A Storm on the Horizon? 'Twister' and the Implications of the Blockchain and Peer-to-Peer Social Networks for Online Violent Extremism

Gareth Mott

Department of Politics and International Relations, Nottingham Trent University, Nottingham, UK

Abstract

'Twister, developed by Miguel Freitas, is a social network platform centred around micro-blogging, much like Twitter. However, rather than relying on centralised servers owned and maintained by a single firm, Twister users operate a blockchain combined with DHT-like and BitTorrent-like protocols to both make posts and send private messages, and also to receive entries from other users. Twister's raison d'etre is that it offers a social networking platform that cannot be censored and cannot itself censor. The software does not record the IP addresses users use to access the service, nor does it notify other users of an account's online/offline status. Growing adoption of blockchain services means that it is possible that the concept of decentralised social networks could become a norm. It is suggested in this paper that blockchain-based peer-to-peer social networks present challenges to the current counter-extremist practices for content removal and censorship. Whilst there are methods to disrupt usage of blockchain-based peer-to-peer services, these approaches may have the net harm of curtailing bona fide use legal and novel technologies. Given this opportunity cost, non-transitory online violent extremist content may need to be tolerated.

Whilst the online social media landscape is today dominated by technology giants, such as Facebook with its roughly 1.94 billion monthly users,[i] this does not necessitate that the centralised, advertising revenue model of social networking will remain the norm. This centralised architecture, in which a service is offered in exchange for valuable data, is not the only viable means for social interaction and virtual community building mediated via the internet. A social media space does not need to be hosted at a centralised web domain. The world-wide-web *is* already decentralised; indeed, decentralisation and resilience are core tenets of the web's raison d'etre. If the contemporary web can be described as 'centralised', this is socially-constructed, rather than preordained.

Using Miguel Freitas's novel micro-blogging social network 'Twister' as a case study, this article considers the challenges that are presented by peer-to-peer blockchain-based social networks to the counter-extremism practice of content removal. The article is divided into four sections. The first section draws from the existing literature on violent extremist usage of social media to highlight: the extent to which violent extremists are deemed to be interested in using social media generally; the effectiveness of counter-extremist measures

CONTACT Gareth Mott gareth.mott@ntu.ac.uk Department of Politics and International Relations, Nottingham Trent University

against this usage; and the propensity of violent extremists to migrate to social media services where such counter-extremist measures become more difficult. The second section details the unique aspects of Twister's methods for user registration and content dissemination. The third section examines the utility of peer-to-peer, blockchain-based microblogging for violent extremists. Lastly, the fourth section considers viable means by which state-based authorities could attempt to mitigate violent extremist activity on such networks, and suggests that a transition from content *removal* to content *contention* may be necessary.

Violent Extremism and Social Media: Existing Literature

A considerable literature exploring the utility of web communication, particularly social media, platforms for violent extremists already exists. However, this is a developing field and research gaps are present. In particular, as Conway has identified, there has been a general focus on particular online violent extremist content, but "not its producers or consumers, *distribution mechanisms*, or its functioning and effects".[ii] Similar sentiment had been expressed by Zelin, who argued that research on the 'conduits' through which violent extremist material is disseminated has been insufficient.[iii] It is in this context that this article is written. It is useful, it is argued herein, to consider the utility of peer-to-peer, blockchain-based social networks for violent extremists because violent extremists have expressed interest in alternative social media. It is also useful to consider the means by which other users of alternative social media and counter-extremist agencies could mitigate the use of such an online communication platform for violent extremist purposes.

It is suggested in this article that Twister is a novel platform for creating virtual communities and disseminating content because of the challenge of censoring material hosted on it. Nevertheless, from a violent extremist perspective, Twister as a micro-blogging service shares some limitations of online communication platforms more broadly. As Burke

suggests, social media can be used to facilitate propaganda dissemination and can provoke people to offer financial support, but it will not kinetically alter on-the-ground power relations in a given violent conflict.[iv] Power exhibited amongst a given online virtual community does not, by default, automatically translate to 'real' power.[v] It is also worth recognising that access to the internet and social media services is not universal. In some cases, not only violent extremists but general populations may be prohibited from accessing social media because of restrictive local laws, the absence of affordable internet service provision, or indeed a dearth of reliable electricity.[vi]

Nonetheless, violent extremists are unlikely to use social media arbitrarily. It has been suggested elsewhere that violent extremists use internet-mediated virtual communities for the planning of terrorist attacks,[vii] for recruiting personnel,[viii] establishing the possibility of a leaderless organisation[ix] and for teaching recruits in 'virtual classrooms'.[x] Social media could be said to have lowered the cost of participating in violent extremist and terrorist activity,[xi] even if cases of self-recruitment as a result of purely online content consumption could be considered rare.[xii] At the very least, for a violent extremist, the acquisition of online 'followers' and the receipt of supportive messages from them is likely to provide a sense of political or ideological validation that, under certain circumstances, may be less forthcoming in their immediate 'real world' circles.[xiii] With text-based online mediums composed of information rather than matter, distinctions of identity and imbalances of power are "deferred, if not effaced"; as Peter Steiner captured in his New Yorker cartoon, on the internet, nobody knows you're a dog.[xiv]

Whilst violent extremist individuals and groups have precedent in maintaining web presences through the use of dedicated basic hypertext markup language (HTML) websites and forums, today such groups may span several networks and social media platforms.[xv] In 2016, Europol's Internet Referral Unit noted that they had identified in excess of 70 platforms used by terrorist organisations to spread propaganda materials.[xvi] Separate two-day joint Europol operations in 2017 identified violent extremist content disseminated across 41 and

52 platforms respectively.[xvii] In 2018, the UK's Home Office revealed that Islamic State supporters had been found to use in excess of 400 online platforms during 2017.[xviii] These findings would suggest that the dissemination of violent extremist online material relies on an increasingly diverse ecosystem. The hosting of a dedicated website or forum posed some drawbacks. For instance, even prior to the Snowden revelations in 2012, it is known that violent extremists were aware that their online spaces were likely to be monitored and they conditioned their own behaviour on this basis.[xix] Users of some dedicated forums were warned against posting sensitive information on how to travel to a conflict zone, or construct an explosive, unless this was considered to already exist in the public domain.[xx] Forcible seizure of a server by law enforcement can reveal not only the content of forum messages and blog posts, but also private messages between users. It has been noted elsewhere that for violent extremists, the maintenance of a stable, persistent web presence has proven challenging.[xxi]

For the violent extremist, outsourcing their web presence to popular social media platforms does not guarantee a persistent online presence. Research in this field has, for example, shown that violent extremist accounts on Twitter have become increasingly transitory. When Berger and Morgan analysed 20,000 Islamic State-supporting Twitter accounts in the period September 2014 to January 2015, they found that just 3.4 percent of these accounts were suspended over the five months.[xxii] Conversely, Conway et al's *Disrupting Daesh* report analysing Islamic State-supporting accounts and broader Jihad-supporting accounts operational on Twitter between 1 February and 7 April 2017 highlighted that Twitter's anti-extremist operations had gained significant traction since 2014, with conservatively 65 percent of Islamic State-supporting accounts suspended during this period.[xxiii] The authors noted that by April 2017, Islamic State-supporting Twitter accounts had increasingly adopted meaningless usernames of jumbled letters and numbers, and either left their avatars as the default 'egg' or uploaded a benign image.[xxiv] Conway et al proposed that Islamic State supporters were likely to be migrating their operations to

Telegram, given that “a conscious, supportive and influential virtual community” had become “almost impossible to maintain”[xxv] on Twitter. Far-right extreme groups have also experienced censorship and account suspension on Twitter’s services, following changes to the Twitter User Agreement which came into force on 18 December 2017.[xxvi]

It is in this context – a hardening social media environment for the outspoken violent extremist – that this article is written. Telegram, an encrypted communication program released in 2013 for smartphones and computers is, of course, not the only alternative to the dominant communication platforms that has attracted interest from violent extremists. One notable alternative social media platform is Diaspora, which launched in 2010. Diaspora is a distributed social networking service that allows users to establish their own ‘pods’, which can either be public or closed. Control of the content hosted on a given pod is governed by the owner of the server, known as the ‘podmin’. In August 2014, it was reported on the Diaspora blog that an unspecified number of Islamic State-supporting accounts had been established on the main Diaspora pod, ‘JoinDiaspora.com’, as well as other pods on the Diaspora network.[xxvii] From the perspective of the violent extremist, however, Diaspora inherits limitations shared by the more prominent mainstream centralised social media networks. The ‘podmin’ of a Diaspora server has read and write privileges over unencrypted data of the users on their pod. Whilst this issue may be partially assuaged in the case of a closed Diaspora pod operated by an individual empathetic to a given violent extremist cause, it remains that their server is a fixed and vulnerable point of attack or seizure by law enforcement. Furthermore, the continued and uninterrupted operation of a given pod relies upon the continual operation of the podmin’s server. Bielenberg et al ‘crawled’ the Diaspora network between June and November 2011, and found that over 35 percent of the servers that they pinged were never online across the period of 150 days, half of the servers had less than 50 percent uptime, and only the top 20 percent of servers were able to maintain an uptime in excess of 90 percent.[xxviii] A hypothetical pod that is amenable to a violent extremist presence may not be able to foster a vibrant virtual community if it is not able to sustain a

persistent uptime. Were a given pod to unexpectedly go offline, users might assume that the server had been seized by law enforcement and may therefore not entrust it with their proscribed communications if it were to return online.

Diaspora and Twister are two alternative social media networks amongst many. Sharing similarities with Diaspora, Mastodon[xxix] is a 'federated' social media microblogging network. Scuttlebutt is a social network that uses a Bitcoin-like blockchain to register users similarly to Twister's model.[xxx]

Twister – or a similar alternative – may offer a partial fix for this inherent trade-off of privacy, trust, and persistence that violent extremists engage with in order to sustain online virtual communities. Twister's implementation consciously adopted the micro-blogging format that has made Twitter a popular 'universalised'[xxxi] form of online communication. Unlike Diaspora, however, Twister's network is not compartmentalised into independently-run servers. Instead, each Twister user operates a 'node' that helps to ensure the continued persistence of the network. Twister offers an encrypted platform for the construction of virtual communities with no single point of attack. The next section describes the technologies that have made a peer-to-peer, blockchain-based social network possible and have given rise to potential virtual communities built upon what can be termed 'trustless trust'.

Twister, BitTorrent and the Blockchain

One of the core technologies that enables Twister to function as a fully decentralised, continually operational social network is the 'blockchain'. Whilst Twister's blockchain is patched and unique to the social network, other blockchains exist. Indeed, amongst other uses, blockchains can be used to share data between health providers and indefinitely store contracts and land registries.[xxxii] However, the seminal utility of the blockchain was demonstrated by Bitcoin. In October 2008, someone – or several persons – using the pseudonym 'Satoshi Nakamoto' posted a white paper to the Cryptography Mailing list. This

white paper detailed the outline of a digital currency called 'Bitcoin'.[xxxiii] 'Bitcoin', which is essentially a computer program, serves two core functions: firstly, it is an electronic commodity, and secondly, it is an open source protocol for pseudo-anonymous trading. Whilst other digital currencies have existed, it was the blockchain that made Bitcoin unique. Bitcoin's blockchain is a distributed public ledger of all transactions that have ever occurred via the Bitcoin protocol. Bitcoins are not printed or distributed by a central bank in the same way that fiat currencies are produced; instead, a computer algorithm ensures that new Bitcoins are created roughly every ten minutes. 'Miners' compete for these freshly minted Bitcoins with their computing power, by directing their machines to multiply large numbers in the search for a unique 'hash'.[xxxiv] These miners serve two core functions for the Bitcoin protocol; firstly, their mining power serves to secure the existence of the network, and secondly, each successful 'hash' that they find creates a new 'block' on the blockchain. Each new block incorporates transactions that Bitcoin users are attempting to make, and once a transaction is included into a block and disseminated across the Bitcoin network it is considered 'confirmed'.

Initially, miners were rewarded with 50 Bitcoins for each block that they successfully generated; however, over time, this reward 'halves', until eventually, in around the year 2140, the finite limit of 21 million mined Bitcoins will have been reached and no more can be generated.[xxxv] Miners are currently rewarded with 12 Bitcoins, and the next 'halving' is set to occur in 2020. Given that, at the time of writing, a Bitcoin trades for around $15,283,[xxxvi] there is a substantial motivation for Bitcoin miners to out-compete their competitors. The extent of this mining competition, which substantially secures the network, is relatively exceptional. As will be detailed later, the incentive to mine the Twister network is exponentially lower. During the outset of Bitcoin's introduction, when a Bitcoin would have been worth fractions of a cent, it was possible to successfully mine blocks with the CPU of a domestic laptop or desktop computer. Competition for reward Bitcoins produced an arms race of computing power however, which caused miners to begin using graphics cards for

their mining operations, until these were replaced by purpose-built 'ASICs',[xxxvii] industrial computers whose sole purpose is to churn out as many hash calculations as their silicon permits. Today it is impossible to profitably mine Bitcoins with a non-ASIC machine. The mining 'difficulty'[xxxviii] has to increase to match the computing power of the network, so that the roughly ten minute rate of block generation can be maintained. In February 2018, the hash rate of the entire network is in excess of 21.5 trillion GH/s; in the same month the year before, it was just over 3.1 trillion GH/s.[xxxix] Concentrated in regions that offer low ambient temperatures and inexpensive electricity – notably mountainous China[xl] and Chelan County in Washington state, USA[xli] – the electricity demanded by global computing power underpinning the Bitcoin network is said to exceed the energy consumption of Nigeria or the Republic of Ireland.[xlii] The computational power underpinning the Twister network is exponentially lower.[xliii] As will be discussed later with reference to two mining experiments conducted by this author, the low difficulty democratises the ability to benefit from Twister's mining reward implementation, but also makes Twister's blockchain theoretically easier to corrupt.

Twister is a social network developed by Miguel Freitas and released in 2014. It is currently at the 'beta' stage of live development, but is freely available to download, compile and use.[xliv] Twister is a microblogging platform that shares similarities with the model offered by Twitter; users can upload character-limited posts for other users to view, 'follow' other users, read their posts and send direct messages between themselves. However, rather than relying on centralised servers to record user activity and disseminate content, Twister is novel in that it uses the Blockchain, Kademlia-like DHT and BitTorrent-like protocols to connect users and distribute data between them. A DHT is a decentralised distribution system that provides a lookup service between nodes; in this case each Twister user represents a unique node. The BitTorrent protocol facilitates a peer-to-peer network for disseminating computer files, including but not limited to: music, films, software and 3D printing designs.[xlv] Computer scientists had, for some time, sought to implement bona fide

peer-to-peer networks.[xlvi] However, overcoming the challenges of data storage and user authentication had proven challenging. Three years into its lifespan, the Twister network is purportedly comprised 1,819,510 posts, or 'twists'.[xlvii]

In order to function as a virtual community in which posts are tied to specific accounts, a social network has to record a given identity for its users. This serves two purposes. Firstly, if a user has registered a particular username, they do not have to register a unique identity each time that they access the service or post content. Secondly, registering a given username prevents other users from using the same identity and falsely posting content under the guise of another user. Rather than registering usernames to a central database, the Twister network uses its own blockchain to keep the records. Accordingly, when a user installs the software onto their computer and has downloaded the full copy of the blockchain, they can input a username that they would like to use, which their 'node' will check against the blockchain. If the username is available, the name is broadcast to other nodes on the Twister network, and the user waits until the name is included in a 'block'. A private encryption key is generated and stored on the user's hard drive; this private key provides the user access to their account in much the same way that a Bitcoin user retains access to their wallet addresses. The private key can be copied by the user and used on other devices to access the same account. Once the username is included into a block, this block is disseminated across the network and other nodes will become aware of the account's existence. Unlike Bitcoin, there is no direct financial incentive for miners to expend electricity and computational power to generate blocks. However, miners on the Twister network are rewarded by entering a lottery for free advertising. These free adverts are disseminated to all nodes, although a user should only encounter one such advert in any given 24 hour period.

The Twister network blockchain would be an inefficient means of distributing post content. Were the blockchain used as the content database, all users would have to indiscriminately download a potentially very large blockchain, irrespective of whether they

were interested posts' content. Using the blockchain for content dissemination would also be unsatisfactory for users who wish to post and access content instantaneously, given that posts would need to wait for a new block to be generated before being accepted by the network. Instead, Kademlia-like DHT and BitTorrent-like protocols are used; when a user sends a request to view a given user's feed, the content should be received almost instantly. There is some precedent for violent extremist usage of the BitTorrent protocol. Violent extremists have used the BitTorrent protocol to access and disseminate extremist material, ideological documents, and guidance manuals for bomb-making.[xlviii] It is also worth noting that micro-blogging is not the only utility that is made possible through the combination of blockchain and BitTorrent technology. 'Zeronet' is a peer-to-peer, blockchain-based network for the hosting of static and dynamic websites.[xlix] Instead of associating a website with a given IP address, websites that are hosted on the Zeronet network are associated with public addresses listed on the blockchain; much like the public-facing addresses of a Bitcoin wallet. So long as at least one computer is 'seeding' a given Zeronet webpage, other users will be able to access it. In theory, Zeronet offers the possibility of technical resilience against traditional means of pressure for content removal, such as DMCA takedown notices. Samata Ullah – jailed in the UK in May 2017 on five terrorism offences including membership of Islamic State and the preparation of terrorist acts – had admitted researching Zeronet and had authored a blog hosted on the network.[l]

Miguel Freitas, Twister's creator, has noted in interviews that whilst he is fond of Twitter and actively uses its services,[li] he became concerned that its utility for quickly disseminating information during a potential future Brazilian riot could be reduced if the Brazilian state or Twitter itself decided that it would be expedient to shut down the free flow of information. Freitas expressed similar alarm about the British government's rhetoric regarding internet communication freedom amidst the 2011 London riots.[lii] For Freitas, the notion of curtailing information flows was "totally against the idea of the internet, where you are supposed to have no single point of failure".[liii]

Twister is a technical solution to resist blocking and censorship of online content and communications. The technical novelty of a blockchain-based peer-to-peer network proffers some legal considerations. Because it does not rely on central hosting by a unitary entity, there is no single figure or organisation for authorities to pursue for content removal. Twister's source code is released and distributed under a MIT/BSD license.[liv] This, the creator has suggested, protects Twister "from most, if not all legal procedures meant to shut it down".[lv] The source code could not be made illegal, and even if legal action were to be pursued against the network's creator, the network would continue to function as a court could not successfully enforce its shutdown. Enforcing legal measures against open-source peer-to-peer blockchain technology in general may be impracticable, whether the blockchain is for the Twister, Zeronet, Bitcoin, Ethereum, Litecoin or indeed other network. In order for there to be potential for successful enforcement against a disseminated blockchain, 'joint liability' would need to be introduced and imposed.[lvi] As Low and Teo point out however, such enforcement would be highly impractical, because copies of a given blockchain are likely to be held across multiple jurisdictions, and users cannot be obligated to update their copy to a particular version.[lvii] As has been demonstrated by the experience of the Ethereum cryptocurrency, two or more communities operating nodes on a blockchain can use differing code to force a 'hard fork'.[lviii] However, a hard fork on a given network does not overwrite an original blockchain with a new one; the new and old blockchains can continue operating independently with separate communities of nodes adhering to different code.

The Twister network does not have a central administrator who can delete user accounts or suspend their ability to make posts, send private messages and commit computational power to compete for advertising. Furthermore, unlike Twitter and Facebook, Twister does not apply an algorithm to filter the content that users see; content is delivered to nodes instantaneously, as-is. Whilst filtering could be implemented, this would be a local filter, configured by a user on their personal node, much like a spam filter on a POP3/IMAP email client.[lix] As a social network, Twister is novel because users are not obligated to trust a

third party in the same way that they would when using Twitter, Facebook, or a federated service such as Diaspora. Trust is a central component of successful human interaction in a contemporary society;[lx] as human beings, we are able to trust other people on the basis of what we know about them, our family ties to them and information garnered about a given person from other sources that we trust, but this kind of trust is limited. If an inter-subjectively valued 'radius of trust' does not exist, every social interaction descends into a prisoner's dilemma. In order for the 'radius of trust' to expand sufficiently to nurture a functional society, a 'trust architecture' needs to exist.[lxi] Werbach argued that until the invention of the blockchain, "there were two primary trust architectures: Leviathan (deference to a central enforcement authority) and peer-to-peer (reliance on social norms and other governance mechanisms in tight-knit communities)".[lxii]

Werbach suggested that 'trustless trust' – epitomised in software form by the blockchain – made it "possible to trust the outputs of a system without trusting any actor within it".[lxiii] Granted, the code underpinning the Twister network's blockchain is subjectively rather than objectively written given that human beings authored it. However, because the source code is open source, anyone with the requisite knowledge can review the code, make alterations and submit them to peer-review, which diminishes – although does not eradicate – the perceived risks of trusting the network's development community.

It is this condition of 'trustless trust' that presents the potential utility of peer-to-peer blockchain-based social networking to political dissidents and violent extremists alike. Similarly, it is the condition of 'trustless trust' that may force a rethink of current counter-extremism efforts that rely on the cooperation of a 'trusted' figure such as a central administrator or domain owner.

A Storm on the Horizon? The Utility of Blockchain-based Social Networks for Violent Extremists

As has been noted above, Twister's current content base is small.[lxiv] Assessing whether any of these posts relate to violent extremist content is difficult. A researcher interested in combing through Twitter user data can do so either through Twitter's search function, or by requesting data from the API. Twister, conversely, does not have this user-friendly functionality. Twister's 'search' bar provides a user limited search functionality to find user names registered to the blockchain, but one cannot search for post content. *TwisterIO.com* and *Twistnik.ru* are advertised as search engines for the Twister network, but at the time of writing, they appear to have limited functionality. In theory, clicking on another user's name will instantly display their posts, in date order. However, not all posts will necessarily be immediately accessible, particularly if they are older posts. On-demand retrieval of historical post content relies on a computer already in possession of the content that can 'seed' it on request via the BitTorrent protocol. This article has *not* been written on the basis of concrete evidence pointing to the existence of violent extremist virtual communities on the Twister network. Nevertheless, given that violent extremists have expressed interest in alternative social media, it is useful to consider the utility of a peer-to-peer, blockchain-based social network for the violent extremist. Similarly, it is useful to consider the means by which other users of alternative social media and counter-extremist agencies could mitigate the use of such an online communication platform for violent extremist purposes.

As discussed above, online communication platforms have offered a degree of utility for violent extremists who wish to disseminate propaganda material relatively quickly and inexpensively. Benson has noted that internet-mediated communication has allowed violent extremists the attractive prospect of dividing their 'operational' wing from their 'propaganda' wing.[lxv] The 'operational' wing can be afforded the anonymity that may be necessary to carry out successful on-the-ground maneuvers, whilst the online platforms empower the 'propaganda' wing which can disseminate material without even having any tangible contact with their kinetically violent counterparts. This broad division structures the ensuing discussion. It is suggested here that a peer-to-peer, blockchain-based microblogging

platform could be useful for both the ‘propaganda’ and ‘operational’ components of violent extremist activity.

For an ‘operational’ community of violent extremists, there is one core utility that Twister could prove useful for. This is Twister’s direct messaging function, which could serve as an alternative to the popular ‘Bitmessage’ service, an encrypted peer-to-peer communication service that violent extremists have been encouraged to use.[lxvi] A violent extremist could create a seemingly innocuous Twister account, using a randomised combination of letters and numbers, and pass this to their peers. These associates, who could have similar accounts, would then be able to ‘follow’ this account, which they can elect to do publicly or privately. Once two accounts are following one another, they are able to send and receive direct messages between themselves. Users can also create ‘groups’ for group messaging. The end-to-end encrypted message will not be visible to any user other than the intended recipient. Direct messages between Twister users are not ‘stored’ or retrospectively viewable in plaintext in the same way that a Twitter direct message, or a conventional email might be. The only means by which a direct message can be accessed is to be in possession of the private key to the sending or recipient account. Additional security may be offered if the users are connecting to the network through a VPN and storing their private keys on a discrete or hidden removable storage device. The extremist could zero-out the removable storage device and smash it apart, or re-use it to store new keys. In principle, this could make the direct messaging service of a peer-to-peer, blockchain-based microblogging platform a feasible means of communicating instantly across long distances, with a degree of plausible deniability. Given that the only direct cost to a user who uses their node to broadcast a request for a new account is the time expended waiting for the name to be included in the next mined block, ‘operational’ violent extremists could discard accounts much like they may discard inexpensive ‘burner’ mobile phones. The tangible cost of creating new accounts – the mining of the requisite block – is shouldered by those voluntarily

choosing to commit computational power to mining and is manifest in their electricity consumption and hardware wear and tear.

A peer-to-peer, blockchain-based microblogging service may also be useful for the 'propaganda' wing of a violent extremist organisation. Propaganda can only serve its purpose if it is seen and digested by an audience. If violent extremist online content – and the user accounts used to upload and re-broadcast the content – are transitory because of active censorship by the host platform, the utility of the content may be limited. Violent extremists would need to play a whack-a-mole game with the administrators and moderators of the host platform. A hosted item of violent extremist content does not necessarily exist in a vacuum. From the perspective of the violent extremist, censorship may be a particular nuisance not just for 'out-links' (links to platforms outside of the host platform), but also for 'in-links' (links within the host platform). Research by Conway et al regarding Islamic State and other Jihadist use of Twitter identified that 14 percent of pro-Islamic State and 7.5 percent of Other Jihadist tweets included an in-link.[lxvii] Such in-linking provides moderators with the ability to map pathways between suspected violent extremist accounts.

A peer-to-peer, blockchain-based microblogging service such as Twister mitigates the necessity for the violent extremist to play the whack-a-mole game in order to maintain a persistent presence. So long as a Twister user retains the private key linked to their public address that registered their account in the blockchain, their free access to their account and their ability to post content is assured. Whilst the overall content base of the Twister network is small, especially vis-a-vis mainstream proprietary social networks, it is possible that a Twister account could serve as a useful violent extremist propaganda resource on several fronts. Firstly, an account could be used as a resilient, non-transitory space for the blogging of updates on the progress of a given violent extremist cause. Particularly of interest for violent extremists who are keen to produce and disseminate video outputs,[lxviii] posts need not necessarily be limited to text. In May 2016, experimental WebTorrent media embedding was introduced to the Twister network, making video and image hosting possible.[lxix]

Secondly, whilst in-linking is not yet implemented in the network, Twister could already provide a service for the archiving of shortened out-links to content elsewhere on the internet.

A third and novel utility draws on Twister's mining-reward implementation. As noted previously, unlike the Bitcoin network which rewards its mining community with the opportunity to win a diminishing supply of freshly-minted Bitcoins, the Twister network rewards its miners with the opportunity to win free advertising. An 'advert' is a single post of 140 characters. When a miner successfully mines a new block to the network's blockchain, a 'promoted' post of their authorship is disseminated and attached – by their choosing – either to their username or to the anonymous 'nobody' tag. Twister users can select a tab on the graphical user interface to specifically view 'promoted' posts in descending chronological order. In addition, miners enter a lottery for 'pushed' advertising, in which there is a chance that their promoted message may be shown to other Twister users on their generic timeline feed.

Because the mining-reward advertising discriminates on the basis of the computational power that a miner commits to calculating hashes, rather than on the content of a promoted message, a violent extremist might find mining to be a useful mechanism for disseminating propaganda. There was an instance on 1 June 2017 when a miner using the anonymous 'nobody' tag successfully mined blocks and was rewarded with five promoted antisemitic messages.[lxx] The next day, a Twister user flagged this to Freitas, who responded publicly with the post "hmmm, I have yet to see these assholes you're talking about. Content filtering, freedom x anonymity x abuse is always a tricky business".[lxxi]

On 18 December 2017, this author committed a desktop computer with a quad-core Intel 5 processor, 8gb of ram and a GeForce GTX 650ti graphics card to mining on the Twister network. This experiment was run to observe the hardware power that a violent extremist might require if they wished to make promoted posts to the network and potentially

benefit from the advertising lottery. The computer mined for four hours, between 1630 and 2030 GMT, when the stated mining 'difficulty' was 0.00355891 and the latest mined block was block 216068. The author set any promoted posts to be distributed under the guise of the anonymous 'nobody' tag, and the text of promoted posts were manually-inputted quotes from the popular television sitcom, Seinfeld. At 1709:20 GMT, the computer had successfully mined its first block, number 216070. Over the four-hour period, the computer was rewarded with a total of eleven promoted Seinfeld quotes. The interface for chronological 'promoted messages' avoids displaying duplicate consecutive promoted messages and the latest identical promoted message subsumes those before it, so the actual number of blocks successfully mined by the computer may be marginally more than eleven. The mining difficulty is set and adjusted by the protocol so that in theory, a new block is added to the blockchain roughly every ten minutes. On paper, over a four-hour period, one would expect that ~24 blocks may be added to the blockchain. In this case, 33 blocks were added to the blockchain over the four-hour period, which is an unexceptional fluctuation. The Intel 5 processor was therefore able to mine at least one-third of the blocks generated during the running of the experiment. It was apparent that blocks were also mined by three people other than the author. On 21 December 2017, the author ran the experiment a second time between 1130 and 1530 GMT, using the same computer. The mining difficulty was the same as it had been during the initial experiment. The latest mined block before the experiment began was 216538. Over the four hours, a total of 32 blocks were added to the blockchain. The computer successfully mined ten of these blocks, the first of which was block 216543 at 1216:14 GMT, and from these the computer was rewarded with seven manually-inputted promoted Seinfeld quotes. During the running of the second experiment, it was apparent that the mining community was slightly more diverse; blocks were mined by five individuals other than the author, three of whom were the same individuals who had successfully mined blocks during the first experiment.

Whilst this data is anecdotal, it does suggest that three years into its lifespan, the computational power underpinning the Twister network's blockchain is small. For comparison, the Bitcoin network's mining operation, with a difficulty of 1,590,896,927,258 on 21 December 2017,[lxxii] would have ignored the computer that the author used for the mining experiments. The Twister network's mining difficulty at the time of the experiments was lower than it had been in June 2017, when the author had initially written this paper for the *Terrorism and Social Media* conference at Swansea University.[lxxiii] The weakness of the computational power underpinning the mining process of the Twister network has implications for the opportunities afforded to both the hypothetical violent extremist and the counter-extremist.

From the perspective of the hypothetical violent extremist, the opportunity is relatively obvious; at the time of writing, with just one unexceptional processor, they could commit computational power to the network and receive a sizeable proportion of the promoted posts afforded to successful miners. Such messages could be disseminated to hundreds or thousands of active users. One use for promoted messages might be to alert potentially like-minded individuals that they could join an extremist community by sending the promoter a private message. Alternatively, given that the Twister network supports hashtags, promoted messages could notify potentially like-minded individuals that they can engage in real-time discussions on extremist matters if they used a particular hashtag. Even if the general user population were not remotely interested in extremist material – and indeed may reject it – the appearance of pushed promoted extremist content could serve as a digital 'graffiti tag', demonstrating a violent extremist's willingness to engage with alternative social media.

Whilst this author does not suggest that a Twister-like platform would *replace* the online platforms currently used by violent extremists, it is apparent that the Twister network may have some utility for a violent extremist's purposes. Particularly because of the censorship-free nature of the network, it has been suggested that violent extremists could be attracted to the possibility of escaping a 'whack-a-mole' operation that they may need to

routinely employ in reaction to moderation activity on proprietary, censored platforms. The next section details approaches that could be used by counter-extremists as part of an operation to mitigate hypothetical violent extremist usage of a peer-to-peer, blockchain-based microblogging platform.

Countering Violent Extremist Usage of Blockchain-based Social Networks

This section considers some approaches that could be undertaken by counter-extremists against peer-to-peer, blockchain-based microblogging platforms. There are some windows of opportunity, which draw on the same opportunities afforded to the hypothetical violent extremist, that are worth considering. It has been remarked by others that technological development is outpacing institutional change and the resources committed to *developing* new technologies exceed those dedicated to *governing* new technologies.[lxxiv] Whilst it may once have been possible to prevent the movement of encrypted technology across borders,[lxxv] today peer-to-peer, encrypted communication services fit with the increasing privatisation and proliferation of consumer-targeted empowering technologies, many of which were once the solely the domain of national defence departments. Such technologies include consumer-oriented drones, 3D printing, driverless cars and cyber-offense toolkits, amongst myriad other technologies. It is in this context that the counter-extremist would approach the task of policing or attempting to exert influence over a peer-to-peer, blockchain-based microblogging platform.

One window of opportunity for the counter-extremist would be to use accounts on the network to post information relating to their endeavor (e.g. promote a link to their anti-extremism website or content). Secondly, whilst violent extremists may be able to use Twister's 'hashtag' functionality, there would be nothing stopping counter-extremists commandeering such hashtags to offer banal or countering narratives.[lxxvi] Thirdly, given that non-direct message posts are publicly viewable, the counter-extremist could identify prolific

'propaganda' accounts and collect associated data for intelligence purposes. The counter-extremist might code a bot specifically for this purpose, which could automatically follow all accounts on the network and download all publicly available posts. Whilst the counter-extremist could not delete these posts nor lobby a central domain owner for their removal, the data could prove useful from open source intelligence (OSINT) and signals intelligence (SIGINT) perspectives.

Just as the mining process does not discriminate against the hypothetical violent extremist, the computational weakness of the mining operation underpinning the Twister network could also present opportunities to counter-extremists. Again, one opportunity is obvious: a counter-extremist could commit some computational power to mining on the network and use any rewarded promoted posts to refute an extremist narrative and provide a shortened out-link to a website or email address for reporting extremist content. This approach would not undermine the network. Alternatively, however, there is the potential to cause disruption against the network itself. This could be achieved by exploiting a vulnerability inherent to decentralised, non-discriminatory peer-to-peer blockchains, which is the risk that they may be undermined by a '51 percent attack'. A '51 percent attack', sometimes known as a 'majority attack', would be a betrayal of the pillar of 'trustless trust' that the blockchain relies upon. In order to conduct a majority attack, a perpetrator would need to modify the code running their 'node'. The attack would be more likely, and sustained, for each percentage point majority that the perpetrator could achieve. The Bitcoin community has expressed concern about the potential of a majority attack, given that in June 2014, the mining pool 'Ghash.io' controlled 51 percent of the hash power on the network.[lxxvii] A successful perpetrator of a majority attack against the Bitcoin network would have the opportunity to reverse recent transactions and double-spend Bitcoins. An attack on the Bitcoin network may be unlikely, because of the profits that a successful attacker would forego as a result of the sabotage.[lxxviii] With the microblogging platform, however, the successful perpetrator of a majority attack could have the opportunity to retrospectively

delete some recently-created accounts, or, perhaps more significantly, prevent new users from creating accounts by intentionally mining empty blocks. However, because the blockchain is used for account registration and not the dissemination of posts, the successful majority attacker could not prevent existing accounts from making public posts or from sending private messages. As a result, it is suggested here that this would be an ineffective counter-extremist measure. The intentional prevention of new account creation would prove irritating to a hypothetical violent extremist looking to join the network, and to those who may wish to replace an existing account with a new 'burner' account, but the net harm of this approach is that *all* potential new users would be prevented from creating accounts. Disgruntled developers would not be structurally prevented from modifying the code and releasing a new version of a peer-to-peer microblogging platform.

Internationally, there appears to be growing official rhetoric regarding the necessity for proprietary mainstream platforms to make greater financial and staffing efforts to prevent their profit-making services from being used for violent extremist purposes.[lxxix] As has been indicated by the literature considered earlier in this article,[lxxx] and by the reports of organisations such as the UK and EU Internet Referral Units,[lxxxi] there is evidence that content removal on such online platforms has gained traction. However, in the future, today may be retrospectively viewed as a 'golden age' for the feasibility of online content removal. As open-source encrypted peer-to-peer technologies become increasingly adopted, the dominance of closed, proprietary online communication platforms that extract advertising revenue from the private data of the individual may not be assured. Within the foreseeable future, counter-extremist organisations such as the UK's Internet Referral Unit may not be afforded the luxury of a central authority that they can pressure for content removal. If a given item of offensive violent extremist content is disseminated through BitTorrent-like protocols on services such as Twister or Zeronet, the content is likely to remain accessible for as long as at least one person is willing to 'seed' the relevant torrent file with their computer. In this sense, whilst certain items of violent extremist content may be proscribed

under the domestic laws of a given jurisdiction, successfully enforcing these laws may not be possible in all cases. With encrypted, fully peer-to-peer hosting, the law of computer code[lxxxii] may override legislated regulation. In an era of decentralised, diffuse technology, 'code is law' can be actioned by both state and non-state agents. Just as 'code is law' enabled, for instance, MI5, MI6 and GCHQ to 'unlawfully' collect the online communication data of British citizens for 17 years,[lxxxiii] the motivated individual – extremist or otherwise – is empowered to make efforts to evade online surveillance and online censorship.

A hypothetical violent extremist could significantly improve the privacy of their seeding operations by connecting to their desired peer-to-peer services through a VPN. However, as has been noted regarding the feasibility of prosecuting music, film and game BitTorrent filesharers,[lxxxiv] even if the perpetrator were to use their true IP address, the evidence collected by monitoring the IP address would tie the activity to a given internet address but not a particular individual. On the basis of IP data alone, a prosecution could not be assured success. A risk of prosecution has not prevented relatively widespread use of BitTorrent services for illicit activity. In 2009, 15 percent of Americans polled by Pew admitted to illicit file-sharing using BitTorrent software.[lxxxv] Research in 2015 by Sandvine found that the overall share of bandwidth in North America used by BitTorrent data had declined due to the increasing popularity of bandwidth-heavy services such as Netflix and Youtube, but BitTorrent traffic still represented 26.83 percent of 'upstream' data, a decline from 36.35 percent two years earlier.[lxxxvi]

Whilst violent extremist content hosted in an encrypted peer-to-peer manner may have the potential to be *technically* resilient, this does not necessarily make it *socially* resilient. The ability to host and access difficult-to-remove violent extremist content through use of encrypted peer-to-peer channels does not mean that the material will be compelling. There is perhaps a risk that fetishising online violent extremist content could artificially manufacture a compelling narrative to the content through overt reactions by law enforcement and policy making communities. Conway has suggested that "there is no yet

proven connection between consumption of and networking around violent extremist online content and adoption of extremist ideology and/or engagement in violent extremism and terrorism".[lxxxvii] Notwithstanding perceived online causality of violent extremism, the notion of 'radicalisation' itself has not been without controversy. In particular, 'radicalisation' as a concept has been criticised for possessing an ambiguous, subjective definition and for lacking empirical data linking causality to violent behaviour.[lxxxviii]

If online extremist content is an ideological 'virus' of sorts[lxxxix] that cannot be eradicated altogether but which may, or may not, have the potential to incite people into committing acts of violence, citizens should be encouraged to develop the effective antibody of a critical mind. When violent extremists elect to use social media to further their agenda – whether the platforms are mainstream or alternative – they give their narrative(s) visibility and open a space for them to be critiqued.[xc] On Twister, for instance, just as with Twitter, Youtube and Facebook, there is nothing structurally preventing non-extremist users from responding to extremist content with satire and ridicule.[xci] When 4chan users reproduced imagery of Islamic State fighters by superimposing rubber ducks and toilet brushes onto them, the bravado of the images was replaced with disarming humour.[xcii] This is, of course, not to promote flippancy or disregard for online material that could be extremely offensive or which could, in some circumstances, provoke individuals to align with a violent cause. However, this author agrees with the suggestion of Bartlett and Krasodomski-Jones; in a context of limited counter-extremist resources, the most worthwhile approach may be to develop users' critical faculties so that ideologies can be rejected and ensure that top-down human resources are best placed to prevent violent behaviour, rather than chase uncomfortable propaganda around the internet.[xciii] The greater the pressure applied to proprietary, mainstream services to enact counter-extremist censorship measures on their services, the faster these platforms will become untenable for sustaining viable violent extremist communities, which will likely encourage them to migrate to services that offer

them technical resilience against disruptive censorship, rather than give up on internet-mediated communication altogether.

Conclusion

Technology and software have empowered individuals to communicate seamlessly across borders either with the assistance of centralised, privately-owned platforms, or without them. 2017 was an exceptional year for the blockchain's most prominent case study, the Bitcoin cryptocurrency, with a surge in public and media interest. According to Google, "How to buy Bitcoin" was the second most-asked 'How to' question of 2017, and "What is Bitcoin" was the fourth most-asked 'What is' question.[xciv] The encrypted peer-to-peer blockchain-based cat is out of the bag.

This article has argued that violent extremists experiencing difficulty maintaining viable, persistent presences on social media platforms may elect to eschew mainstream platforms on which they are increasingly censored, in favour of alternative platforms where they are not. A violent extremist who made a conscious decision to operate a node on the Twister network, for instance, could retain sovereignty over the content that they post and access. It has been suggested that a network such as Twister could offer utility for both 'operational' and 'propaganda-producing' violent extremists. Policing and moderating violent extremist communities on alternative social media platforms is likely to present challenges for counter-extremist organisations such as the UK's Internet Referral Unit, which rely on the cooperation of domain owners and ISPs for content removal. Encryption and internet-mediated communication has significantly bolstered the UK economy,[xcv] which makes disrupting the technologies that enable peer-to-peer blockchain-based online platforms to exist an untenable approach to counter-extremism. It is plausible that counter-extremist practices towards online content may, not through preference but through necessity, need to shift from a focus on content *removal*, to content *contention*.

[i] Jessica Guynn, "Facebook's ad sales machine roars," *USA Today*, last modified 3 May 2017. Available at https://www.usatoday.com/story/tech/news/2017/05/03/facebook-first-quarter-2-billion-users-topped-revenue-estimates/101254122/ (accessed 19 May 2017).

[ii] Maura Conway, "Determining the Role of the Internet in Violent and Extremism and Terrorism: Six Suggestions for Progressing Research," *Studies in Conflict and Terrorism* 40(1) (2017), p. 82, emphasis added.

[iii] Aaron Zelin, *The State of Global Jihad Online: A Qualitative, Quantitative, and Cross-Lingual Analysis* (Washington, DC: New America Foundation, 2013), p.1

[iv] Jason Burke, "Al-Shabab's Tweets won't Boost its Cause," *The Guardian*, last modified 16 December 2011. Available at https://www.theguardian.com/commentisfree/2011/dec/16/al-shabab-tweets-terrorism-twitter (accessed 13 December 2017).

[v] Walter Laqueur, *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (Oxford: Oxford University Press, 1999), p. 262.

[vi] Christina Archetti, "Terrorism, Communication and New Media: Explaining Radicalisation in the Digital Age," *Perspectives on Terrorism* 9(1) (2015), p. 54-55.

[vii] Timothy Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning'," *Parameters: US Army War College* 33(1) (2003), pp. 112-123.

[viii] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington DC: United States Institute of Peace Press, 2006). See also Gabriel Weimann, "Using the Internet for Terrorist Recruiting," in Boaz Ganor, ed., *NATO Security through Science Series: Hypermedia Seduction for Terrorist Recruiting* (Amsterdam: IOS Press, 2007).

[ix] Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century* (Philadelphia: University of Pennsylvania, 2008).

[x] David Cole, "Virtual Terrorism and the Internet E-learning Options," *E-Learning* 4(2) (2007), pp. 116-127.

[xi] Javier Argomaniz, "European Union Responses to Terrorist Use of the Internet," *Cooperation and Conflict* 50(2) (2015), p. 253.

[xii] Anja Dalgaard-Nielsen, "Violent Radicalisation in Europe: What we Know and What we do not Know," *Studies in Conflict and Terrorism* 33(9) (2010), pp. 797-814; Tim Stevens and Peter Neumann, *Countering Online Radicalisation: A Strategy for Action* (London: ICSR, 2009).

[xiii] Lorraine Bowman-Grieve, "Exploring 'Stormfront': A Virtual Community of the Radical Right," *Studies in Conflict and Terrorism* 32(11) (2009), pp. 989-1007; Jerold Post, Kevin Ruby and Eric Shaw, "From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism," *Terrorism and Political Violence* 12(2) (2000), pp. 97-122.

[xiv] Lisa Nakamura, *Cyber Types: Race, Ethnicity, and Identity on the Internet* (New York: Routledge, 2002), p. 35. See also Judith Donath, "Identity and Deception in the Virtual Community," in Peter Kollock and Marc Smith, eds., *Communities in Cyberspace* (London: Routledge, 1999).

[xv] Derek O'Callaghan et al, "Uncovering the Wider Structure of Extreme Right Communities Spanning Popular Online Networks", proceedings of the 2010 International Conference on Advances in Social Networks Analysis and Mining (2010). Available at https://arxiv.org/pdf/1302.1726.pdf (accessed 13 December 2017). See also Stewart Bertram and Keith Ellison, "Sub Saharan African Terrorist Groups' use of the Internet," *Journal of Terrorism Research* 5(1) (2014), pp. 5-26.

[xvi] Europol, *EU Internet Referral Unit: Year One Report Highlights* (The Hague: Europol, 2016), p. 5

[xvii] See Europol, "Europol Coordinates Joint Action Days to Flag Online Terrorist Content," *Europol Newsroom*, last modified 27 February 2017. Available at https://www.europol.europa.eu/newsroom/news/europol-coordinates-joint-action-days-to-flag-online-terrorist-content (accessed 19 December 2017); Europol, "Europol Coordinates EU-wide Hit Against Online Terrorist Propaganda," *Europol Newsroom*, last modified 2 May 2017. Available at https://www.europol.europa.eu/newsroom/news/europol-coordinates-eu-wide-hit-against-online-terrorist-propaganda (accessed 19 December 2017).

[xviii] Home Office, "New technology revealed to help fight terrorist content online", *Gov.uk*, last modified 13 February 2017. Available at https://www.gov.uk/government/news/new-technology-revealed-to-help-fight-terrorist-content-online (accessed 23 February 2018).

[xix] Anne Stenersen, "The Internet: A Virtual Training Camp?," *Terrorism and Political Violence* 20(2) (2008), pp. 215-233.

[xx] Ibid.

[xxi] Manuel Soriano, "The Vulnerabilities of Online Terrorism," *Studies in Conflict and Terrorism* 35(4) (2012), p. 268.

[xxii] J.M. Berger and Jonathan Morgan, *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter* (Washington DC: Brookings, 2015), p. 33.

[xxiii] Maura Conway et al, *Disrupting Daesh: Measuring Takedown of Online Terrorist Material and its Impacts* (Dublin: Vox-Pol, 2017), p. 5.

[xxiv] Ibid., p. 30. Whilst the choice of an avatar may seem banal, users of online communication services develop associations with their avatars and can view them as extensions of themselves. See Edward Castronova, *Synthetic Worlds: The Business and Culture of Online Games* (Chicago: University of Chicago Press, 2005), p. 45. See also William Bainbridge, *The Warcraft Civilisation: Social Science in a Virtual World* (London: MIT Press, 2010), p. 181.

[xxv] Ibid., p. 30. See also Nico Prucha, "IS and the Jihadist Information Highway: Projecting Influence and Religious Identity via Telegram," *Perspectives on Terrorism* 10(6) (2006), pp. 48-58.

[xxvi] See Lorand Bodo, "Account Suspended: Twitter and Extreme Right-wing Groups in the UK," *VOX-Pol*, last modified 20 December 2017. Available at http://www.voxpol.eu/account-suspended-twitter-extreme-right-wing-groups-uk/ (accessed 23 December 2017). See Twitter's rules at Twitter, "The Twitter Rules," https://help.twitter.com/en/rules-and-policies/twitter-rules (accessed 23 December 2017). See also DFRLab, "Alt-Right and Alt-Social Media", *Medium*, last modifed 8 September 2017. Available at https://medium.com/dfrlab/alt-right-and-alt-social-media-4fa23eb2fbd1 (accessed 23 December 2017).

[xxvii] Diaspora Foundation, "Islamic State Fighters on Diaspora," *Diaspora*, last modified 20 August 2014. Available at https://blog.diasporafoundation.org/4-islamic-state-fighters-on-diaspora (accessed on 14 December 2017). See also Samuel Gibbs, "Islamic State moves to other Social Networks after Twitter Clampdown," *The Guardian*, last modified 21 August 2014. Available at https://www.theguardian.com/technology/2014/aug/21/islamic-state-isis-social-media-diaspora-twitter-clampdown (accessed on 14 December 2017); BBC News, "Islamic State shifts to New Platforms after Twitter Block," *BBC News*, last modified 21 August 2014. Available at http://www.bbc.co.uk/news/world-middle-east-28843350 (accessed on 14 December 2017); Sophie Curtis, "Islamic State invades Diaspora Social Network after Twitter Ban," *The Telegraph*, last modified 22 August 2014. Available at http://www.telegraph.co.uk/technology/social-media/11050712/Islamic-State-invades-Diaspora-social-network-after-Twitter-ban.html (accessed on 14 December 2017).

[xxviii] Ames Bielenberg, "The Growth of Diaspora – A Decentralised Online Social Network in the Wild," *IEEE*, last modified 3 May 2012. Available at http://ieeexplore.ieee.org/document/6193476/ (accessed 14 December 2017).

[xxix] Mastodon, https://joinmastodon.org/ (accessed 22 December 2017).

[xxx] Scuttlebutt, https://www.scuttlebutt.nz/ (accessed 22 December 2017).

[xxxi] Colin Koopman, *Genealogy as Critique: Foucault and the Problems of Modernity* (Bloomington: Indiana University Press, 2013), p. 19.

[xxxii] See Udit Sharma, "Blockchain in Healthcare: Patient Benefits and More," *IBM*, last modified 30 October 2017. Available at https://www.ibm.com/blogs/blockchain/2017/10/blockchain-in-healthcare-patient-benefits-and-more/ (accessed 23 December 2017); Frederick Reese, "Land Registry: A Big Blockchain use Case Explored," *Coindesk*, last modified 19 April 2017. Available at https://www.coindesk.com/blockchain-land-registry-solution-seeking-problem/ (accessed 23 December 2017); Coindesk, "How do Ethereum Smart Contracts Work?," https://www.coindesk.com/information/ethereum-smart-contracts-work/ (accessed 23 December 2017).

[xxxiii] 'Satoshi Nakamoto', "Bitcoin: A Peer to Peer Electronic Cash System," *Bitcoin.org*. Available at https://bitcoin.org/bitcoin.pdf (accessed 23 December 2017).

[xxxiv] In essence, this is simply a very long number. The Bitcoin protocol rewards the mining computer which successfully finds the correct number of binary zeros at the beginning of the number.

[xxxv] In theory, the Bitcoin protocol accomodates for the reality that miners are self-interested rather than altruistic. In the absence of a 'reward' of fresh Bitcoins, it is envisaged that miners would still compete for the 'transaction fee' that users set and include with their transaction. When a miner successfully generates a new block, they are able to retain the transaction fees of all the transactions included within that block. As miners will prioritise the transactions with the highest fee, the fee system simultaneously serves to reward miners post-21409 and to discourage 'spam' transactions on the network.

[xxxvi] XE, "XE Currency Converter: XBT to USD," http://www.xe.com/currencyconverter/convert/?Amount=1&From=XBT&To=USD (accessed 23 December 2017).

[xxxvii] An 'application specific integrated circuit'.

[xxxviii] An increase in the mining difficulty increases the number of binary zeros at the beginning of the sought-after hash for a given block generation.

[xxxix] BitcoinWisdom, "Bitcoin Difficulty and Hashrate Chart," https://bitcoinwisdom.com/bitcoin/difficulty (accessed 23 February 2018).

[xl] Simon Denyer, "The Bizarre World of Bitcoin 'Mining' Finds a New Home in Tibet", *The Washington Post*, last modified 12 September 2016. Available at https://www.washingtonpost.com/world/asia_pacific/in-chinas-tibetan-highlands-the-bizarre-world-of-bitcoin-mining-finds-a-new-home/2016/09/12/7729cbea-657e-11e6-b4d8-33e931b5a26d_story.html (accessed 23 December 2017).

[xli] Chelan County, with a population of ~76,000, has three hydroelectric plants on the Columbia River. United States Census Bureau, "Chelan County, Washington," https://www.census.gov/quickfacts/table/PST045215/53007 (accessed on 23 December 2017).

[xlii] Peter Martinez, "Bitcoin Mining Consumes More Energy than 159 Countries," *CBS News*, last modified 27 November 2017. Available at https://www.cbsnews.com/news/bitcoin-mining-energy-consumption/ (accessed on 23 December 2017).

[xliii] Twister Network, 127.0.0.1:28332/network.html (accessed 23 December 2017).

[xliv] Miguel Freitas, "Download", *Twister*, post 24 November 2013. Availablle at http://twister.net.co/?page_id=23 (accessed 23 December 2017).

[xlv] Anna Leach, "The Pirate Bay Torrents Printable 3D Objects," *The Register*, last modified 25 January 2012. Available at https://www.theregister.co.uk/2012/01/25/pirate_bay_3d_printer_files/ (accessed 23 December 2017). See also Anne Lewis, "The Legality of 3D Printing: How Technology is Moving Faster than the Law," *Tulane Journal of Technology and Intellectual Property* 17 (2014), pp. 303-318.

[xlvi] For instance, see Markus Ackermann et al, "Helloworld: An Open Source, Distributed and Secure Social Network," WC3 Workshop on the Future of Social Networking-Position Papers (2008). Available at https://www.w3.org/2008/09/msnws/papers/HelloWorld_paper.pdf (accessed 17 December 2017); David Koll, Jun Li and Xiaoming Fu, "SOUP: An Online Social Network by the People, for the People," *ACM Press* (2014). Available at https://dl.acm.org/citation.cfm?doid=2663165.2663324&preflayout=flat (accessed 17 December 2017), pp.193-204; Alireza Mahdian, "MyZone: A Next-Generation Online Social Network," *arXiv.org* (2011). Available at https://arxiv.org/abs/1110.5371 (accessed 17 December 2017); Robert Gehl, "Alternative Social Media: From Critique to Code," *SSRN* (2015). Available at https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2955827_code2077148.pdf?abstractid=2955827 (accessed 17 December 2017).

[xlvii] Data taken from MaximAL, "Twistnik: About," *Twistnik*, https://twistnik.ru/about (accessed on 23 February 2018).

[xlviii] Paul Gill et al, *What are the Roles of the Internet in Terrorism: Measuring Online Behaviours of Convicted UK Terrorists* (Dublin: Vox-Pol, 2015), p. 21. See also Donald Holbrook, "A Critical Analysis of the Role of the Internet in the Preparation and Planning of Acs of Terrorism," *Dynamics of Asymmetric Conflict* 8(2) (2015), p. 126.

[xlix] For information, FAQs and installation instructions, see "Zeronet." Available at https://zeronet.io/ (accessed 18 December 2017).

[l] The Guardian, "Cardiff Terrorist who hid Extremist Data on Bond-style Cufflink is Jailed," last modified 2 May 2017. Available at https://www.theguardian.com/uk-news/2017/may/02/cardiff-terrorist-extremist-data-bond-style-cufflink-jailed-samata-ullah (accessed 18 December 2017).

[li] Klint Finley, "Out in the Open: An NSA-Proof Twitter, Built with Code from Bitcoin and BitTorrent," *Wired*, last modified 13 January 2014. Available at https://www.wired.com/2014/01/twister/ (accessed 23 December 2017).

[lii] For instance, see Josh Halliday anmd Juliette Garside, "Rioting Leads to Cameron Call for Social Media Clampdown", *The Guardian*, last modified 11 August 2011. Available at https://www.theguardian.com/uk/2011/aug/11/cameron-call-social-media-clampdown (accessed 17 December 2017); Christopher Williams, "Cameron Told not to Shut Down Internet", *The Telegraph*, last modified 1 November 2011. Available at http://www.telegraph.co.uk/technology/news/8862335/Cameron-told-not-to-shut-down-internet.html (accessed 17 December 2017).

[liii] See interview transcript at Robert Gehl, "Building a Better Twitter: A Study of the Twitter Alternatives GNU Social, Quitter, rstat.us, and Twister," *SSRN* (2015). Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2595247 (accessed 17 December 2017), p. 9.

[liv] See Open Source Initiative, "The MIT License." Available at https://opensource.org/licenses/MIT (accessed 17 December 2017).

[lv] Robert Gehl, "Building a Better Twitter: A Study of the Twitter Alternatives GNU Social, Quitter, rstat.us, and Twister." p. 12.

[lvi] See Kelvin Low and Ernie Teo, "Bitcoins and Other Cryptocurrencies as Property?", *Law Innovation and Technology* 9(2) (2017), pp. 235-268.

[lvii] Ibid., p. 264.

[lviii] For an overview of the Ethereum blockchain fork, see Alyssa Hertig, "Ethereum's Two Ethereums Explained," *Coindesk*, last modified 28 July 2017. Available at https://www.coindesk.com/ethereum-classic-explained-blockchain/ (accessed 18 December 2017). The Bitcoin cryptocurrency experienced its own hard fork in August 2017, when 'Bitcoin Cash' split from the 'Bitcoin' network. See Alyssa Hertig, "Bitcoin Cash: Why it's Forking the Blockchain and what that Means," *Coindesk*, last modified 26 July 2017. Available at https://www.coindesk.com/coindesk-explainer-bitcoin-cash-forking-blockchain/ (accessed 18 December 2017).

[lix] See interview transcript as Robert Gehl, "Alternative Social Media: From Critique to Code." p. 10.

[lx] Francis Fukuyama, *Trust: The Social Virtues and the Creation of Prosperity* (New York: Free Press, 1995).

[lxi] Kevin Werbach, "Trust, but Verify: Why the Blockchain needs the Law," *SSRN* (2017). Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2844409 (accessed 23 December 2017), p. 4.

[lxii] Ibid., p. 4-5.

[lxiii] Ibid., p. 4-5.

[lxiv] Data taken from MaximAL, "Twistnik: About."

[lxv] David Benson, "Why the Internet is not Increasing Terrorism," *Security Studies* 23(2) (2014), p. 299.

[lxvi] See 'Amreeki', "Al-Khilafah Aridat The Caliphate has Returned: Remaining Anonymous Online," *Wordpress*, last modified 20 August 2014. Available at https://alkhilafaharidat.wordpress.com/2014/08/20/remaining-anonymous-online/comment-page-1/ (accessed 20 December 2017). See also Jamie Bartlett and Alex Krasodomski-Jones, *Online Anonymity Islamic State and Surveillance* (London: Demos, 2015).

[lxvii] Maura Conway et al, *Disrupting Daesh: Measuring the Takedown of Online Terrorist Material and its Impacts*, p. 33.

[lxviii] Virginie Andre, "The Janus Face of New Media Propaganda: The Case of Patani Neojihadist Youtube Warfare and its Islamophobic Effect on Cyber-Actors," *Islam and Christian-Muslim Relations* 25(3) (2014), pp. 335-356; Imogen Richards, "'Flexible Capital Accumulation in Islamic State Social Media," *Critical Studies on Terrorism* 9(2) (2016), pp. 205-225; James Farwell, "The Media Strategy of ISIS", *Survival* 56(6) (2014), pp. 49-55.

[lxix] See Miguel Freitas, "File Attachment and WebTorrent Support", *Twister News*, post 9 May 2016. Available at http://twister.net.co/?page_id=215 (accessed 22 December 2017).

[lxx] These objectionable messages posted on 1 June 2017 read: "GAS THE KIKES RACE WAR NOW!!!".

[lxxi] See Miguel Freitas '@mfreitas', http://127.0.0.1:28332/home.html#profile?user=mfreitas, post 7 June 2017 (accessed 20 December 2017). [requires Twister to be installed and running].

[lxxii] BitcoinWisdom, "Bitcoin Difficulty and Hashrate Chart," https://bitcoinwisdom.com/bitcoin/difficulty (accessed 21 December 2017).

[lxxiii] Twister Network, 127.0.0.1:28332/network.html (accessed 21 June 2017).

[lxxiv] Ben FitzGerald and Jacqueline Parziale, "As Technology goes Democratic, Nations Lose Military Control," *Bulletin of the Atomic Scientists* 73(2) (2017), p. 106.

[lxxv] See Wystan Ackerman, "Encryption: A 21st Century National Security Dilemma," *International Review of Law, Computers and Technology* 12(2) (1998), pp. 371-394.

[lxxvi] Russian authorities have deployed this strategy in the past against protestors who had been using Twitter. See BBC News, "Russian Twitter Political Protests 'Swamped by Spam'," last modified 8 March 2012. Available at http://www.bbc.co.uk/news/technology-16108876 (accessed 27 December 2017). A similar approach was taken by Mexican authorities, see Klint Finley, "Pro-Government Twitter Bots try to Hush Mexican Activists," *Wired*, last modified 23 August 2015. Available at https://www.wired.com/2015/08/pro-government-twitter-bots-try-hush-mexican-activists/ (accessed 27 December 2017). Similar strategies have been deplpyed in Morocco, Syria, Bahrain, Egypt and Iran. See Jillian York, "Syria's Twitter Spambots," *The Guardian*, 21 April 2011. Available at https://www.theguardian.com/commentisfree/2011/apr/21/syria-twitter-spambots-pro-revolution (accessed 27 December 2017).

[lxxvii] Members of the mining pool withdrew their computing power from the group in order to avoid the majority stake persisting. See Alex Hern, "Bitcoin Currency could have been Destroyed by '51%' Attack," *The Guardian*, last modified 16 June 2014. Available at https://www.theguardian.com/technology/2014/jun/16/bitcoin-currency-destroyed-51-attack-ghash-io (accessed 23 December 2017).

[lxxviii] Frederick Reese, "As Bitcoin Halving Approaches, 51% Attack Question Resurfaces", *Coindesk*, last modified 6 July 2017. Available at https://www.coindesk.com/ahead-bitcoin-halving-51-attack-risks-reappear/ (accessed 23 December 2017).

[lxxix] For instance, see Home Affairs Committee, *Hate Crime: Abuse, Hate and Extremism Online* (London: Prevent Directorate, 2017); Mike Wright, "Facebook 'Reviewing' Britiain First Page after Twitter Suspends Far-right Group's Accounts," *The Telegraph*, last modified 19 December 2017. Available at http://www.telegraph.co.uk/technology/2017/12/19/facebook-reviewing-britain-first-page-twitter-suspends-far-right/ (accessed 23 December 2017); Committee on Oversight and Government Reform House of Representatives, *Radicalization: Social Media and the Rise of Terrorism* (Washington: US Government Publishing Office, 2015); Cara McGoogan, "Germany to Fine Facebook and Youtube €50m if they Fail to Delete Hate Speech," *The Telegraph*, last modified 30 June 2017. Available at http://www.telegraph.co.uk/technology/2017/06/30/germany-fine-facebook-youtube-50m-fail-delete-hate-speech/ (accessed 23 December 2017).

[lxxx] Maura Conway et al, *Disrupting Daesh: Measuring Takedown of Online Terrorist Material and its Impacts*.

[lxxxi] The Counter Terrorism Internet Referral Unit removes more than 1,000 pieces of content from the internet each week. See Gov.uk, "Guidance: Online Radicalisation," last modified 26 November 2015. Available at https://www.gov.uk/government/publications/online-radicalisation/online-radicalisation (accessed 23 December 2017). In 2013, 17.541 items were removed, in 2015, 55,556 items were removed, and in 2016 this figure had reached around 100,000. See Vikram Dodd, "Counter-terrorism Drive for Public to Report Online ISIS Propaganda", *The Guardian*, last modified 14 April 2016. Available at https://www.theguardian.com/uk-news/2016/apr/15/police-launch-crackdown-on-isis-internet-extremism (accessed 23 December 2017). From July 2015, the CTIRU was superceded by the European Internet Referral Unit at the European level. This unit had removed 12,000 pieces of terrorist-related content by October 2016. See Ben Wallace, "Terrorism: Social Media Written Question 48934," *Parliamnet.uk*, answered 2 November 2016. Available at https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2016-10-17/48934/ (accessed 23 December 2017).

[lxxxii] Lawrence Lessig, "Code is Law," *Harvard Magazine*, last modified 1 January 2000. Available at hhttps://harvardmagazine.com/2000/01/code-is-law-html (accessed 22 December 2017). See also Lawrence Lessig, *Code* (New York: Basic Books, 2006), pp. 1-8.

[lxxxiii] Alan Travis, "UK Security Agencies Unlawfully Collected Data for 17 Years, Court Rules", *The Guardian*, last modified 17 October 2016. Available at https://www.theguardian.com/world/2016/oct/17/uk-security-agencies-unlawfully-collected-data-for-decade (accessed 22 December 2017).

[lxxxiv] BBC News, "BitTorrent Study Finds Most File-Sharers are Monitored," last modified 4 September 2012. Available at http://www.bbc.com/news/technology-19474829 (accessed 22 December 2017).

[lxxxv] Mary Madden, "The State of Music Online: Ten Years after Napster," *Pew*, last modified 15 June 2009. Available at http://www.pewinternet.org/2009/06/15/the-state-of-music-online-ten-years-after-napster/#footnote9 (accessed 22 December 2017).

[lxxxvi] Sarah Perez, "Netflix, HBO Streaming Video Traffic Increases as BitTorrent Declines," *TechCrunch*, last modified 28 May 2015. Available at https://techcrunch.com/2015/05/28/netflix-hbo-streaming-video-traffic-increases-as-bittorrent-declines/ (accessed 22 December 2017). See also Sandvine, *Global Internet Phenomena Report* (Waterloo: Sandvine, 2013), p. 6.

[lxxxvii] Maura Conway, "Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research", p. 77.

[lxxxviii] See Anthony Richards, "The Problem with 'Radicalisation': The Remit of 'Prevent' and the Need to Refocus on Terrorism in the UK," *International Affairs* 87(1) (2011), pp. 143-152; Charlotte Heath-Kelly, "Counter-Terrorism and the Counterfactual: Producing the 'Radicalisation' Discourse and the UK PREVENT Strategy," *The British Journal of Politics and International Relations* 15 (2013), pp. 394-415; Jonathan Githens-Mazer, "Rethinking the Causal Concept of Islamic Radicalisation: Political Concepts," Committee on Concepts and Methods Working Paper Series, 42 (2010); Jonathan Githens-Mazer and Robert Lambert, "Why Conventional Wisdom on Radicalisation Fails: The Persistance of a Failed Discourse," *International Affairs* 86(4) (2010), pp. 889-901; Michael King and Donald Taylor, "The Radicalisation of Homegrown Jihadists: A Review of Theoretical Modles and Social Psychological Evidence," *Terrorism and Political Violence* 23(4) (2011), pp. 602-622; Mark Sedgwick, "The Concept of Radicalisation as a Source of Confusion," *Terrorism and Political Violence* 22(4) (2010), pp. 479-494; Charlotte Heath-Kelly, "Algorithmic Autoimmunity in the NHS: Radicalisation and the Clinic," *Security Dialogue* 48(1) (2016), pp. 29-25.

[lxxxix] Norman Bettison, "Preventing Violent Extremism: A Police Response," *Policing* 3(2) (2009), pp. 129-138.

[xc] Soriano calls this a 'peril' of Web 2.0. See Manuel Soriano, "The Vulnerabilities of Online Terrorism", pp. 272-274.

[xci] Charlotte Heath-Kelly, “Can we Laugh Yet? Reading post-9/11 Counterterrorism Policy as Magical Realism and Opening a Third Space of Resistance”, *European Journal of Criminal Policy and Research*, 18 (2012), pp. 343-360.

[xcii] Joel Gunter, “ISIS Mocked with Rubber Ducks as Internet Fights Terror with Humour”, *The Guardian*, last modified 28 November 2015. Available at https://www.theguardian.com/world/2015/nov/28/isis-fighters-rubber-ducks-reddit-4chan (accessed 22 December 2017).

[xciii] Jamie Bartlett and Alex Krasodomski-Jones, *Online Anonymity Islamic State and Surveillance*, p. 17.

[xciv] Margi Murphy, “Bitcoin Mania: Google’s Top Searches in 2017 Dominated by Digital Currency Craze”, *The Telegraph*, last modified 13 December 2017. Available at http://www.telegraph.co.uk/technology/2017/12/13/bitcoin-mania-googles-top-searches-2017-dominated-digital-currency/ (accessed 22 December 2017).

[xcv] The UK was identified as a net exporter of e-commerce goods in 2009, exporting £2.80 for every £1 imported. See Carl Kalapesi, Sarah Willersdorg and Paul Zwillenberg, *The Connected Kingdom: How the Internet is Transforming the UK Economy*, (Boston: Boston Consulting Group, 2010), p. 5. In 2016, the internet economy was estimated to account for 12.4% of British GDP, a figure that would have characterised the UK as more reliant on internet mediated commerce than all of its G20 counterparts, with South Korea at 8% and the USA at 5.4%. See David Dean et al, *The Internet Economy in the G20: The $4,2 Trillion Growth Opportunity*, (Boston: Boston Consulting Group, 2012), p. 9. By 2016, 45.9 million people, or 87.9% of the British population, were regareded as internet users. See Office for National Statistics, “Internet Users in the UK: 2016”, last modified 20 May 2016. Available at https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2016/ (accessed 22 December 2017).