Blockchain Technologies and Extremism: What does the Future Hold?

Dr Gareth Mott
Lecturer, Politics and International Relations
Nottingham Trent University
gareth.mott@ntu.ac.uk

Mott, G. (2019) “A Storm on the Horizon? ‘Twister’ and the Implications of the Blockchain and Peer-to-Peer Social Networks for Online Extremisn”, *Studies in Conflict and Terrorism*, Vol. 42 No.1-2, pp.206-227

Contents

- Broader context
- Defining cyberspace
- Defining blockchain
- Ascribing value to the blockchain: citizen and state
- Countering extremism: current approaches
- Escaping censorship from mainstream to…
- - alternative
- - federated
- - darknet
- - P2P
-
- Debate: From the perspective of the state, the advent of Blockchain technologies entails the end of a ‘golden era’ of control over ‘communicating’ and ‘funding’ violence

Broader context

- Fitzgerald and Parziale (2017):
- “technological development will continue to outpace institutional change. This is to be expected. Of more concern is the stark imbalance between the resources dedicated to *developing* new technologies and those dedicated to *governing* new technologies. This imbalance in resources produces increasingly clear risks for which practical solutions are scarce”
-
- Lawrence Lessig (1999):
- Code is law…
-
- Stewart (1988)
- “information wants to be free”

Broader context

- Bad Religion (2000), *I Love my Computer*
- “I love my computer, for all you give to me, predictable errors and no identity … all I need to do, is click on you, and we’ll be joined in the most soul-less way … the world outside is so big, but it’s safe in my domain, because to you I’m just a number and a clever screen name”
-
- Humans may care about policies, legislation and law
-
- But computers do *not*
- Computers adhere to the laws of binary code and the limitations of their Operating Systems
-
- *Identity* attribution overrides the technology itself… the human realm is the space in which legislation can most easily be articulated

Defining cyberspace

- Sheldon (2012):
- “by 2012, there are at least 18 competing definitions of cyberspace and several competing definitions of cyberpower being actively used and debates on a worldwide platform”
- But, broadly, these adhere to two types:
-
- ‘Uniformity’ definitions
- - cyberspace is tied to its physical manifestations
-
- ‘Exclusive model’ definitions
- - physical element is not mentioned; cyberspace is a virtual space existing within an infrastructure
-
- Discussion: Which approach do you prefer? Why?

Defining cyberspace

- The British Government defines cyberspace as…
-
- “an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services” (Cabinet Office, 2011)
-
- So… an economic realm and an economic technology
-
- Bear in mind though… that these technologies present *both* economic and social upheavals

Defining blockchain

- This economic leaning correlates with many interpretations (or assumptions) relating to blockchain technology
-
- Government Office for Science (2016), *Distributed Ledger Technology: Beyond Blockchain*
- “the ‘blockchain’ … was invented to create the peer-to-peer digital cash Bitcoin in 2008. Blockchain algorithms enable Bitcoin transactions to be aggregated in ‘blocks’ and these are added to a ‘chain’ of existing blocks using a cryptographic signature. The Bitcoin ledger is constructed in a ‘permissionless’ fashion, so that anyone can add a block of transactions if they can solve a new cryptographic puzzle”
-
- Report suggests that computer code could encode human law…

Acribing value to the Blockchain: citizen and state

- In October 2008, someone using the pseudonym ‘Satoshi Nakamoto’ posted a white paper to the Crytography Mailing list
- This white paper outlined a digital currency called ‘Bitcoin’
-
- This was *not* the first instance of a non-state digital currency
- But was *was* the first implementation of a ‘Blockchain’
-
- Remember:
- - a Blockchain is a distributed, provably accurate record
- - anyone with an internet connection and computer can maintain a copy of a dyamically-updated ledger
- - the ledger has not central administrator (although coding may be governed)
- - the utility of Blockchains are not constrained to cryptocurrencies
-

Acribing value to the Blockchain: citizen and state

- Pounds, dollars, Euros and other fiat currencies are printed by central banks
- But this is not the case with Bitcoin
- A total of 21 million coins will be created by an algorithm
- In order to be valuable, the public ledger must be secure
- ‘Miners’ compete for freshly minted coins with computational power
- Incentive to support, rather than degrade, the network
-
- The computers multiply two exceedinly large numbers
- In order to find a unique ‘hash’
- Each successful hash adds a new ‘block’ to the Blockchain
- Mining difficulty adjusts to regulate that new blocks will be created roughly every ten minutes

Acribing value to the Blockchain: citizen and state

- Competitive…
- Mining is concentrated in regions with low ambient temperatures and inexpensive electricity
- The entire electricity consumption of the network is said to exceed the electricity consumption of Nigeria and Ireland
- Which significantly secures the Blockchain…
- But are there potential negative security implications of this electricity demand?
- Is this an arms race, of sorts?

Acribing value to the Blockchain: citizen and state

- The Blockchain and cryptocurrency enables:
-
- - owners of a ‘private key’ undiminished access to, and control of, their wallets
- - transactions that can be sent instantaneously, irrespective of national laws and borders
- - a trading system that offers pseudo anonymity
- - a trading ecosystem that operates 24/7
- - a trading ecosystem that does not discriminate
-
- Discussion:
- Why might national governments feel threatened by Blockchain-based cryptocurrency?
- Which actors might be empowered? Why?

Countering extremism: current approaches

UK interior minister says social media firms must act after New Zealand shootings

1 MIN READ

Countering extremism: current approaches

Davos 2018

This article is more than **1 year old**

May calls on social media giants to do more to tackle terrorism

Prime minister to ask shareholders to pressure firms such as Twitter and Facebook

Heather Stewart *and* Jessica Elgot

Wed 24 Jan 2018 22.30 GMT

82

▲ Theresa May will use a speech at the World Economic Forum to call for more action from tech companies to identify and take down extremist content. Photograph: Jack Taylor/Getty Images

Countering extremism: current approaches

NEWS

Home | UK | World | Business | Politics | Tech | Science | Health | Family & Education | Entertainment & Arts | Stories | Video & Audio | In Pictures | Newsbeat | More

Politics | Parliaments | Brexit | England Local Elections 2019 | NI Local Elections 2019

Tech giants ignored government invitation - Matt Hancock

Only four of the 14 biggest tech companies invited to a government meeting about improving online behaviour turned up, the culture secretary has said.

Speaking on the Andrew Marr Show about minimum age limits for websites and the circulation of extremist material, Matt Hancock argued that Britain needed stronger legislation to ensure co-operation from social media sites.

Mr Hancock did not specify which companies had turned up to the meeting.

20 May 2018

Share

Countering extremism: current approaches

- Gov.uk, 2015:
- “tackling extremist content on the internet is vital in countering the terrorist narrative and stopping offences that incite terrorism. There is considerable effort going into removing extremist material from the internet”
-
- Counter-terror strategies for social networks are incorporated into the Prevent strategy

Countering extremism: current approaches

- Counter Terrorism Internet Referral Unit (CTIRU)
- Removes 1,000+ pieces of content from the internet each week (a concentration of which relates to Syria and/or Iraq)
- Established in 2010
- Acts under the remit of Section 3 of the Terrorism Act 2006 to remove content that incites or glorifies terrorist acts
- Maintains a blacklist of websites that are hosted abroad, which the British authorities cannot police
- Heavily reliant on cooperative relationships with the oweners of social networking services (which are mostly based outside of the UK)
- Also reliant on social networking users contacting the authorities via the gov.uk/report-terrorism url or contacting social network services directly
- Also reliant on ISPs blocking blacklisted sites

Countering extremism: current approaches

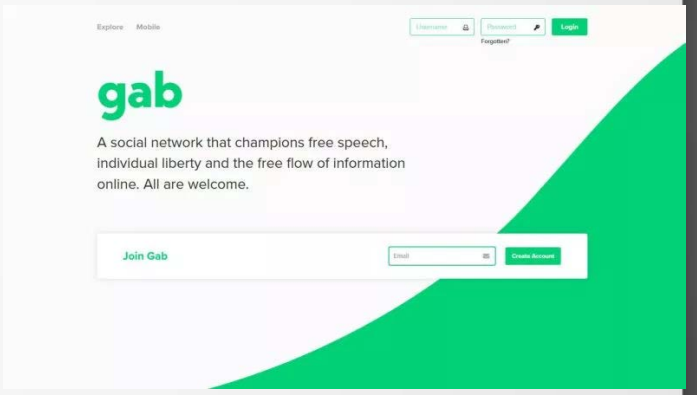
- This would appear to be an escalating challenge…
-
- 17,541 items removed in 2013
- 55,556 items removed in 2015
- ~100,000 items removed in 2016 (Dodd, 2016)
-
- European Internet Referral Unit superceded British unit at European level, from July 2015
- Removed 12,000 pieces of terrorist-related content by October 2016 (Wallace, 2016)
-
- Discussion:
- To what extent do you think this model of content removal can scale?

Countering extremism: current approaches

- Committee report from 2016 highlighted need for CTIRU to expand
- Specifically with a desire for representatives from social networks to be ‘co-located’ within CTIRU itself
-
- The report was somewhat despondent:
- It is “… alarming that [Facebook, Twitter and Youtube] have teams of only a few hundred employees to monitor networks of billions of accounts and that Twitter does not even proactively report extremist content to law enforcement agencies”
- The firms “… are hiding behind their supranational legal status to pass the parcel of responsibility and refusing to act responsibly in case they damage their brands” (Home Affairs Committee, 2016)
- Firms may be coy? Particitation and non-participation may harm brands...

Escaping censorship: from mainstream to alternative

- Reseach produced by Conway et al (2019) has identified that mainstream social networking platforms have become increasingly conscious of – and adverse to – their servers being used for the dissemination of extremist material
-
- Are extremists likely to give up?
- No!
-
- So we have seen a proliferation of platforms used…
-
- Different platforms offer varying benefits and drawbacks…
-
- What are the benefits and drawbacks of using ‘Gab’ rather than ‘Twitter’?



Escaping censorship: from mainstream to federated

- Some evidence that extremists were prompted – from 2014 onwards – to begin using ‘Federated networks’
-
- ‘Federated’ networks offer a greater degree of censorship flexibility/immunity…
-
- But are not foolproof
- - downtime
- - still reliant on a central server

Escaping censorship: from mainstream to darknet

- The ‘darknet’ is often touted as a lawless, censorship free environment
- And to a certain degree, it is
-
- Refers to servers and clients that use specific software to host and access web content
- Most popuylar is The Onion Router (Tor)
- - connections tunelled through Tor relays (proxies) around the world, to obfuscate their true IP address
- - encrypted with each hop
-
- Estimated user base of 1 million in October 2011 rose to ~2 million by 2016
- Bandwidth usage increased from just a few Gbit/s to ~75 Gbit/s

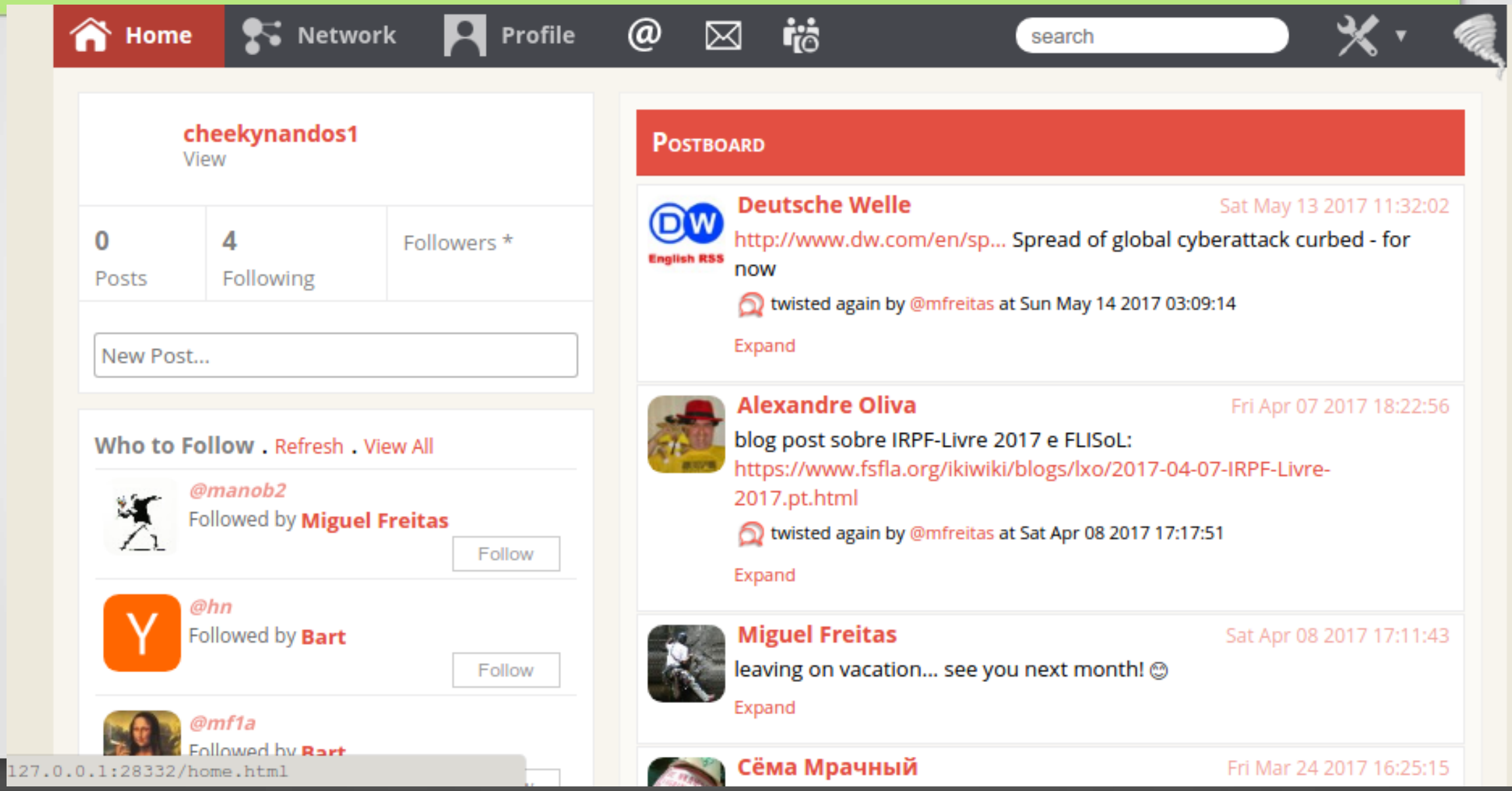
Escaping censorship: from mainstream to darknet

- But! Most of this data relates to the Tor network being used to access ‘surface’ or ‘deep’ web, rather than ‘darknet’ pages… ~96.6%!
-
- Guitton (2013)
- 45% of the accessible services are of an unethical nature
-
- Owen and Savage (2015) – controlled 40 exit relays
- Greatest concentration is for child-abuse…
-
- We know that terrorist groups have advocated using Tor clients to improve security, but…
-
- Moore and Rid (2016) identified that there are almost no *active* terrorist pages on the darknet

Escaping censorship: from mainstream to darknet

- A darknet website may obfuscate its location, but it is still limited by:
- - central server
- - risk of identification and punishment
-
- So… not really an ideal alternative
-
-
-
-
-
- Twister, release in 2014

Escaping censorship: from mainstream to P2P



Escaping censorship: from mainstream to P2P

- Combines:
- Blockchain
- BitTorrent
- DHT
-
- The technology alters the role of ‘trust’
-
- Werbach:
- Leviathan trust
- Peer-to-peer trust
- Trustless trust
-
- So the human condition of mistrust is turned into a *strength* of the network

Escaping censorship: from mainstream to P2P

- Source code released and distributed under a Massachusettes Institute of Technology and Berkeley Software Distribution license
- Open source; ‘free’ as in freedom
-
- Is it possible to prosecute on the basis of possessing or using the technology?
- Not really…
- ‘Joint liability’ would need to be introduced… copies of a Blockchain are likely to be held across multiple jurisdictions… and users cannot be obligated to update their copy to a particular version

Escaping censorship: from mainstream to P2P

- Two wings of terrorist organisations?
- ‘Propaganda’ and ‘operational’
-
- Both may find aspects of a network like Twister to be useful
- But these users differ
-
- Remember: the operational wing and the propaganda wing may be entirely separate entities… indeed, it is probably best from the organisations’ standpoint if this is the case

Escaping censorship: from mainstream to P2P

- Propaganda:
- - take advantage of the ‘advertising lottery’
- - more broadly, take advantage of the opportunity to post non-transitory material
-
- Operational:
- - take advantage of the direct messaging functionality
- - ‘burner phone’ approach to communication

Escaping censorship: from mainstream to P2P

- There is some evidence that extremists have toyed with the platform ‘Zeronet’
- Zeronet is an example of a ‘decentralised web’
- - domains are registered to a blockchain
- - webpage content is disseminated through a BitTorrent-like network
-
- But!
- I have not idenfied any noticeable extremist presence on Twister…
- So… a problem for the future?
-
- Discussion:
- Why might extremists have largely avoided Twister, so far?
- Is it possible that a proliferation in extremist usage of Twister could be triggered by an internal or external event? Give an example

Questions?

- Any questions?

Debate

- Debate the motion:
-
- From the perspective of the state, the advent of Blockchain technologies entails the end of a ‘golden era’ of control over ‘communicating’ and ‘funding’ violence