, have much broader reach than others. Bitcoin, for instance, has a great reach, while social media DWeb platforms are not widely known at all. In addition, it is unclear how many users the DWeb will be able to attract or support in the future. In other words, will the DWeb movement convince users to give up the conveniences of the current Internet? Based on our analysis, we argue that even if that is the case, the DWeb is actually already experiencing re-centralisation, jeopardising the very ideal it was thought to pursue.

2.1 Historical and Ideological Background

The World Wide Web we know and its underlying Internet infrastructure has undoubtedly transformed our lives. But since its creation by Tim Berners-Lee in 1989, the Internet has steadily evolved in a centralised manner due to the reality of established dominance by a handful of supranational, largely US-based companies.[11] As a result, these few but extremely powerful companies can enforce decisions and, most significantly, control the data of their users.[12]

Shifting the power from these few, large corporations back into the hands of users is critical to adherents of the DWeb, who aim to 're-decentralize' the Web.[13] There is no universally agreed definition of what the Decentralised Web is. In fact, the term DWeb can mean different things to different people.[14] According to the Oxen Privacy Tech Foundation (OPTF),[15] "The decentralized web is about a shift of power; shifting power away from large corporations (centralization) and towards individual people (decentralization). The ways this manifests and the consequences it has are myriad depending on contextual factors."[16]

10 Or, in the words of the Trust & Safety Professional Association (TSPA): "Consistent ideological frame around agency, freedom, and independence." TSAP Staff. 'Trust and Safety and the Decentralized Web. This Recap Was Prepared by TSPA Staff and Accompanies the March 24, 2022 Webinar Discussion "Trust and Safety and the Decentralized Web"'. April 2022. https://tspa.memberclicks.net/assets/pdfs/2022_03_24_Trust%20and%20Safety%20and%20the%20Decentralized%20Web.pdf.

11 See: Zdeněk Smutný, Stanislav Vojíř, and Jan Kučera. 'Social and Technical Aspects of Re-Decentralized Web'. Interdisciplinary Information Management, September 2020, 107–16.; Berners-Lee, Tim. 'Three Challenges for the Web, According to Its Inventor'. World Wide Web Foundation, 12 March 2017. https://webfoundation.org/2017/03/web-turns-28-letter/; CERN. 'The Birth of the Web'. Accessed 14 June 2022. https://home.cern/science/computing/birth-web; Barabas. 'Defending Internet Freedom through Decentralization'; Mozilla. 'Introducing the Dweb'. Mozilla Hacks – the Web developer blog, 2017. https://hacks.mozilla.org/2018/07/introducing-the-d-web.

12 Ibid.; Bodo, Lorand. 'Decentralized Terrorism: The Next Big Step for the So-Called Islamic State (IS)?'. VoxPol Blog, 2018. https://www.voxpol.eu/decentralised-terrorism-the-next-big-step-for-the-so-called-islamic-state-is/

13 Barabas. 'Defending Internet Freedom through Decentralization'.

14 See Syracuse University. 'What Is the Decentralized Web? 25 Experts Break It Down'. SYR-UMT (blog), 22 July 2016. https://onlinegrad.syracuse.edu/blog/what-is-the-decentralized-web/.

15 To find out more about the OPTF, visit https://optf.ngo/

16 Interview with the Oxen Privacy Tech Foundation, 2022.

At the root of the DWeb movement is a fundamental unhappiness about the centralised tendencies, culminating in the criticism that over 50% of Internet traffic is controlled by Amazon, Apple, Facebook, Google, Microsoft and Netflix. Therefore, a re-decentralisation needs to take place in order to unravel those unfortunate developments. Following that line of thinking, the DWeb will be a 'Web 3.0', as it should follow Web 2.0, the era during which the Internet was supposed to be democratised but instead was taken over by gigantic corporations who introduced online services enabling users to communicate and share information through centralised services.[17] (Web 1.0 refers to the early stages of the World Wide Web, where static pages were linked to each other and users had read-only access.[18]) Alongside the companies mentioned above, other social media behemoths, especially Twitter, are also regularly referenced by Web 2.0 critics. This is because Twitter is seen as yet another example of the social problems stemming from dynamics related to those centralised powers: misinformation, ideological polarisation, data mining, mass surveillance and algorithms that amplify sensationalism above all else.[19]

A major risk in the context of online violent extremism is that DWeb technology could be exploited for data storage and retrieval purposes. In that case, "decentralized methods of data storage could make it difficult, if not practically impossible, for a single entity to censor content".[20] In other words, extremist content cannot be removed and will thus be accessible to anyone who knows where to find it.

Peer-to-peer connectivity is just one characteristic of decentralisation; in essence, decentralisation would mean moving away from large, centralised nodes. This would break down the immense databases that have been created by Internet companies over recent years and are centrally held by them (instead of having the individual users in control). A move away from this state of affairs should better protect individuals from different forms of surveillance, as data would no longer be stored in a way that is easy for third parties to access.[21]

Early attempts at achieving this decentralisation were pursued in the financial sector by the establishment of cryptocurrencies. Crypto-advocates understand centralisation as imposed by intermediaries; therefore an early aim was to remove those intermediaries (in this case, banks) from financial transactions. But there are different, more nuanced ways to think about centralisation.[22] For example, centralisation and decentralisation can also be framed as a matter of choice: are there alternatives to whatever you want to do? Or is there really just one company that provides this service? This way of thinking actually highlights the relatively decentralised nature of banking in most parts of the world.

17 Edelman. 'The Father of Web3 Wants You to Trust Less'.; see also Zarrin, Javad, Hao Wen Phang, Lakshmi Babu Saheer, and Bahram Zarrin. 'Blockchain for Decentralization of Internet: Prospects, Trends, and Challenges'. Cluster Computing 24, no. 4 (1 December 2021): 2,841–66. https://doi.org/10.1007/s10586-021-03301-8; Corbyn, Zoe. 'Decentralisation: The next Big Step for the World Wide Web'. The Guardian, 8 September 2018. https://www.theguardian.com/technology/2018/sep/08/decentralisation-next-big-step-for-the-world-wide-web-dweb-data-internet-censorship-brewster-kahle; O'Reilly, Tim. 'What Is Web 2.0', 2005. https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html

18 Webfoundation, World Wide Web Foundation. 'History of the Web'. World Wide Web Foundation, 2022. https://webfoundation.org/about/vision/history-of-the-web/; Meunier, Thibault, and In-Young Jo. 'Web3 – A Vision for a Decentralized Web'. The Cloudflare Blog, 1 October 2021. http://blog.cloudflare.com/what-is-web3/; also, browse the world's first website: http://info.cern.ch/hypertext/WWW/TheProject.html

19 O'Gieblyn, Meghan. 'Can Social Media Be Redeemed?'. Wired, 13 May 2022. https://www.wired.com/story/can-social-media-be-redeemed/; Berners-Lee. 'Three Challenges for the Web'.

20 Barabas. 'Defending Internet Freedom through Decentralization'.

21 This actually harks back to the original philosophy behind the Internet, which was first created to decentralise US communications during the Cold War to make them less vulnerable to attack. Harbinja and Karagiannopoulos, 2019.

22 Edelman, Gilad. 'Paradise at the Crypto Arcade: Inside the Web3 Revolution'. Wired, 18 May 2022. https://www.wired.com/story/web3-paradise-crypto-arcade/

Another inconsistency in the promotion of decentralisation is that decentralised systems do not necessarily abolish unequal power structures but can instead replace one structure with another. For instance, Bitcoin operates in a manner that records of financial transactions are saved on a network of computers. With this, it can circumvent established financial institutions that more directly give people control over their finances. However, centralisation tendencies are tangible as a large percentage of Bitcoin wealth is owned by relatively few people.[23] For Bitcoin adherents and supporters, however, the underwriting blockchain technology counterbalances the oligarchic tendencies within the system.[24]

However, there is a criticism of tendencies of re-centralisation with regard to DWeb platforms and technologies that has been heard on multiple occasions: Jack Dorsey, former CEO of Twitter and founder of Block, Inc., suggested that those technologies were already in the hands of a small number of venture capitalist firms.[25] These re-centralisation tendencies have practical origins: it is quite inconvenient, at times even impossible, for an app on your phone to interact directly with the blockchain. As a result, many DWeb apps rely on either Infura or Alchemy,[26] two infrastructure development apps for blockchain technologies, to facilitate just that, re-introducing the intermediary.

This situation is further heightened when it comes to wallets for cryptocurrencies. ConsenSys owns both Infura and the most popular wallet, MetaMask.[27] Apps ultimately often rely on a few companies to read and make changes to the blockchain on their behalf – in turn jeopardising the promoted "radical openness" and decentralization.[28] Due to these capitalist market developments, Edelman suggests using the term "consolidation" instead of centralisation to adequately capture the criticism at the heart of the DWeb movement.[29] If we do that, then it becomes clear that the problem is not with the Internet per se but capitalism more broadly, highlighting the shortfalls of antitrust policies and actions with regard to the web.[30]

Cory Doctorow, an activist and journalist who also works for the Electronic Frontier Foundation, summed the situation up by arguing that among the DWeb movement there is consensus "that something is rotten" but fault lines then emerge along the reasons for why it is rotten: was "the original sin" company models developed around ad-based targeting? Or was it the non-enforcement or adaptability of antitrust laws?[31]

However, a decentralised technology does not guarantee a decentralised market. There are existing possibilities for disassembling centralisations, for example with regard to emails. Theoretically, everyone could set up their own email server, but instead, the majority

23 Martindale, Jon. 'Big Fish in the Crypto-Pond – Who Owns All the Bitcoin?' Digital Trends, 16 March 2018. https://www.digitaltrends.com/computing/who-owns-all-the-bitcoin/
24 See Edelman. 'Paradise at the Crypto Arcade'.
25 Finley, Klint. 'Jack Dorsey Wants to Help You Create Your Own Twitter'. Wired, 11 December 2019. https://www.wired.com/story/jack-dorsey-help-you-create-own-twitter/
26 These are also called blockchain node providers. A node is a program that runs on a single computer and allows users to connect with the rest of the blockchain network (Cheng, 2021).
27 Edelman. 'Paradise at the Crypto Arcade'.
28 Hendrix. 'Is Web3 the Answer?'.
29 Cerović, Ljerka, Vedrana Maravić, and Aleksandar Mihoković. 'Microsoft – Anti Trust Case' in The 33rd International Convention MIPRO, 2010: 926–30.
30 Haucap, Justus, and Torben Stühmeier. 'Competition and Antitrust in Internet Markets'. Handbook on the Economics of the Internet, 27 May 2016: 183–210.
31 Interview with Cory Doctorow, 2022.

of people use email clients that facilitate services people want to use. The market has centralised heavily, with Gmail being the most prominent example. Even if you personally opt out of using Gmail, you are likely to be sending emails to someone with a Gmail account, so a copy of your email lives on Google's servers.

Given these possibilities, some of our interviewees introduced caveats and expressed that they do not think of today's Internet as strictly centralised, because "if someone has the knowledge, time, and money it is fairly straightforward to self-host a website, and the technologies required to do so (DNS, etc.) are fairly decentralized and the narrative that all content hosted on the Internet has become stored on Facebook or Google servers seems a bit exaggerated."[32]

The fear of these capitalist tendencies that jeopardise the entire re-decentralisation endeavour of the DWeb was also voiced in our interviews. In particular, the onus that is put on the individual user to take up the DWeb and move towards decentralised tech is seen as a potential weakness for the spread and strength of the DWeb. In the words of Molly White, who served three terms on Wikipedia's Arbitration Committee and is a crypto-sceptic:[33]

> *"It is very easy to post online in the fairly centralized web we experience today – people can create Facebook accounts in minutes or spin up a new website using a hosting provider, without doing any kind of server maintenance or even writing HTML. It's also cheap or free – people don't have to buy physical servers to host a website, and there are a lot of free services for creating social media profiles or websites."*

One unresolved question is therefore how attractive the DWeb is or ever can be. Again, Molly White:

> *"What's gained in control and privacy is often at the expense of ease-of-use, cost, and discovery (…) The discovery issue also remains even if someone self-hosts a website or uses a peer-to-peer solution (…) The lack of a central host also means that content takedowns are complicated, and have to be achieved at a different layer (for example with an ISP or domain registrar) rather than a social network or web hosting service."*[34]

Another interviewee from the OPTF added that

> *"The current tech ecosystem has clear advantages when it comes to usability, convenience, and speed. For example, there are existing, reliable platforms such as YouTube, Soundcloud and Dropbox where content – especially multimedia content which requires very large amounts of data to be routed – can easily be stored, and links can be shared so other people can easily access this content."*[35]

In sum, the DWeb certainly carries potential to have individual users (re-)gain power but for this fundamental change to happen, major shifts for many people would need to happen about how they perceive the

32 Interview with Molly White, 2022.
33 Ibid. For more see: https://web3isgoinggreat.com/
34 Ibid.
35 Interview with the Oxen Privacy Tech Foundation, 2022.

Web, what their expectations are and what their commitments would be. Whether the benefits of the DWeb will be sufficient to attract enough users away from convenient services, such as Gmail, to make it viable seems relatively unlikely. However, with governments introducing more and more regulatory proposals for the Internet, the DWeb might actually offer a more liberal alternative in the long run.[36] Meanwhile, it is important not to forget the vulnerability of centralised platforms to shutdowns or censorship by authoritarian regime actors. The OPTF reminded us of the fact that state actors are able to strategically time these attacks, such as Twitter removing accounts critical of the Indian government during the 2020–2021 farmers' protests.[37] The hopes linked to 'a new internet' that would (finally) fulfil the aspirations attached to Web 2.0 are therefore likely to survive, since the current Internet disappoints in many ways.

2.2 Key Terms

In order to address discrepancies in the existing literature, we conducted interviews with experts in this field. In these semi-structured interviews, all interviewees were asked the same questions, but individual follow-up questions were posed depending on interviewee answers and expertise.[38] The following list of key terms is informed by the existing literature but enriched with the interview data. It does not aim to be comprehensive but rather convey an understanding necessary for the assessment this report provides.

DWeb: The decentralised web is a version of the web that relies mostly on self-administered servers and peer-to-peer technologies instead of major hosting providers. Hand in hand with this technical decentralisation goes a decentralisation of power structure which includes dismantling existing power houses such as Google and Meta (as opposed to the simple distribution of hosting).[39] Within this second dynamic exists an internal split of understanding as well since some think strictly in terms of decentralisation of power (service hosts as proxies for power) but others ascribe superiority to a certain method to achieve this aim over others.[40] Generally, decentralisation is supposed to give the individual user more power (again): in the centralised web the agency of individual users when it comes to decisions around data management (privacy, security), governance (security), and moderation (censorship) has been marginalised. While centralisation does have utility, it fundamentally requires ongoing and ultimate trust in the operating party. For example, on the decentralised web, a social media platform would give users more impactful choices around where and how their data was stored, who was able to participate on the platform, and how the platform was moderated. "Whereas centralized social media platforms tend towards a hypothetical set of all people on one platform, decentralized social media would tend towards more specific, diasporic communities".[41]

36 Härting, Niko, and Max Valentin Adamek. 'Digital Services Act – ein Überblick: Neue Kompetenzen der EU-Kommission und hoher Umsetzungsaufwand für Unternehmen'. Computer und Recht 37, no. 3 (1 March 2021): 165–71. https://doi.org/10.9785/cr-2021-370311; Trengove, Markus, Emre Kazim, Denise R. S. Almeida, Airlie Hilliard, Elizabeth Lomas, and Sara Zannone. 'A Digital Duty of Care: A Critical Review of the Online Safety Bill'. SSRN Scholarly Paper. Rochester, NY, 1 April 2022. https://doi.org/10.2139/ssrn.4072593.

37 Interview with the Oxen Privacy Tech Foundation, 2022.

38 All interviewees were asked the following questions: what is the Decentralised Web? What is Web 3.0? How does the Decentralised Web differ from Web 3.0? What are the advantages and disadvantages of the current tech ecosystem in terms of storing and sharing data online? What are the advantages and disadvantages of the decentralised web in terms of storing and sharing data online? Do you believe the DWeb can be exploited by terrorists or other entities and if so, how could we stop them?

39 Interview with Molly White, 2022.

40 Interview with Cory Doctorow, 2022.

41 Interview with Oxen Privacy Tech Foundation (OPTF), 2022.

Web3: While the DWeb does not inherently rely on cryptocurrencies or the blockchain to function, Web3 proponents are adamant in their argument that these are the right ways to achieve decentralisation in their vision of the future web.[42] Two concepts are the main defining features for Web3: decentralisation and game theory. These two concepts are supposed to be the driving forces of all Web3 applications. Central to the concept but also the term specifically is Polkadot founder and Ethereum co-founder Gavin Wood, who coined the term in 2014.[43] Ethereum is a blockchain that borrowed Bitcoin's key features and added a major innovation: it was designed with its own programming language so developers could build apps and eventually a whole new decentralised digital infrastructure to run on the Ethereum network.[44] The term Web3 is intimately tied to the blockchain technology in the context of the Ethereum network.[45]

Web 3.0: Whereas commentators started referring to Web3 and Web 3.0 as if the former was simply an abbreviation of the latter,[46] anyone who has kept an eye on the development of the World Wide Web and Tim Berners-Lee's concept for a semantic web will have good reason to be confused.[47] In 2006, he explained the semantic web as a component of Web 3.0, which is not the same as Web3 in the context of cryptocurrencies. The semantic web is an extension of the World Wide Web through standards set by the World Wide Web Consortium. The goal of the semantic web is to make Internet data machine-readable. The semantic web is a web of data, of dates and titles and part numbers and chemical properties and any other data of which one might conceive. This vision describes a web of linked data-encompassing technologies to enable people to create data stores online, build vocabularies and write rules for handling data.[48]

Blockchain: A blockchain is a public, decentralised and immutable database that lives across various interlinked computers (nodes) rather than one server. Therefore, no individual entity (person or organisation) can control or own it. This is a shield against manipulation since all changes are logged on the public chain and changing one part of the blockchain would require changes on all subsequent parts, which is almost impossible.[49]

2.3 DWeb Services

The following table outlines some prominent DWeb services that we have categorised into four main services: (1) Social Media Services, (2) Domain Name Services, (3) App/File Hosting & Sharing Services, and (4) Private Server Services. It is important to note that this list is not exhaustive and should only demonstrate examples of current DWeb capabilities.

42 Interview with Molly White, 2022.
43 Fagan, Siobhan. 'Web3 vs. Web 3.0: Key Differentiators and Why It's Important'. reworked.co. Simpler Media Group, Inc., 24 March 2022. https://www.reworked.co/information-management/why-web3-and-web-30-are-not-the-same/.
44 Edelman. 'The Father of Web3 Wants You to Trust Less'.
45 Richards et al. 'Web2 vs Web3'. ethereum.org, 2022. https://ethereum.org/en/developers/docs/web2-vs-web3/
46 Alford, H. 'Crypto's Networked Collaboration Will Drive Web 3.0'. 2021. https://techcrunch.com/2021/09/16/cryptos-networked-collaboration-will-drive-web-3-0/; Khoshafian, Setrag. 'Can the Real Web 3.0 Please Stand Up?' RTInsights (blog), 12 March 2021. https://www.rtinsights.com/can-the-real-web-3-0-please-stand-up/
47 Berners-Lee, Tim, James Hendler, and Ora Lassila. 'The Semantic Web'. Scientific American 284, no. 5 (2001): 34–43.
48 Fagan. 'Web3 vs. Web 3.0'.
49 Zarrin et al. 'Blockchain for Decentralization of Internet'.

Category	DWeb Service	Overview	Website
Social Media	LivePeer	Decentralised video streaming network built on the Ethereum blockchain	https://livepeer.org/
	Activity Pub	Decentralised social networking protocol	https://activitypub.rocks/
	Fleek	Enabling developers to build websites and apps on "the new open web: permissionless, trustless, censorship resistant, and free of centralised gatekeepers"	https://fleek.co/
	LBRY	Using blockchain technology, LBRY is a protocol that allows developers to build apps that interact with digital content on the LBRY network	https://lbry.com
Domain Names	ENS Domains	Decentralised 'domain name system'	https://ens.domains/
	Unstoppable Domains	Decentralised 'domain name system'	https://unstoppable domains.com/
App/File Hosting & Sharing Services	BitTorrent	Communication protocol for peer-to-peer file sharing	https://www.bittorrent.org/
	Skynet	Skynet is a decentralised storage and app hosting platform	https://skynetlabs.com/
	IPFS	A protocol and peer-to-peer network for storing and sharing data in a distributed file system	https://ipfs.io/
Private Server Services	Freedombox	A global project that provides a private server system to empower people to host their own internet services, such as websites, encrypted messengers, file sharing, and more.	https://freedombox.org
	Solid	Creating interoperable ecosystems of applications and data where individuals store their data in Solid Pods and are free to use their data seamlessly across different services and applications.	https://solidproject.org/

3 Literature Review

3.1 Content Moderation and the DWeb

Content moderation and the DWeb might sound like a counterintuitive angle to explore at first. Shouldn't the answer be straightforward? Surely, a decentralised web and its platforms would not have any content moderation. This line of thinking has been referenced by authors such as Hadley and Clifford who argue that existing content moderation regimes largely rely on companies to enforce them.[50] Therefore, the existence and implementation of content moderation regimes by private corporations that are able to access and remove content of individual users is paramount. As a consequence, the removal of these intervening factors results in the de facto removal of any content moderation, including that of extremism-related content. In the past, major tech companies have addressed legislative obscurity with respect to designating terrorist content and organisations by devising their own rules and regulations. In the future, a proliferating DWeb would mean that content moderation is much more difficult, potentially even impossible.[51]

As mentioned, one impetus for advocates of a DWeb is the aim to remove the Internet from the control of major players, mainly domineering tech companies. Content moderation, however, is only partially reliant on tech companies' intrinsic drive towards moderation. Hence it is not a system that requires our trust, as it is also under significant regulatory pressure and partially enforced by legislation.[52] These regulatory pressures, for instance, also force 'anti-censor' platforms such as Telegram occasionally to comply with content moderation requests.[53]

However, the DWeb is set out to be a new thing entirely, as it aims to be entirely built on network infrastructure that is far less accessible for one company or agency, restricting the ability to remove content.[54] For example, existing platforms like RocketChat inhibit the platform's own developers from acting against content when it's stored on user-operated servers. One might compare this to other anti-censor platforms like Parler, which relied on Amazon Web Services and hence was vulnerable to takedowns by centralised actors – in this case, Amazon.[55]

50 Hadley, Adam. 'Terrorists Will Move to Where They Can't Be Moderated'. Wired UK, 31 May 2021. https://www.wired.co.uk/article/terrorists-dweb; Clifford, Bennett. 'Moderating Extremism: The State of Online Terrorist Content Removal Policy in the United States'. n.d.: 24.

51 See Hadley, Adam, 2021.

52 Gillespie, Tarleton. 'Content Moderation, AI, and the Question of Scale'. Big Data & Society 7, no. 2 (1 July 2020). https://doi.org/10.1177/2053951720943234; West, SM. 'Censored, suspended, shadowbanned: User interpretations of content moderation on social media platforms.' *New Media & Society* 20, no. 11 (2018): 4366–4383. Nonetheless, companies often evade transparency attempts. See: Miller, Carly. 'Can Congress Mandate Meaningful Transparency for Tech Platforms?' Brookings (blog), 1 June 2021. https://www.brookings.edu/techstream/can-congress-mandate-meaningful-transparency-for-tech-platforms/

53 Nicas, Jack, and André Spigariol. 'Brazil Lifts Its Ban on Telegram After Two Days'. The New York Times, 20 March 2022, sec. World. https://www.nytimes.com/2022/03/20/world/americas/brazil-telegram-bolsonaro.html

54 King, Peter. 'Islamic State group's experiments with the decentralized web'. https://www.europol.europa.eu/publications-events/publications/islamic-state-group's-experiments-decentralised-web; to read more about volunteer moderation in Web2, see Matias, Nate. 'The Civic Labor of Volunteer Moderators Online'. To read more about future possibilities of moderation in Web3, see Feerst, Alex. 'A New Hope For Moderation And Its Discontents?'. TechDirt.

55 Peters, Cameron. 'Why Parler Is Disappearing from the Internet'. Vox, 10 January 2021. https://www.vox.com/2021/1/10/22223250/parler-amazon-web-services-apple-google-play-ban

The development of the DWeb is happening in a piecemeal manner which means there are several different dynamics at play which leave room for (some) content moderation. This content moderation is of a different nature than commercial content moderation by the most prominent existing approaches of big tech companies, such as Meta or Twitter.[56] In addition, there is one overshadowing notion that is promoted as a harbinger for content moderation in a decentralised web – 'tokenomics:' the idea to incentivise people to become involved in decentralised platforms and develop an interest not to ruin them.[57] Edelman explains that by distributing tokens and linking increased usage of a platform to value increase of the tokens, the individual users would develop an interdependent interest in seeing the platform flourish.[58] While this idea is radical in its conceptualisation of ownership, already today content moderation relies on users to a certain degree. York outlines how a combination of user reporting, or 'flagging,' and automation define content moderation.[59]

Hassan et al. undertook an in-depth case study of content moderation on Pleroma, a microblogging platform, that relies on 'federation policies', just as other DWeb platforms, such as Mastodon (microblogging), Hubzilla (cyberlocker) and PeerTube (video sharing) do.[60] The main difference in those attempts at content moderation are that they rely on moderation on a per-instance basis (versus centralised services who employ a per-user granularity).[61] So-called instance administrators enforce policies within their instance (server) to moderate the content coming from other federated instances. For example, administrators of one instance can block (that is, reject) any material from other instances that match specific criteria. This instance-based approach shifts the moderation responsibility to administrators. In their study, the authors argue that the existing moderation on Pleroma leads to collateral damage (or over-blocking) as the 'reject' action is most popular: it affects over 80% of users and almost 90% of posts. This harsh policy rejects entire instances, even though only a subgroup on any particular instance might be transgressing.[62]

Finally, several authors reason that content moderation is a major effort to keep users safe and create an internet that is not only accessible but also enjoyable for users.[63] As Edelman argues, one of the central areas in which tech companies have made major advancements

56 York, Jillian: The Global Impact of Content Moderation'. ARTICLE 19, 7 April 2020. https://www.article19.org/resources/the-global-impact-of-content-moderation/

57 Malinova, Katya, and Andreas Park. 'Tokenomics: When Tokens Beat Equity'. SSRN Scholarly Paper. Rochester, NY, 18 November 2018. https://doi.org/10.2139/ssrn.3286825

58 In addition, people who have the most tokens will actually have more power and they'll get to vote on what happens, and it'll all be very participatory. And again, there's no one in the middle calling the shots, Listen to Edelman in the following interview with Hendrix, Justin, 2022.

59 See York, Jillian, 2020.

60 Hassan, Anaobi Ishaku, Aravindh Raman, Ignacio Castro, Haris Bin Zia, Emiliano De Cristofaro, Nishanth Sastry, and Gareth Tyson. 'Exploring Content Moderation in the Decentralized Web: The Pleroma Case', 2021: 8.

61 Halevy, Alon, Cristian Canton Ferrer, Hao Ma, Umut Ozertem, Patrick Pantel, Marzieh Saeidi, Fabrizio Silvestri, and Ves Stoyanov. 'Preserving Integrity in Online Social Networks'. arXiv, 25 September 2020. https://doi.org/10.48550/arXiv.2009.10311. For other work on content moderation in social media, see, *inter alia*, Halevy et al., Fortuna et al., Ribeiro et al., Zannettou. There have also been a set of studies looking specifically at DWeb services. Raman et al. measured the challenges in deploying DWeb applications, particularly related to network issues, Zignani et al. studied the growth of Mastodon while comparing its structure with Twitter. Similarly, La Cava et al. explored the evolution of Mastodon at an instance level, as well as the connectivity between instances. Doan et al. investigated the performance of a decentralized video streaming platform (DTube) by developing an app that streams from both centralized and decentralized services. However, none of these focused on content moderation.

62 Overall, according to Hassan et al., moderation affects the overwhelming majority of Pleroma's users: 97.7% users and 97.8% posts are impacted by policies.

63 Douek, Evelyn. 'Content Moderation as Administration'. SSRN Scholarly Paper. Rochester, NY, 10 January 2022. https://doi.org/10.2139/ssrn.4005326; Myers West, Sarah. 'Censored, Suspended, Shadowbanned: User Interpretations of Content Moderation on Social Media Platforms'. New Media & Society 20, no. 11 (1 November 2018): 4,366–83. https://doi.org/10.1177/1461444818773059; see discussions about content moderation controversies with regard to Cloudflare and OnlyFans or Filecoin.

over the last years is content moderation, albeit moderation is still far from being perfect.[64] Admittedly, the impetus was not only internal but also driven by tightened legislation (such as Germany's Network Enforcement Act) and frightening individual instances, such as the 2019 livestreaming of a terrorist attack in Christchurch, New Zealand.[65] Still, existing efforts have led to improvements and internet users writ large are unlikely to crave exposure to awful content or be keen to take on a more active role in platform governance. The outlined intricacies with content moderation, and with trust and safety in the DWeb more broadly, emphasise a general, ongoing set of questions regarding the DWeb: would people actually use it? Would there be an uptake in people using it to a greater degree? What would prompt such an uptake? Uncertainty around content moderation could easily stand in the way.

3.2 Online Extremism and the DWeb

Literature on the decentralised web in the context of online extremism remains scarce and the evidence base is limited. Up to the present day, only a few publications have mentioned the DWeb as a possible threat that could be exploited to increase online resilience against content and account removals.[66] As King and Bodo noted, IS has already experimented with DWeb technology, such as ZeroNet and Riot.[67] King further noted that IS began experimenting with such technology mid-2014 in response to Twitter's significant clamp down on IS accounts.[68] Europol's most recent review of Online Jihadist Propaganda (2021) highlights that IS supporter networks were actively experimenting in 2021 with DWeb technology, such as Ethereum Name Service (ENS), Inter-Planetary File System (IPFS) and D.Tube.[69] Most notably, IS supporters were found to exploit a private file hosting service to maintain an archive of 2.2 TB of IS propaganda material.[70]

While numerous experiments by IS and its supporter networks have been documented over the last five years, IS and its supporters do not appear to have found a safe haven that offers maximum security, stability, usability, and audience reach, vital factors that are considered when choosing to settle on a specific platform.[71]

64 See Edelman in the interview with Hendrix, 2022.
65 Ganesh, Bharath, and Jonathan Bright. 'Countering Extremists on Social Media: Challenges for Strategic Communication and Content Moderation'. Policy & Internet 12, no. 1 (2020): 6–19. https://doi.org/10.1002/poi3.236
66 Bodo. 'Decentralized Terrorism'; King. 'Islamic State group's experiments'; see also Jihadoscope's findings published on Twitter: https://twitter.com/JihadoScope/status/1084822532388282369 (Jan 2019); https://twitter.com/JihadoScope/status/1116443685233799189 (Apr 2019); https://twitter.com/JihadoScope/status/1143566875340812290 (Jun 2019); https://twitter.com/JihadoScope/status/1308420675925946377 (Sep 2020); https://twitter.com/JihadoScope/status/1353708987879972864 (Jan 2021); https://twitter.com/JihadoScope/status/1429782600609148933 (Aug 2021).
67 See: Bodo. 'Decentralized Terrorism'; and King. 'Islamic State group's experiments'.
68 King. 'Islamic State group's experiments': 5.
69 Europol. European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/cms/sites/default/files/documents/Online_Jihadist_Propaganda_2021_in_review.pdf p. 22-3, 2022. https://data.europa.eu/doi/10.2813/169367
70 Ayad, M., A. Amarasingam, and A. Alexander. 'The Cloud Caliphate: Archiving the Islamic State in Real-Time'. Combating Terrorism Center at West Point, p.5-6, 13 May 2021. https://ctc.westpoint.edu/the-cloud-caliphate-archiving-the-islamic-state-in-real-time/
71 Tech Against Terrorism. 'Analysis: ISIS Use of Smaller Platforms and the DWeb to Share Terrorist Content – April 2019 – Tech Against Terrorism', 29 April 2019. https://www.techagainstterrorism.org/2019/04/29/analysis-isis-use-of-smaller-platforms-and-the-dweb-to-share-terrorist-content-april-2019/, https://www.techagainstterrorism.org/2019/04/29/analysis-isis-use-of-smaller-platforms-and-the-dweb-to-share-terrorist-content-april-2019/
See Europol, 2022.

In the context of right-wing extremism and the far-right in more general,[72] scholarship has not specifically discussed the exploitation of DWeb technology per se but instead focused on introducing and characterising specific DWeb platforms, such as Bitchute[73] and Odysee.[74] In a similar vein, other work has focused more on analysing 'alt-tech' platforms and its user bases, e.g. Gab[75]; Gettr[76]; or, Parler.[77] These alternative platforms[78] have emerged as an important new ecosystem that has become popular following increased content moderation and de-platforming of far-right organisations and activists[79], especially in the wake of the 2017 'Unite the Right' rally in Charlottesville;[80] the ecosystem largely exists due to the "perceived risks of censorship in mainstream spaces."[81] Regardless of whether far-right entities exploit DWeb technology or not, it is vital to consider the current ecosystem of alt-tech platforms when assessing to what extent DWeb technology could contribute to the spread of extremist material online.

Because there is little known about to what extent right-wing extremist and Islamic State advocates exploit DWeb technologies, this review also consulted the wider literature on the current threat landscape to inform the risk assessment. With regards to Salafi-jihadism in general, Comford et al. found that Online Salafism among Gen-Z identities constitutes a cross platform phenomenon, which still includes big social media platforms, such as Facebook, Instagram, TikTok, and YouTube, but also gaming platforms like Discord[82] – all of which are not based on DWeb technology. Similarly, the exploitation of cloud services for archiving and distribution purposes must be noted as highlighted in the so-called Cloud-Caliphate report – an archive that grew to 2.2 TB from the fall of 2019 through the spring of 2021.[83]

72 The term 'far-right' is often used as an umbrella term that encompasses an array of different ideologies. For a more nuanced explanation see: Bjørgo, Tore and Aasland Ravandal, Jacob. Extreme-Right Violence and Terrorism: Concepts, Patterns, and Responses, p. 2-3. Last accessed 26 June 2022. Available at: https://icct.nl/app/uploads/2019/09/Extreme-Right-Violence-and-Terrorism-Concepts-Patterns-and-Responses-4.pdf
See also: Macdonald, Stuart, Kamil Yilmaz, Chamin Herath, J. M. Berger, Suraj Lakhani, Lella Nouri, and Maura Conway. 'The European Far-Right Online: An Exploratory Twitter Outlink Analysis of German & French Far-Right Online Ecosystems', p.7-8, 26 May 2022. Last accessed 10 June 2022.

73 Trujillo, Milo, Maurício Gruppi, Cody Buntain, and Benjamin D. Horne. 'What Is BitChute? Characterizing the "Free Speech" Alternative to YouTube'. arXiv, 29 May 2020. http://arxiv.org/abs/2004.01984

74 Leidig, Eviane. 'Odysee: The New YouTube for the Far-Right'. GNET (blog). Accessed 5 June 2022. https://gnet-research.org/2021/02/17/odysee-the-new-youtube-for-the-far-right/

75 Zannettou, Savvas, Barry Bradlyn, Emiliano De Cristofaro, Haewoon Kwak, Michael Sirivianos, Gianluca Stringhini, and Jeremy Blackburn. 'What Is Gab? A Bastion of Free Speech or an Alt-Right Echo Chamber?' In Companion of the Web Conference 2018 on The Web Conference 2018 – WWW '18, 1007–14, 2018. https://doi.org/10.1145/3184558.3191531

76 Paudel, Pujan, Jeremy Blackburn, Emiliano De Cristofaro, Savvas Zannettou, and Gianluca Stringhini. 'An Early Look at the Gettr Social Network'. arXiv, 12 August 2021. http://arxiv.org/abs/2108.05876

77 Aliapoulios, Max, Emmi Bevensee, Jeremy Blackburn, Barry Bradlyn, Emiliano De Cristofaro, Gianluca Stringhini, and Savvas Zannettou. 'An Early Look at the Parler Online Social Network'. arXiv, 18 February 2021. http://arxiv.org/abs/2101.03820

78 These are also called 'Fringe Platforms'. See for example: Conway, Maura, Scrivens, Ryan, and Macnair, Logan. Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends. ICCT Policy Brief, p. 8. Last accessed 26 June 2022. Available at: https://icct.nl/app/uploads/2019/11/Right-Wing-Extremists-Persistent-Online-Presence.pdf
For a detailed explanation of the online extremist ecosystem, see: Williams, Heather J.; Evans, Alexandra T.; Ryan, Jamie; Mueller, Erik E.; and Downing, Bryce. The Online Extremist Ecosystem, p.18. RAND Report. Last accessed 22 June 2022. Available at: https://www.rand.org/content/dam/rand/pubs/perspectives/PEA1400/PEA1458-1/RAND_PEA1458-1.pdf

79 Ibid.

80 Jasser, Greta, Jordan McSwiney, Ed Pertwee, and Savvas Zannettou. '"Welcome to #GabFam": Far-Right Virtual Community on Gab'. New Media & Society, 28 June 2021, 14614448211024546. https://doi.org/10.1177/14614448211024546 See also: Donovan, Joan, Becca Lewis, and Brian Friedberg. 'Parallel Ports. Sociotechnical Change from the Alt-Right to Alt-Tech'. In Edition Politik, edited by Maik Fielitz and Nick Thurston, 1st ed., 71:49–66. Bielefeld, Germany: transcript Verlag, 2019. https://doi.org/10.14361/9783839446706-004

81 Trujillo, Milo, Maurício Gruppi, Cody Buntain, and Benjamin D. Horne. 'What Is BitChute? Characterizing the "Free Speech" Alternative to YouTube'. arXiv, 29 May 2020. http://arxiv.org/abs/2004.01984

82 Comerford, Milo, Moustafa Ayad, and Jakob Guhl. 'Gen-Z & The Digital Salafi Ecosystem. Executive Summary', p. 7. Accessed 5 June 2022. https://www.isdglobal.org/wp-content/uploads/2021/11/Executive-summary.pdf

83 Ayad, M., A. Amarasingam, and A. Alexander. 'The Cloud Caliphate: Archiving the Islamic State in Real-Time'. Combating Terrorism Center at West Point, p.5-6, 13 May 2021. https://ctc.westpoint.edu/the-cloud-caliphate-archiving-the-islamic-state-in-real-time/

Another noteworthy area is that of understanding Extremists' use of gaming (adjacent) platforms that has become a critical issue, especially since the 2019 livestreamed terror attack in Christchurch, New Zealand.[84] According to Europol's assessment of the terrorist situation in the EU in 2020, evidence suggests that right-wing extremists were increasingly using video games and gaming platforms to propagate their ideology.[85]

Another current main threat that needs to be highlighted is that of terrorist and violent extremist operated websites (TVEWOs) on the surface web. Tech Against Terrorism (TAT)[86] has identified 198 websites, operated by violent Sunni and Shia as well as violent far right entities. According to TATs assessment, these websites pose one of the most significant threats and are primarily used for disseminating and archiving material, as well as for recruitment and internal communication purposes.[87]

Given this literature review, we conclude that DWeb technologies have been on the radar of extremist entities for quite some time but the limiting features and related limitations of audience reach have been restraining their exploitation. However, the pressing concern is whether the general expansion of the DWeb would go hand-in-hand with an increased exploitation by extremist actors.

84 European Commission. Migration and Home Affairs. Extremists' use of gaming (adjacent) platforms – Insights regarding primary and secondary prevention measures, August 2021. Last accessed 15 June 2022. Available at: https://ec.europa.eu/home-affairs/networks/radicalisation-awareness-network-ran/publications/extremists-use-gaming-adjacent-platforms-insights-regarding-primary-and-secondary-prevention_en

85 Europol (2021), European Union Terrorism Situation and Trend Report, Publications Office of the European Union, Luxembourg, p.9. Last accessed 15 June 2022. Available at: https://www.europol.europa.eu/publications-events/main-reports/european-union-terrorism-situation-and-trend-report-2021-tesat

86 Learn more about TAT: https://techagainstterrorism.org

87 Tech Against Terrorism. 'Report: The Threat of Terrorist and Violent Extremist Operated Websites'. Accessed 10 June 2022. https://www.techagainstterrorism.org/2022/01/28/report-the-threat-of-terrorist-and-violent-extremist-operated-websites/; see also Europol, 2022, p.22.

4 How Do Extremists Exploit the DWeb?

4.1 Methodology

Ethics: Data collection, management and analysis was carried out while taking the principles as laid out by the British Psychological Society in its Ethics Guidelines for Internet Mediated-Research 2021 and King's College London's ethical guidance into consideration.[88] The researchers followed strict internal guidelines as well to maximise operational security when conducting the research and handling the data. In this regard, it is critical to highlight that any data collected or received for this report:

- was not shared with anyone;
- was stored on one local drive;

Furthermore:

- the analysis was carried out offline to avoid accidently clicking on any URLs;
- the report does not mention specific websites or individual groups/persons;
- any reported findings are presented as aggregated results to avoid inadvertently explaining where to find extremist content online.

With regards to Tech Against Terrorism's dataset, it is important to highlight:

- the analysis was carried out offline to avoid accidently clicking on any URLs
- this report will not mention specific websites or individual groups/persons
- any reported findings are presented as aggregated results to avoid inadvertently explain where to find extremist content online
- the dataset contained already aggregated results
- the dataset contained only domain names[89] and the number of how often it occurs in the dataset
- the dataset was deleted after the analysis as there was no reason to keep it[90]
- most importantly, the findings will not mention any URL or domain name to inadvertently explain where to find extremist content online

88 Last accessed 10 June 2022. Available at: https://www.bps.org.uk/news-and-policy/ethics-guidelines-internet-mediated-research

89 A domain name provides a human-readable address for any web server available on the Internet and is made up of several parts. For more information see: Mozilla. What is a domain name? Last accessed 12 June 2022. Available at: https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_domain_name

90 For researchers who like to replicate our analysis or use the same dataset for a different research project, please get in touch with Tech Against Terrorism.

Data Collection: This research project uses two different datasets to assess the risk of DWeb technology being exploited by right-wing extremists (RWE) and the so-called Islamic State (IS). It is important to note that this is not a comparative analysis but two different case studies.

Right-Wing Extremist Dataset: For this dataset, we solely relied on Telegram data as it has been a popular messenger app among far-right entities, including right-wing extremists[91]. To this end, a sample of thirty Telegram channels was created that fulfilled the following four sample criteria:

(1) The content promoted by the channel owner must be classed as right-wing extremist content. To this end, we followed the conceptualisation as set out by Ravik Jupskås and Beau Segers, which describes right wing extremism as: "Right-wing extremism is usually defined as a specific ideology characterized by 'anti-democratic opposition towards equality'. It is associated with racism, xenophobia, exclusionary nationalism, conspiracy theories, and authoritarianism."[92]

(2) The channel must have at least 500 subscribers

(3) The channel must actively share URLs

(4) The content must be in English.

In terms of timeline, the export included all messages since the creation of the channel. The oldest message found in the dataset was from 16 October 2019. The data export excluded any multimedia data and was then processed with a custom Python script to extract all shared domain names alongside the number of how often it was shared.

Islamic State Dataset: The dataset for the so-called Islamic State was provided by the UN-supported Public-Private Partnership Tech Against Terrorism (TAT)[93]. TAT's mission is to support the tech industry tackling terrorist exploitation of the Internet, whilst respecting human rights. In 2020, with support of Public Safety Canada[94], TAT launched the Terrorist Content Analytics Platform (TCAP), which collates the world's largest database of verified terrorist content. The TCAP detects and verifies terrorist content in real-time from messaging platforms and apps and then alerts smaller tech platforms to support them with content moderation

91 See: Bump, Phillip. 'Analysis | The Platform Where the Right-Wing Bubble Is Least Likely to Pop'. Washington Post, 2022. Last accessed 17.06.2022. https://www.washingtonpost.com/politics/2022/04/23/telegram-platform-right-wing/
See also: Urman, Aleksandra, and Katz, Stefan. 'What they do in the shadows: examining the far-right network on Telegram', in: Information, Communication & Society, Vol. 25, Issue 7, 2022. https://doi.org/10.1080/1369118X.2020.1803946

92 Ravik Jupskås, Anders and Beau Segers, Iris. What is right-wing extremism? in: Knowing what's (far) right. A compendium, edited by Ravik Jupskås, Anders and Leidig, Evianne, p.7. Last Accessed 22 June 2022. Available at: https://www.sv.uio.no/c-rex/english/groups/compendium/c-rex-compendium-print-version.pdf
For a minimal definition see: Carter, Elisabeth. Right-wing extremism/radicalism: reconstructing the concept. Last accessed 22 June 2022. Available at: https://eprints.keele.ac.uk/2221/1/JPI%20Revised%20Final.pdf

93 TAT Homepage. Last accessed 16 June 2022. Available at: https://www.techagainstterrorism.org/

94 Press Release by Tech Against Terrorism. Last accessed 16 June 2022. Available at: https://www.techagainstterrorism.org/2019/06/27/press-release-tech-against-terrorism-awarded-grant-by-the-government-of-canada-to-build-terrorist-content-analytics-platform/

efforts[95]. The dataset obtained from TAT contained an aggregated result of the top 50 shared domain names alongside the number of how often it was shared. The data was collected by TAT's OSINT team through their active monitoring and passive scraping activities between 26 November 2020 until 17th of June 2022.

Caveats: This research project is based on a sample of thirty right-wing extremist English-speaking Telegram channels. Therefore, any findings should be interpreted carefully because of four main reasons:

First, the data heavily relies on Telegram and does not include any other platform, which is used by RWEs. Second, it only includes the English language. Third, it does not take other ideologies into account, even though as Lee argues, "Ideologies cannot be considered mutually exclusive and crosspollination is likely to be common."[96] Lastly, it could be argued that the sample used was not large enough.

Taking all these caveats into consideration, we believe that even though the findings from the right-wing extremist dataset may not be overall representative for all right-wing extremists globally, they still led to valid insights that have not been identified in previous research. Furthermore, we believe that this research can pave the way for follow-up and more targeted research projects to generate deeper insights that differentiate between different ideologies, regions, and languages.

With regards to the IS dataset, we believe that the findings presented here are valid due to the high quality of the data which was collected, processed, and verified by Tech Against Terrorism's OSINT team for the TCAP – an online system that was developed specifically to detect, verify, and alert tech companies about the existence of terrorist content on their platforms.

Data Analysis: To provide an accurate and evidence-based risk assessment, this research analysed shared URLs in (violent) extremist and terrorist online spaces. Similar research projects have generated useful results, as McDonald et al. 2022 noted[97]. The analysis was conducted offline using Tableau[98] and focused on only the top 50 most shared URLs, or more respectively, domain names. All reported findings are aggregated results.

95 TCAP Homepage. Last accessed 15 June 2022. Available at: https://www.terrorismanalytics.org/. Read more about the TCAP in its latest Transparency Report. Last accessed 15 June 2022. Available at: https://www.techagainstterrorism.org/wp-content/uploads/2022/03/Tech-Against-Terrorism-TCAP-Report-March-2022_v6.pdf
96 Also see McDonald et al. 2022: p. 6-7.
97 See: McDonald et al. 2022, p. 10.
98 Tableau Homepage. Last accessed 16 June 2022. Available at: https://www.tableau.com/.

4.2 Overview of the Data

Right-Wing Extremist Dataset

The right-wing extremist Telegram dataset comprises 30 Telegram channels that produced from 16 October 2019 to 9 June 2022 a total of **387,090** messages of which **143,483** are URLs. The combined number of subscribers for all channels is **173,555**.

Total number of messages	Total number of subscribers	Total number of shared URLs
387,090	173,555	143,483

Findings

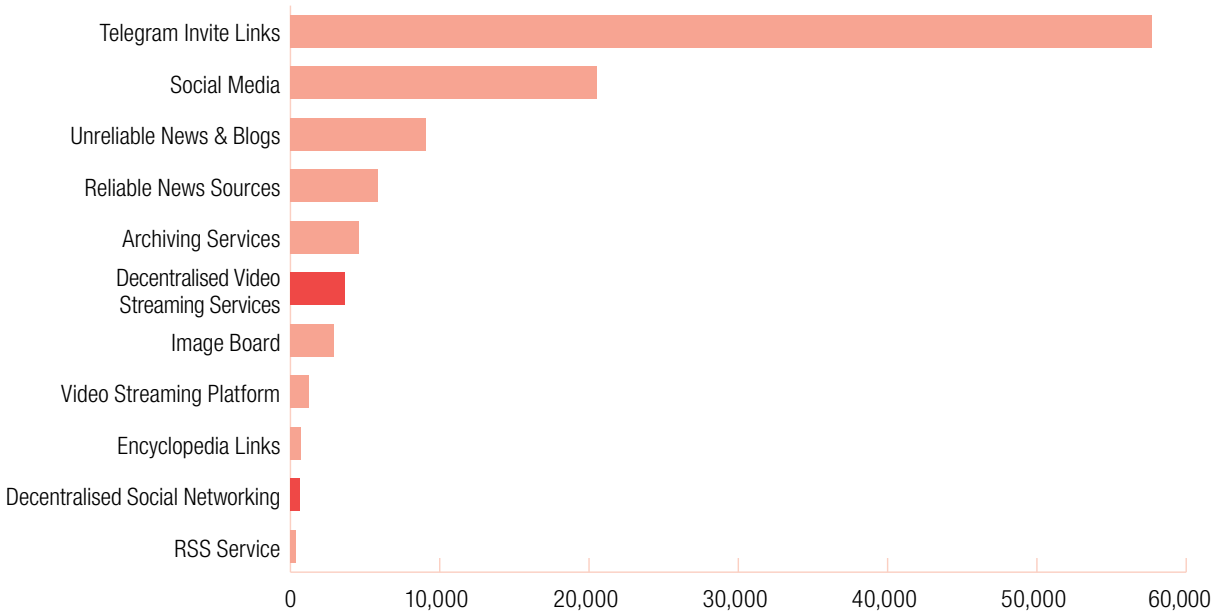
Types of Outlinks

We have identified 11 different types of sites to which the 30 Telegram channels outlinked. The following aggregation is sorted by the total number of URL shares.

Category	Clarification	Total Number of Shares
Telegram Invite Links	Links to other Telegram chats and channels.	57,736
Social Media	Our sample included two major social media platforms	20,505
Unreliable News & Blogs	These are news sources & blogs considered unreliable[99]	9,050
Reliable News Sources	These are prominent news sources that are widely considered reliable[100]	5,879
Archiving Services	In total five archiving services have been identified.	4,604
Decentralised Video Streaming Services	In total three DWeb-based video streaming services were identified.	**3,630**
Image Board	One image board has been identified.	2,901
Video Streaming Platform	One particular antisemitic video streaming platform has been identified.	1,251
Encyclopedia Links	These are links to online encyclopedia entries.	699
Decentralised Social Networking	One DWeb-based social networking site has been identified.	**644**
RSS Service	This service automatically retrieves new or updated content from particular websites.	355

99 Our assessment was strongly based on iffy.news – an index of unreliable news sources. Where data was not available, we researched the websites ourselves relying on a variety of fact-checking/verification sites. Those sites that were not listed or where no evidence was found to suggest an unreliable source, the website was classified as Prominent News Sources. This category includes only well-established and prominent news organizations around the world.

100 See next footnote.



Finding I: DWeb services are not significantly represented
Evidence suggests that DWeb services have not been used extensively in our RWE sample. In fact, less than 4% of the URLs led to a DWeb service.[101] Furthermore, only four DWeb services have been identified, of which three are video streaming platforms and only one social networking site. This suggests that DWeb services play a minor role within the current online ecosystem.

Finding II: The majority of outgoing links led to two major social media platforms
The most shared URLs led to two major social media platforms.[102] A total of 20,505 links were shared in our sample. Therefore, it could be argued that despite increasing efforts by social media companies against right-wing extremist entities, traditional social media platforms still represent an important pillar within the wider online ecosystem.

Finding III: The right-wing extremist sample shared more links to unreliable news and blogs than more reliable news sources
Evidence suggests that right-wing extremists consume more unreliable news and blogs than more reliable news sources. In fact, 9,050 URLs led to unreliable sources, whereas 5,879 URLs led to more reliable news sources. This suggests an important role played by unreliable websites in the right-wing extremism online ecosystem.

Finding IV: Archiving Services are used just as much as DWeb services
In total, 4,604 URLs were shared that led to five different Archiving Services. This suggests that these services play a role in the current online ecosystem; however, almost to the same degree as DWeb services, which have accounted for a total of 4,274 shared URLs.

101 4,274 shared URLs led to DWeb services out of our sample of 102,580 shared URLs (Top 50 most shared domain names)
102 For this analysis we excluded Telegram invite links as this is a very common behaviour among channels and chats

Islamic State Dataset

The Islamic State dataset contains **31,951** URLs that led to verified terrorist content, of which **26,176** were subjected to further analysis as these belong to the top 50 shared domain names.

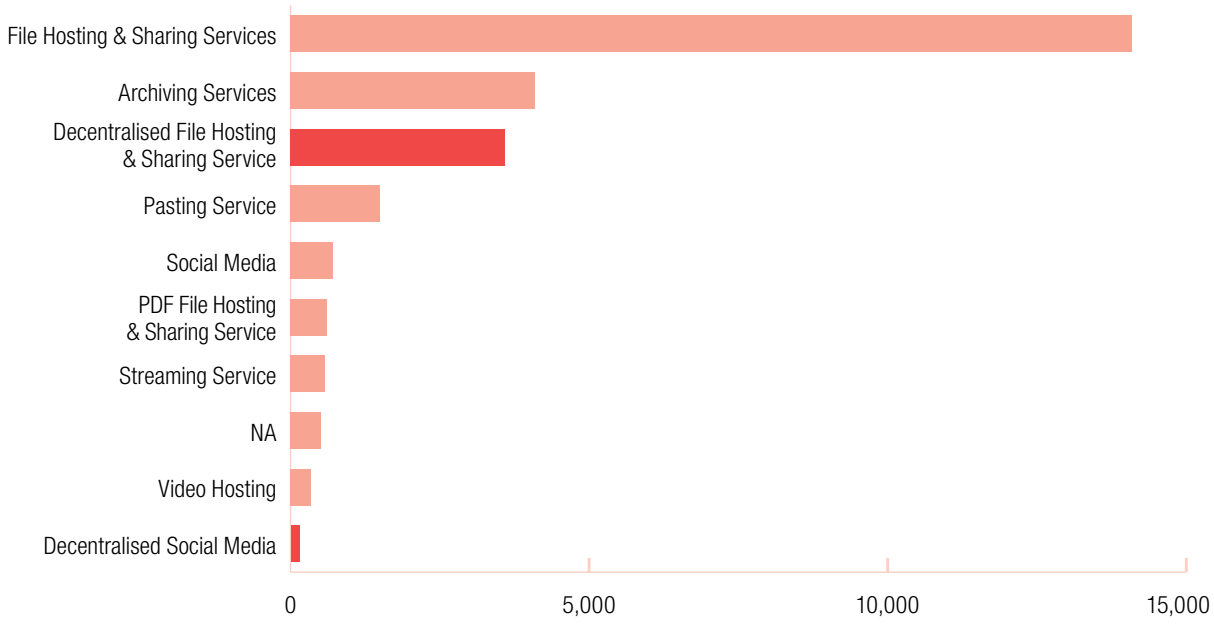
Total number of shared URLs
31,951 (26,176)

Findings

Types of outlinks

We have identified 10 different types of websites to which IS entities have outlinked on various platforms. The following aggregation is sorted by the total number of URL shares.

Category	**Clarification**	**Total Number of Shares**
File Hosting & Sharing Services	These are services that allow anyone to upload and share any files they like.	14,092
Archiving Services	These services are used to preserve any content (text and multimedia) for an unlimited amount of time.	4,096
Decentralised File Hosting & Sharing Service	These services are very similar to file hosting & sharing services with the exception that they are decentralised and thus hosted not on a single server.	**3,584**
Pasting Service	These services allow users to paste any text (including images) and redistribute that content using a unique link.	1,500
Social Media	This category includes three social media platforms/apps.	714
PDF File Hosting & Sharing Service	These services are specifically designed for hosting and sharing PDF content.	610
Streaming Service	Streaming refers to the delivery of the content. Instead of downloading videos, users can immediately consume it.	571
NA	These websites were taken down and thus excluded.	513
Video Hosting	These are services that enable users to upload their video content so it can be consumed by others.	346
Decentralised Social Media	These are decentralised social media platforms.	**150**



Finding I: Decentralised services are exploited but not to the same extent as centralised ones
Evidence suggests that decentralised services are exploited to a much lesser degree than centralised ones. In fact, out of the total sample of 26,176 URLs only 14% (3,734 URLs) led to verified terrorist content on decentralised services, whereas 75% (19,688 URLs) of the verified terrorist content was found on centralised services, in particular file hosting and sharing, archiving, as well as pasting services.

Regarding social media, only 0.5% of all URLs (150) led to verified terrorist content on decentralised social media platforms. This also suggests that decentralised social media solutions are currently not attractive to terrorist users.

Finding II: File hosting and sharing services are prime targets
The most exploited category in our sample is the file hosting and sharing service. In 54% (14,092 URLs) of the cases, verified terrorist content was found on such a service. This suggests that so-called Islamic State members and supporters heavily exploit such services to host and distribute their terrorist content.

Finding III: There is more verified terrorist content on file hosting and sharing, archiving as well as pasting services than on social media
When comparing it with social media platforms, evidence suggests that less than 3% (714 out of 26,176 URLs in total) of terrorist content was uploaded to social media. In contrast, 75% (19,688 out of 26,176 URLs) of the verified terrorist content was found on file hosting and sharing, archiving, as well as pasting services. This suggests that the latter services play a more significant role in hosting and distributing terrorist content than social media platforms.[103]

103 In fact, social media platforms usually act as beacons with the goal of reaching as many people as possible and redirecting them to sites where the terrorist content is hosted. See for a detailed explanation: Tech Against Terrorism. GIFCT Technical Approaches Working Group. Gap Analysis and Recommendations for deploying technical solutions to tackle the terrorist use of the internet, p. 15-6, July 2021. Last accessed 20.06.2022. Available at: https://gifct.org/wp-content/uploads/2021/07/GIFCT-TAWG-2021.pdf

5 How Could Extremists Exploit the DWeb?

Before providing an answer to this question, it is necessary to underline one important characteristic when talking about extremist or terrorist exploitation of technology, namely in what ways these differ from average users. In reality there is little to no difference. According to Fishman who used to be the director of Facebook's Counterterrorism and Dangerous Organisations team, "[…] terrorists use the Internet in much the same way as other people".[104] With regards to exploiting technologies, OPTF argues that "all forms of technologies can be exploited by nefarious actors."[105] In a similar vein, interviewee Molly White stressed that any technology which enables privacy and places more control with users than with a centralised entity, can be used for evil as well as good.[106]

So, how could extremists exploit the DWeb? In theory, they could utilise DWeb file-hosting services, launch websites or employ video streaming services that host violent extremist, terrorist and other harmful content. As things stand on the DWeb, the control over a site and its underlying data lie with the entity that established them. In other words, it will be extremely difficult, if not impossible, to take down any content or a given website itself.

Does this mean emerging DWeb technology is dangerous and could thus offer a safe haven to such entities? The short answer is no.

It is important to stress that there is no need for emerging DWeb technologies, as current technologies are sufficient for extremists to achieve their objectives. As White says, "If someone has the knowledge, time, and money it is fairly straightforward to self-host a website, and the technologies required to do so (DNS, etc.)."[107] Other examples include the exploitation of archiving services as evidenced in the findings and by Europol's targeted operation against Salafi-jihadist content on Internet archive platforms;[108] or in the context of cybercrime, using the TOR network for selling illicit drugs as seen in the case of Silk Road, which operated from 2011 to 2013.[109] These examples, however, should not imply that nothing should be done to mitigate the risks as TAT's Senior OSINT Analyst, Arthur Bradley, warns that the "DWeb is definitely of interest" to terrorist entities.[110]

104 Fishman, Brian. Crossroads: Counter-terrorism and the Internet, 2019. Last accessed 16.06.2022. Available at: https://tnsr.org/2019/02/crossroads-counter-terrorism-and-the-internet/
105 Interview with Oxen Privacy Tech Foundation (OPTF), 2022.
106 Interview with Molly White.
107 Ibid.
108 Press Release by Europol. Last accessed 15 June 2022. Available at: https://www.europol.europa.eu/media-press/newsroom/news/jihadist-content-targeted-internet-archive-platform
109 Flamand, Claudia. And David Décary-Hétu. 'The open and dark web. Facilitating cybercrime and technology-enabled offenses', in The Human Factor of Cybercrime, edited by Leukfeldt, Rutger, and Thomas J. Holt, Routledge, London, 2020: 55–6.
110 Interview with Senior OSINT analyst Arthur Bradley at Tech Against Terrorism.

The OPTF, for example, recognises and acknowledges that "the closed and private nature of the DWeb and encrypted and secure technologies will attract nefarious actors."[111] That said, it is vital to underline that despite the appeal of censorship resistance, high security, and full control over the data, DWeb services can counter the exploitation of their services. OPTF, for example, has been working on various technical and design strategies to mitigate such risks. This includes, for example, limiting file-transfer size and the use of hashing techniques to detect uploads of illegal content. Furthermore, OPTF is engaging with other entities to discuss further approaches.[112]

All in all, the DWeb should not be perceived negatively. In fact, it's a technology movement that aims to return autonomy to users, which arguably is more positive than negative. How and if this is going to be achieved are different questions, but even though the DWeb could be exploited – just as any other current or future technology could be – DWeb services can mitigate the risks and should thus not be perceived as a possible safe haven for extremists.

111 Interview with Oxen Privacy Tech Foundation (OPTF), 2022.
112 Ibid.

6 Risk Assessment & Discussion

Based on the literature review, conducted interviews and analysis, the following can be summarised:

We assess that DWeb services are at medium risk of being exploited by RWE and IS entities.

It must be emphasised that the DWeb is far from being as popular as the current World Wide Web we know. The analysis demonstrated that DWeb services are being exploited but not to a high degree. In fact, only 4% of the URLs in the RWE sample led to a DWeb service. In the context of IS, just 14% of the URLs led to a DWeb service.

While DWeb services may attract nefarious actors due to being more resilient against account and content removals, extremist entities also assess online platforms before choosing which ones to use for what. This assessment is often based on four criteria: security, stability, audience reach, and usability.[113] Because the DWeb is far from being as developed as today's World Wide Web,[114] an argument could be made that the DWeb may offer security and stability, but it lacks the usability and potential audience reach of current services in today's World Wide Web. Thus, the DWeb is not highly attractive at the moment.

Furthermore, we assess the DWeb is not necessarily needed to enable extremist entities to host, distribute, and control their content as required services to achieve this already exist.

In the case of right-wing extremism, a wide range of platforms is used. In fact, the virtual ecosystem is described as dynamic[115] and adaptive to new technologies, sites, and virtual tools.[116] Similarly terrorist entities, such as IS, use a wide range of platforms that serve different purposes within its online ecosystem[117].

113 See Annex 1 for a detailed breakdown, in: Tech Against Terrorism. GIFCT Technical Approaches Working Group. Gap Analysis and Recommendations for deploying technical solutions to tackle the terrorist use of the internet, p. 33, July 2021. Last accessed 20.06.2022. Available at: https://gifct.org/wp-content/uploads/2021/07/GIFCT-TAWG-2021.pdf
See also: King, Peter, p.8 'This Paper Was Presented at the 3rd Conference of the European Counter Terrorism Centre (ECTC) Advisory Network, 9-10 April 2019, at Europol Headquarters, The Hague. The Views Expressed Are the Authors' Own and Do Not Necessarily Represent Those of Europol.'https://www.europol.europa.eu/publications-events/publications/islamic-state-group's-experiments-decentralised-web

114 See for example: O'Reilly, Tim. Why it's too early to get excited about Web3. Last accessed 22.06.2022. Available at: https://www.oreilly.com/radar/why-its-too-early-to-get-excited-about-web3/
See also: Corbyn, Zoe. 'Decentralisation: The next Big Step for the World Wide Web'. The Guardian, 8 September 2018. https://www.theguardian.com/technology/2018/sep/08/decentralisation-next-big-step-for-the-world-wide-web-dweb-data-internet-censorship-brewster-kahle

115 Stephane J. Baele, Lewys Brace & Travis G. Coan (2020) Uncovering the Far-Right Online Ecosystem: An Analytical Framework and Research Agenda, Studies in Conflict & Terrorism.

116 Williams, Heather J.; Evans, Alexandra T.; Ryan, Jamie; Mueller, Erik E.; and Downing, Bryce. The Online Extremist Ecosystem, p.4. RAND Report. Last accessed 22 June 2022. Available at: https://www.rand.org/content/dam/rand/pubs/perspectives/PEA1400/PEA1458-1/RAND_PEA1458-1.pdf

117 Tech Against Terrorism. GIFCT Technical Approaches Working Group. Gap Analysis and Recommendations for deploying technical solutions to tackle the terrorist use of the internet, p. 14-5, July 2021. Last accessed 20.06.2022. Available at: https://gifct.org/wp-content/uploads/2021/07/GIFCT-TAWG-2021.pdf

As the analysis demonstrated, the role of archiving services was prevalent in both samples. In both cases, these services ranked among the most shared URLs. This demonstrates how important archiving services are in both online ecosystems. In the wider context of salafi-jihadism, that may explain why the European Union Internet Referral Unit conducted an operation in late 2021, specifically targeting Salafi-jihadist content on the Internet Archive platform.[118]

Regarding the RWE online ecosystem, the adoption of alternative platforms needs to be highlighted. As Conway et al. argues "Beyond the major social media platforms, a diversity of more fringe platforms host increasing amounts of RWE content, due at least in part to increased takedown by major platforms."[119] In light of these platforms, it could be argued that there may not be a need for a DWeb service should fringe platforms satisfy right-wing extremist users.

Furthermore, current technology, or more respectively services, exist that enable anyone to self-host and thus self-regulate any content they like. The so-called 'Bulletproof hosting services' allow anyone to host malicious things, such as malware, botnets, ransomware, or other nefarious content on someone else's server. These services are operated by companies or individuals that are very lenient in terms of what can be hosted on their servers.[120] In a similar vein, as the analysis has demonstrated in the case of IS, file hosting and sharing services are heavily exploited and thus constitute a major pillar in their online ecosystem.[121]

Finally, we assess that DWeb services can mitigate the risks of being exploited and thus, it does not necessarily constitute a safe haven for extremists.

As mentioned earlier, various technical and design strategies to mitigate such risks can be implemented. This includes and is not limited to, for example, file-transfer size limitations and the use of hashing techniques to detect uploads of illegal content.[122]

Furthermore, content moderation policies can be also implemented and enforced. In the context of a federalised social network, for example, so-called instance (server) administrators enforce policies within their instance to moderate the content coming from other federated instances. For example, administrators of one instance can block any material from other instances should it violate their policies.[123] Nevertheless, to what extent these policies cover terrorist and extremist content as well as how well these are enforced is a different question.

118 Press Release by Europol. Jihadist content targeted on Internet Archive platform. Last accessed 26 June 2022. Available at: https://www.europol.europa.eu/media-press/newsroom/news/jihadist-content-targeted-internet-archive-platform

119 Conway, Maura, Scrivens, Ryan, and Macnair, Logan. Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends. ICCT Policy Brief, p. 9. Last accessed 26 June 2022. Available at: https://icct.nl/app/uploads/2019/11/Right-Wing-Extremists-Persistent-Online-Presence.pdf

120 What is bulletproof hosting? Last accessed 27 June 2022. Available at: https://us.norton.com/internetsecurity-emerging-threats-what-is-bulletproof-hosting.html

121 For a detailed explanation, see: Tech Against Terrorism. GIFCT Technical Approaches Working Group. Gap Analysis and Recommendations for deploying technical solutions to tackle the terrorist use of the internet, p. 14-7, July 2021. Last accessed 20.06.2022. Available at: https://gifct.org/wp-content/uploads/2021/07/GIFCT-TAWG-2021.pdf

122 Interview with Oxen Privacy Tech Foundation (OPTF), 2022.

123 Hassan, Anaobi Ishaku, Aravindh Raman, Ignacio Castro, Haris Bin Zia, Emiliano De Cristofaro, Nishanth Sastry, and Gareth Tyson. 'Exploring Content Moderation in the Decentralized Web: The Pleroma Case', 2021, 8.

Policy Section

This policy section has been written by Inga Kristina Trauthig and Amarnath Amarasingam, Senior Research Fellow, at the International Centre for the Study of Radicalisation (ICSR) at King's College London. It provides policy recommendations and is produced independently. Recommendations do not necessarily represent the views of the report authors.

The key findings of this report carry corresponding policy implications for technology companies as this report provides empirical analysis on extremist actors using decentralised services and platforms, including broader assessments of the viability and usefulness of the DWeb for individual and group actors. Governments around the world are well aware that terrorists have been able to exploit various technologies in order to increase their reach, with such steps increasing their threat potential. Technology companies regularly face new forms of exploitation of their services by extremist actors. Therefore, DWeb proponents would be well-advised to follow and react to extremist actors relying on DWeb technologies and affordances. The following section seeks to achieve a threefold aim: first, to deliver concrete policy recommendations for governmental stakeholders; second, to outline policy options and strategic foresight for technology companies; and, finally, in hand with [1] and [2], to serve as a reference point for a future evaluation of tech policies in order to assess dos and don'ts of technology legislation.

With this, the policy section ensures that the Global Network on Extremism and Technology (GNET), the academic research arm of the Global Internet Forum to Counter Terrorism (GIFCT), is academically advising and supporting technology companies and policymakers on how to better understand the ways in which terrorists are using information technology. This is designed to fulfil not only GIFCT's pillar of learning, but ultimately to improve prevention and responses to terrorist and violent extremist attacks.

1. Focus: Policymakers

The outlined dynamics that underlie the development of (more) DWeb technologies and services are overwhelmingly driven by notions of disruption and speediness. In other words, two characteristics that are fundamentally different to how policy and law-making work. How can policy makers who are interested in fostering a healthy Internet and not stifling innovative progress react to DWeb developments? This report has raised three main areas of concern: first, implications for existing and future content moderation; second, existing and potential future oligarchic tendencies due to the tech knowledge often necessary to operate the DWeb; and third, the ethos cultivated by DWeb proponents that governments and Web 2.0 companies are hindrances to a better future. These are relevant points that should be addressed and factored in by governmental stakeholders in charge of keeping their societies safe. In addition, national politicians and international

and regional policymakers, especially security policymakers and stakeholders working on counterterrorism policies, could take note and consider incorporating the results of this analysis when discussing future threat potentials and how to counter them.

- To start with, a centralised web makes it at least easier for governments to push large corporations to comply with regulations. In a decentralised web, this chain of command is more difficult, and it would be even more unclear which country's laws applied to a particular platform or service since it is likely that the content is hosted in various parts of the world. This point emphasises the necessity of dialogue between policy makers and the DWeb community. Some regulations that have been vital with regard to the Web 2.0 might not be necessary anymore on the same scale due to the difference in operations in the DWeb; instead of trying to replicate regulations that guide content moderation on Web 2.0 social media platforms, for instance, governments would be well-advised to employ significant resources to understand the DWeb before regulating it.

- However, there is a caveat that was also uncovered in this report, and which should be taken into account by government stakeholders when assessing if these additional resources are worth it: the question around the viability, and ultimately, the success of a DWeb. The analysis has shown that with regard to extremist actors, DWeb services have grown important but terrorist threats that endanger societies are unlikely to rely heavily on the DWeb. Terrorists have been known to be adaptive but also to rely on platforms due to convenience rather than just security levels. Therefore, it is likely that also in the future traces of extremist content and terrorist planning will (still) be spread on more mainstream social media platforms. Given existing monitoring regimes (by Europol, for example) and regulations around takedown of terrorist content with regard to Web 2.0 platforms, policy makers would be well-advised to focus on these – while nonetheless watching DWeb developments.

- Most important for policy makers is to keep abreast of developments because law, with all its faults, is still more or less the most effective way for preventing people and corporations from going rogue. When interacting with stakeholders in the DWeb community, law makers could be confident enough that government is not (another) problem DWeb developers need to circumvent as it is another institution which demands trust without earning it. While keeping pace, Western law makers are well-advised not to become distracted by specific but less impactful questions such as what defines 'legal but harmful' content exactly, but instead could be much more ambitious in considering how to apply existing laws about criminal conduct online more effectively. For this, the need clear demarcations, such as enforcing that designated terrorist organisations cannot register their own domain names or generally undertaking regular reviews of terrorist designations to accommodate an evolving threat landscape. Those actions would improve more stringent but also adaptable policies with regard to extremism online.

2. Focus: Technology Companies

In addition to the report findings and their implications for political stakeholders, the analysis is also relevant for technology companies aiming to rein in the exploitation of their platforms for malevolent purposes, including emergent technologies.

- The main policy implication of this report is the need for technology companies to co-operate towards terrorist exploitation of existing and newly emerging technologies and platforms. The tech backlash is prevalent in 2022 and Web 2.0 social media companies would be well-advised to open up about past mistakes and engage with developers of DWeb platforms about lessons learned. This co-operation is particularly relevant as arguably also actors like Meta are still learning as the social and legal norms around online speech are complex and evolving. If societies are supposed to benefit from technologies, small and big tech companies could adopt a sense of humility.

- This report has outlined that extremist actors are unlikely to abandon big players such as Meta or Telegram anytime soon. Therefore, those companies are well-advised to stay vigilant and pass on information to DWeb services and platforms if they can follow significant redirection – or potentially even alarm law enforcement if extremist entities direct largely to their own websites, for example.

- Finally, one of the biggest concerns is around trust and safety in the DWeb. One insight this report has provided is that with regard to content moderation the DWeb actually faces two simultaneous but paradoxical challenges: no established, existing content moderation regime, on the one hand, but existing studies show the overreliance on takedowns on DWeb platforms, such as Pleroma, on the other. DWeb services and platforms would be well-advised to apply certain principles that Web 2.0 platforms are still catching up with, such as notice, transparency, due process, the availability of multiple venues for expression, and robust competition as well as the increased agency of users to structure their own experience as much as possible. Whether a decentralised community can moderate content seems to depend on the nature of the community; in other words, communities that are focused around a specific purpose, where members sign up because they believe or support that purpose, self-moderation seems achievable. However, if a community is open to a range of users with a range of agendas, then community-based moderation will become more difficult.[124]

124 For DWeb platforms that carry out moderation in a similar fashion to Pleroma (e.g. Mastodon), some concrete recommendations would be: (1) New generic policies could be designed that rely on a trusted/curated list of well-known instances in the fediverse that may need to be blocked. Thus, an administrator could simply select the relevant lists (which would need to be regularly updated by experts who ensure that the instances have limited collateral damage); (2) New user-driven policies could be designed that enable administrators to moderate on a per-user basis.

3. Focus: Strategic Foresight and Broader Implications

In addition to the policy recommendations derived directly from this report, broader implications and strategic deliberations are also evident from this study of how extremists already are but also could exploit the DWeb in the future.

- In general, the DWeb follows in the policy footsteps of end-to-end encryption as these technologies blatantly show us the double-edged sword of technological features. For counterterrorism, there is both good and bad news related to this. The good news is that terrorists have never and likely will never just rely on one platform, which means they are (still) easier to trace than when those malevolent actors solely rely on DWeb services. The bad news is this situation requires better understanding among analysts at any given platform about what happens at another platform in order to conduct a better threat assessment. One big-picture question is whether, given these relentless technological innovations, the approach should shift from prevention to accountability. In other words, terrorist groups would be prosecuted for their crimes via a justice system that relies less on surveillance of the masses and foregoes attempting to prevent them from using internet technologies at all. If groups exploit technologies, mitigation efforts should focus on co-operation.

- Finally, Rebecca MacKinnon outlines five principles that DWeb companies would be well-advised to keep in mind if they did not want to repeat mistakes from the past: (1) Recognise that if you think you are neutral, you are not; (2) Work to understand what it really means for your business to make a meaningful commitment to respect and protect data integrity and human rights; (3) Be proactive in identifying potential human rights risks; (4) Consider the impact of business models and corporate incentives; (5) Therefore, establish effective impact assessment, stakeholder feedback, participation, and grievance mechanisms from the beginning.

Global Network
on Extremism & Technology

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.