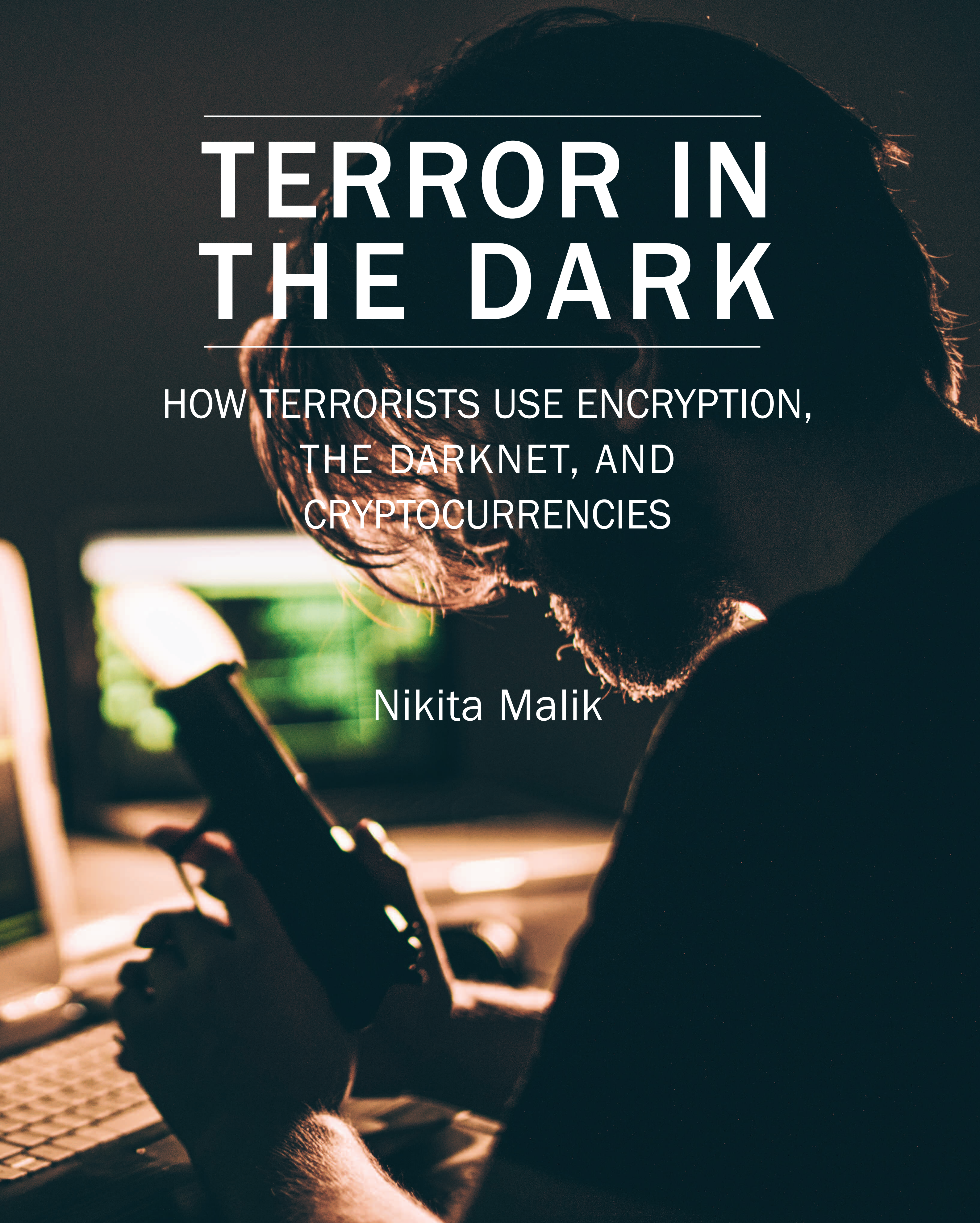


TERROR IN THE DARK

HOW TERRORISTS USE ENCRYPTION, THE DARKNET, AND CRYPTOCURRENCIES

Nikita Malik

CRT
Centre for the Response to Radicalisation and Terrorism
At The Henry Jackson Society

THE HENRY JACKSON SOCIETY
DEMOCRACY·FREEDOM·HUMAN RIGHTS

“This report is a remarkable contribution to the literature on the use of the Darknet by criminals and terrorists. While the first decade of the century was defined by the battle against jihadist ‘safe havens’ – physically located in Afghanistan, North West Pakistan, Yemen, Islamic State, and so on -- this report draws attention to the possible rise of ‘virtual safe havens’: encrypted communication channels, hidden portions of the internet, cryptocurrency accounts that are not registered with any banks, and more. While there is no doubt that these new technologies can provide a huge social benefit, this report outlines recommendations to ensure that this benefit is not used to the advantage of criminals and terrorists.”

The Rt Hon. the Lord Trimble,
former First Minister of Northern Ireland and
member of the National Security Strategy
Joint Committee

“This is a deeply disturbing report, illustrating how extremist content and instructional terrorist material, as well as funding campaigns to raise money for terrorist groups, can be found on the internet – with varying degrees of accessibility. It brings into the light of day things we may well have heard about, material we may even think we know about. And it reveals just how ignorant we are. The author has laid bare by her meticulous research matters that threaten our domestic, social and national life. This report stresses that UK regulation must be created specifically for auditing the internet, in which transparency and accountability can be guaranteed. This can be achieved through either internal supervisory powers, or an external supervisory body. It is about time we address these issues, and the Government should carefully consider the recommendations made within this welcome report.”

The Lord Griffiths of Burry Port,
Shadow Spokesperson in the Lords for Digital,
Culture, Media and Sport.

TERROR IN THE DARK

HOW TERRORISTS USE ENCRYPTION, THE DARKNET, AND CRYPTOCURRENCIES

Nikita Malik

With Research Assistance from Ojima Salifu and Arthur Bradley

Published in 2018 by The Henry Jackson Society

The Henry Jackson Society
Millbank Tower
21-24 Millbank
London SW1P 4QP

Registered charity no. 1140489
Tel: +44 (0)20 7340 4520

www.henryjacksonsociety.org

The views expressed in this publication are those of the author and are not necessarily indicative of those of The Henry Jackson Society or its Trustees.

Title: “Terror in the Dark: How Terrorists use Encryption,
the Darknet, and Cryptocurrencies”
By Nikita Malik

ISBN 978-1-909035-45-4
£9.95 where sold

About the Author

Nikita Malik is the Director of the Centre for the Response to Radicalisation and Terrorism (CRT) at The Henry Jackson Society, where her work focuses on protecting women, children, families, and asylum seekers against radicalisation and terrorism.

She has published several ground-breaking reports backed and endorsed by the United Nations Children's Fund (UNICEF), the United Nations Educational, Scientific and Cultural Organization (UNESCO), Child Soldiers, Solidarity for Refugees, and Child to Child.

Malik has presented findings and evidence to the British and EU Parliament, the Foreign and Commonwealth Office (FCO), the Department of State (DoS), the EU Radicalisation Awareness Network (RAN), International Centre for Counter-terrorism – The Hague (ICCT), the United Nations, and SO15 Counter Terrorism Command (CTC).

Malik holds a BA (Hons) in Economics and Management and an MSc in South Asian Studies, both from the University of Oxford. She also holds an MSc in Middle Eastern Politics and Arabic from SOAS, University of London. She is fluent in four languages.

About CRT at The Henry Jackson Society

The Centre for the Response to Radicalisation and Terrorism (CRT) is unique in addressing violent and non-violent extremism. By coupling high-quality, in-depth research with targeted and impactful policy recommendations, we aim to combat the threat of extremism in our society.

The Henry Jackson Society is a think-tank and policy-shaping force that fights for the principles and alliances that keep societies free, working across borders and party lines to combat extremism, advance democracy and real human rights, and make a stand in an increasingly uncertain world.

The Henry Jackson Society is a company limited by guarantee registered in England and Wales under company number 07465741 and a charity registered in England and Wales under registered charity number 1140489.

For more information, please see www.henryjacksonsociety.org.

Acknowledgements

I am grateful for assistance provided by The Henry Jackson Society research interns Ojima Salifu, Arthur Bradley, Genevieve Hull, and Virginia Romero.

This project benefited from advice and input provided by representatives in the National Crime Agency (NCA) and SO15 Counter Terrorism Command (CTC).

Executive Summary

Following the five terror incidents on British soil in 2017, the Government has devoted greater attention to the presence of online extremism, recognising that it has a role to play in the fostering of "homegrown" terrorism within the UK. However, this report makes a strong case for greater attention to be placed on the "Darknet" – portions of the internet that are not easily accessible by the public at large, without dedicated expertise. This report demonstrates how terrorists and extremists have utilised the Darknet to mask their communication and propaganda efforts, to recruit and radicalise, and to gain material benefits such as illicit goods: including, but not limited to, weapons and fraudulent documents. In addition, this report notes the growing tendency of these individuals to utilise cryptocurrencies for transactions and fundraising, enabling them to evade detection by law enforcement entities.

While the first decade of the century was defined by the battle against jihadist "safe havens" – physically located in Afghanistan, North West Pakistan, Yemen, Islamic State, and so on – this report draws attention to the possible rise of "virtual safe havens": encrypted communication channels, hidden portions of the internet, cryptocurrency accounts that are not registered with any banks, and more. In doing so, it highlights the following trends:

- **Terrorists using encryption to hide:** Better monitoring of the surface web by social media companies and security officials has resulted in a faster rate of removal of extremist content from social media platforms.[1] Correlated to this is an increased use by extremist networks of the Darknet as a "jihadist safe haven" for planning attacks. Evidence suggests that recruiters use the Darknet to plan and launch terrorist attacks, because detection by law enforcement is less likely.[2] While initial contact can be made on surface web platforms, further instructions are often given on end-to-end encryption apps such as Telegram on how to access jihadist websites on the Darknet.

- **Terrorists using the Darknet for recruitment purposes:** Given the largely inaccessible nature of encrypted channels like Telegram and areas of the Darknet, it is perhaps unsurprising that mass recruitment rarely takes place on these channels. Instead, IS aims to draw interested sympathisers from the surface web and social media into the more secure recesses of the Darknet for further interaction and indoctrination.

- **Terrorists using the Darknet as a reservoir of propaganda:** The removal of extremist and terrorist content from the surface web and deep web – particularly in the case of artificial intelligence programs that may do "bulk" removals – increases the risk that evidence needed to prosecute individuals disseminating content or providing material support to terrorist organisations may be lost. Much of this material later resurfaces on the Darknet. Technology companies should work with law enforcement to ensure that this material is archived effectively to understand patterns of behaviour.

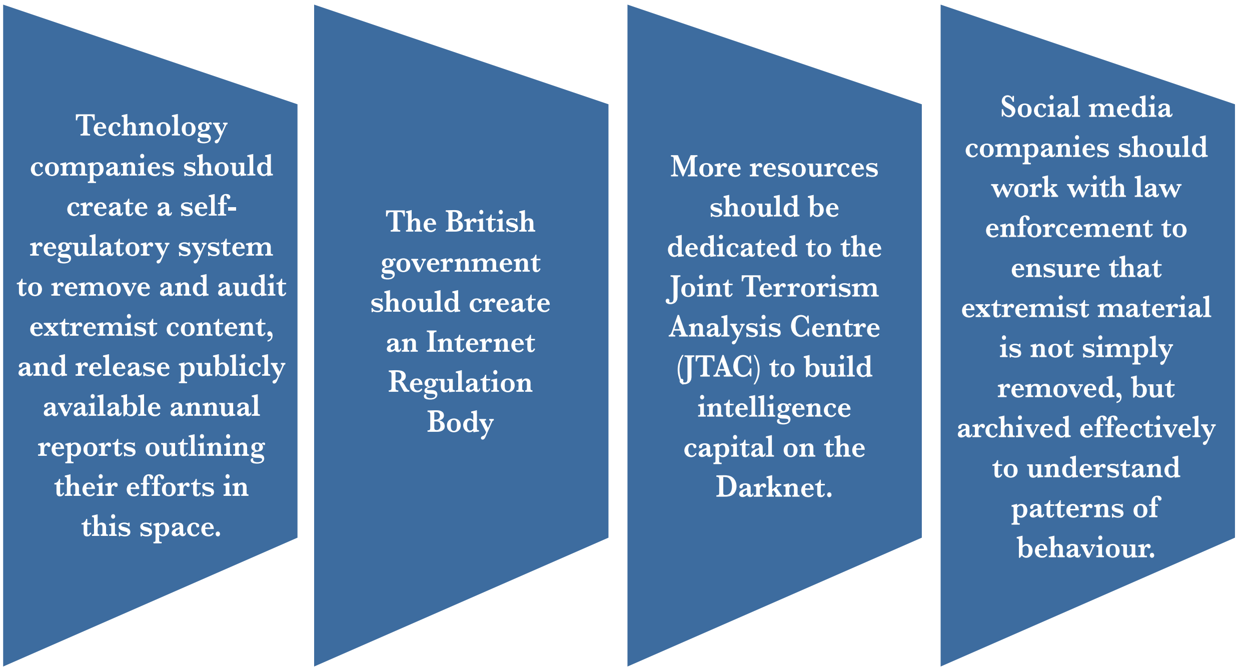
- **Terrorists using cryptocurrency to evade detection and to fundraise:** Terrorists, like other criminals, use cryptocurrency because it provides the same form of anonymity in the financial setting as encryption does for communication systems. By fundraising and making financial transactions online with bitcoin, terrorists and other criminals can avoid interference from financial regulators or other third parties who might otherwise take steps to prevent their operations. According to a 2015 Europol

[1] See, for example: The YouTube Team, 'An update on our commitment to fight terror content online', *YouTube Official Blog*, 1 August 2017, available at: https://youtube.googleblog.com/2017/08/an-update-on-our-commitment-to-fight.html, last visited: 17 March 2018; Huddleston, T., 'Four Tech Giants Team Up to Fight Terrorism', *Fortune*, 26 June 2017, available at: http://fortune.com/2017/06/26/twitter-facebook-youtube-microsoft-global-forum-terrorism/, last visited: 14 March 2018.

[2] Dearden, L., 'ISIS urged undercover BBC reporter to launch terror attacks in London Bridge and Westminster', *Independent*, 4 September 2017, available at: http://www.independent.co.uk/news/uk/home-news/isis-undercover-bbc-reporter-london-bridge-terror-attacks-westminster-borough-market-online-a7928641.html, last visited: 14 March 2018.

report, bitcoin featured in high-profile investigations involving payments between criminals, and was used in more than 40% of these transactions in the European Union (EU).[3]

The report includes the following policy recommendations:



Technology companies should create a self-regulatory system to remove and audit extremist content, and release publicly available annual reports outlining their efforts in this space.

The British government should create an Internet Regulation Body

More resources should be dedicated to the Joint Terrorism Analysis Centre (JTAC) to build intelligence capital on the Darknet.

Social media companies should work with law enforcement to ensure that extremist material is not simply removed, but archived effectively to understand patterns of behaviour.

[3] 'The Internet Organised Crime Threat Assessment (IOCTA) 2015', *Europol*, available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015, last visited: 14 March 2018, p. 11.

Contents

Page

List of Tables and Figures 3
Glossary of Abbreviations 4
Glossary of Terms 5
Glossary of Arabic Terms 7
Introduction 9
Methodology 11

Chapter 1: Surface Web, Deep Web, and Darknet **12**

What is the Surface Web? How Does it Differ from the Deep Web? 12
The Darknet 13
Encryption 13
Public key encryption and Asymmetric cryptography 14
The Tor Network 15
Freedom of Speech and Privacy 15
Case Study: Reporters Without Borders 16

Chapter 2: Terrorist Communication and Recruitment on the Darknet **17**

The Use of Encryption by IS 17
Telegram 17
Use of the Darknet 18
Radicalisation 19
Case Study: Tower Hamlets v. B 20
Propaganda 21
Case Study: Prosecuting for the Dissemination of Terrorist Content Online 22
Direct Recruitment 22

Chapter 3: Terrorism and the Darknet **24**

Crime on the Darknet 24
Drugs 24
Case Study: Ricin in Liverpool, UK 24
Case Study: The Silk Road 1.0 25
Case Study: Blake Benthall (aka 'Defcon) and Silk Road 2.0 27
Other Criminal Activity on the Darknet 28
Case Study: The "Playpen" Case 29
The Crime-Terror Nexus 31
Drug Trafficking 31
Kidnap for Ransom 32
Document Fraud 32
Weapons 34
Training 36

Page

Chapter 4: Cryptocurrency **37**

The *Hawala* Payment System 37

Example: *Hawala* Payments 37

Case Study: The Merits of Cryptocurrencies and Distributed Ledger Technology 38

The Bitcoin Payment System 39

Material Support 40

Islamic State 40

Other Terrorist Organisations 41

How Anonymous is Bitcoin? 42

New Technological Advancements 43

Conclusions and Policy Recommendations **45**

1. Technology companies should create a self-regulatory system to remove and audit extremist content, and release publicly available annual reports outlining their efforts in this space. 45
2. The British government should create an Internet Regulation Body. 46
3. More resources should be dedicated to the Joint Terrorism Analysis Centre (JTAC) to build intelligence capital on the Darknet. 47
4. Social media companies should work with law enforcement to ensure that extremist material is not simply removed, but archived effectively to understand patterns of behaviour. 47

Appendix

I. Extremist Content on Search Indexes (Surface Web) using Case Study: Tower Hamlets v. B. **49**

List of Tables and Figures

Page

Table 1 Case Study Tower Hamlets v. B search results on Google and Duckduckgo 20

Figure 1 Surface web, deep web, Darknet 12

Figure 2 Encryption 14

Figure 3 Case study techniques used to identify Darknet users 30

Figure 4 Document fraud on Dream Market 33

Figure 5 Screenshot of *Al-Sadaqah* campaigning for bitcoin funding on Twitter 42

Glossary of Abbreviations

AML	Anti-Money Laundering
BTC	Bitcoin
CPS	Crown Prosecution Service
CTIRU	Counter Terrorism Internet Referral Unit
DEA	Drug Enforcement Agency
DHS	Department of Homeland Security
DoS	Department of State
DPR	Dread Pirate Roberts
EU	European Union
EUR	Euro
Europol	European Union Agency for Law Enforcement Cooperation
FBI	Federal Bureau of Investigation
GB£	British Pound
GCHQ	Government Communication Headquarters
HSI	Homeland Security Investigations
ICCT	International Centre for Counter-Terrorism
IED	Improvised Explosive Device
IISS	International Institute for Strategic Studies
IP	Internet Protocol
IRS	Internal Revenue Service
IS	Islamic State
JTAC	Joint Terrorism Analysis Centre
MDMA	Methylenedioxymethamphetamine
MI5	Security Service (Military Intelligence, Section 5)
NCA	National Crime Agency
NIT	Network Investigative Technique
NPS	New Psychoactive Substance
Ofcom	Office of Communications
Ofgem	Office of Gas and Electricity Markets
Ofsted	Office for Standards in Education, Children's Services and Skills
Ofwat	Water Services Regulation Authority
PGP	Pretty Good Privacy
RSS	Rich Site Summary
RUSI	Royal United Services Institute
SR	Silk Road
SR2	Silk Road 2.0
TATP	Triacetone Triperoxide
UK	United Kingdom
UNSC	United Nations Security Council
US$	United States Dollar
USPIS	United States Postal Inspection Service
URL	Uniform Resource Locater
US	United States
VPN	Virtual Private Network

Glossary of Terms

Al-Qaeda (AQ), includes Al-Qaeda in Iraq (AQI), Al-Qaeda in the Arabian Peninsula (AQAP), and Al-Qaeda in the Islamic Magreb (AQIM): Inspired by and led by Osama bin Laden, the group's aims include the expulsion of Western forces from Saudi Arabia, the destruction of Israel, and the end of Western influence in the Muslim world.

Council in the Environs of Jerusalem or *Mujahideen Shura*: A coalition of Al-Qaeda-affiliated Salafi-Jihadist groups active in the Gaza Strip and the Sinai Peninsula. The group is a proscribed terrorist organisation according to the US Department of States (DoS).

Cryptocurrency: A decentralised digital currency that operates independently of a central bank by using encryption techniques to regulate the generation of units of currency and verifying the transaction of funds via a blockchain transaction database. As cryptocurrency transactions are largely anonymous and untraceable, they are attractive to criminals and other individuals looking to avoid the traceability inherent in most fiat currency systems.

Cryptocurrency exchange: Online platforms that allow individuals to buy, sell, and trade between cryptocurrencies and, in some cases, between cryptocurrencies and fiat currencies.

Darknet, including Black Net or Dark Web: A small segment of the deep web (see below) that requires specialist encryption software to access. Though it is not exclusively used for illicit purposes, the anonymous nature of the Darknet means that it is often exploited for the sale of illegal goods and for the distribution, storage, and consumption of illegal material, including child pornography and terrorist propaganda.

Deep web, including invisible net or hidden web: Areas of the World Wide Web that are not indexed by standard search engines. Data in the deep web is accessed via a direct URL, and may require a password or an alternative security pass to grant access.

Extremism: An ideology, which when implemented, would significantly and negatively impact the human rights of certain sectors of society, such as women, religious or ethnic groups, persons with disabilities, and so on. By extension, violent extremism is an ideology that would justify the use of violence against these sectors of society.

Internet Protocol (IP) address: A unique set of numbers which can identify and physically locate a digital device using the internet, such as a computer. IP addresses work in a similar manner to traditional telephone numbers, enabling digital devices to share data and communicate with one another.

Islamic State (IS) or *Daesh*: Islamic State is a brutal Sunni Islamist terrorist group primarily active in Iraq and Syria. The group adheres to a global jihadist ideology, following an extreme interpretation of Islam, one that is anti-Western and promotes sectarian violence. IS aims to establish a *caliphate* governed by strict *sharia* law in the region and imposes its rule on people using violence and extortion. IS was previously proscribed as part of AQ.

Islamism: The belief that Islam is a totalitarian political ideology. It claims that political sovereignty belongs to God rather than the people. Islamists believe that their reading of *sharia* should be state law, and that it is the religious duty of all Muslims to work towards and pledge allegiance to an Islamic state that reflects these principles.

Jihadism: A militant strand of Sunni Islamism which advocates the use of violence against non-Muslims (or other Muslim groups such as Shia or Sufi Islam) as part of a broader struggle for the establishment of an Islamic state. Variations of this ideology are subscribed to and espoused by numerous terrorist groups, most notably AQ and IS.

Lone wolf: An individual who prepares and commits violent acts alone, outside of any command structure, and without material assistance from any group. The individual may be influenced or motivated by the ideology and beliefs of an extremist group or terrorist organisation, and may act to support it.

Network Investigative Technique (NIT) or Computer Network Exploitation: A form of malware or hacking designed to gain access to a computer in order to acquire information about the system or data contained on that computer. Information obtained through the use of a NIT may include the IP address or name of a computer, complete files, web history, webcam activity, and more.

Pen register: A term originally used to refer to devices that record the numbers called from a particular telephone line. This term now includes devices or programs that perform similar functions in monitoring internet communications from a given IP address. Though pen register devices are used to capture records of communications, they typically do not capture the contents of those communications.

Radicalisation: The process by which individuals and/or groups come to adopt extremist ideologies. Scholars often use the terms "radicalisation" and "violent radicalisation" to distinguish between engagement in violent activities and radicalised non-violent thinking.

Self-starter terrorist: An individual who is not completely alone in their radicalisation process (unlike a "lone wolf") and is loosely connected to an overarching terrorist network. Although unlikely to have met recruiters in person, they use instructions, manuals, and low-investment techniques to carry out their attacks.

Source code: A set of information written by a programmer in a computer programming language. It serves as a set of instructions on how a program operates.

Supporters of Islam or *Ansar al Islam*: A proscribed Sunni terrorist group based in Iraq and Syria. In August 2014, the group merged with IS. However, some factions within the group rejected the merger, and continued to function as an independent organisation.

Surface web, including Clear net, Open net, Visible web, Indexed web: The segment of the internet that is easily accessible to users through the use of standard search engines such as Google or Bing.

Terrorism: The use of violence or illegal force targeted at civilians by non-state actors that seeks to bring about political or societal change.

The Emigrants or *Al-Muhajiroun*, includes Islam4UK, Muslims Against Crusades, Al Ghurabaa, The Saved Sect, Call to Submission, Need4Khilafah: A proscribed Islamist extremist group originating in the UK, with links abroad. Set up by Omar Bakri Muhammad and later led by Anjem Choudary, the group has known connections to IS, with numerous members being involved in terrorism both inside the UK and overseas.

Trap and trace device: A device that performs the inverse function to a pen register device, serving to capture the incoming data of a given IP address. The term is often used in combination with a pen register, because some devices or programs are capable of performing both functions simultaneously.

Virtual Private Network (VPN): Typically, a paid service that encrypts an internet user's web traffic as it travels from their device to a network through what is known as a "tunnel". VPNs are commonly used in corporate environments to enable remote working, but can also be used to help internet users to connect to proxy servers for the purpose of protecting their identity and obscuring their true IP address.

Glossary of Arabic Terms[4]

Amaq: literally translates as "storyteller"; an official news outlet of the Islamic State, responsible for producing and publishing propaganda, posting news related to the operations of the group and publishing claims of responsibility for international terrorist operations.

Al-Sadaqah: literally translates as "donation" or "voluntary giving". In the context of this report, an AQ-affiliated organisation which campaigns online for donations in the form of bitcoin to fund jihadist groups in Syria.

Dar al-Islam: "Land of Islam"; Islamists commonly define *Dar al-Islam* as any land under Muslim control which implements the religious principles of *sharia* as divine law.

Dar al-kufr: "land of disbelief".

Emir (pl. *emirs*): a leader.

Fatwa (pl. *fatawa*): "religious edict"; an authoritarian statement on a point of practical knowledge of *sharia* law (*fiqh*) from an Islamic scholar.

Dar al-Harb: literally translates to "Lands of War"; a reference to territories outside of the *Dar al-Islam* (Land of Islam), or Islamic State. An ancient Islamic concept dating back to long before the emergence of contemporary jihadism, it is frequently used by Islamist extremists in reference to lands outside of the Islamic caliphate such as Europe or North America. Sometimes also referred to by Islamist extremists as *Dar al-kufr* (see above).

Dawah: literally translates as "invitation"; the proselytising or preaching of Islam.

Hawala: literally translates as "transfer" or "trust"; a traditional system of financial transfer used in South Asian and Middle Eastern countries that is based on a large network of brokers known as *Hawaladars.* The system exists outside of traditional banking systems and the system has no identifiable paper trail. As a result, it has become attractive to criminal and terrorist groups as it does not require either the sender or the recipient of funds to provide personal details.

Hijrah: emigration in the way of Allah to a perceived Muslim land. Islamic dating begins with the Hijrah of Islam's prophet Mohammad from Mecca to Media (both in Saudi Arabia), in 622 CE.

Isdarat: literally translates as "publications" or "releases"; a pro-Islamic State website that hosts IS videos, news and other propaganda. In the light of the site's removal from the surface web, sites bearing this name and containing extremist material have been observed on the Darknet.

Jihad: literally translates as "struggle"; interpretations range from a personal effort to live according to Islam to defending Islam by means of an armed struggle, and physically fighting in the way of Allah in order to establish Islam. In the context of this report (unless stated otherwise), jihad should be taken to mean "armed struggle".

Jihadism: Non-state violence used in the cause of Islamism. Just as Islamism is the politicisation of Islam, jihadists take the traditional concept of *jihad* and use it as a political and military tool to achieve a political end.

Kafir (pl. *kaffir* or *kuffar*): "non-believer" (referring to non-Muslims); the term could also be used derogatorily to suggest a (Muslim or non-Muslim) person's disbelief in God and/or denial of truth.

[4] Adapted from Bewley, A., *Glossary of Islamic Terms* (London: Ta-Ha Publishers, 1998).

Khilafa / *Caliphate*: Islamic state; an expansionist state governed by a *khalifa* and implementing sharia as state law.

Khalifa / *Caliph*: the ruler of a caliphate.

Kufr: disbelief.

Mujahid (pl. *mujahideen*/*mujahidin*): a person who takes part in *jihad* as armed struggle.

Shahada: one of the five pillars of Islam; used for legal testimony in a court of law, means bearing witness – in most cases that there is no God but Allah, and that Mohammed is the messenger of Allah; can also mean "martyrdom".

Shamikh: translates as "glory" or "highness". In the context of this report, a password-protected *jihadist* messaging forum used by Islamic State and Al-Qaeda supporters and members primarily concerned with the jihadist struggle in Syria.

Shahid / *Shaheed*: a witness, someone who testifies; can also mean a martyr who dies fighting in the way of Allah.

Sharia/*Shariah*: literally translates as "road"; the Muslim religious code of conduct; a range of diverse traditions and interpretations of Islamic jurisprudence, from strict rules to broad principles and objectives.

Introduction

While encryption, the Darknet, and cryptocurrencies have a key role to play in protecting the civil liberties of many individuals, they are frequently used for criminal purposes. This report assesses how new technologies are used by criminals, extremists, and terrorists. First, it examines how encrypted communication systems are used to secure anonymity when planning for acts of terror. Second, it studies how the Darknet is used for operational purposes (for raising funds and to secure illicit goods such as forged documents and weapons). Finally, it studies the way in which terrorists and other criminal entities have benefited from the use of cryptocurrencies.

The British government has devoted greater attention to the presence of online extremism, especially following the five terror incidents that occurred in 2017 alone. However, this report makes a strong case for more attention to be paid to the Darknet – portions of the internet that are not easily accessible by the public at large without dedicated expertise. This report demonstrates that terrorists and extremists can utilise the Darknet to mask their communication and propaganda efforts, to recruit and radicalise, and to gain material benefits in the form of illicit goods, such as weapons and fraudulent documents. In addition, the report notes the growing tendency of individuals to utilise cryptocurrencies for transactions and fundraising, enabling them to evade detection by law enforcement entities. This paper relies on case studies based on publicly available information to indicate broader themes. In addition, primary research and analysis was undertaken on the Darknet itself.

The first chapter differentiates between the surface web, which is used by all internet users, the deep web, which are areas of internet sites only accessible to certain users, and the Darknet, which contains hidden sites that can be accessed with specialist expertise. It also provides an assessment of the Darknet browser The Onion Router (Tor).

The second chapter notes the capacity of terrorist groups to utilise encrypted messaging services such as Telegram, as well as to communicate within the Darknet, to maintain anonymity. It highlights the way that this secrecy often enables radicalisation, recruitment, and the spread of propaganda. Case studies are used to highlight potential trends.

Chapter three looks at the way terrorists can use the Darknet to gain material advantages – often in the form of financial contributions, fraudulent documents, weapons, and paramilitary training.

Chapter four examines the use of cryptocurrencies, in particular the way in which cryptocurrencies have been, and could be, utilised by terrorist groups. It compares the emergence of these financial instruments and the crypto-financial system with the *hawala* system of finance, an informal system of payments used to send money primarily to the Middle East, Africa, and South Asia. Special attention is given to bitcoin and the emergence of other cryptocurrencies.

Such findings, although preliminary, present an interesting conundrum: while the Darknet is used to protect privacy advocates, whistle-blowers, and human rights activists, it also provides a dangerous platform for those engaging in illicit activities by granting them anonymity through encryption. This report ends by making several key policy recommendations for government regulation, and for further intelligence building to better understand the Darknet and its use by terrorist organisations.

Limitations of Research

A large portion of the evidence connecting the Darknet to extremism and terrorism in this report is anecdotal in nature. Organised crime on the Darknet is, however, widespread. While this report highlights a number of cases where IS members or supporters have used the Darknet or cryptocurrency to further a terrorist agenda, these technologies have not yet been embraced by any terrorist group on an organisational level. Nevertheless, the anonymity granted by the Darknet, combined with the services offered on its marketplaces, remains of great interest to both technologically savvy terrorists and aspiring terrorists.

This report therefore serves to demonstrate how the Darknet represents a medium through which terrorists can anonymously proselytise, socialise, consume illegal content, and purchase illegal goods with confidence that they will not be identified or caught.

This paper does not suggest that terrorists are using technologies like Tor and bitcoin on a mass scale. Rather, it uses terrorist and criminal case studies to demonstrate how, if not effectively addressed, these technologies are likely to continue to serve as facilitators of both crime and terrorism. Given that these are relatively “young” and growing areas of interest, these trends are likely to worsen in the future if appropriate policy is not implemented.

As access was granted to intelligence officials working on the Darknet in the UK, this study is limited primarily to analysis in the UK, and includes US case studies mentioned by UK intelligence officials. Analysis of law enforcement agencies in Europe and worldwide would be an important area for future research.

Both the analysis and the resulting policy recommendations in this report are limited by the strict vetting procedures regarding freedom of information on the investigative methods used by law enforcement in the US and UK, particularly in cases where hacking or malware appear to have been used by authorities. However, this limitation has been overcome, where possible, through the analysis of publicly available court transcripts and through conversations with officials working on the Darknet at the National Crime Agency (NCA) and SO15 Counter Terrorism Command.

Methodology

Research for this report was formed through an analysis of academic literature and open-source material on terrorism, cryptocurrency, and organised crime on the Darknet. An extensive study of publicly available British and US court cases that resulted in the conviction of individuals providing material support for terrorism, often through criminal activity on the Darknet, was also conducted. This was coupled with an investigation into the dissemination of terrorist propaganda, financing, and criminal activity on Darknet marketplaces.

Primary sources for the report include statements by policymakers and law enforcement officials on relevant case studies, as well as primary research conducted on Darknet cryptomarkets where accounts were created to understand the availability of extremist content and instructional manuals. In January and February 2018, conversations with the NCA helped guide researchers to marketplaces on the Darknet. Accounts were created to browse marketplaces rated on the website "Deep Dot Web" by "Invite/Referral", "Specific Language or Country" and "Dead/Scam Markets": these yielded the sites Libertas Market, Wall Street Market, Dream Market, and Berlusconi Marketplace. Content searches were then carried out on the marketplaces using key words such as "extremist", "bombs", "fake documents British", "jihadist", "security", and other iterations of the above. Where relevant, the total number and availability of results were noted to add to trends observed. Proselytisation and fundraising by extremist groups on social media were also analysed to understand the availability of extremist material on the surface web.

Secondary sources used include reports from academic institutions and international law enforcement agencies such as Europol. Indictments and publicly available documents of offenders were used to understand and illustrate how individuals committing crimes on the Darknet were captured. Court transcripts were also utilised to understand how Darknet marketplaces were identified and closed by intelligence agencies (see Case Studies of Silk Road 1.0, Silk Road 2.0, and Playpen included in the report). Other secondary material includes media and newspaper reports pertaining to terrorism and organised criminality on the Darknet.

Chapter 1: Surface Web, Deep Web, and Darknet

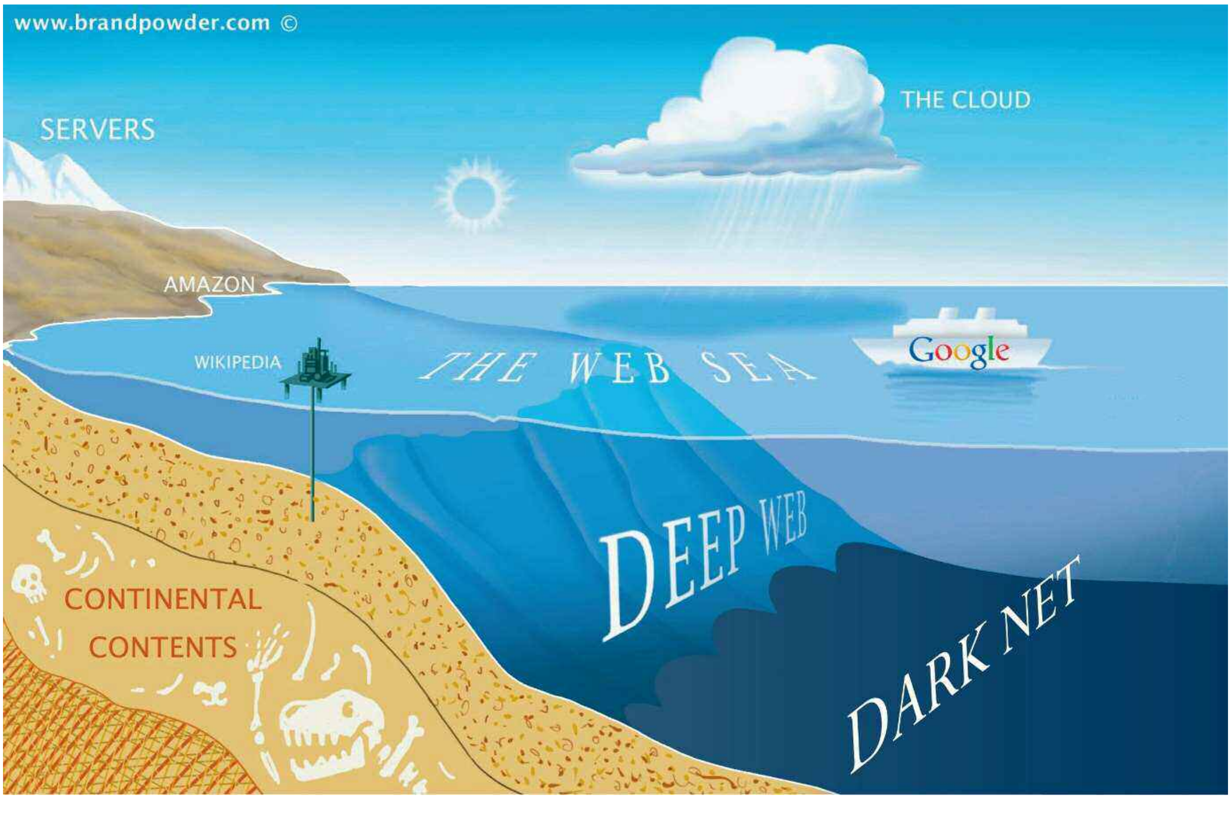
The following chapter differentiates between the surface web, used by all internet users, the deep web, areas of internet sites only accessible by certain users, and the Darknet, hidden sites that can only be accessed with specialist expertise. This chapter also provides an assessment of the Darknet browser The Onion Router (Tor).

What is the Surface Web? How Does it Differ from the Deep Web?

The surface web, the part of the internet most familiar to everyday users, contains information and websites that are accessed by using standard search engines such as Yahoo, Google, or Bing.[5] Information obtained from these sites is visible to those who want to see it, without any restrictions.

The deep web is approximately 400 to 500 times larger than the surface web.[6] As a result, it holds 400 times more content: 7,500 terabytes of information compared to 19 terabytes on the surface web.[7] In terms of documents, there are approximately 550 billion documents on the deep web (made up of social media pages, email domains, and online banking data), compared to one billion documents available on the surface web.[8] In short, the deep web is the depth of the sea, compared to the surface (see Figure 1).

<u>Figure 1</u>: Surface web, deep web, Darknet



Source: Reproduced and modified with permission from Brandpowder

Unlike the surface web, the deep web has certain user restrictions when it comes to access. Though internet users use the deep web regularly, its data is generally only accessible through application programming interfaces (APIs) in which the user is granted access to the required database.[9] Internet sites

[5] Chertoff, M., 'A public policy perspective of the Dark Web', *Journal of Cyber Policy* Vol. 2 (1), (2017): pp. 26-38, last visited: 5 October 2017, p. 26.
[6] Bergman, M. K., 'White Paper: The Deep Web: Surfacing Hidden Value', *Journal of Electronic Publishing* 7.1 (2001), last visited: 24 October 2017.
[7] ibid.
[8] ibid.
[9] Chertoff, M., op. cit., p. 27, last visited: 14 March 2018.

such as Facebook, Twitter or Snapchat, for example, as well as file-sharing services such as Dropbox, Google Drive, Webmail, and online banking pages, are part of the deep web because they require verified logins to clear a level of security before access is granted.[10]

The Darknet

The Darknet exists within the deep web. Although the two are often confused, the Darknet is even harder to access, is largely unregulated and contains a smaller portion of information stored on the internet.[11] It is effectively a repository of "hidden" sites accessible through uniquely downloadable software programmes that support encryption.[12] The deep web accounts for an estimated 90% of content hosted on the internet, while the Darknet accounts for approximately 0.01%.[13] However, since 2014, research points to an increased amount of data being hosted on the Darknet – from 10,000 websites in 2014 to 30,000 websites in 2015.[14] To date, there is no exact figure on the number of sites hosted on the Darknet, which is an area for further research. However, studies indicate that content on Darknet sites ranges from secret files of journalists, conversations between human rights activists, illicit trading sites and images of child pornography to terrorist sites that proselytise violent extremist viewpoints.[15] Several terms are used to refer to the Darknet, including "the dark web" and "the black net". For the purpose of this report, the term "Darknet"[16] is employed to refer to these largely unregulated parts of the internet.

Encryption

Encryption is the process of encoding information using mathematical algorithms, ensuring that communication is obfuscated to protect against unauthorised access.[17] Encrypted content is wrapped in layers of coded information, preventing third party access until the data reaches its intended destination. By doing this, encryption protects the identity of both the sender and the receiver.[18] Encryption is widely supported in email correspondence, on messaging applications such as WhatsApp and Telegram, and in online banking.

To access the Darknet, unique downloadable software programmes that support encrypted channels must be used. Darknet software programmes hide a computer's Internet Protocol (IP) address in various layers of encrypted web traffic,[19] much like the layers of an onion. Encrypted data is moved through randomly selected computers across a network, known as relay computers, and channelled through a series of passages called "nodes".[20] Each node only reveals the destination of the next computer.[21] The last node is revealed when the message arrives at its intended destination (see Figure 2). These special browsers generally allow users to access Darknet websites securely, without being identified, monitored or traced.

[10] Chertoff, M., op. cit., p. 27, last visited: 14 March 2018; Egan, M., 'What is the Dark Web, What is the Deep Web? How to Access the Dark Web', *Tech Advisor*, 10 January 2018, available at: http://www.techadvisor.co.uk/how-to/internet/dark-web-3593569/ , last visited: 14 March 2018.

[11] Egan, M., op. cit.

[12] Moore, D. and T. Rid, 'Cryptopolitik and the Darknet Survival' *Survival: Global Politics and Strategy* Vol. 58 (1), (2016): pp. 7-38. Encryption is understood as the act of "scrambling communication to prevent access to others apart from the intended recipient". For more, see: Titcomb, J., 'What is encryption, how does it work and what apps use it?', *The Telegraph*, 29 March 2017, available at: http://www.telegraph.co.uk/technology/0/encryption-should-using/, last visited: 14 March 2018.

[13] Chertoff, M., op. cit., p. 27; Greenberg, A., 'Hacker Lexicon: What is the Dark Web?', *Wired*, 19 November 2014, available at: https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/, last visited: 14 March 2018.

[14] Greenberg, A., op. cit.; Cox, J., 'The dark web as you know it is a myth' *Wired*, 18 June 2015, available at: https://www.wired.com/2015/06/dark-web-know-myth/, last visited: 14 March 2018.

[15] See, for example: Murray, A., 'The dark web is not just for paedophiles, drug dealers and terrorists', *Independent*, 12 December 2014, available at: http://www.independent.co.uk/voices/comment/the-dark-web-is-not-just-for-paedophiles-drug-dealers-and-terrorists-9920667.html, last visited: 14 March 2018; Chen et al., 'Uncovering the dark Web: A case study of Jihad on the Web', *Journal of the Association for Information Science and Technology*, Vol. 59(8) (2008), pp. 1347-1359; Crawford, A. 'Dark net "used by tens of thousands of paedophiles"', *BBC News*, 19 June 2014, available at: http://www.bbc.co.uk/news/technology-27885502, last visited: 14 March 2018.

[16] There is some disagreement over the terms 'Darknet' and 'Dark Net'. Some believe that the former refers to all encrypted networks while the latter is used specifically to refer to The Onion Browser (Tor) network.

[17] Titcomb, J., 'What is encryption, how does it work and what apps use it', op. cit.

[18] Murgia, M., 'WhatsApp adds end-to-end encryption: What is it and what does it mean for you?' *The Telegraph*, 6 April 2016, available at: http://www.telegraph.co.uk/technology/2016/04/05/whatsapp-encryption-what-is-it-and-what-does-it-mean-for-you/, last visited: 14 March 2018.

[19] Greenberg, A., op. cit.

[20] Greenberg, A., op. cit.; Goldschlag, D., M. Reed and P. Syverson, 'Onion Routing for anonymous and private internet connections', *Communications of the ACM* Vol. 42(2) (1999): pp. 1-5, p. 2. A relay computer is a publicly listed Tor node that forwards users' web traffic. For more, see: 'Glossary', *Tor Metrics*, 2017, available at: https://metrics.torproject.org/glossary.html#directory-authority, last visited: 14 March 2018.

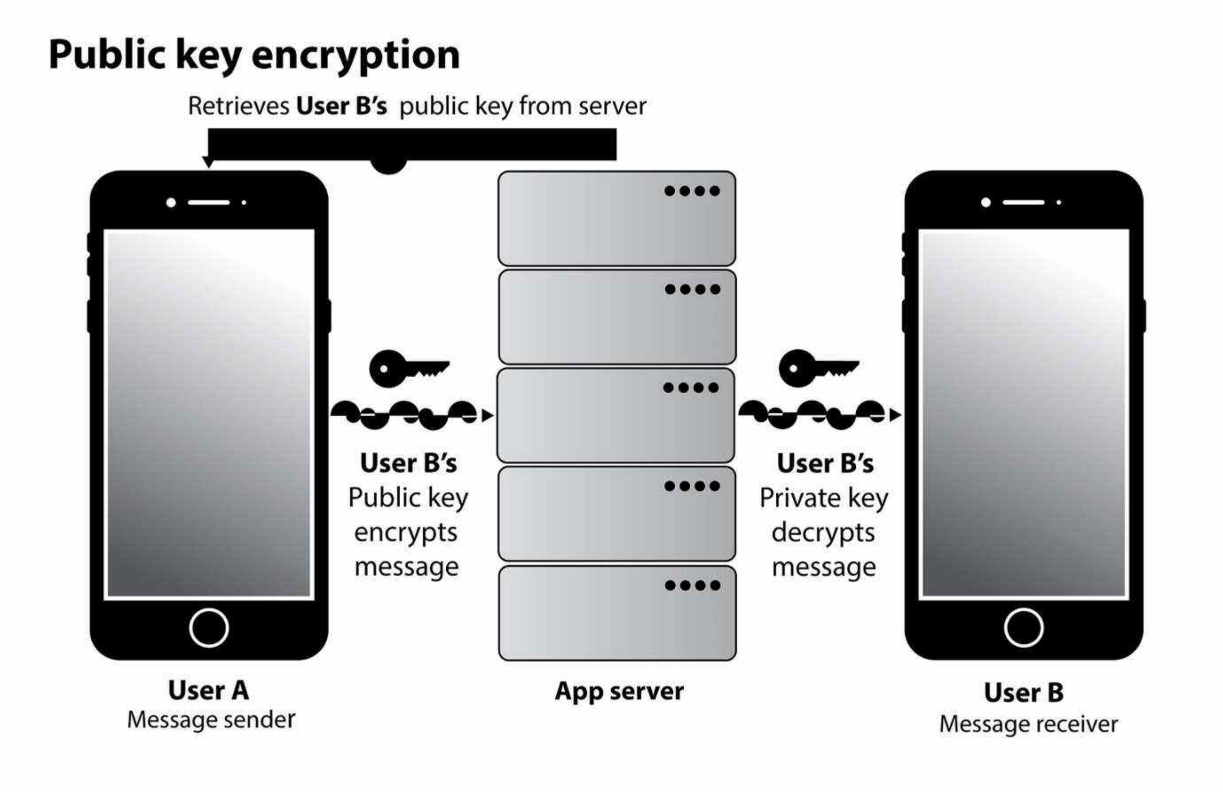
[21] Goldschlag, D., M. Reed and P. Syverson, op. cit., pp. 1-2.

As a result, the Darknet is shrouded in secrecy and anonymity, making efforts by law enforcement to counter criminality more difficult.

Public Key Encryption and Asymmetric Cryptography

Public key encryption or asymmetric cryptography was pioneered by the UK's Government Communications Headquarters (GCHQ), who first conceived of the "possibility of secure non-secret digital encryption".[22] Public key cryptography is characterised by the use of a pair of keys: a public and a private key, associated with an "entity that needs to authenticate its identity electronically or to sign or encrypt data".[23] While public keys can be widely disseminated, their corresponding private keys are kept secret and known only to individual computers. In this way, the public key is used to encrypt data which can only be decrypted with its corresponding private key.[24]

Figure 2: Encryption


Public key encryption
Retrieves User B's public key from server
User B's Public key encrypts message
User B's Private key decrypts message
User A
Message sender
App server
User B
Message receiver

Source: Modified from Titcomb, J., 'What is encryption, how does it work and what apps use it?', *The Telegraph*, 29 March 2017, available at: http://www.telegraph.co.uk/technology/0/encryption-should-using/, last visited: 14 March 2018.

Public key encryption differs from symmetric key encryption in that two keys perform two separate and unique functions, as opposed to a unique key enabling both encryption and decryption. Prime factorisation often underpins asymmetric cryptographic algorithms, whereby the public key enabling encryption represents the product of two large prime numbers, and the secret key is the two prime numbers that allow decryption.[25] This type of cryptography is often used to secure communications data in open network, susceptible environments like the internet, to ensure that information remains confidential when in transit. It is considered an extremely secure encryption system when public keys are

[22] Lawson-Perfect, C., 'GCHQ has declassified James Ellis's papers on public key cryptography', *The Aperiodical*, 20 March 2016, available at: http://aperiodical.com/2016/03/gchq-has-declassified-james-elliss-papers-on-public-key-cryptography/, last visited: 14 March 2018.
[23] 'Public key cryptography', *IBM*, available at: https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.13/gtps7/s7pkey.html, last visited:14 March 2018.
[24] ibid.
[25] Mann, C., 'A Primer on Public-Key Encryption', *The Atlantic*, September 2002, available at: https://www.theatlantic.com/magazine/archive/2002/09/a-primer-on-public-key-encryption/302574/, last visited: 14 March 2018.

known to authentic users, and is widely used in Secure Socket Layer (SSL) or Transport Layer Security (TLS)[26] and Secure Shell (SSH)[27] protocols, digital signatures and digital currencies.

The Tor Network

A commonly used Darknet browser is the Tor network. Tor was created by the US Navy Research laboratory in the mid-1990s, to allow US military personnel to use the internet securely when stationed abroad.[28] In 2003, Tor was decommissioned for public use in a bid to anonymously mask US military traffic in a web of civilian users.[29] Following this decision, the network was made freely available to the public.

The Tor programme transmits information through the network of a computer by moving data through various "network relays" operated by volunteer computers around the world.[30] Tor provides anonymity by concealing a computer's identity and location, as well as anonymising visited websites and their operators.[31] This protective mechanism ensures that the identity of users and their computer servers remain anonymous in the event that either is being monitored.[32] Since 2003, the Tor network has gained popularity among users of the Darknet. As of November 2017, Tor had more than 3 million users directly connecting to the network, an increase compared to figures from October 2017, which registered 2.5 million direct users.[33] Further to this, in October 2017 there were approximately 40,000 domains hosted on the Tor network, which increased to just over 50,000 by November of the same year, indicating scalability.[34] These statistics display a growing usage of Tor for browsing anonymously and for hosting domains.

Freedom of Speech and Privacy

Tor has been adopted as a free service to encourage unrestricted access to the internet in societies with strict internet censorship, or where there is a significant threat of persecution for expressing views deemed illegal by repressive states. Against this backdrop, the Darknet has been used by many (including dissidents, human rights activists, and journalists) to ensure safe passage of information, given that the Darknet protects the identity of its users.[35]

Human rights activists throughout the Middle East have used the Tor network to communicate during state-sanctioned media censorship. During the 2011 Arab uprisings, Tor helped to connect people, foster communication, and disseminate information amid the clamour for democratic political transition in much of the Middle East. In Egypt, dissidents and sympathisers of the pro-democracy demonstrations actively used Tor to conceal their internet activity, owing to considerable online censorship by the

[26] Secure Socket Layer/Transport Layer Security protocols provide privacy and integrity of data, enabling "secure communications between clients and server applications" over unprotected networks such as the internet, becoming the "*de facto* standard for cryptographic protocols". See Hwang, J., 'The Secure Sockets Layer and Transport Layer Security, *IBM*, 6 June 2012, available at: https://www.ibm.com/developerworks/library/ws-ssl-security/, last visited: 14 March 2018.

[27] Secure Shell is a cryptographic network protocol used for operating network services securely over unsecured networks. It is used for the remote management of systems and applications, allowing network administrators to "log in to another computer over a network, execute commands and move files from one computer to another". See Rouse, M., 'Secure Shell (SSH)', *SearchSecurity*, March 2016, available at: http://searchsecurity.techtarget.com/definition/Secure-Shell, last visited: 14 March 2018.

[28] This occurred in partnership with organisations from the not-for-profit sector, including the Electronic Frontier Foundation, the Knight Foundation and the Swedish International Development Agency. A large proportion of funding was provided by the US Department of Defense and the US State Department. For more, see: Buxton, J. and T. Bingham, 'The Rise and Challenge of Dark Net Drug Markets', *Global Drug Policy Observatory*, Policy Brief No.7, Swansea University, 7 January 2015, available at: https://www.swansea.ac.uk/media/The%20Rise%20and%20Challenge%20of%20Dark%20Net%20Drug%20Markets.pdf, last visited: 14 March 2018, p. 5.

[29] Chertoff, M., op. cit., p. 27.

[30] 'Tor', *Tor Project*, available at: https://www.torproject.org/, last visited: 14 March 2018.

[31] Tor is often used for two differentpurposes. The first relates to the protection of the identity of users wishing to browse anonymously and the second is primarily to conceal the location of sites, forums and marketplaces that are hosted on the Darknet, referred to as "hidden services" with a domain name, such as an onion domain site. These two different but common uses of the Darknet ensure that a user's identity is concealed while browsing, and can protect the location of a site hosted on the Darknet. For more, see: Moore, D. and T. Rid, 'Cryptopolitik and the Darknet Survival', op. cit.

[32] Loesing, K., S. J. Murdoch and R. Dingledine, 'A case study on measuring statistical data in the Tor Anonymity Network', in *Financial Cryptography and Data Security* (eds. Sion, R., R. Curtmola, S. Dietrich, A. Kiayias, J. M. Miret, K. Sako and F. Sebé) (Spain: SpringerLink, 2010), pp. 203-215.

[33] 'Users', *Tor Metrics*, 2017, available at: https://metrics.torproject.org/userstats-relay-country.html, last visited: 14 March 2018.

[34] 'Users' *Tor Metrics*, op.cit.

[35] Moore, D. and T. Rid, 'Cryptopolitik and the Darknet Survival', op. cit., p. 17.

Mubarak regime. Tor was equally used by pro-democracy Syrian rebel groups to disseminate digital evidence of human rights violations taking place under the Assad regime in the early years of the Syrian conflict.[36]

In 2014, Facebook launched a version of its website on the Tor network for dissidents and activists in societies where access to Facebook is blocked, restricted or heavily monitored by the state. Facebook's Tor site now caters to more than a million users looking to maintain privacy and conceal evidence of digital footprints.[37] In October 2017, *The New York Times* announced the launch of an experimental version of its publication on the Tor network.[38] The news agency expressed the need for the service because some readers were blocked from accessing its surface web page. Others were heavily monitored or preferred to access the site anonymously.[39]

Case Study: Reporters Without Borders

One of the earliest advocates of Tor was Reporters Without Borders, an organisation promoting press freedom.[40] In 2008, Reporters Without Borders provided to foreign journalists reporting from China practical tips on installing Tor software before travelling to China, and encrypting emails with Pretty Good Privacy (PGP) to protect their online interactions. This was in response to a state-sponsored internet censorship programme maintained by the Chinese government to prevent users from using Tor, and against the backdrop of human rights abuses taking place during the Beijing Olympics.[41] The following year, China attempted to block the public relay computers that Tor employs to mask user identities, to disrupt the flow and spread of information on the network. In a counter-move, Reporters Without Borders provided 250 new relay computers to the Tor network, which were not made public, to prevent the Chinese government from blocking them.[42]

[36] ibid., p. 17.

[37] 'Tor's "dark web" enables Facebook access for more than a million people', *Firstpost*, 25 April 2016, available at: http://www.firstpost.com/tech/news-analysis/tors-dark-web-enables-facebook-access-for-more-than-a-million-people-3680645.html, last visited: 14 March 2018.

[38] Sandvvik, R., 'The New York Times is Now Available as a Tor Onion Service', *Times Open*, 27 October 2017, available at: https://open.nytimes.com/https-open-nytimes-com-the-new-york-times-as-a-tor-onion-service-e0d0b67b7482, last visited: 14 March 2018.

[39] ibid.

[40] 'Reporters Without Borders and Torservers.net, partners against online surveillance and censorship', *Reporters Without Borders*, 25 April 2014, updated 25 January 2016, available at: https://rsf.org/fr/actualites/reporters-sans-frontieres-et-torserversnet-partenaires-contre-la-surveillance-et-la-censure-en-ligne, last visited: 14 March 2018.

[41] Advice for foreign journalists covering human rights situation during Beijing Games', *Reporters Without Borders*, 30 July 2008, updated 20 January 2016, available at: https://rsf.org/en/news/advice-foreign-journalists-covering-human-rights-situation-during-beijing-games, last visited: 14 March 2018.

[42] 'Reporters Without Borders and Torservers.net, partners against online surveillance and censorship', op. cit.

Chapter 2: Terrorist Communication and Recruitment on the Darknet

This chapter illustrates the capacity of terrorist groups to utilise encrypted messaging services such as Telegram, as well as the Darknet, to maintain anonymity. It highlights how the secrecy encryption enables radicalisation and recruitment, as well as the dissemination of propaganda. Case studies are used to highlight potential trends.

The Use of Encryption by IS

Following Abu Bakr al-Baghdadi's declaration of a *caliphate* in July 2014, Islamic State (IS) flooded mainstream social media websites with content, hijacking otherwise unrelated Twitter "trending" topics and proselytising on Facebook and YouTube. Foreign fighters for IS would regularly update social media followers on their experiences as *mujahideen* (fighters) for IS in Syria and Iraq. While authorities and social media companies made some progress in recognising, responding to, and removing terrorist and extremist content on the surface and the deep web,[43] IS and its supporters responded to crackdowns by continuing to communicate on encrypted messaging applications. These applications are subject to less regulation and can protect communications from interception by authorities or security services.[44] This shift was recognised in the United Nations Security Council (UNSC) Report S/2017/97, which stated that "the internal communication and recruitment methods of [IS] are increasingly moving towards more covert methods, such as the use of the dark web, encryption and messengers".[45]

The military campaign against IS in Iraq and Syria[46] has forced IS and its followers to be more secretive and clandestine in their communications to ensure that their operatives are difficult to trace or locate. While continuing to rely on encrypted messaging programs such as Telegram, the Darknet has also been used by IS for radicalisation and propaganda purposes, as well as for direct recruitment to their cause.

Telegram

Telegram is an end-to-end encrypted messaging application that offers its users secure and anonymous data protection, including the option of a self-destruct timer that permanently deletes shared media and messages after they are viewed. Owing to the privacy offered by Telegram, the application has become an extremely popular platform for communication between IS members and supporters.[47]

Following the 2015 Paris attacks, for example, IS sent communicative feeds through the Rich Site Summary (RSS)[48] enabled feature of Telegram, reaching an estimated 20,000 people.[49] IS also shared a message on *Al-Hayat*, its official media centre, where it encouraged supporters to communicate on Telegram.[50] Adel Kermiche, one of the attackers who murdered an 85-year-old French priest in Saint-

[43] Berger, J. M. and H. Perez, 'The Islamic State's Diminishing Returns on Twitter: How suspensions are limiting the social networks of English-speaking ISIS supporters', *George Washington Program on Extremism*, February 2016, available at https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Berger_Occasional%20Paper.pdf, last visited: 15 March 2018; Kahn, J., 'Facebook Says 99% of IS, Al Qaeda Content Spotted by AI', *Bloomberg*, 29 November 2017, available at: https://www.bloomberg.com/news/articles/2017-11-29/facebook-says-99-of-is-al-qaeda-content-spotted-by-ai, last visited: 15 March 2018; 'Google Pledges 10,000 staff to tackle extremist content', *BBC News*, 5 December 2017, available at: http://www.bbc.co.uk/news/technology-42232482, last visited: 15 March 2018.

[44] Bloom, M., H. Tiflati and J. Horgan, 'Navigating ISIS's Preferred Platform: Telegram', *Terrorism and Political Violence* (2017): pp. 1-13, p. 1.

[45] 'Fourth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat', S/2017/97, *UN Security Council*, 2 February 2017.

[46] The Iraqi city of Mosul and the Syrian city of Raqqa were IS strongholds from 2014 onwards; the latter city was declared by IS as its de facto capital. After months of intensive fighting by the Iraqi army and its allies, the city of Mosul was declared liberated from IS by Iraqi Prime Minister Haider Al-Abadi on 9 July 2017. The Syrian Democratic Forces, supported by the United States, declared Raqqa to be liberated from IS on 17 October 2017.

[47] Burke, J., 'The Age of Selfie Jihad: How Evolving Media Technology is Changing Terrorism', *CTC Sentinel*, Vol. 9(11) (2016): pp. 16-22.

[48] RSS is a type of web feed where online content is presented to the user in a digestible format. These feeds allow users to keep up to date with the posts of a number of different users in a single aggregator.

[49] Ragan, S., 'After Paris, ISIS moves propaganda machine to Darknet', *CSO*, 15 November 2015, available at: https://www.csoonline.com/article/3004648/security-awareness/after-paris-isis-moves-propaganda-machine-to-darknet.html, last visited: 15 March 2018.

[50] ibid.

Etienne-du-Rouvray, Normandy, in July 2016, had been an avid user of Telegram. He posted multiple audio messages to his followers on the app about his failed attempt to travel to Syria to join IS and indicating his intention to carry out an attack at home in France. Before the attack, Kermiche shared a video of himself and a fellow attacker pledging allegiance to the group, which was subsequently rebroadcast by IS' official *Amaq* news agency, using Telegram. Kermiche reportedly forced a hostage in the church to film the proceedings on their smartphone, with the intention of uploading the footage – though he was shot dead by French police before he could do so.[51]

In August 2017, British authorities reported the conviction of Naweed Ali, Khobaib Hussain, Mohibur Rahman, and Tahir Aziz for plotting to commit a Lee Rigby-style[52] terrorist attack (the modus operandi of which involves running over an individual with a vehicle and then stabbing them), specifically targeting members of the armed forces.[53] The men had reportedly used Telegram to communicate and were apprehended with deadly weapons in their possession, including an incomplete pipe bomb, a pistol, a samurai sword, and a meat cleaver with the word *kafir* (unbeliever) inscribed on it.[54] These men had joined extremist social media groups online and engaged with violent material with the intention of committing a deadly act of terror.[55] The Crown Prosecution Service (CPS) stated that "these men shared the same radical belief in violent jihad and had reached a stage where they were planning to take action".[56]

In January 2018, four teenagers were sentenced to jail for committing acts of terrorism. Ahmedeltigani Alsyed, his brother Yusef Alsyed of Feltham, Middlesex, and two others had contacted a "terrorist fixer" to purchase tickets to Turkey.[57] The suspects were found with camp gear and kitchen knives in their possession.[58] It was alleged that they discussed how to join a terrorist group in 2016 by communicating on Telegram under the group name "Peace". They were convicted for preparing acts of terrorism and distributing terrorist-related material.[59]

Use of the Darknet

Like Telegram, the Darknet is an encrypted platform that IS and its affiliates use for communication purposes. Following the 2015 attacks in Paris, a new IS propaganda hub was found on the Darknet by researcher Scot Terban (aka "@krypt3ia"),[60] who reportedly made the discovery via a message on the *Shamikh* forum, a known jihadist messaging board. The post detailed an address for the new website and instructions on how to reach it. On the site were translations in English, Turkish and Russian of claims by *Al-Hayat* of the attacks in Paris, and a selection of propaganda videos and images.[61]

The issue of terrorist communication on encrypted sites has been raised by several governments, and was brought to light following the 2015 San Bernadino terrorist attack. Following their deaths, the seizure of suspects Syed Farook and Tashfeen Malik's electronic devices revealed the use of encrypted messaging

[51] Burke, J., op. cit., p. 20.

[52] Dodd, V. and A. Ross, '"Three musketeers" convicted of plotting terrorist attack', *The Guardian*, 2 August 2017, available at: https://www.theguardian.com/uk-news/2017/aug/02/three-musketeers-convicted-of-plotting-terrorist-attack, last visited: 15 March 2018. In May 2013 in Woolwich, London, British Army soldier Fusilier Lee Rigby of the Royal Regiment of Fusiliers was run over and then stabbed by two Islamist extremists outside Woolwich barracks. For more, see: 'Return to old-style terror', *The Economist*, 25 May 2013, available at: https://www.economist.com/news/britain/21578453-shocking-killing-reminder-disorganised-jihadists-are-harder-stop-organised, last visited: 15 March 2018.

[53] Dodd, V. and A. Ross, op. cit.

[54] '"Three Musketeers" guilty of planning UK terror plot', *BBC News*, 2 August 2017, available at: http://www.bbc.co.uk/news/uk-40802787, last visited: 15 March 2018. *Kafir* is an Arabic term meaning "one who covers the truth", referring to those who reject or who do not believe in God according to the teachings of the Prophet Muhammad. It can also be translated as "infidel" or "unbeliever". Islamist extremists use the word as a derogatory reference to anyone who they regard not to be a "true" Muslim and who is, therefore, deserving of death.

[55] 'Gang guilty of planning UK terror attack', *Crown Prosecution Service*, 2 August 2017, available at: http://www.cps.gov.uk/news/latest_news/gang-guilty-of-planning-uk-terror-a/index.html, last visited: 15 March 2018.

[56] ibid.

[57] 'Michel Massih QC And Zarif Khan Act In Terrorist Plot Trial', *Drystone Chambers*, 12 January 2018, available at: https://drystone.com/news/michel_massih_qc_and_zarif_khan_act_in_terrorist_plot_trial/, last visited: 15 March 2018.

[58] ibid.

[59] ibid.

[60] Paganini, P., 'A few hours after the Paris attacks, a new ISIS propaganda hub appeared on the Darknet', *Security Affairs*, 16 November 2015, available at: http://securityaffairs.co/wordpress/42022/intelligence/paris-attacks-darkweb-hub.html, last accessed: 15 March 2018.

[61] Paganini, P., op. cit.

systems within their Apple iPhones,[62] which resulted in a significant legal dispute over encryption between law enforcement and Apple.[63] In a 2015 speech to the US Senate Judiciary Committee, former FBI Director James Comey argued that terrorists who communicate on encrypted messaging platforms are protected because "increasingly, we are unable to see what they say, which gives them a tremendous advantage against us".[64]

In the UK, similar concerns have been raised about the misuse of encrypted messaging. Following the Westminster attack in 2017, Home Secretary Amber Rudd reiterated the need for government access to encrypted services to protect the public, stating that "we need to make sure that organisations like WhatsApp, and there are plenty of others like that, don't provide a secret place for terrorists to communicate with each other",[65] with the aim of intercepting planned terrorist attacks and infiltrating possible terror-cell networks. Following the UK's most recent attacks, the Director General of The Security Service (MI5), Andrew Parker, noted in October 2017 that technological advancements have an "unintended side-effect" which "aid the terrorists, whether it's the ease of online purchasing, social media content or encrypted communications".[66] A balance must be struck, therefore, between protecting the communication and privacy of ordinary citizens and reducing opportunities for encryption to be exploited for criminal purposes. Largely in response to these trends, British police started a campaign in 2017 to inform the public about the dangers of visiting the Darknet, stating that it is a site used to smuggle firearms, raise funds for terrorists, assist terrorists and criminals in their communications, and recruit members into criminal and terrorist networks.[67]

While calls have been made by governments to allow "backdoors"[68] to encryption in apps such as Telegram, the privacy offered by the app is an essential part of its brand.[69] Criticisms concerning allowing security services access to private communications have included the idea that criminals and terrorists can use other, rival programmes that offer more privacy for their communications. However, it is clear that mechanisms such as infiltration, sting operations and user records of points of sale (see Figure 1) – which have been used successfully in the past to capture criminals purchasing drugs and firearms – can also be used to study terrorist communications and recruitment.

Radicalisation

The internet can be used to expose potential recruits repeatedly to extremist content.[70] A recent report published by The Henry Jackson Society found that in more than a third (35%) of the 269 total Islamist-related offences researched, the internet was cited as a major site for offenders' engagement with extremism.[71] Almost one in ten (9%) of Islamist related offences were committed by individuals who were known to have watched beheading videos.[72] Instructional material such as the *Mujahideen Poisons Handbook*, which details how to make and use explosives and firearms as well as plan and carry out

[62] Ahmed, S. 'Who were Syed Rizwan Farook and Tashfeen Malik?' *CNN*, 5 December 2015, available at: https://edition.cnn.com/2015/12/03/us/syed-farook-tashfeen-malik-mass-shooting-profile/index.html, last visited: 15 March 2018.

[63] Rubin, J., J. Queally and P. Dave, 'FBI unlocks San Bernadino shooter's iPhone and ends legal battle with Apple, for now', *Los Angeles Times*, 28 March 2016, available at: http://www.latimes.com/local/lanow/la-me-ln-fbi-drops-fight-to-force-apple-to-unlock-san-bernardino-terrorist-iphone-20160328-story.html, last visited: 15 March 2018.

[64] Thomas, P., 'Feds Challenged by Encrypted Devices of San Bernardino attackers', *ABC News*, 9 December 2015, available at: http://abcnews.go.com/US/feds-challenged-encrypted-devices-san-bernardino-attackers/story?id=35680875, last visited: 15 March 2018.

[65] 'Terrorists use the Dark web to hide', *Press From*, 28 March 2017, available at: http://us.pressfrom.com/news/science-and-technology/-35619-terrorists-use-the-dark-web-to-hide/, last visited: 15 March 2018.

[66] Dodd, V., 'UK facing most severe terror threat ever, warns MI5 chief', *The Guardian*, 17 October 2017, available at: https://www.theguardian.com/uk-news/2017/oct/17/uk-most-severe-terror-threat-ever-mi5-islamist, last visited: 15 March 2018.

[67] 'Visiting the darkweb is a sign of terrorism, warns U.K [sic] police', *Deep Dot Web*, 6 July 2017, available at: https://www.deepdotweb.com/2017/07/06/visiting-darkweb-sign-terrorism-warns-u-k-police/, last visited: 15 March 2018.

[68] Haynes, J., 'Backdoor access to WhatsApp? Rudd's call suggests a hazy grasp of encryption', *The Guardian*, 27 March 2017, available at: https://www.theguardian.com/technology/2017/mar/27/amber-rudd-call-backdoor-access-hazy-grasp-encryption, last visited: 15 March 2018.

[69] 'Telegram FAQ', *Telegram*, available at: https://telegram.org/faq, last visited: 15 March 2018.

[70] For example, after being shut down by Godaddy and Google for violating the terms of agreement, a major neo-Nazi and white supremacist site called The Daily Stormer moved to the Darknet. See more in: 'After being shut down by Google and Godaddy, major Neo-Nazi site moves to the darknet', *Deep Dot Web*, 31 August 2017, available at: https://www.deepdotweb.com/2017/08/31/shut-google-godaddy-major-neo-nazi-site-moves-darknet/, last visited: 15 March 2018.

[71] Stuart, H., 'Islamist Terrorism: Key Findings and Analysis', *The Henry Jackson Society* (2018, Publication Pending), p. 18.

[72] ibid., p. 11.

assassinations and other terrorist acts, do appear on the surface web. However, any copies of such material are, in theory, subject to removal by internet companies such as Google as part of their crackdown on online extremist content.[73] Darknet websites are, by definition, not privy to the same level of monitoring or regulation, so individuals seeking this content for terrorist purposes are provided with a reliable space to access it.[74]

It is important to note that terrorist forums on the Darknet not only encourage individual radicalisation, but also promote a "self-starter" type of terrorism.[75] This is a strategy endorsed by IS both online and offline, and motivates vulnerable individuals to commit violence in the organisation's name in an attempt to "crowdsource" terrorism.[76] A pertinent example highlighting how the Darknet plays a contributory factor in radicalisation involves the case of US resident Noelle Velentzas, of Puerto Rican and Greek heritage.[77] In 2015, Velentzas was arrested by US law enforcement for conspiracy charges and distributing information detailing how to make a weapon of mass destruction,[78] to which she pled not guilty.[79] It is believed that Velentzas was self-radicalised and had expressed the belief that launching terrorist attacks in the US would be more beneficial to the "global jihadi" than travelling to Syria or Iraq.[80] Velentzas had been exposed to numerous violent extremist materials online, had watched YouTube videos of IS beheading Syrian soldiers, watched suicide bombings, and learned how to use the Darknet to assist in her radicalisation process.[81] Another example is Roshonara Choudhry, who was sentenced to life imprisonment in the UK for stabbing MP Stephen Timms in 2010. Choudhry had been radicalised by internet sermons by Anwar al-Awklaki, an infamous Islamist preacher whose videos have now been removed by platforms like YouTube. These cases, including more recent court cases on individuals who have been prevented from joining Islamic State, such as Tower Hamlets v. B,[82] illustrate the dangers of self-radicalisation on the internet.

Case Study: Tower Hamlets v. B

A recent case in the UK Royal Courts of Justice involved the radicalisation of a 16-year-old girl through the surface web and Darknet over a period of seven months in 2014, culminating in her attempted flight to Syria to join IS.[83] "B" (her name has been kept secret to protect her and her family) grew up in a Muslim household in London along with five siblings. Unlike her siblings, B was home-schooled by their mother, who has been described as extremely pious and controlling. B was not allowed out of the house unaccompanied.[84] Unlike the rest of her family, who enjoyed outdoor sports and activities, B was described as "bookish".[85] Indeed, though B attempted to recruit her sister, her sister was active in sports

[73] An online copy of the *Mujahideen Poisons Handbook* was identified by researchers at The Henry Jackson Society as the first result of a Google search on 14 December 2017, and reported on that day. By 20 December 2017 the same file could no longer be located through the same Google search. However, PDPs of the document were available on the second page of a Google search on 12 January 2018, hosted on Wordpress websites such as 'shariaunveiled'. Page 3 of the search revealed two direct links to the handbook, and there was a series of quotes and links to the handbook on the site Pinterest.

[74] Berton, B., 'The dark side of the web: ISIL's one stop shop?', *European Union Institute for Security Studies*, 26 June 2015, available at: https://www.iss.europa.eu/content/dark-side-web-isil%E2%80%99s-one-stop-shop, last visited: 15 March 2017, p. 1.

[75] Bloom, M., H. Tiflati and J. Horgan, op. cit., p. 9.

[76] Webb, S., 'Daesh in the digital age: online extremism and the new Terror', *The Mackenzie Institute* (2016), available at: www.academia.edu/30413200/DAESH_IN_THE_DIGITAL_AGE_ONLINE_EXTREMISM_AND_THE_NEW_TERROR, last visited: 15 March 2018.

[77] Simcox, R., '"We will conquer your Rome": A study of the Islamic State Terror Plots in the West', *The Henry Jackson Society* (2015), available at: http://henryjacksonsociety.org/wp-content/uploads/2015/09/ISIS-brochure-Web.pdf, last visited: 15 March 2018, pp. 25-26.

[78] Sanchez, R., 'N.Y. women accused of ISIS-inspired bomb plot plead not guilty', *CNN*, 7 May 2015, available at: http://edition.cnn.com/2015/05/07/us/new-york-terror-court-pleas/index.html, last visited: 15 March 2018.

[79] ibid.

[80] Simcox, R., op. cit., p. 26; Sanchez, R., op. cit.

[81] Simcox, R., op. cit., p. 26; *US v. Noelle Velentzas and Asia Siddiqui*, Complaint and Affidavit in Support of Arrest Warrants, *United States District Court Eastern District of New York*, April 2015, available at: https://extremism.gwu.edu/sites/extremism.gwu.edu/files/Velentzas%20and%20Siddiqui%20Criminal%20Complaint%2C%20Affidavit.pdf, last visited: 15 March 2018, pp. 11-12. Referred to as "dark internet" in the complaint document.

[82] *London Borough Tower Hamlets v. B*, UK Royal Courts of Justice [2016] EWHC 1707 (Fam), available at: https://www.judiciary.gov.uk/wp-content/uploads/2016/07/lbth-v-b-160713.pdf, last visited: 15 March 2018.

[83] ibid.

[84] ibid., paras. 132, 149.

[85] ibid., para. 96.

and other activities outside the house, and was therefore less susceptible to radicalisation. Following the 2014 events in Gaza – specifically the killing of civilians – B became interested in more extremist views of Islam. Her father would often show his children images and videos of Muslims being killed,[86] and neither parent took steps to monitor B's internet access. B also had access to her father's computer, which contained IS propaganda and other such material.

Subsequently, B began accessing material on recruitment to jihad through the Darknet, taking steps to hide her online presence: B cleared her data and browsing history via a CC cleaner and used a 16-digit alphanumeric password.[87] (A summary of the material she accessed can be found in Appendix 1.) In her testimony, B described herself as "addicted"[88] to IS material and numb to images of brutality and death. B eventually encountered recruiters via the online platform Kik,[89] after which she made plans to fly to Syria, as she wanted to live under *sharia*, understanding this as the best way to be a good Muslim.[90] She got as far as boarding the plane.

This case serves to highlight how a young girl was easily radicalised through recruitment on the Darknet. While there are confounding factors to her radicalisation that were not present for her siblings, the ease with which she was able to access jihadist propaganda material is a clear and pertinent factor.

Propaganda

IS' online messaging campaign has been amplified by use of an army of so-called "media *mujahideen*". These IS-supporting internet users meticulously share and repost official content across a number of social media platforms, as part of a coordinated effort to maximise the organisation's impact and relevance, and to assist in recruitment to the group.[91] Efforts have been made by social media companies, including Twitter, Facebook and YouTube, to disrupt the proliferation of terrorist propaganda,[92] and in its most recent annual report, Europol stated that this had resulted in the volume of messaging gradually decreasing on the surface web.[93]

Given the inaccessible nature of encrypted channels like Telegram and areas of the Darknet, it is perhaps unsurprising that mass recruitment rarely takes place on these channels. Instead, IS aims to draw interested sympathisers from the surface web and social media into the more secure recesses of the Darknet for further interaction and indoctrination. In 2015, for example, *Al-Hayat* posted a link accompanied by a detailed explanation on how to get to its new Darknet site on a forum associated with the group.[94] Links to the site were also published by several Twitter accounts linked to jihadists.[95] Analysis of the site's content revealed that it was a mirror of another IS site, likely transferred to counteract any potential takedown by law enforcement. The site contained IS material, including calls for jihadists to attack Balkan countries, and the documentary-style propaganda film *The Flames of War*, which chronicles the successes of the insurgency by IS in Syria and Iraq in 2014.[96]

[86] ibid., para. 78.
[87] ibid., para. 137.
[88] ibid., para. 119.
[89] ibid., para. 105(v).
[90] ibid., para. 128(2).
[91] Fisher, A., 'Swarmcast: How Jihadist Networks Maintain a Persistent Online Presence', *Perspectives on Terrorism*, Vol. 9(3) (2015); Winter, C., 'Media Jihad: The Islamic State's Doctrine for Information Warfare', *The International Centre for the Study of Radicalisation and Political Violence* (2017), available at: http://icsr.info/wp-content/uploads/2017/02/Media-jihad_web.pdf, last visited: 15 March 2018.
[92] Bergen, M., 'Google begins biggest ever crackdown on extremist YouTube videos', *Independent*, 25 August 2017. Available at: http://www.independent.co.uk/news/business/news/google-youtube-video-crackdown-extremism-islamist-neo-nazi-far-right-alphabet-advertising-a7911651.html, last visited: 15 March 2018.
[93] 'EU Terrorism Situation and Trend Report (TE-SAT) 2017', *Europol*, 2017, available at: https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017, last visited: 15 March 2018, p. 29.
[94] Cox, J., 'ISIS Now Has a Propaganda Site on the Dark Web', *Motherboard*, 16 November 2017, available at:
https://motherboard.vice.com/en_us/article/d7yzy7/isis-now-has-a-propaganda-site-on-the-dark-web, last visited: 15 March 2018.
[95] ibid.
[96] Ruble, K., 'Islamic State Documentary Style Video Says the "Flames of War" Have Just Began', *Vice News*, 19 September 2014, available at: https://news.vice.com/article/islamic-state-documentary-style-video-says-the-flames-of-war-have-just-begun, last visited: 15 March 2018.

Though IS propaganda is likely to exist in relative abundance on the Darknet and other encrypted platforms, proselytisation and recruitment on the Darknet is not central to the organisation's aims. As one IS supporter put it in a post to a private Telegram channel: "rarely would you find someone from general public following you [here]. That's why our main platform is [w]here the general public is found [...] We are here for *Dawa* [proselytization]. Not to entertain each other and talk to each other...let Telegram be like an archive".[97]

Case Study: Prosecuting for the Dissemination of Terrorist Content Online

Shafi Mohammed Saleem was convicted of, and pled guilty to, encouraging terrorism online.[98] Throughout 2016 and 2017, Saleem had used more than 20 Twitter and Instagram accounts to share pro-IS material.[99] One of the tweets he posted was an image of "zombie knives", which are illegal in the UK.[100] Included in what detectives recovered from Saleem's home was a photo saved on the Telegram app of Saleem holding a handgun, as well as videos of IS propaganda and Osama bin Laden. Commander Dean Haydon of the Met's Counter Terrorism Command noted how important it is to hold accountable those who share subversive material: "Every tweet has the potential to radicalise vulnerable people."[101] As of February 2018, Saleem had been sentenced to two years in prison.[102]

Direct Recruitment

Better monitoring of the surface web by social media companies and security officials has resulted in a faster rate of removal of extremist content from social media platforms.[103] Correlated to this is an increased use by extremist networks of the Darknet as a "jihadist safe haven"[104] for planning attacks.[105] In 2015, an undercover BBC reporter made contact on Twitter with Junaid Hussain, an IS recruiter who travelled from Birmingham to Syria in 2013. Although Hussain was killed in a drone strike in August 2015, the conversation was continued by another anonymous recruiter, who invited the reporter to chat privately on an encrypted messaging site. Once on the private site, the recruiter reportedly attempted to persuade the undercover journalist to carry out attacks in London, suggesting plans that bore "striking similarities" to the attacks that later occurred in Westminster and on London Bridge in March and June 2017 respectively.[106] Although it is unclear how Youssef Zaghba, one of the London Bridge attackers, was radicalised, owing to his computer skills he may have encountered IS websites on the Darknet.[107]

The evidence uncovered suggests that recruiters like Hussain use the Darknet to plan and launch terrorist attacks, because detection by law enforcement is less likely. While initial contact can be made on surface web platforms, further instruction is often given on end-to-end encryption apps, such as Telegram, on how to access jihadist websites on the Darknet.[108] Discussions on "how to make bombs, plan lone actor terrorist attacks ... how to use vehicles as weapons, where to stab people for maximum effect, and how to create a fake suicide vest or mask their activity, with the aim of convincing potential recruits to undertake

[97] Berger, J. M. and H. Perez, op. cit., p. 19.
[98] 'Man pleads guilty to terror offence', *Metropolitan Police*, 23 November 2017, available at: http://news.met.police.uk/news/man-pleads-guilty-to-terror-offence-279755, last visited: 15 March 2018.
[99] 'Man who posted terrorist messages online is convicted', *Metropolitan Police*, 14 February 2018, available at: http://news.met.police.uk/news/man-who-posted-terrorist-messages-online-is-convicted-294564, last visited: 15 March 2018.
[100] '"Zombie knives" ban to come into force', *BBC News*, 15 August 2016, available at: www.bbc.co.uk/news/uk-37080682, last visited: 15 March 2018.
[101] 'Man who posted terrorist messages online is convicted', *Metropolitan Police*, 14 February 2018.
[102] ibid.
[103] See, for example: The YouTube Team, 'An update on our commitment to fight terror content online', op.cit.; Huddleston, T., 'Four Tech Giants Team Up to Fight Terrorism', *Fortune*, 26 June 2017, available at: http://fortune.com/2017/06/26/twitter-facebook-youtube-microsoft-global-forum-terrorism/, last visited: 15 March 2018.
[104] Berton, B., op. cit., pp: 1-2.
[105] Pantucci, R., 'How Isil's shadowy "online manipulators" lure Britons into committing terrorist attacks' *The Telegraph*, 4 September 2017, available at: http://www.telegraph.co.uk/news/2017/09/04/isils-shadowy-online-manipulators-lure-britons-committing-terrorist/, last visited: 15 March 2018.
[106] Dearden, L., 'ISIS urged undercover BBC reporter to launch terror attacks in London Bridge and Westminster', *Independent*, 4 September 2017, available at: http://www.independent.co.uk/news/uk/home-news/isis-undercover-bbc-reporter-london-bridge-terror-attacks-westminster-borough-market-online-a7928641.html, last visited: 15 March 2018.
[107] ibid.
[108] Pantucci, R., op. cit.

their own attacks" are often the focal points on these Darknet forums.[109] Raffaello Pantucci, director of international security studies at the Royal United Services Institute (RUSI), recently described the Darknet as "the beating heart of the online terror threat".[110] For many terrorist groups, the Darknet eliminates the need for a physical meeting place to plan an attack and provides a virtual meeting ground for terrorist operations, where communications may encourage recruits to single-handedly carry out attacks with minimal training or experience. This is similar to how the Darknet is used by those who purchase drugs, firearms or child pornography, as the risks of being physically caught committing criminal acts are reduced. Law enforcement agencies have therefore had to move towards online policing for these crimes (see Figure 1 and Chapter 5).

[109] ibid.
[110] ibid.

Chapter 3: Terrorism and the Darknet

The following chapter examines the way in which terrorists to use the Darknet to gain material advantages in the form of financial contributions, fraudulent documents, weapons, and paramilitary training.

Crime on the Darknet

Drugs

Though the Darknet can serve as a shield of protection for human rights activists and campaigners, it is also exploited by criminals. A common form of criminal activity on the Darknet is the sale and distribution of illicit drugs, which has been bolstered by a change in the legal status of products or substances from "legal" or "unregulated" to "illegal", "controlled" or "banned" substances.[111] These changing legal statuses, combined with stricter regulation and the implementation of new laws by law enforcement, have meant that sales of the highest category of banned drugs and substances have increasingly migrated to marketplaces on the Darknet. A case in point is a previously unknown drug by the name of New Psychoactive Substance (NPS), which, when initially unregulated, was sold on the surface web.[112] However, following its regulation, sales shifted to the Darknet.[113]

<ins>Case Study</ins>: Ricin in Liverpool, UK

Mohammed Ali, 31, a software programmer from Liverpool, UK, was jailed for eight years after attempting to buy ricin from the Darknet on 4 February 2015. Using the online moniker "Weirdos 0000", Ali approached a supplier on the Darknet to discuss prices of the deadly substance, and possible discounts for larger orders and repeat business. He paid the vendor "Psychochem" 2.1849 bitcoins (around US$225 at the time)[114] for 500mg of ricin powder – enough to kill between 700 and 1,400 people.[115] The vendor was, in reality, an undercover FBI agent, who notified police in England before dispatching a harmless package containing ersatz ricin to Ali. Once Ali had received the package, police moved quickly to arrest him. No evidence was found to suggest that Ali had been planning a terrorist attack, or even that he had intended to harm anyone with the substance. In court, Ali contended that he had been simply "curious" about the Darknet: "I found lots of different items ranging from drugs, guns, other illegal items, and because I had been watching *Breaking Bad* I just had ricin in my mind."[116] Still, on prosecution the judge concluded: "I am satisfied that Mohammed Ali had no intention of disposing of [the] ricin immediately. He intended to keep it. That created a real risk that, at some stage in the future, he might decide to experiment with it or it fall into the wrong hands."[117]

Online black-market sites, such as the now infamous "Silk Road" (SR), provide host sites for the sale of illegal drugs. Silk Road received earnings of more than US$13 million in commissions for allowing distributors to use the platform[118] (see Case Study "The Silk Road 1.0" below). Between 2011 and 2013, its period of operation, an estimated US$1.2 billion in sales took place on the Silk Road forum, involving 150,000 customers and 4,000 distributors.[119] The 2013 shutdown of Silk Road did not hamper the sale and exchange of illicit goods on the Darknet.[120] On the contrary, alternative marketplaces have developed to replace it, including Libertas Market, Wall Street Market, Dream Market, Berlusconi Marketplace and

[111] 'European Union Serious And Organised Crime Threat Assessment: Crime In The Age Of Technology', *SOCTA* (2017), available at https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017, last visited: 15 March 2018, p. 22.
[112] ibid., p. 23.
[113] ibid., p. 23.
[114] 'Bitcoin (USD) Price', *Coindesk*, available at: https://www.coindesk.com/price/, last visited: 15 March 2018.
[115] 'Breaking Bad fan jailed over Dark Web ricin plot', *BBC News*, 18 September 2015, available at: http://www.bbc.co.uk/news/uk-england-34288380, last visited: 15 March 2018.
[116] 'Breaking Bad fan jailed for trying to buy ricin', *The Guardian*, 18 September 2015, available at: https://www.theguardian.com/uk-news/2015/sep/18/breaking-bad-fan-jailed-over-ricin-plot, last visited: 15 March 2018.
[117] 'Breaking Bad fan jailed over Dark Web Ricin Plot', op. cit.
[118] Chertoff, M., op. cit., p. 30.
[119] ibid.
[120] ibid.

many more.[121] The 2017 Report by Global Drug Survey further demonstrates the resilient nature of the drug trade on the Darknet, stating that "despite disruptions from law enforcement efforts and scams, the size and scale of darknet markets for drugs continues to grow". At the time of the report there were more than 20 functioning markets.[122]

Efforts by law enforcement agencies, including the NCA, SO15 Counter Terrorism Command (CTC) and the US Federal Bureau of Investigation (FBI), as well as collaborations between multiple agencies on an international level, have focused on human intelligence and technology to infiltrate and target customers consuming and disseminating criminal products on the Darknet (see Figure 3). These techniques have relied on the use of pen or trap orders (as was the case in SR 1.0, below) to gather data on communications, criminal error (which can assist in uncovering details which lead to identification of the user) and sting operations which target the user at the point at which criminal activity is conducted, or an illegal package is received.

Case Study: The Silk Road 1.0

The Silk Road was the largest Darknet marketplace, operating online between 2011 and 2013.[123] Users of the site predominantly traded in illegal drugs, false identification documents, and hacking software. Transactions on the site were made exclusively with bitcoin. According to US government documents, in the two years that the site was active, thousands of anonymous vendors used it to sell approximately US$183 million worth of prohibited products and services to "well over a hundred thousand" buyers worldwide.[124] The individual behind the site, Ross William Ulbricht, was a 29-year-old who lived in the US. Operating under the username "Dread Pirate Roberts" (DPR), Ulbricht accrued millions of dollars in bitcoin from the commissions he collected on transactions made on SR.[125] While DPR was known to be the administrator of SR from the initial stages of the investigation, his true identity was unknown.

Ulbricht's arrest in San Francisco in October 2013 was the outcome of a painstaking process involving cross-agency cooperation between the Drug Enforcement Agency (DEA), the Federal Bureau of Investigation (FBI), Homeland Security Investigations (HSI), the Internal Revenue Service (IRS), the Secret Service and the United States Postal Inspection Service (USPIS).[126] Attempts to identify DPR reportedly began with "an extensive search of the internet", with investigators sifting through countless web pages in an attempt to piece together DPR's online footprint.[127] Ulbricht was first implicated in the case when two posts by a user called "Altoid" to online forums, made months apart, were identified by investigators. The first of the posts was to a forum devoted to the discussion of hallucinogenic mushrooms. In the post, Altoid was observed promoting the SR to other users as a good place to buy and sell illegal drugs. Altoid's second post, made on a different forum, asked fellow users for advice on the use of bitcoin, and included a Gmail address for correspondence containing Ulbricht's full name.[128] This was a significant breakthrough in the investigation, and, after obtaining a warrant, investigators were able to search the Google and Facebook accounts associated with that name, and gain access to the IP addresses associated with the email account.[129] Separately, meticulous analysis of SR's source code revealed a function that only permitted one IP address to log in to regulate the site.[130] Despite Ulbricht's attempts to divert investigators through the use of a Virtual Private Network (VPN) to produce a fake IP address, the FBI was able to obtain the genuine one from the VPN provider – which matched up with the location used to log in to

[121] Researcher analysis on the Darknet in January 2018: these sites are rated on the website "Deep Dot Web" by "Invite/Referral", "Specific Language or Country" and "Dead/Scam Markets". Alphabay, a notorious marketplace used to replace SR and SR2, is now dead.

[122] Marsh, S., 'UK accounts for largest share of darknet fentanyl sales in Europe', *The Guardian*, 16 October 2017, available at: https://www.theguardian.com/society/2017/oct/16/uk-accounts-for-largest-share-of-darknet-fentanyl-sales-in-europe?CMP=share_btn_link, last visited: 15 March 2018.

[123] *United States of America v. Ross William Ulbricht*, US District Court, Southern District of New York, 4 February 2014, available at: https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/US%20v.%20Ross%20Ulbricht%20Indictment.pdf, last visited: 15 March 2018, pp. 1-2.

[124] *United States of America v. Ross William Ulbricht*, Second Circuit Court of Appeals, No.15-1815, (2016; 2017), available at: https://www.pbwt.com/content/uploads/2017/05/15-1815_opn.pdf, last visited: 15 March 2018, pp. 1-2.

[125] 'United States Court of Appeals for the Second Circuit v. Ross William Ulbricht', op. cit., p. 5.

[126] Bearman, J. and T. Hanuka, 'The Rise and Fall of Silk Road, Part 1', *Wired*, May 2015, available at: https://www.wired.com/2015/04/silk-road-1/, last visited: 15 March 2018.

[127] Lee, D., 'Silk Road: How FBI closed in on suspect Ross Ulbricht', *BBC News*, 2 October 2013, available at: http://www.bbc.co.uk/news/technology-24371894, last visited: 15 March 2018.

[128] ibid.

[129] ibid.

[130] In computing, a "source code" is information that is written by the programmer in a computer programming language, which acts as a set of instructions for how a program (in this case, the Silk Road website) should function.

Ulbricht's Gmail account.[131] By this point it was known that DPR and Ulbricht had, at the very least, been in the same location at the same time.

In addition to these developments, a package of fake identification documents was discovered during a routine border check, each with a photograph of Ulbricht on them, heading to his address in San Francisco. On SR, DPR was observed asking other users for advice on obtaining fake documents that he said he needed in order to procure more servers.[132] By September 2013, Ulbricht had become the primary suspect in the investigation, and the government ordered five pen register and trap and trace processes or devices on his IP address. These measures allowed investigators to gather data on Ulbricht's communications via his wireless router and laptop, without capturing the contents of those communications.[133] Thus, investigators could identify source and destination addresses, along with dates, times, durations, and ports of transmission, therefore linking them to DPR's online activity on SR. After his arrest in a public library in San Francisco, Ulbricht was found guilty on seven counts arising from his creation and running of SR, and sentenced to life in prison. An appeal of his sentence in 2016 was unsuccessful.[134]

Research indicates that the UK is the largest host of fentanyl sales on the Darknet in Europe.[135] Fentanyl is a controlled synthetic opioid substance approximately 100 times stronger than heroin.[136] The Darknet constitutes a supply chain where drugs imported from China and Hong Kong are sold to UK-based customers.[137] Since 2016, at least 60 people in the UK have died from fentanyl-related drug use.[138] Approximately 1,000 sales of fentanyl took place on the Darknet between April and October 2017.[139] On AlphaBay, at least 225 sales were made during the four-month period from June to September 2015.[140] As recently as December 2017, Kurt Lai Lan, a drug dealer in the UK, was convicted for using the Darknet to sell illegal drugs and receive payments in bitcoin.[141] In a sting operation, British authorities intercepted a parcel containing 11,000 tablets of Methylenedioxymethamphetamine (MDMA) with a street value of GB£80,000.[142] Lai Lan was apprehend at Gatwick airport in June 2017, attempting to board a one-way flight to South Africa.[143]

These figures, as well as multiple case studies and convictions, clearly reveal that the Darknet provides access to illegal drugs and banned substances. Moreover, sales are expected to increase as the platform remains largely unregulated. Although British authorities have successfully made some arrests to curb sales on these forums, the continued availability of drugs on the Darknet hampers efforts to control supply.[144] A promising development in this area is collaboration between bitcoin exchange companies, intelligence agencies on user records, and the infiltration of staff areas of marketplaces on the Darknet by intelligence agents, as was the case with SR 2.0, below.

[131] Lee, D., 'Silk Road: How FBI closed in on suspect Ross Ulbricht', op. cit.

[132] ibid.

[133] 'United States Court of Appeals for the Second Circuit v. Ross William Ulbricht', op. cit., pp. 6-7.

[134] ibid.

[135] Marsh, S., op. cit.

[136] ibid.

[137] Perraudin, F. and H. Siddique, 'At least 60 UK drug deaths in the past eight months linked to fentanyl', *The Guardian*, 1 August 2017, available at: https://www.theguardian.com/society/2017/aug/01/at-least-60-uk-drug-deaths-in-past-eight-months-linked-to-fentanyl, last visited: 15 March 2018.

[138] McKenzie, C. and N. N. Daeid, 'War on fentanyl: the drug that killed Prince is linked to 60 deaths in the UK since 2016', *Independent*, 14 August 2017, available at: http://www.independent.co.uk/life-style/health-and-families/fentany-drug-linked-to-60-deaths-uk-since-2016-opioids-a7884231.html, last visited: 15 March 2018.

[139] Marsh, S., op. cit.

[140] ibid. Note that Alphabay is now a dead market.

[141] 'Robert Bryan secures conviction of drug dealer who used the "Darknet" and bitcoin payment methods', *Drystone Chambers*, 20 December 2017, available at: https://drystone.com/news/robert_bryan_secures_conviction_of_drug_dealer_who_used_the_darknet_and_bitcoin_payment_methods/, last visited: 15 March 2018.

[142] ibid.

[143] ibid.

[144] Perraudin, F. and H. Siddique, op. cit.

Case Study: Blake Benthall (aka "Defcon") and The Silk Road 2.0

The Silk Road 2.0 (SR2) appeared on the Darknet in November 2013, approximately five weeks after the US government shut down the original Silk Road and arrested Ross Ulbricht. It was virtually identical to the original version in terms of appearance and function: access was possible exclusively through the Tor browser, and transactions on the marketplace could be made only using bitcoin. By October 2014, the site contained more than 13,000 listings for controlled substances, and a variety of listings for other products including computer hacking tools and services, and fraudulent documents.[145] Initially, the site was administered by an unknown individual who adopted the familiar Dread Pirate Roberts (DPR) username, but by December 2013 a new administrator called "Defcon" had taken on the role. Before the marketplace was closed down in November 2014 and Defcon's true identity was revealed as Blake Benthall (a former SpaceX engineer based in the US), SR2 had around 150,000 regular users and was amassing sales of at least US$8 million per month.[146] The government investigation into those responsible for administering the site involved the FBI and its Cyber Branch in New York, alongside Homeland Security Investigations (HSI) and its Cyber Crime Centre. The investigation was coordinated with a number of international law enforcement agencies from 16 countries outside of the US, under the authority of Europol's European Cybercrime Centre and the European Union's Judicial Cooperation Unit (Eurojust). In the UK, investigations were carried out on a local level by police, operating under the direction of the NCA.[147]

The trail of the FBI investigation into SR2 made its first significant lead in May 2014, when imaging and forensic analysis of a server suspected to be the host of the illicit site abroad caused SR2 to go briefly offline, thus confirming its server location.[148] The FBI has not publicly verified how the SR2 server was correctly identified.[149] Nevertheless, based on records provided to law enforcement by the provider of the SR2 server, it was ascertained that the individual maintaining the SR2 server used the email account "blake@benthall.net".[150] At the time of the imaging of the server when SR2 was briefly disconnected, the provider received a succession of messages through its online customer support system from the user of the blake@benthall.net address. Using records obtained from the service provider, these communications were traced to a particular IP address. The contents of the interaction between the user of the address and the provider were concerning the issues with the server, demonstrating to investigators that the user of the address was responsible for administering the SR2 server.[151] A court-authorised search warrant of the account associated with the email address was revealing: investigators found multiple occasions where Blake Benthall had signed off emails with his own name, and on another occasion he had emailed himself weblinks to messages that were accessible exclusively to members of the SR2 forum.[152]

Since November 2013, the month that SR2 was launched, Blake Benthall had a stable income in the form of bitcoin. A US-based bitcoin exchange company provided investigators with the records of an account registered with the same email address and bearing Benthall's full name. These records indicated that Benthall engaged in his first bitcoin transaction the day after SR2 went live, and following that day he received around BTC575.58 into the account, exchanging approximately BTC543.63 for fiat currency. At the time, this was equivalent to US$273,626.60.[153]

During the investigation, an undercover HSI agent successfully infiltrated the support staff involved in the administration of SR2, and was therefore given access to private, restricted areas of the site that were otherwise reserved for Defcon and his administration staff. Assuming the role of a paid staff member of SR2, the agent was able to interact directly with Defcon and observe a variety of technical features, including the operating system and web browser used by administrators. Defcon's operating system was

[145] US Attorney, Southern District of New York, 'Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court', *Federal Bureau of Investigation*, 6 November 2014, available at: https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court, last visited: 15 March 2018.

[146] ibid.

[147] Zagaris, B., 'International Raids Take Down Illegal Internet Sites Selling Contraband', *International Enforcement Law Reporter*, Vol. 30(14) (2014): p. 542.

[148] *United States of America v. Blake Benthall*, Southern District of New York, available at: https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/Benthall%2C%20Blake%20Complaint.pdf, last visited: 15 March 2018, p. 21.

[149] The indictment documents regarding Blake Benthall are vague about how the FBI correctly identified the server of SR2, and simply state that they "correctly identified the server located in the foreign country". There is, however, a theory in the media about how this was achieved, though it has not been officially verified. For more, see: Hill, K., 'How did the FBI Break Tor?', *Forbes*, November 2014, available at: https://www.forbes.com/sites/kashmirhill/2014/11/07/how-did-law-enforcement-break tor/#564867914bf7, last visited: 6 February 2018.

[150] 'United States of America v. Blake Benthall', op. cit., p. 23.

[151] ibid., p. 24.

[152] ibid., p. 25.

[153] ibid., p. 26.

noted and compared to records provided by the bitcoin exchange company. The records indicated that on the same day that Defcon's operating system was recorded, Benthall had logged into his bitcoin account using the same, relatively unusual, combination of computer software.[154]

Investigators used online and offline surveillance in combination in the latter stages of the investigation to confirm the suspected connection between Blake Benthall and the online moniker "Defcon". The day after obtaining a judicial order, investigators began gathering pen register data from the IP address associated with the email account, which revealed a significant volume of Tor-related traffic to and from the address. This data was compared with Benthall's real-world movements, and found to match up in time and in space.[155] Benthall was charged with conspiracy to trade narcotics.[156] Unofficial reports claim he is no longer in custody.[157]

Other Criminal Activity on the Darknet

Besides drugs, the Tor network is used for the sale of pornography, fraudulent documents, instructional manuals on criminal activities, and firearms. A 2015 study conducted by the Global Commission on Internet Governance and Chatham House found that the Tor network contains many sites relating to gambling, the sale of weapons, child abuse material, pornography, the sale of fraudulent documents and the narcotics trade.[158] In this study, sites selling illegal drugs were found to constitute around 15.5% of all sites identified on the network. There was a significant margin between that and the next two largest categories, fraud and marketplaces selling miscellaneous goods, which each constituted approximately 9% of the total sample. Though sites containing child abuse material represented approximately 2% of the sample, requests by Tor users to these sites came close to 83% of the total number of requests observed.[159] In a similar vein, a 2016 study published in the International Institute for Strategic Studies' (IISS) *Survival* journal found that more than half of the active sites on the Darknet were used for criminal purposes: 57% of content on the Darknet catered to the sale of arms, drugs, illicit pornography, hacking and violence combined.[160] A forthcoming study by the University of Technology Business School has indicated that 47% of all bitcoin transactions involve illegal transactions on the Darknet.[161]

Such findings, although preliminary, present an interesting conundrum: while the Darknet is used to protect privacy advocates, whistle-blowers, and human rights activists, it also provides a dangerous platform for those engaging in illicit activities by granting them anonymity through encryption. Moreover, efforts to infiltrate the Darknet by intelligence agencies using computer network exploitation, as in the case of "Playpen" below, are shrouded in secrecy, and the technicalities of network investigative techniques are highly classified and rarely shared on the public record, even when it comes to court cases.[162]

[154] ibid., p. 27.
[155] ibid., pp. 28-30.
[156] US Attorney, Southern District of New York, 'Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court', op. cit..
[157] Southurst, J. 'Senior Silk Road 2.0 Admin Gets Eight Years Prison', *Bitcoin.com*, 11 June 2016, available at: https://news.bitcoin.com/silk-road-2-admin-prison/, last visited: 15 March 2018.
[158] Owen, G. and N. Savage, 'The Tor Dark Net', *Global Commission on Internet Governance*, Paper Series No. 20, September 2015, available at: https://www.cigionline.org/sites/default/files/no20_0.pdf, last visited: 15 March 2018, p. 6.
[159] ibid., p. 6.
[160] Moore, D. and T. Rid, op. cit., p. 21. The study revealed a total of 2,723 actives on the darknet. Of these, 1,547 were illicit; 'European Union Serious and Organised Crime Threat Assessment: Crime in The Age of Technology', *SOCTA*, op. cit., p. 22.
[161] 'Research: 47% of all Bitcoin transactions involves illegal trading mostly on "darkweb"', *Deep Dot Web*, 8 January 2018, available at: https://www.deepdotweb.com/2018/01/08/research-47-bitcoin-transactions-involves-illegal-trading-mostly-darkweb/, last visited: 15 March 2018.
[162] 'Child porn case dropped to prevent FBI disclosure', *BBC News*, 6 March 2017, available at: http://www.bbc.co.uk/news/technology-39180204, last visited: 15 March 2018.

Case Study: The "Playpen" Case

Playpen was a members-only Darknet website which hosted material relating to the sexual exploitation of children. The site had around 160,000 members worldwide, making it, at the time, the largest child pornography website that the FBI had ever come across.[163] Its members used the site as a place to upload, share, and view tens of thousands of posts involving the sexual abuse of children, all operating under the impression that their use of the .onion Tor browser made their online activity untraceable.[164] The investigation into the identities of the site's users was "one of the largest and most challenging ever" in the fight against online child exploitation.[165] It was led by the FBI and the US Department of Justice and supported by other law enforcement agencies, including Europol, and led to the opening of hundreds of follow-up investigations globally.

The first lead in the investigation came in December 2014 when a "foreign entity" shared the true IP address of the Playpen server, reportedly found because of two errors made by the designer of the website.[166] Using what are described in court documents as "standard investigation measures", the FBI located the site on four hard drives on a server in North Carolina. Seizing a copy, it then arrested the man deemed to be its owner in Naples, Florida: Steven Chase, who was then sentenced to 30 years in prison.[167] The seized copy of the site was placed on to a government-owned server in the Eastern District of Virginia, and a warrant was obtained to deploy a Network Investigative Technique (NIT) to help reveal the true identities of the site's users.[168] Playpen was hosted on the government-owned server for 13 days, from 20 February to 4 March 2015. During this time, the NIT was implemented thousands of times, gathering crucial information which was compiled into "lead packages" and sent to relevant offices or authorities inside the US and around the world.[169]

One of the thousands of Playpen members whose identity was revealed using the NIT was user "abcdefghijk123", who had accessed many posts on the site with file descriptions that were "consistent with child exploitative material". The user had created a Playpen account during August 2014, and had spent a total of 82 hours logged in to the site between this time and the FBI's seizure of the server and implementation of the NIT around six months later.[170] On 3 March 2015, user abcdefghijk123 opened a link to a video depicting the sexual abuse of a 13-year-old girl, and the NIT transmitted to the FBI's server information about the user, including their true IP address. This was connected to its owner, Jason Dean Barnes, and after a search warrant was issued, his house was searched and the suspect arrested. He admitted to FBI agents on the day of his arrest that he had viewed child pornography on the Darknet.[171] In this instance, the NIT was an essential tool used by the FBI in its investigation, and directly led to the identification and arrest of multiple individuals seeking child pornography on the Darknet. Though it was not long after the shutdown of Playpen that another website "grew to become the largest child pornography website on the Tor network", the investigation was a success in that it produced at least 870 arrests worldwide (368 of which were in Europe) and led to the identification or rescue of at least 259 sexually abused children outside of the United States.[172]

[163] *United States of America v. Jason Dean Barnes*, No. 3:15-CR-112-J-39PDB, United States District Court for the Middle District of Florida, Jacksonville Division, 2017 U.S. Dist. Lexis 136157, p. 3, 8 May 2017, Decided, 8 May 2017, Filed.

[164] 'Kentucky Man Sentenced to Prison for Engaging in a Child Exploitation Enterprise', *US Department of Justice, Office of Public Affairs*, 7 February 2017, available at: https://www.justice.gov/opa/pr/kentucky-man-sentenced-prison-engaging-child-exploitation-enterprise, last visited: 15 March 2018.

[165] 'Major Online Child Sexual Abuse Operation Leads to 368 Arrests in Europe', Press Release, *Europol*, 5 May 2017, available at: https://www.europol.europa.eu/newsroom/news/major-online-child-sexual-abuse-operation-leads-to-368-arrests-in-europe, last visited: 15 March 2018.

[166] *United States of America v. Jason Dean Barnes*, op. cit., p. 3.

[167] ibid. See also: 'Florida Man Sentenced to Prison for Engaging in a Child Exploitation Enterprise', *US Department of Justice*, 1 May 2017, available at: https://www.justice.gov/opa/pr/florida-man-sentenced-prison-engaging-child-exploitation-enterprise, last visited: 15 March 2018.

[168] The NIT was a computer code that caused a computer, upon visiting Playpen and accessing certain content, to communicate with the government-owned server and provide several identifiers, most notably the Playpen user's IP address. All websites send content to their users, which is downloaded by the user's computer, appearing as a web page on the user's computer screen. Under the NIT authorised by the warrant in this case, the content sent by Playpen to its users' computers included additional instructions that were designed to make the user's computer transmit information to the computer controlled by the investigation. This was done without the knowledge of the Playpen users. The NIT had no effect on the functionality of the user's computer, nor its ability to access web material. For more, see: *United States of America v. Jason Dean Barnes*, op. cit., p. 3.

[169] ibid., p. 4. He faces a minimum mandatory penalty of five years, up to 20 years, in federal prison. For more, see: 'Jacksonville Man Guilty of Downloading Sexual Abuse Videos and Images Using the "Dark Web"', *US Department of Justice, Middle District of Florida*, 19 September 2017, available at: https://www.justice.gov/usao-mdfl/pr/jacksonville-man-guilty-downloading-sexual-abuse-videos-and-images-using-dark-web, last visited: 15 March 2018.

[170] ibid.

[171] ibid., p. 5.

[172] ibid., p. 4. These figures are dated 5 May 2017. It is possible that the figures have risen since this date, given that some investigations are ongoing. Figures from: 'Major Online Child Sexual Abuse Operation Leads to 368 Arrests in Europe', op. cit.

Figure 3: Case study techniques used to identify Darknet users

Pen or Trap Orders:

- Gathers data on communications to and from an IP address, without revealing the contents of the communications.
- Trap and trace shows what numbers (or IP addresses) have contacted the IP address being monitored. A pen register shows outgoing communications.
- *Case Study: SR1.*

Bitcoin Exchange Companies:

- Can provide governments with user records.
- *Case Study: Blake Benthall (SR2).*

Infiltration of "staff areas" of Cryptomarketplaces:

- Software data of the administrator can be viewed by FBI or other intelligence agents. This is then matched with records gathered from the bitcoin exchange company.
- *Case Study: Blake Benthall (SR2).*

Sting:

- This technique targets customers, not vendors. The buyer is apprehended upon receipt of the illicit package.
- *Case Study: Liverpool ricin case.*

Network Investigative Technique (NIT):

- Requires seizure of server of site.
- Also known as Computer Network Exploitation, and involves the use of malware to proactively hack a site.
- *Case Study: Playpen.*

Criminal Error:

- Extensive search of the internet and user's "digital history" to uncover details which lead to identification, e.g. email address (in the case of both SR1 and SR2). Once email address is known, IP address can be found.
- This was also significant in the Playpen case – configuration errors by the site's creator led to the discovery of the true IP address of Playpen's server.

Source: compilation of information in report

The Crime-Terror Nexus

IS has made concentrated efforts to recruit members from the criminal underworld of European societies, proclaiming that by joining IS, prospective supporters will achieve redemption for their sins.[173] Moreover, IS encourages raising funds through criminal activities, promoting this as a divinely sanctioned method of raising money for jihad when operating in the *Dar al-Harb* (Lands of War).[174] In a study conducted for the International Centre for Counter-Terrorism (ICCT) and the George Washington Program on Extremism, Lorenzo Vidino found that, of his dataset comprising all terrorist attacks in Europe and North America between June 2014 and June 2017, more than half (57%) of perpetrators had been involved in criminal activity unrelated to terrorism prior to carrying out their attacks.[175]

The link between the Darknet and terrorism is not always clear cut, as non-terror-related crime often funds or supports terrorism indirectly. In recent years, however, the convergence of criminal and terrorist networks has become more pronounced.[176] It is common practice for terrorists to engage in myriad organised criminal activities, such as prostitution, the sale of human organs, weapons, antiquities, the taxation of drug and people smuggling routes, kidnap for ransom, and money laundering, to raise funds for terror-related activities.[177] This largely takes place in source-of-conflict countries, such as Iraq and Syria in the case of IS. However, self-starter terrorists in the United Kingdom and Europe can benefit from criminality: the sale of instructional manuals, firearms or firearm components, drugs, and fraudulent documents on the Darknet. The two areas are not mutually exclusive, and often overlap: drugs trafficked from Libya or Iraq, for example, could be sold on a host of platforms, including on the Darknet. Equally, money obtained through kidnap for ransom could be funnelled into various terrorism-related areas, including the recruitment of fighters, some of whom may be recruited on the Darknet. Similarly, document fraud and the availability of weapons on the Darknet can aid operations by simplifying the logistics for terrorists who plan to launch attacks in Europe and beyond.

Drug Trafficking

The relationship between drug traffickers and jihadists in North Africa is an important example of the intertwined nature of crime and terror. Since 2014, IS in Libya has profited from taxing the passage of illicit drugs through newly established drug routes stretching from Morocco to Libya, and then onwards to Europe.[178] Drug traffickers have benefited from weak state structure in Libya and collaborated with IS in the region to enable illicit drugs to pass through IS-controlled areas in Libya, where the group is able to exact a tax in return for passage.[179]

Since 2015,[180] IS has partnered with members of Italian organised crime groups to smuggle cannabis resin, also known as North African hash, from Morocco through Algeria, then Tunisia, to the east of Libya, and then into Europe.[181] IS has a strong power base along the drug route in the city of Sirte, where it controls

[173] Basra, R., P. Neumann and C. Brunner, 'Criminal Pasts, Terrorist Futures: European Jihadists and the New Crime-Terror Nexus', *ICSR*, 11 October 2016, available at: http://icsr.info/2016/10/new-icsr-report-criminal-pasts-terrorist-futures-european-jihadists-new-crime-terror-nexus/, last visited: 15 March 2018.

[174] 'EU Terrorism Situation and Trend Report (TE-SAT) 2017', op. cit.

[175] Vidino, L., F. Marone and E. Entenmann, 'Fear Thy Neighbor: Radicalization and Jihadist Attacks in the West', *ISPI*, June 2017, available at https://icct.nl/wp-content/uploads/2017/06/FearThyNeighbor-RadicalizationandJihadistAttacksintheWest.pdf, last visited: 15 March 2018, p. 57. However, the report states that the "criminal activity of many in the dataset is not known", p. 58.

[176] Basra, R., P. Neumann and C. Brunner, op. cit.

[177] 'European Union Serious And Organised Crime Threat Assessment: Crime In The Age Of Technology', *SOCTA*, op. cit.

[178] Osipova, N. V. and R. Callimachi, video: 'ISIS and the new route of Hashish', *New York Times*, 13 September 2016, available at: https://www.nytimes.com/video/world/europe/100000004602800/isis-and-the-new-route-of-hashish.html?action=click&contentCollection=world&module=embedded&region=caption&pgtype=article, last visited: 15 March 2018.

[179] ibid.

[180] In 2015, IS lost a significant part of its *caliphate* in Syria's northern border with Turkey. The size of this territory enabled IS to exert a significant population tax on its residents. According to IHS, IS territorial defeat meant its earnings dropped from around US$1.2 billion in the third quarter of 2014 to US$56 million by the fourth quarter of 2015. For more, see: 'Islamic State's Caliphate Shrinks by 14 Percent in 2015', *IHS Markit*, 21 December 2015, available at: http://news.ihsmarkit.com/press-release/aerospace-defense-security/islamic-states-caliphate-shrinks-14-percent-2015, last visited: 15 March 2018; Farmer, B., 'Islamic State income "falls 30 percent as it loses territory"', *The Telegraph*, 17 April 2016, available at: http://www.telegraph.co.uk/news/2016/04/17/islamic-state-income-falls-30-per-cent-as-it-loses-territory/, last visited: 15 March 2018.

[181] Scherer, S., 'Decriminalizing cannabis would hurt Islamic State, mafia- Italy prosecutor', *Reuters*, 18 April 2016, available at: https://www.reuters.com/article/us-italy-mafia-islamic-state-cannabis/decriminalizing-cannabis-would-hurt-islamic-state-mafia-italy-prosecutor-idUSKCN0XF11D, last visited: 15 March 2018. Recent

ports,[182] enabling drug transfers through Libya to the Mediterranean Sea.[183] This symbiotic partnership between IS and Italian organised crime groups has enabled IS to benefit from the illegal drug trade, which yields profits of US$36 billion.[184]

Although there is no concrete evidence that drugs smuggled through Libya by IS end up for sale on the Darknet, there are reports that indicate that cannabis resin is among the leading drugs purchased on the Darknet. Moreover, European officials have established a link between the sale of cannabis resin, which primarily originates from Morocco and Afghanistan,[185] and the Darknet. While there is no way to ascertain the origin of drugs available on the Darknet, statistics provided by the Global Drug Survey indicate a growth from 4.5% in 2015 to 6.7% in 2016 in customers who bought drugs on the Darknet, and lists cannabis among the top drugs commonly purchased.[186]

Kidnap for Ransom

Kidnap for ransom has helped contribute towards the funding of IS operations. Though the majority of financing for IS is derived from extortion and oil within its territories, these income streams have been supplemented by a kidnap business targeting foreign journalists and aid workers, earning IS between US$20 and $45 million in 2014 alone.[187]

In West Africa, too, kidnap for ransom provided Al-Qaeda in the Islamic Maghreb (AQIM) with a sizeable portion of its funding.[188] From 2003 to 2012, the group reportedly accrued between USD$1 million and USD$4 million per western hostage, buttressing terror activities in the region.[189]

Owing to the close-knit and secretive nature of terrorist financing, it is difficult to ascertain how money obtained from kidnap for ransom is utilised. However, small portions of these profits may be transferred through various financial conduit systems, including bitcoin and *hawala* systems, discussed in Chapter 4.

Document Fraud

According to a Europol report, document fraud is the means through which counterfeit and genuine documents are produced, stolen, and used for the purposes of deception or misrepresentation.[190] Several sites on the Darknet provide access to fraudulent travel documents for customers. Alphabay was among the largest of these, with more than 200,000 users and 40,000 vendors prior to its takedown by the FBI and global law enforcement partners in July 2017.[191] While it was still active, the site was reported to have hosted more than 100,000 listings for stolen and fraudulent documents, as well as other counterfeit goods.[192]

studies have also indicated the flow of drugs in the reverse: Nadeau, B. L., 'The Italian Mob is Peddling Pills to ISIS', *The Daily Beast*, 3 February 2018, available at: https://www.thedailybeast.com/the-italian-mob-is-peddling-pills-to-isis, last visited: 15 March 2018.

[182] Ensor, J., 'Isil and Italian Mafia teaming up to smuggle cannabis into Europe', *The Telegraph*, 19 April 2016, available at: http://www.telegraph.co.uk/news/2016/04/19/isis-and-italian-mafia-teaming-up-to-smuggle-cannabis-into-europ/, last visited: 15 March 2018.

[183] 'European Union Serious And Organised Crime Threat Assessment: Crime In The Age Of Technology', *SOCTA*, op. cit.

[184] Scherer, S., 'Decriminalising cannabis would hurt Islamic State, mafia- Italy prosecutor', op. cit.

[185] 'United Kingdom Country Drug Report 2017', *EMCDDA* (2017), available at: http://www.emcdda.europa.eu/countries/drug-reports/2017/united-kingdom/drug-markets_en, last visited: 15 March 2018, p. 16.

[186] 'The Global Drug Survey 2016 findings', *Global Drug Survey* (2016), available at: https://www.globaldrugsurvey.com/past-findings/the-global-drug-survey-2016-findings/, last visited: 15 March 2018.

[187] Napoleoni, L., *Merchants of Men: How Kidnapping, Ransom and Trafficking Fund Terrorism and ISIS* (London: Atlantic Books, 2017), p. 41; Goldman, Z. K., E. Maruyama, E. Rosenberg, E. Saravalle and J. Solomon-Strauss, 'Terrorist Use of Virtual Currencies: Containing the Potential Threat', *CNAS*, May 2017, available at: http://www.lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReport-TerroristFinancing-Final.pdf, last visited: 15 March 2018, p. 10.

[188] Nossiter, A., 'Millions in Ransoms Fuel Militants' Clout in West Africa', *The New York Times*, 12 December 2012, available at: http://www.nytimes.com/2012/12/13/world/africa/kidnappings-fuel-extremists-in-western-africa.html, last visited: 16 March 2018.

[189] Napoleoni, L., op. cit., p. 41.

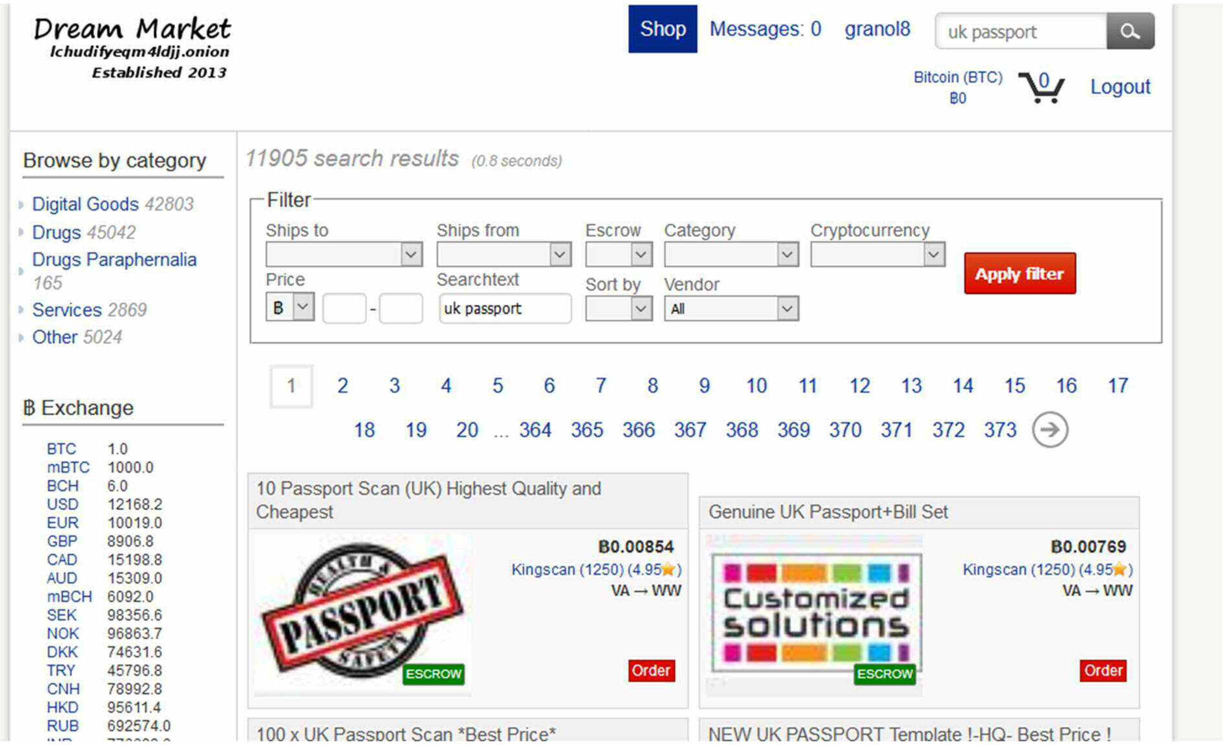
[190] 'European Union Serious And Organised Crime Threat Assessment: Crime In The Age Of Technology', *SOCTA*, op. cit., p. 20.

[191] 'The Internet Organised Crime Threat Assessment Report (IOCTA) 2015', op. cit., p. 51; Aliens, C., 'A Globally Coordinated Operation Just Took Down AlphaBay and Hansa', *Deep Dot Web*, 20 July 2017, available at: https://www.deepdotweb.com/2017/07/20/globally-coordinated-operation-just-took-alphabay-hansa/, last visited: 16 March 2018.

[192] 'The Internet Organised Crime Threat Assessment Report (IOCTA) 2015', op. cit., p. 51; Sterling B., 'Alphabay as described by the FBI', *Wired*, 20 July 2017, available at: https://www.wired.com/beyond-the-beyond/2017/07/alphabay-described-fbi/, last visited: 16 March 2018.

Many Darknet sites serve as cross-cutting enablers for criminal behaviour.[193] By facilitating access to counterfeit documents for fraudulent activities, Darknet sites assist in human trafficking and illegal immigration, and weaken border control systems; this can increase the risk of terrorist activities by providing terrorists with the means to acquire travel documents. A preliminary search on Dream Market on 16 January 2018, for example, yielded 373 pages of results for fraudulent UK passports, some of which came with bills, bank statements, and driving licences as proof of identity (see Figure 4). A 2016 study conducted by the University of East London reported that the sale of forged documents, including passports, driving licences and utility bills aids in the movement of terrorists to the UK.[194]

Figure 4: Document fraud on Dream Market



Browse by category

- Digital Goods 42803
- Drugs 45042
- Drugs Paraphernalia 165
- Services 2869
- Other 5024

฿ Exchange

BTC	1.0
mBTC	1000.0
BCH	6.0
USD	12168.2
EUR	10019.0
GBP	8906.8
CAD	15198.8
AUD	15309.0
mBCH	6092.0
SEK	98356.6
NOK	96863.7
DKK	74631.6
TRY	45796.8
CNH	78992.8
HKD	95611.4
RUB	692574.0

11905 search results (0.8 seconds)

Filter

Ships to: | Ships from: | Escrow: | Category: | Cryptocurrency:
Price: B | Searchtext: uk passport | Sort by: | Vendor: All

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
18 19 20 ... 364 365 366 367 368 369 370 371 372 373

10 Passport Scan (UK) Highest Quality and Cheapest
B0.00854
Kingscan (1250) (4.95★)
VA → WW

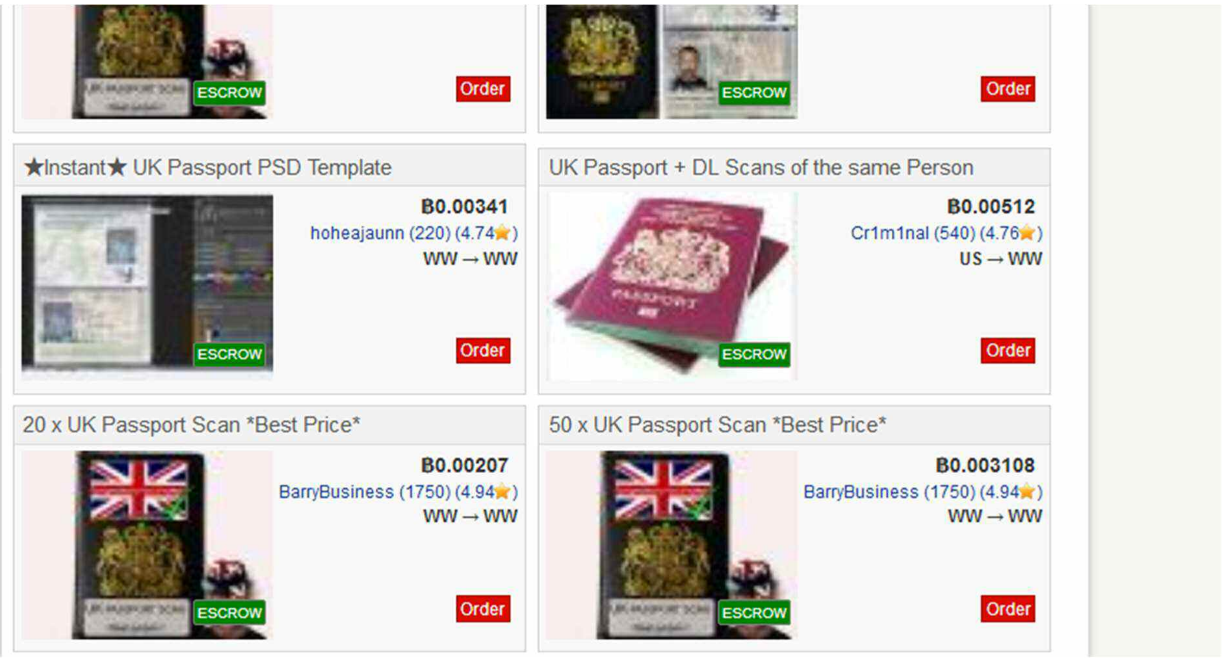
Genuine UK Passport+Bill Set
B0.00769
Kingscan (1250) (4.95★)
VA → WW

100 x UK Passport Scan *Best Price*

NEW UK PASSPORT Template !-HQ- Best Price !

[193] 'The Internet Organised Crime Threat Assessment (IOCTA) 2017', *Europol*, available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017, last visited: 16 March 2018, p. 12.

[194] 'UK fears the sale of fake documents on dark net could aid terror in the country', *Deep Dot Web*, 3 October 2016, available at: https://www.deepdotweb.com/2016/10/03/uk-fears-sale-fake-documents-dark-net-aid-terror-country/, last visited: 16 March 2018.



ESCROW Order

ESCROW Order

★Instant★ UK Passport PSD Template

B0.00341
hoheajaunn (220) (4.74★)
WW → WW

ESCROW Order

UK Passport + DL Scans of the same Person

B0.00512
Cr1m1nal (540) (4.76★)
US → WW

ESCROW Order

20 x UK Passport Scan *Best Price*

B0.00207
BarryBusiness (1750) (4.94★)
WW → WW

ESCROW Order

50 x UK Passport Scan *Best Price*

B0.003108
BarryBusiness (1750) (4.94★)
WW → WW

ESCROW Order

Source: Dreammarket search on 16 January 2018. Comparable results were also found on 'Berlusconi' marketplace, and other marketplaces.

Some evidence indicates that terrorists have used falsified travel documents to travel within Europe. Following the 2016 Berlin Christmas Market Terror attack that killed 12 people and injured 56, German authorities reported that the perpetrator, identified as Anis Amri,[195] was a rejected Tunisian asylum seeker with links to IS.[196] When his request for asylum was rejected, the suspect used different identity documents under various aliases to travel through Europe, eventually committing a terror attack in Berlin.[197] It was also reported that the perpetrators responsible for the Bataclan and Stade de France terror attacks that killed 130 people in Paris in November 2015 had travelled to Syria earlier that year, where they plotted multiple attacks in Paris, and then travelled back to Europe on fake passports to carry out the deadly plot.[198] While it is unclear how the perpetrators of the Berlin Christmas Market attack and the Bataclan and Stade de France attacks obtained their fake travel documents (on the Darknet or through other means), it is important to note that the availability of falsified travel documents on the Darknet has facilitated, and may continue to facilitate, the illegal migration of people involved in various illicit activities, including terrorism.

Weapons

To date, evidence of a direct link between Darknet weapons markets and terrorism has mostly been anecdotal. A week after the attacks in Paris in November 2015, for example, it was reported that the four assault rifles used in the attack had been originally obtained on the Darknet by a man in Germany, who was later arrested on suspicion of running an illegal arms business and selling firearms online.[199] This claim has yet to be verified by French or German authorities, however, and remains unconfirmed. According to official documents from the prosecutor's office in Stuttgart, Germany, the weapons used in the

[195] Oltermann, P., 'Berlin attack: security services feared suspect would commit "act of violence"', *The Guardian*, 22 December 2016, available at: https://www.theguardian.com/world/2016/dec/21/berlin-attack-german-police-leads, last visited: 16 March 2018.
[196] 'European Union Serious And Organised Crime Threat Assessment: Crime In The Age Of Technology', *SOCTA*, op. cit., p. 20.
[197] Huggler, J., M. Benllakehal, J. Mckenna and O. Mckenna, 'Everything we know about Anis Amri, the suspected Berlin Christmas market attacker', *The Telegraph*, 23 December 2016, available at: https://www.telegraph.co.uk/news/2016/12/20/everything-know-suspected-berlin-christmas-market-attacker/, last visited: 19 March 2018.
[198] Ensor, J., 'Fourth British Isil Kingpin unmasked', *The Daily Telegraph*, 26 September 2017, available at: https://www.pressreader.com/uk/the-daily-telegraph/20170926/281487866538883, last visited: 20 November 2017.
[199] Huggler, J., 'Man arrested in Germany on suspicion of illegal arm dealing in terror crackdown', *The Telegraph*, 27 November 2015, available at: http://www.telegraph.co.uk/news/worldnews/europe/germany/12020249/Paris-attackers-bought-weapons-from-arms-dealer-in-Germany.html, last visited: 16 March 2018.

November 2015 Paris attacks were purchased on the Darknet from a German supplier known by the user name "'DW Guns'.[200]

In another case, it was reported that Ali David Sonboly, a teenage attacker of Iranian descent who was allegedly inspired by Anders Breivik's 2011 Far Right terror attacks in Oslo, Norway, had purchased his weapons on the Darknet before shooting and killing nine people in Munich, Germany, on 22 July 2016.[201]

There is, however, much evidence to demonstrate an ongoing presence of criminal arms traffickers operating inside Europe, both online and offline. In 2014, Europol estimated that of the approximately 80 million privately owned firearms in the EU, as many as 500,000 were lost or stolen.[202] The individual connected by the media to the weapons used in the Paris attacks had, in the back of his vehicle, a significant arsenal of weapons, including multiple Kalashnikovs, hand grenades, a pistol, and 200 grams of dynamite.[203] Firearms traffickers use marketplaces on the Darknet to sell weapons of this kind. In December 2016, for example, two individuals were arrested in Slovenia for selling various items, including automatic rifles, hand grenades, and ammunition on the Darknet, receiving payment in the form of bitcoin.[204] Indeed, in a 2017 study conducted by RAND Europe, the Darknet was found to be an enabler for the circulation of illegal weapons, in an online trade which researchers estimated to be worth around US$80,000 per month.[205] This phenomenon is likely to facilitate the nexus between criminal firearms traffickers and terrorists, as it removes the need for a physical connection between vendor and buyer. Self-starter terrorists will be attracted to marketplaces that allow them to obtain weapons behind a virtual veil of anonymity.

Reports have also surfaced about a possible weapons network operating in the UK, raised in a case involving two men charged by British authorities for the sale and distribution of illegal weapons to organised crime syndicates. In September 2017, UK authorities revealed that Umair Khan from Birmingham had used the Darknet to purchase ammunition for firearms classified as "obsolete", because they were outdated and ammunition for those weapons was no longer in circulation. However, he successfully adapted them into fully functioning illegal weapons for sale to criminal gangs.[206] Between August 2014 and February 2017, Khan spent an estimated GB£50,000 procuring more than 50 revolvers and more than 1,600 rounds of ammunition. Two of his weapons were later found in the possession of 16-year-old boys.[207] Khan "was an armourer for organised crime groups and had 'no thought' for where or how the weapons would be used".[208] A second man, Nazim Hussain from West Bromwich, was also convicted for organising the storage of the merchandise and delivery to various locations across Birmingham.[209] Although these cases are not directly linked to terrorist groups, they highlight the availability of weapons that could potentially be used by terrorists.

[200] Vitáris, B., 'Allegedly: German DNM Vendor Sold the Weapons Used at Paris Terror Attacks' *Deep Dot Web*, 2 December 2015, available at: https://www.deepdotweb.com/2015/12/02/german-dnm-vendor-sold-weapons-to-paris-terror-attacks/, last visited: 16 March 2018.

[201] Bender, R. and C. Alessi, 'Munich shooter likely bought reactivated pistol on dark net', *The Wall Street Journal*, 24 July 2016, available at: https://www.wsj.com/articles/munich-shooter-bought-recommissioned-pistol-on-dark-net-1469366686, last visited: 19 March 2018.

[202] 'Europol Review 2014', *Europol* (2014), available at: https://www.europol.europa.eu/activities-services/main-reports/europol-review-2014, last visited: 16 March 2018, p. 9.

[203] Freeman, C., 'Inside the "Ant Trade" – how Europe's terrorists get their guns', *The Telegraph*, 23 November 2015, available at: http://www.telegraph.co.uk/news/worldnews/europe/12010458/Inside-the-Ant-Trade-how-Europes-terrorists-get-their-guns.html, last visited: 16 March 2018.

[204] 'European Serious and Organised Crime Threat Assessment: Crime in the Age of Technology', *SOCTA*, op. cit., p. 23.

[205] Paoli, G. P., J. Aldridge, N. Ryan and R. Warnes, *Behind the Curtain: The illicit trade of firearms, explosives and ammunition on the dark web* (Santa Monica, CA and Cambridge, UK: RAND Europe, July 2017), available at: https://www.rand.org/pubs/research_reports/RR2091.html, last visited: 16 March 2018, p. xiv.

[206] 'Men jailed for buying and selling illegal guns and ammunition', *Crown Prosecution Service*, 18 September 2017, available at: http://www.cps.gov.uk/news/latest_news/men-jailed-for-buying-and-selling-i/index.html, last visited: 16 March 2018.

[207] Southern, K., '"Premier League" underworld arms dealers who sold guns to criminals as young as 16 but were caught trying to buy grenade from undercover officer are jailed for total of 31 years', *Mail Online*, 18 September 2017, available at: http://www.dailymail.co.uk/news/article-4896266/Premier-League-gangland-arms-dealers-jailed-31-years.html, last visited: 16 March 2018.

[208] 'Umair Khan supplied guns and ammunition to crime gangs', *BBC News*, 18 September 2017, available at: http://www.bbc.co.uk/news/uk-england-birmingham-41306909, last visited: 16 March 2018.

[209] 'Men jailed for buying and selling illegal guns and ammunition', *Crown Prosecution Service*, op. cit.; Southern, K., '"Premier League" underworld arms dealers who sold guns to criminals as young as 16 but were caught trying to buy grenade from undercover officer are jailed for total of 31 years', op. cit.

Training

Homemade explosives continue to be the most commonly used weapon in attacks where the perpetrator uses an improvised explosive device (IED).[210] In the aftermath of the March 2017 bombing of a concert in Manchester, UK, it was reported that the perpetrator had accessed information online about how to construct a bomb using triacetone triperoxide (TATP).[211] At the time, bomb-making tutorials were reported to be freely available on YouTube and Facebook.[212] This is significant because TATP has become, in recent years, the "go-to explosive" for IS terrorism in Europe, in part because it is made up of easily obtainable ingredients which can be found among ordinary household goods, such as hair bleach.[213] Indeed, the compound has been a common denominator in a succession of jihadist attacks in Europe, including Paris in November 2015, Brussels in March 2016, Manchester in May 2017, and Parsons Green, London, in September 2017. For self-starter terrorists who are unable to locate these guides through surface web search engines, this information can be easily found on the Darknet, often through links on web forums available on the surface web.[214] In the 2017 RAND study mentioned previously, for example, of the 811 arms-related listings found across 24 Darknet cryptomarkets by researchers, 208 (25%) were eBooks providing instructions for the manufacture of explosives or firearms at home.[215]

The extent to which material support provides credible fodder for terrorism was recently highlighted in a case involving an IS member who used his cyber skills in support of the organisation's cause. In May 2017, British authorities convicted Sumata Ullah, a resident of Cardiff, for being a member of IS. He had used his cyber expertise to create a "one-stop shop" that offered vast amounts of information, including how to avoid detection by law enforcement and expert guidance about missile systems.[216] Ullah provided guided tutorials on how to use encryption programmes such as Tor and PGP to hide online extremist material from law enforcement, and developed mechanisms for IS to distribute its propaganda on the Darknet.[217] Authorities confirmed that IS was actively engaged with the material, using it for "guidance" and "instruction".[218] The CPS argued that the nature of the offences was so serious that, if "left unchecked, the actions of Sumata Ullah could well have helped others carry out further terrorist attacks either in the UK or abroad".[219]

A preliminary search on the Dream Market marketplace using the Tor browser on 18 January 2018 found 1,101 results for instructional material related to "security", including guides on drugs, fraud, hacking, and the use of firearms. The Anarchist Cookbook, which contains bomb-making instructions as well as information on telecommunications phreaking devices and weapons use, was available for sale for BTC0.0003.[220]

[210] 'EU Terrorism Situation and Trend Report (TE-SAT) 2017', op. cit., p. 15.

[211] Hamilton, F. and A. Mostrous, 'Manchester Arena killer Salman Abedi used YouTube to build bomb', *The Times*, 24 June 2017, available at: https://www.thetimes.co.uk/article/ariana-grande-manchester-concert-killer-salman-abedi-used-youtube-to-build-bomb-qzcbs55s3, last visited: 16 March 2018.

[212] ibid.

[213] Callimachi, R., 'How ISIS Built the Machinery of Terror Under Europe's Gaze', *The New York Times*, 29 March 2016, available at: https://www.nytimes.com/2016/03/29/world/europe/isis-attacks-paris-brussels.html, last visited: 16 March 2018.

[214] Dilipraj, E., 'Terror in the Deep and Dark Web', *Air Power Journal*, Vol. 9(3) (2014): pp. 120–140.

[215] Paoli, G. P. et al., *Behind the Curtain: The illicit trade of firearms, explosives and ammunition on the dark web*, op. cit., p. 34.

[216] Pennink, E., 'Cyber jihadi with James Bond-style USB cufflinks jailed for eight years over online terror hub', *Independent*, 2 May 2017, available at: http://www.independent.co.uk/news/uk/crime/cyber-jihadi-samata-ullah-james-bond-usb-cufflinks-isis-cardiff-jailed-8-years-online-terror-dabiq-a7713486.html, last visited: 16 March 2018.

[217] Pennink, E., op. cit.; 'Daesh cyber-terrorist Sumata Ullah jailed', *Crown Prosecution Service*, 2 May 2017, available at: http://www.cps.gov.uk/news/latest_news/daesh-cyber-terrorist-sumata-ullah-/index.html, last visited: 16 March 2018.

[218] Pennink, E., op. cit.

[219] 'Daesh cyber-terrorist Sumata Ullah jailed', op. cit.

[220] Possession of the Anarchist Cookbook has been used in previous court cases in the United Kingdom to link to terrorist activity under Section 58 of the Terrorism Act 2000, available at: https://www.legislation.gov.uk/ukpga/2000/11, last visited: 16 March 2018. In 2010, a member of the violent neo-Nazi group "Wolf Pack" was convicted of a terrorism offence for possessing the book. In 2011, a man was sentenced to three years in prison for selling the Cookbook and Al-Qaeda training manuals. For more, see: Gallagher, R., 'How the U.K. prosecuted a student on terrorism charges for downloading a book', *The Intercept*, 28 October 2017, available at: https://theintercept.com/2017/10/28/josh-walker-anarchist-cookbook-terrorism-act-uk/, last visited: 16 March 2018. It is important to note that a full, and free, copy of the Anarchist Cookbook was available to download as the fourth result of a Google search on 17 January 2018.

Chapter 4: Cryptocurrency

The following chapter looks at the way in which cryptocurrencies have – and could be – utilised by terrorist groups. This chapter compares the emergence of these financial instruments and the crypto-financial system with the hawala system of finance, an informal system of payments used to send money to countries primarily in the Middle East, Africa, and South Asia. Special attention is given to bitcoin and the emergence of other cryptocurrencies.

The *Hawala* Payment System

Since 9/11, international law enforcement agencies have uncovered various means to facilitate the movement of money in support of terrorism. The *hawala* network, translated from Arabic to mean "transfer" or "trust", is a commonly used conduit.[221] *Hawala* has been linked to a number of terrorist organisations, including Al-Qaeda and IS, and has often been used in place of modern online banking systems, with an estimated GB£258.9 billion passing through the network every year.[222] The *hawala* system can be described as an informal way of transferring money across borders, given that it is based on existing relationships of trust between members of the same ethnic group.[223] The *hawala* system flourishes in many regions of the Middle East and South Asia which tend to have relatively under-developed and less formalised banking structures, or where large communities of diaspora populations live. It accounts for an estimated US$500 billion in global remittances.[224]

<u>Example</u>: *Hawala* Payments

A Somali worker in London wants to send £1,000 to a family member in Mogadishu. He goes to a *hawaladar* (the *hawala* broker) and gives him the money in cash (or deposits it into a bank account). The *hawaladar* in return contacts his colleague, a fellow *hawaladar* in Mogadishu, and requests a payment of the Somali Shilling equivalent of £1,000 to the family member of the Somali worker in London. Both the family member and the Mogadishu *hawaladar* are given a security code which is matched at the final pick-up point. The *hawaladar* in Mogadishu is obligated to take the money to the family member's house or arrange a pick-up location. The London-based *hawaladar* is indebted to the Mogadishu-based *hawaladar* and must repay him in due course or provide a service to the value of the £1,000 transaction.

The *hawala* system is readily used by criminals because of the network of trust established within the group, because it avoids high banking fees and because it is suitable for transfers to remote parts of the world. It also evades the bureaucratic administrative process associated with standard banking verification practices, as senders are not required to provide details such as a passport, visa or residence permit information. As the book-keeping systems within *hawala* networks are rudimentary, there is no identifiable paper trail, making it extremely cumbersome for those outside the community to investigate transactions.[225] For this reason, it has often been abused by criminals and terrorists.[226]

Prior to 11 September 2001 terrorist attacks in the US, terrorist groups used these financial systems to transfer money in support of terror-related activities. A 2004 report released by the National Commission on Terrorist Attacks Upon the United States confirmed that before 9/11, Al-Qaeda used *hawala* networks

[221] Moore, J., 'Hawala: the Ancient Banking Practice Used to Finance Terror Groups', *Newsweek*, 24 February 2015, available at: http://www.newsweek.com/underground-european-hawala-network-financing-middle-eastern-terror-groups-307984, last visited: 16 March 2018.
[222] Moore, J., op. cit.
[223] Kochan, N., *The Washing Machine: Money, Crime and Terror in the Offshore system* (London: Duckworth, 2006), p. 212.
[224] Moore, J., op. cit.; Freeman, M. and M. Ruehsen, 'Terrorism financing method: an overview', *Perspectives on Terrorism,* Vol. 7(4) (2013): pp. 5-26, p. 9, last visited: 13 October 2017.
[225] Kochan, N., op. cit., p. 212.
[226] Looney, R., 'Hawala: The Terrorists' Informal Financial Mechanism', *Middle East Policy Journal,* Vol. 10(1) (2003): pp. 164-167.

to transfer money to operations in Afghanistan.[227] Like Al-Qaeda, IS has also used *hawala* systems to pay salaries to its fighters[228] and to transfer money.[229]

Investigations into terrorist-related offences have revealed the use of *hawala* networks to transfer money. In Iraq, two Kurdish individuals were arrested for using *hawala* networks to transfer US$148,000 to *Ansar al Islam* (Supporters of Islam), a proscribed Sunni terrorist group which eventually joined IS.[230] Ali Khan, a Pakistani national residing in Massachusetts, was convicted for transferring a sum of US$4,900 to Faisal Shahzad in February 2010 using a *hawala*-linked transaction.[231] Khan's family later received an equivalent amount of money in Pakistan.[232] Shahzad was subsequently convicted for the attempted May 2010 car bombing of Times Square, New York.[233]

More recently, advances in modern technology have created alternative and sophisticated means of transferring money. Many of these new financial systems, which include cryptocurrency exchanges, offer a degree of anonymity, which may give terrorists an alternate means of conducting financial transactions. While anecdotal evidence shows that some terrorists are using this technology, there is no indication that it has yet been adopted on a large scale. Nevertheless, the cases where terrorists have used cryptocurrency represent a potentially disturbing trend, highlighting the possibility that this could develop further in the future.

Case Study: The Merits of Cryptocurrencies and Distributed Ledger Technology

Distributed Ledger Technology[234] (DLT) can have important benefits as the technology underlying virtual currencies, at both the individual and the institutional levels. Cryptocurrencies such as bitcoin possess the ability to remove the need for intermediaries such as banks and financial institutions, enabling individual transacting parties to interact directly in secure, private, fast and cost-efficient ways.[235] By enabling the cheap transfer of funds across borders, virtual currencies can provide financial empowerment through their use of an inexpensive remittance system, which is able to provide financial services to poor and unbanked populations across the world.[236]

Notwithstanding their current fluctuating value, cryptocurrencies may generally provide an alternative store of value for populations across countries where national fiat currencies are subject to government manipulation, currency over-issuing, and hyperinflation. Dissidents in closed societies who might have their assets frozen for engaging in political opposition may ostensibly use cryptocurrencies to fund activities deemed illegal by repressive governments.

DLT may also benefit financial institutions. If employed, it can eliminate problems associated with banking corruption and fraud by removing the need for intermediaries and, by virtue of representing a computerised system that validates transactions without human intervention, preventing double-spending. Moreover, the technology could be harnessed in anti-money laundering and counter-terrorist financing (AML/CTF) initiatives. Given the ineffectiveness of the current AML/CTF regime, the use of DLT could

[227] Roth, J., D. Greenburg and S. Wille, 'Monograph on Terrorist Financing', *National Commission on Terrorist Attacks Upon the United States* (2004), available at: https://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf, last visited: 16 March 2018, p. 25.

[228] Moore, J., op. cit.

[229] Fitzpatrick, M. and S. F. Lynch, 'Stopping Terror Finance: Securing the U.S. Financial Sector', Report by *Staff of the U.S. Task Force to Investigate Terrorism Financing, Committee of Financial Services, U.S. House of Representatives*, 20 December 2016, available at: https://financialservices.house.gov/uploadedfiles/terror_financing_report_12-20-2016.pdf, last visited: 16 March 2018.

[230] Ritter, K., 'Two Iraqis charged in Sweden with transferring money to al-Zarqawi', *Associated Press*, 4 April 2005.

[231] 'Pakistani Man Sentenced on Unlicensed Money Transmitting and Immigration Fraud Charges', *FBI: U.S. Attorney's Office District of Massachusetts*, 12 April 2011, available at: https://archives.fbi.gov/archives/boston/press-releases/2011/pakistani-man-sentenced-on-unlicensed-money-transmitting-charges-and-immigration-fraud, last visited: 16 March 2018.

[232] ibid.

[233] 'Times Square car bomber Faisal Shahzad pleads guilty "100 times"', *The Telegraph*, 22 June 2010, available at: http://www.telegraph.co.uk/news/worldnews/northamerica/usa/7845570/Times-Square-car-bomber-Faisal-Shahzad-pleads-guilty-100-times.html, last visited: 16 March 2018.

[234] A digital, decentralised, permanent record of transactions.

[235] Nakamoto, S., 'Bitcoin: A Peer-to-Peer Electronic Cash System' (no date), available at: https://bitcoin.org/bitcoin.pdf, last visited: 16 March 2018

[236] Brito, J. and A. Castillo, 'Bitcoin: A Primer for Policymakers', *Mercatus Center, George Mason University* (2013), available at: https://www.mercatus.org/system/files/Brito_BitcoinPrimer.pdf, last visited: 16 March 2018; Duhaime, C., 'The non-techie guide to the Blockchain, distributed ledger tech and Bitcoin'. *Duhaime Law* (2017), available at: http://www.antimoneylaunderinglaw.com/2017/09/the-non-techie-guide-to-the-blockchain-distributed-ledger-tech-and-bitcoin.html, last visited: 19 March 2018.

channel its "cryptographically secure, decentralised, and immutable nature"[237] to identify suspicious financial transactions, utilising the permanent record to "follow the money" and trace back the sources of illicit funds. Moreover, virtual currencies can also benefit businesses, as these "facilitate micro-payments", allowing for the monetisation of "low-cost goods or services sold on the internet".[238]

The legitimate uses of virtual currencies and DLT also carry a number of wide-ranging advantages that extend beyond those purely benefiting the realm of finance and financial services. For instance, DLT can be used by governments across the world for a wide range of purposes, such as verification, ownership and identification.[239] The implementation of DLT solutions could allow public sector institutions to quickly, efficiently and securely verify licences, proofs of records, transactions and processes; to keep track of the "chain of custody" for physical assets; as well as to issue "e-identities" to allow citizens access to multiple services and rights.[240]

The Bitcoin Payment System

Released in 2009, bitcoin is a cryptographic peer-to-peer version of electronic money which allows payments to be delivered online from one party to another by circumventing traditional financial institutions.[241] Driven by the growing desire for a monetary regime independent of third party financial regulators, bitcoin creators developed a decentralised payment system which is neither issued nor backed by a financial intermediary such as a bank. The technology that supports bitcoin is based on a blockchain system which acts as a virtual public ledger that processes and verifies each bitcoin transaction in the network.[242] The blockchain system is defined as a "record of all validated transactions grouped into blocks, each cryptographically linked to predecessor transactions down to the genesis block, thereby creating a 'chain of blocks'".[243]

A key defining feature of bitcoin is its decentralised network, which has no central authority that processes or verifies transactions, but is instead connected through a chain of networks on the blockchain that verifies and confirms each transaction. This means that anyone can access bitcoins without going through a bank or financial institution, which would require the provision of verifiable personal details. Bitcoins are created through a process of "mining" to verify each transaction on the blockchain. While information relating to each transaction is recorded on the blockchain, this information is not directly linked to names, physical addresses or other identifying information, which makes it anonymous to a certain degree, complicating efforts by law enforcement agencies to identify individual transactions and link them to users.[244] According to a 2015 Europol report, bitcoin featured in high-profile investigations involving payments between criminals, and was used in more than 40% of these transactions in the EU in that year.[245]

Terrorists and criminals use bitcoin for illicit transitions because it offers similar benefits to the *hawala* system. Bitcoin provides financial security as the blockchain acts as an impartial intermediary, ensuring that coins are irrevocable once spent. The network hampers any attempt to recall a verified bitcoin transaction unless the recipient actually sends the coins back to the sender.[246] In this context, it prevents

[237] De Costa, F., 'Blockchain for AML: Harnessing Technology to Detect and Prevent Money Laundering', *International Banker* (2017), available at: https://internationalbanker.com/technology/blockchain-aml-harnessing-blockchain-technology-detect-prevent-money-laundering/, last visited: 19 March 2018.

[238] 'Virtual Currencies: Key Definitions and Potential AML/CTF Risks', *Financial Action Task Force* (2014), available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, last visited: 19 March 2018, p. 11.

[239] Mougayar, W., 'Why the Blockhain is perfect for Government Services', *Observer*, 8 September 2016, available at: https://www.observer.com/2016/09/why-the-blockchain-is-perfect-for-government-services/, last visited: 16 March 2018.

[240] ibid.

[241] Nakamoto, S., 'Bitcoin: A Peer-to-Peer Electronic Cash System', op. cit.

[242] Hileman, G. and M. Rauchs, 'Global Cryptocurrency Benchmarking Study', *Judge Business School, University of Cambridge* (2017), available at: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf, last visited: 16 March 2018, p. 13.

[243] ibid.

[244] Miners are responsible for grouping unconfirmed transactions into new blocks and adding them to the global ledger (the "blockchain"). Each block added to the blockchain by a miner generates a reward. Additional blocks make it more difficult for a potential attacker to reorganise the blockchain and double spend transactions. For more, see: Hileman, G. and M. Rauchs, 'Global Cryptocurrency Benchmarking Study', op. cit., p. 89.

[245] 'The Internet Organised Crime Threat Assessment (IOCTA) 2015' op. cit., p. 11.

[246] Rotman, S., 'Bitcoin Versus Electronic Money', *CGAP*, January 2014, available at: https://www.cgap.org/sites/default/files/Brief-Bitcoin-versus-Electronic-Money-Jan-2014.pdf, last visited: 16 March 2018.

double spending and ensures that money cannot be duplicated within the network.[247] A network of "miners" ensures that each bitcoin transaction is unique and legitimate.[248] If an attempt at duplication is made, the blockchain rejects the transaction as forged and faulty.[249] As such, it benefits both criminals and terrorists purchasing goods and services on the Darknet, who otherwise would be at risk of being scammed by rival criminal organisations on the other side of the network.

Material Support

Islamic State

Stringent border and legal controls have made it increasingly difficult for jihadist sympathisers to travel to Syria and Iraq. As a result, IS has increased its calls for material support.[250] IS uses money obtained from supporters for an array of activities that tie into the group's broader ideology.[251] Material support can provide for the personal needs of operatives (who require income, training, and travel) and may extend to their dependants. Alternatively, it could be used to facilitate terrorist operations.[252] To this extent, the group continually raises funds by any means possible: from the sale of oil and extortion, by diverting funds from legitimate charities, and through public appeals for donations from its supporters.[253]

In August 2015, US authorities convicted Mohamed Elshinawy, from Maryland, for providing material support of a financial nature to IS.[254] According to official records, Elshinawy had received approximately US$8,700 through various financial channels, including Western Union and PayPal accounts, from individuals with known connections to IS, for the purpose of funding terrorist operations.[255] Elshinawy, who had received the money between March and June 2015 from various overseas companies located in the UK and Bangladesh, intended to use the funds to launch terrorist attacks in the US.[256] According to the US Department of Justice, Elshinawy and other members of IS had used various means of "secret communication in order to conceal their criminal association and activities from law enforcement".[257]

Since 2014, there have been reports of high-ranking jihadist fighters in Raqqa, a former IS stronghold in Syria, making use of money transfer offices for small or domestic purchases, and using advanced modern technology in the form of bitcoin for long-distance international transactions.[258] In January 2015 it was reported that IS, in what was then an unprecedented move, had started raising funds through bitcoin. A fundraiser identified as Abu-Mustafa argued that a massive crackdown by US law enforcement on mainstream financial platforms, coupled with a lack of financial and other resources available to IS supporters in the US and South America, meant that the Darknet should be used to raise funds in bitcoin.[259] Abu-Mustafa raised about five bitcoins, valued at approximately US$1,000 (at the time), before the account was closed.[260]

[247] Double-spending is referred to as using the same bitcoins more than once or several times. See: 'What is Bitcoin Double Spending', *Bitcoin.com Academy*, 23 June 2017, available at: https://www.bitcoin.com/info/what-is-bitcoin-double-spending, last visited: 16 March 2018.

[248] 'What is Bitcoin Mining', *Cointelegraph* (no date), available at: https://cointelegraph.com/bitcoin-for-beginners/what-is-mining, last visited: 16 March 2018.

[249] 'What is Bitcoin Double Spending?', *Bitcoin.com Academy*, op. cit.

[250] Berton, B., 'The dark side of the web: ISIL's one stop shop?', *European Union Institute for Security Studies*, 26 June 2015, available at: https://www.iss.europa.eu/content/dark-side-web-isil%E2%80%99s-one-stop-shop, last visited: 16 March 2018. pp. 1-2; Webb, S., 'Daesh in the Digital Age: Online Extremism and the New Terror', *The Mackenzie Institute* (2016), available at: www.academia.edu/30413200/DAESH_IN_THE_DIGITAL_AGE_ONLINE_EXTREMISM_AND_THE_NEW_TERROR, last visited: 16 March 2018.

[251] Goldman, Z. K. et al, op cit. p. 10.

[252] ibid., p. 10.

[253] ibid., p. 10.

[254] 'Maryland Man Pleads Guilty for Conspiring to Provide and for Providing Material Support to IS', *The United States Department of Justice*, 15 August 2017, available at: https://www.justice.gov/opa/pr/maryland-man-pleads-guilty-conspiring-provide-and-providing-material-support-isis, last visited: 16 March 2018.

[255] Goldman, Z. K. et al, op. cit., p. 11.

[256] Bui, L., 'Md. man pleads guilty to accepting nearly $9,000 to help carry out U.S. terrorist attack', *The Washington Post*, 15 August 2017, available at: https://www.washingtonpost.com/local/public-safety/md-man-pleads-guilty-to-accepting-nearly-9000-to-help-carry-out-us-terror-attack/2017/08/15/88fb2dc8-81fc-11e7-ab27-1a21a8e006ab_story.html?utm_term=.f1986cd900f7, last visited: 16 March 2018.

[257] Bui, L., op. cit.

[258] Ensor, J., op. cit.

[259] Harman, D., 'U.S.-based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests', *Haaretz*, 29 January 2015, available at: https://www.haaretz.com/middle-east-news/.premium-1.639542, last visited: 16 March 2018.

[260] Goldman, Z. K. et al, op. cit., p. 12.

In June 2015, US authorities convicted Shukri Amin, a 17-year-old in Virginia, for lending material support to IS. Amin was charged with helping IS supporters travel to Syria by using social media sites to ask donors to pay in bitcoin currency as financial support for the group.[261] In another case, a woman was arrested in New York in December 2017 for fraudulently obtaining US$62,000 in bitcoin, which she then allegedly wired to fund IS. After a failed attempt to join IS in January 2016, the woman used false information to acquire loans and multiple credit cards, which she then converted into bitcoin and other cryptocurrencies before sending the money via Pakistan, China and Turkey to fund IS.[262] Prosecutors accused the woman of fraud and providing material support of a terrorist organisation.

In December 2017, an IS-affiliated Darknet site by the name *Isdarat,* accessible through the Tor browser, was also seeking bitcoin contributions from supporters.[263] Though it is unclear how successful the site was in raising bitcoin funds, these examples demonstrate an awareness and interest on the part of terrorist networks in the merits of bitcoin as a medium through which to finance themselves online.

Other Terrorist Organisations

The borderless nature of bitcoin is likely to attract terrorists, particularly international terrorist organisations such as IS whose operations are global in scope. By fundraising and making financial transactions online with bitcoin, terrorists and other criminals can avoid interference from financial regulators or other third parties, who might otherwise take steps to prevent their operations. In a case reported in 2016, the media division of the *Mujahideen Shura* (Council in the Environs of Jerusalem), a coalition of Salafi-jihadist groups located in Gaza and a proscribed terrorist organisation according to the US Department of State (DoS), began a public social media campaign to raise bitcoin.[264] The fundraising campaign requested the amount of US$2,500 for each fighter and had received approximately US$540 in total by July 2016.[265] In another similar case documented in January 2017, Indonesian authorities revealed that Islamist militants based in the Middle East used bitcoin to transfer money to fund domestic terrorist attacks in the country.[266] One of the alleged donors, Bahrun Naim,[267] an Indonesian with links to IS, played an instrumental role in organising terror attacks in Indonesia by sending money via PayPal and bitcoin to his associates in the country.[268] These events, while anecdotal in nature, point to the possibility that cryptocurrencies may be used to fund terrorism if not regulated.[269]

In November 2017, a case was identified in a social media campaign run on Facebook by an Al-Qaeda linked organisation called *Al-Sadaqah* (voluntary giving).[270] Though the relevant Facebook accounts were quickly shut down, the group continued to campaign for bitcoin funding through a public channel on Telegram, as well as more publically on Twitter. "Donate anonymously and securely with bitcoin," read one post in a request for donations to help with what was described as camp facilities and reinforcements

[261] Goldman, Z. K., et al, op. cit., p. 13.

[262] Alexander, H., 'New York woman charged with sending $85,000 in Bitcoin to support ISIL', *The Telegraph*, 14 December 2017, available at: http://www.telegraph.co.uk/news/2017/12/14/new-york-woman-charged-sending-85000-bitcoin-support-isil/, last visited: 16 March 2018.

[263] ibid.

[264] 'Foreign Terrorist Organizations', U.S. Department of State (no date), available at: https://www.state.gov/j/ct/rls/other/des/123085.htm, last visited: 16 March 2018; Fanusie, Y. J., 'The New Frontier in Terror Fundraising: Bitcoin', *Foundation for Defense of Democracies*, 24 August 2016, available at: www.defenddemocracy.org/media-hit/yaya-j-fanusie-the-new-frontier-in-terror-fundraising-bitcoin/, last visited: 16 March 2018.

[265] Fanusie, Y. J., op. cit.

[266] Soeriaatmadja, W., 'Militant Bahrun Naim used PayPal, bitcoin to transfer funds for terror attacks in Indonesia', *The Straits Times*, 9 January 2017, available at: http://www.straitstimes.com/asia/se-asia/militant-bahrun-naim-used-paypal-bitcoin-to-transfer-funds-for-terror-attacks-in, last visited: 16 March 2018.

[267] Bahrun Naim is purportedly still in Syria. See: 'Police unable to confirm reports of Bahrun Naim's death', *The Jakarta Post*, 5 December 2017, available at: http://www.thejakartapost.com/news/2017/12/05/police-unable-to-confirm-reports-of-bahrun-naims-death.html, last visited: 16 March 2018. He is on the UN Security Council financial sanctions list for his affiliation with IS: 'QDi.404 Muhammad Bahrun Naim Anggih Tamtomo', *UN Security Council, ISIL (Da'esh) & Al-Qaida Sanctions Committee*, 20 July 2017, available at: https://www.un.org/sc/suborg/en/sanctions/1267/aq_sanctions_list/summaries/individual/muhammad-bahrum-naim-anggih-tamtomo, last visited: 16 March 2018.

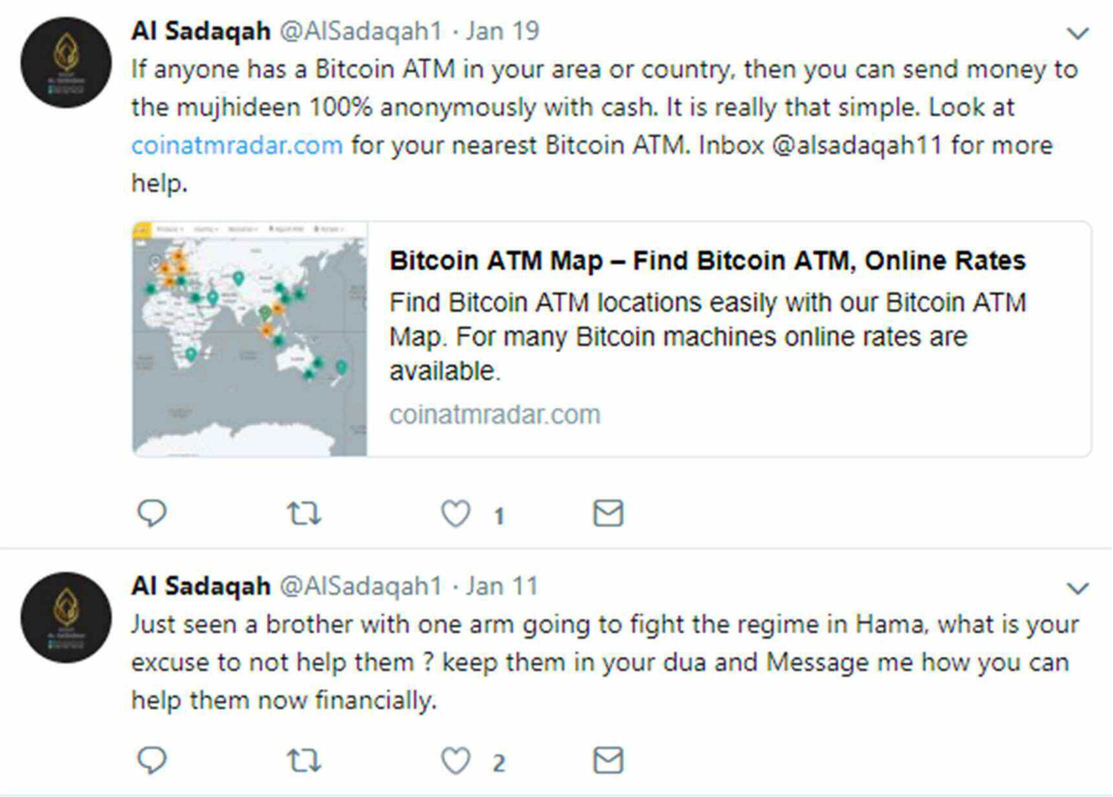
[268] Yuniar, W, R., 'Bitcoin, Paypal Used to Finance Terrorism, Indonesian Agency Says', *The Wall Street Journal*, 10 January 2017, available at: https://www.wsj.com/articles/bitcoin-paypal-used-to-finance-terrorism-indonesian-agency-says-1483964198, last visited: 16 March 2018.

[269] Naim also used Telegram. For more, see: Karmini, N., 'Indonesia Lifts Threat to Ban Encrypted App Telegram', *Bloomberg*, 1 August 2017, available at: https://www.bloomberg.com/news/articles/2017-08-01/indonesia-lifts-threat-to-ban-encrypted-app-telegram, last visited: 16 March 2018.

[270] 'Online Campaign in English Raising Funds for the Jihad in Syria in Bitcoin', *MEMI Cyber & Jihad Lab*, 13 November 2017, Available at: http://cjlab.memri.org/latest-reports/online-campaign-in-english-raising-funds-for-the-jihad-in-syria-in-bitcoin/, last visited: 16 March 2018.

in Latakia province, Syria.[271] On 30 November 2017, a donation of BTC0.075 (US$685 at the time) was sent by an unknown individual to the organisation's advertised bitcoin address. The following day, the funds (which had risen in value to US$803 overnight) were forwarded to another address.[272] When the group's Telegram account was taken down by administrators, it shifted its fundraising activities to an alternative Telegram account, and by late December 2017 it was still sharing Islamist propaganda and imploring supporters to donate securely with bitcoin.[273] In March 2018, the group was still active on Twitter.

Figure 5: Screenshot of *Al-Sadaqah* campaigning for bitcoin funding on Twitter



Al Sadaqah @AlSadaqah1 · Jan 19

If anyone has a Bitcoin ATM in your area or country, then you can send money to the mujhideen 100% anonymously with cash. It is really that simple. Look at coinatmradar.com for your nearest Bitcoin ATM. Inbox @alsadaqah11 for more help.

Bitcoin ATM Map – Find Bitcoin ATM, Online Rates

Find Bitcoin ATM locations easily with our Bitcoin ATM Map. For many Bitcoin machines online rates are available.

coinatmradar.com

Al Sadaqah @AlSadaqah1 · Jan 11

Just seen a brother with one arm going to fight the regime in Hama, what is your excuse to not help them ? keep them in your dua and Message me how you can help them now financially.

How Anonymous is Bitcoin?

Terrorists and criminals use bitcoin because of its anonymity. However, bitcoin is not as anonymous as commonly perceived, as it uses a blockchain system which serves as a virtual record of all transactions on the network. The blockchain is publicly accessible, meaning that someone with a sufficient level of computer literacy can trace the digital footprints of anonymous traders.[274] Because of this, bitcoin is often used on the Darknet with the anonymising software Tor for increased security and anonymity. In this context, criminals use cryptocurrency because it provides the same form of anonymity in the financial setting as encryption does for communication systems.[275]

Both systems hamper efforts by law enforcement to unravel complicated encrypted messaging sites and blockchain payments on the internet. The dangers of cryptocurrency have been highlighted by Europol,

[271] Fanusie, Y. J., 'Terrorist Networks Eye Bitcoin as Cryptocurrency's Price Rises', *The Cipher Brief*, 21 December 2017, available at: https://www.thecipherbrief.com/terrorist-networks-eye-bitcoin-cryptocurrencys-price-rises, last visited: 16 March 2018.

[272] Fanusie, Y. J., 'The New Frontier in Terror Fundraising: Bitcoin', *Foundation for Defense of Democracies*, 24 August 2016, available at: www.defenddemocracy.org/media-hit/yaya-j-fanusie-the-new-frontier-in-terror-fundraising-bitcoin/, last visited: 16 March 2018.

[273] ibid.

[274] Rotman, S., op. cit., pp. 1-2.

[275] 'The Internet Organised Crime Threat Assessment' (IOCTA) 2017', op. cit. p. 49.

Interpol and the Basel Institute on Governance, who identified that "there is a clear consensus that digital currencies pose a money laundering and terrorist financing threat".[276] In 2017, the US government proposed that the Department of Homeland Security (DHS) study the link between bitcoin and terrorism, largely because of the level of anonymity offered by these cryptocurrencies which provides terrorists with the "privacy" they seek.[277]

Since its release in 2009, bitcoin has experienced significant volatility in market value. Continued surges in bitcoin's market price value within an unregulated financial cryptocurrency system can lure more criminals, including terrorists, to use bitcoin. In November 2017, bitcoin's market price had reached US$8,000,[278] and leaped to just over US$11,000 in early December 2017.[279] However, it slumped in value in early 2018.[280] The UK Treasury Department has initiated attempts to increase regulation and requires cryptocurrency and virtual currency exchange users to disclose their identities.[281] It is believed that the measure will likely limit bitcoin's anonymity and thus its appeal to criminals, bringing the currency in line with existing anti-money laundering (AML) and counter-terrorism financial legislation.[282]

New Technological Advancements

As previously highlighted, bitcoin is not completely anonymous because transactions on the blockchain can be unravelled and traced to users, which serves as a possible disincentive to criminals and terrorists[283] (see Case Study SR2, for example). Because of this, some terrorists prefer the "dark wallet", a software program seen as more anonymous than bitcoin. Dark wallet was considered to be largely "unstable" when it was initially created in 2014.[284]

The dark wallet "securely store[s], send[s] and receive[s] cryptocurrencies" by the use of "private and public cryptographic keys".[285] The programme obfuscates transactions through a process of complex encryptions and combines multiple transactions, making it practically impossible to trace the origin and destination of a given transaction.[286] In 2014, an online post by an alleged IS supporter detailed the frustrations that members of the group had with money transfers to its members. The purported yet unverified IS publication, entitled 'Bitcoin and the Charity of Violent Physical Struggle'[287] by Taqi'ul-Deen al-Munthir, argues that in order for IS to successfully fund its terror operations, it has to operate beyond the ambit of the Western financial system.[288] The post explained that "one cannot send a bank transfer to a *mujahid* [jihad fighter] or suspected *mujahid* without the *kafir* [disbeliever] governments ruling today immediately being aware".[289] The author called for supporters to hide financial transaction

[276] Aliens, C., 'UK Targets Dark Web Users in Anti-terrorism Pamphlet', *Deep Dot Web*, 10 July 2017, available at: https://www.deepdotweb.com/2017/07/10/uk-targets-dark-web-users-anti-terrorism-pamphlet/, last visited: 16 March 2018.

[277] Aliens, C., 'Homeland Security May Study Bitcoin's Link to Terrorism', *Deep Dot Web*, 5 June 2017, available at: https://www.deepdotweb.com/2017/06/05/homeland-security-may-study-bitcoins-link-terrorism/, last visited: 16 March 2018.

[278] Davies, R., 'Bitcoin breaks $8,000 barrier amid speculation over spin-off', *The Guardian*, 17 November 2017, available at: https://www.theguardian.com/technology/2017/nov/17/bitcoin-breaks-8000-barrier-amid-speculation-over-spin-off?CMP=share_btn_link, last visited: 16 March 2018.

[279] Mendick, R. and G. Rayner, 'Treasury crackdown on Bitcoin over concerns it is used to launder money and dodge tax', *The Telegraph*, 3 December 2017, available at: http://www.telegraph.co.uk/news/2017/12/03/bitcoin-crackdown-amid-fears-money-laundering-tax-dodging/, last visited: 16 March 2018.

[280] Hopps, K., 'Bitcoin price prediction: Will 2018 be the worst year yet for cryptocurrency?', *Express*, 21 February 2018, available at: https://www.express.co.uk/finance/city/920003/Bitcoin-price-prediction-2018-cryptocurrency-crypto-news, last visited: 16 March 2018.

[281] Mendick, R. and G. Rayner, op. cit.

[282] Kollewe, J., 'Bitcoin: UK and EU plan crackdown amid crime and tax evasion fears', *The Guardian*, 4 December 2017, available at: https://www.theguardian.com/technology/2017/dec/04/bitcoin-uk-eu-plan-cryptocurrency-price-traders-anonymity, last visited: 16 March 2018.

[283] Goldman, Z. K. et al, op. cit., p. 6.

[284] Johnson, A. B., 'Dark Wallet Walkthrough', *Bitcoin Magazine*, 31 October 2014, available at: https://bitcoinmagazine.com/articles/dark-wallet-walkthrough-1414730735/, last visited: 16 March 2018, p. 50.

[285] Hileman, G. and M. Rauchs, op. cit.

[286] Greenburg, A., '"Dark Wallet" is About to Make Bitcoin Money Laundering Easier Than Ever', *Wired*, 29 April 2014, available at: https://www.wired.com/2014/04/dark-wallet/, last visited: 16 March 2018.

[287] Al-Munthir, T., 'Bitcoin and the Charity of Violent Physical Struggle' (no date), available at: https://alkhilafaharidat.files.wordpress.com/2014/07/btcedit-21.pdf, last visited: 20 October 2017. The publication was accessed through a standard Google search on the surface web. It is also available on Duckduckgo.com, a surface web search engine that does not track the identity of users or sites visited.

[288] Wile, R., 'Supporter of Extremist Group ISIS Explains How Bitcoin Could Be Used to Fund Jihad', *Business Insider*, 8 July 2014, available at: http://www.businessinsider.com/isis-supporter-outlines-how-to-support-terror-group-with-bitcoin-2014-7?IR=T, last visited: 16 March 2018.

[289] Al-Munthir, T., op. cit., p. 1.

trails by using the so-called "dark wallet", which makes it difficult for law enforcement to trace transactions.[290]

The emergence of new cryptocurrencies with added security features has made alternate financial payment systems more attractive to terrorist organisations. In using these newer models, transactions are not linked to any identifiable user.[291] Unlike bitcoin, many newer cryptocurrencies have added security features. Monero, launched in 2014, is an example of a cryptocurrency that has advanced features and provides better privacy settings. It is now accepted on various Darknet marketplaces. By January 2018, three months after Europol had acknowledged Monero as a cryptocurrency that was "gaining popularity within the digital underworld", it was reported that criminals were losing interest in bitcoin in favour of Monero, because the latter offered more security and anonymity.[292] Against this backdrop, the UK and other EU governments plan to introduce regulations for bitcoin and other cryptocurrencies, which will take effect later in 2018.[293] The new legislation will increase transparency by placing cryptocurrencies under the purview of AML and counter-terrorist financing legislation.[294]

[290] ibid.
[291] 'The Internet Organised Crime Threat Assessment (IOCTA) 2017, op. cit., p. 61.
[292] Kharif, O., 'Bitcoin is being dropped by criminals in favour of privacy coins like monero', *Independent*, 2 January 2018, available at: http://www.independent.co.uk/news/business/analysis-and-features/bitcoin-latest-updates-price-privacy-coins-cryptocurrency-monero-digital-currency-price-a8137901.html, last visited: 16 March 2018.
[293] Hodgson, C., 'The UK and EU want to force bitcoin users to reveal their identities', *Business Insider UK*, 4 December 2017, available at: http://uk.businessinsider.com/anti-money-laundering-cryptocurrencies-regulation-eu-uk-identity-2017-12, last visited: 16 March 2018.
[294] ibid.

Conclusions and Policy Recommendations

This report evaluates the ways in which extremists and terrorists use new technologies – encrypted communication technologies, the Darknet, and cryptocurrencies – in aspects of their operations and activities. This paper does not reveal wide-scale use of the new technologies by terrorists and extremists, and the evidence presented of this use is limited. However, case studies are used to indicate that, unless appropriately addressed, emerging trends may burgeon into major challenges in the future.

As this report has shown, the internet can be classified into the surface web, the deep web, and the Darknet. Extremist content and instructional terrorist material, as well as funding campaigns to raise money for terrorist groups, can be found on all parts of the internet, with varying degrees of accessibility. While some of these issues have been addressed in the UK by the 2016 Investigatory Powers Bill, there remains work to be done to further research on extremism and terrorism on the Darknet and to understand its links to, and overlap with, the surface web.

The following recommendations focus on fostering human intelligence and capacity building in this area:

1. Technology companies should create a self-regulatory system to remove and audit extremist content, and release publicly available annual reports outlining their efforts in this space.

The existing powers and regulations available in the United Kingdom to audit and regulate the internet are unclear. Further complicating the matter is the fact that companies such as Google and Facebook operate as quasi-monopolies and enjoy dominant market positions. The first and most desirable option is to apply greater pressure on these companies to promote, implement and approve a self-regulatory model where transparency and accountability concerning the removal of extremist content hosted on these platforms is made publicly available through an annual report. Such reports should reference statistics on content flagged by users, outcomes of investigated content, decision-making systems employed by these companies on content removal, case studies, and areas for improvement. Transparency will further incentivise technology companies to cooperate in this field, and has the potential to foster further innovation in the successful removal of extremist and hate content.

Surface Web

The public should be able to report and flag extremist content found on the surface web to those companies hosting such content. For example, there is still no "flagging" system for users to report instructional terrorist manuals or disturbing extremist content on Google search results, with software often auto-predicting extremist literature or directing vulnerable people who may consume this content to more extremist literature (in multiple languages). An example of a solution could be the creation and dissemination of trusted third-party programs for platforms like Google, and other search engines, to make such extremist material less visible (see Appendix 1).

Deep Web

Self-regulation mechanisms should also be applied by technology companies such as Facebook and Twitter, who have an equivalent social responsibility towards their users. Again, annual reports on internal auditing mechanisms should be made publicly available, bolstered by online reporting mechanisms involving the public.

Darknet

The Government should lead campaigns to deconstruct myths around the Darknet. The 2017 report by David Anderson QC, the former Independent Reviewer of Terrorism Legislation in the UK, indicated a new commitment by MI5 to allow knowledge derived from intelligence to be shared more widely beyond intelligence circles.[295] Building and sharing intelligence capital in this way will help to deconstruct myths about the Darknet, by providing explanations and evidence on its use.

GCHQ can also share knowledge with ordinary researchers and universities to train them on understanding internal Darknet hidden market communities, as well as on regulation and the code of conduct for intelligence gathering (see Figure 1).

External Auditing and Supervisory Powers

While a self-regulatory model to remove and audit extremist content is an ideal solution, it has yet to be realised to date. Extremist content is still widely available online, and there remains further work to be done by technology companies to remove this material (see Appendix 1). If such self-regulation continues to fail, the need for a regulatory body to supervise and assess the efforts of these technology companies in this space only grows.

Expanding the Supervisory Powers of Existing Bodies

The debate on whether the existing supervisory powers of the Office of Communications (Ofcom) can be expanded to achieve the above depends on whether social media companies can be classified as publishers. While this presents a potential solution, it requires a change in classification, and the lack of resources available to Ofcom may mean that such regulation is not possible.[296]

2. The British government should create an Internet Regulatory Body.

Creating a New Internet Regulatory Body

If resources to expand and include the supervisory powers of existing bodies are insufficient, an external body of experts (an Internet Regulatory Body) should be appointed with the role of regulating, scrutinising, and auditing the efforts of technology companies to remove extremist content and instructional terrorist content.

The Internet Regulatory Body must first review the efforts of social media companies to self-regulate content off their own platforms, with the potential for fines being placed on those companies that consistently fail to remove instructional terrorist material, material support campaigns that fund terrorism, or propaganda shared by proscribed terrorist organisations and preachers. Fines can follow the model of breaching UK competition law,[297] and the Internet Regulatory Body should work closely with the Counter Terrorism Internet Referral Unit (CTIRU) and other existing regulatory bodies to achieve this. Part of the auditing process should include regular annual reports, which measure key metrics on compliance and reflect on areas of improvement, and are available to the public.

Money created from potential fines on companies that fail audit reviews can potentially be used to fund intelligence capital on crime and terrorism on the Darknet. This can involve funding research and analysis of marketplaces on the Darknet, the use of cryptocurrency and encryption by terrorists, and learning how to infiltrate, study, examine, and source terrorist content and data into an archive for researchers and law enforcement who need to refer to this material. Regarding internet policing, while polls in 2015[298] indicated

[295] Anderson, D., 'Attacks in London and Manchester March-June 2017', *Independent Assessment of MI5 and Police Internal Reviews*, December 2017, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/664682/Attacks_in_London_and_Manchester_Open_Report.pdf, last visited: 17 March 2018, p. 33.

[296] Mayhew, F., 'Lord Burns tells MPs Ofcom would be "suitable vehicle" to regulate social media as he is approved next chairman', *PressGazette*, 13 December 2017, available at: www.pressgazette.co.uk/lord-burns-tells-mps-ofcom-would-be-suitable-vehicle-to-regulate-social-media-as-he-is-approved-next-chairman/, last visited: 17 March 2018.

[297] Firms involved in anti-competitive behaviour, including abuse of a dominant market position, risk being fined up to 10% of group global turnover. Anti-competitive behaviour within the UK is specifically prohibited by Chapters I and II of the Competition Act 1998 and the Enterprise Act 2002. However, it should be noted that fines are fiscally complicated. For more, see: 'Competition law – the basics', *Out-Law.com*, April 2014, available at: https://www.out-law.com/en/topics/eu--competition/competition/competition-law---the-basics/, last visited: 17 March 2018; 'An overview of the UK competition rules', *Slaughter and May*, June 2016, available at: https://www.slaughterandmay.com/media/1515647/an-overview-of-the-uk-competition-rules.pdf, last visited: 17 March, 2018; Titcomb, J., 'Google hit with record £2.1bn EU fine for abusing internet search monopoly', *The Telegraph*, 27 June 2017, available at: https://www.telegraph.co.uk/technology/2017/06/27/eu-hits-google-record-21bn-fine-abusing-internet-search-monopoly/, last visited: 17 March 2018.

[298] See: Bartlett, J. and A. Krasodomski-Jones, 'Online Anonymity Islamic State and Surveillance' *Demos*, (2015), available at: https://www.demos.co.uk/files/Islamic_State_and_Encryption.pdf?1426713922, last visited: 17 March 2018, p. 4.

that public concern about internet privacy was increasing, a 2017 study by Demos found that the public would be open to sacrificing civil liberties to protect social safety (32% were in favour of a safety-first approach, compared to 23% in favour of protecting civil liberties).[299] The same study found that 90% of the British public believe that technology companies have a responsibility to police their content, and would be willing to wait more than three minutes on average to send a text message in exchange for stricter regulation.[300]

3. More resources should be dedicated to the Joint Terrorism Analysis Centre (JTAC) to build intelligence capital on the Darknet.

The monitoring of instructional terrorist material on the Darknet, and how criminals and terrorists may use funding to drive document fraud, guns, and proceeds from drug sales, will require the cooperation of diverse approaches of national cyber security. The NCA and GCHQ set up a specialist unit to look at the Darknet in 2014.[301] While this focuses on child abuse, similar coordination can be used to examine terrorism. More resources should be dedicated to JTAC in coordinating intelligence approaches on policing online markets, using human intelligence to monitor activity.

Moreover, terrorist funding campaigns such as those seen on the deep web and on the Darknet involving bitcoin and other cryptocurrencies and referenced in this report should fall under the remit of the new Anti-Money Laundering Watchdog,[302] and JTAC can work with this body to disrupt financial flows to terrorist and extremist groups.

4. Social media companies should work with law enforcement to ensure that extremist material is not simply removed, but archived effectively to understand patterns of behaviour.

The removal of extremist and terrorist content from the surface web, deep web, and Darknet – particularly in the case of artificial intelligence programs that may do "bulk" removals – creates a risk that evidence needed for prosecution of individuals disseminating content or providing material support to terrorist organisations may be lost. Social media companies should work with law enforcement to ensure that this material is not simply removed, but archived effectively to understand patterns of behaviour.

Further complicating ambiguities of any auditing process is legal interpretation. More than ever, there is a need for legislation to understand context, intent, and anonymity in cases of prosecution of those disseminating extremist or terrorist content online, including, but not limited to, Section 2 of the Terrorism Act 2006[303] and Section 58 of the Terrorism Act 2000.[304] Therefore, greater transparency is required on government definitions of terrorism and extremism for legislative purposes,[305] particularly on definitions of terrorism online. Given there is no comprehensive international legal definition of terrorism,[306] and the internet is a global space, more international cooperation is recommended regarding the responsibility of prosecution.

The limited number of prosecutions against individuals promoting terrorism on the internet suggests a lack of effectiveness.[307] However, better evidence-gathering online can help form an understanding of

[299] Bartlett, J. and S. Gaston, 'Public Views on Technology Futures', *Centre for Analysis of Social Media, Demos*, 29 November 2017, available at https://www.demos.co.uk/project/public-views-on-technology-futures/, last visited: 17 March 2018.

[300] ibid.

[301] Watt, N., '"Dark web": GCHQ and National Crime Agency join forces in hunt for child abuse', *The Guardian,* 11 December 2014, available at: https://www.theguardian.com/society/2014/dec/11/gchq-national-crime-agency-dark-web-child-abuse, last visited: 17 March 2018.

[302] For more, see: Glen, J., 'UK launches new anti-money laundering watchdog', *HM Treasury,* 23 January 2018, available at: https://www.gov.uk/government/news/uk-launches-new-anti-money-laundering-watchdog, last visited: 17 March 2018.

[303] *Terrorism Act 2006*, United Kingdom of Great Britain and Northern Ireland (2006), Chapter 11, Section 2, available at: https://www.legislation.gov.uk/ukpga/2006/11/section/2, last visited: 17 March 2018.

[304] *Terrorism Act 2000*, United Kingdom of Great Britain and Northern Ireland (2000), Chapter 11, Section 58, available at: https://www.legislation.gov.uk/ukpga/2000/11/section/58, last visited: 17 March 2018.

[305] Anderson, D., 'Attacks in London and Manchester March-June 2017', op. cit..

[306] It will become harder to prosecute as individuals are not in physical territory, but online, meaning allegiances will be harder to find – and must be consistent with international human rights definitions about freedom of speech and the right to consume information.

[307] Walker, C., 'The War of Words with Terrorism: An Assessment of Three Approaches to Pursue and Prevent' *Journal of Conflict and Security Law,* Vol. 22(3), December 2017, available at: https://academic.oup.com/jcsl/article-abstract/22/3/523/4554473?redirectedFrom=fulltext, last visited: 17 March 2018.

profiles, groups, and networks disseminating extremist or terrorist content on multiple platforms (see Case Study: Prosecuting for the Dissemination of Terrorist Content Online) to feed into national court systems and auditing processes.

Appendix

The following table is a summary of a search done on Google and the search engine Duckduckgo on 26 January 2018. Following the analysis of Case Study: Tower Hamlets v. B,[308] researchers wanted to understand how much of the content accessed by B was still available on the surface web.

Not only were all the documents (in the case of lectures by radical preacher Anwar al Awlaki, transcripts) still available from a Google search, in many cases searches yielded direct PDFs of the documents on the first page of the results. In some instances, the search autopredicted the title of extremist literature before the sentence could be completed, and offered translations of the text or audio clip in Bengali, Urdu or Hindi to appeal to wider audiences. Following this search, researchers in this project briefed Google on 29 January 2018, which may have changed search results.

Over and above this, researchers found that manuals available on surface web chat forums and blogs provide "how to" guides on accessing marketplaces for drugs, weapons, and false identities on the Darknet. These sites also provide instructions on how to access material glorifying terrorism, extremist propaganda, and jihadist chat forums on the Darknet.

Table 1: Case Study Tower Hamlets v. B search results on Google and Duckduckgo

Title of Document	Contents	Google Search	Duckduckgo
A Mujahid Guide to the West	Guides to weapons and bomb-making, and "hiding the extremist identity". Possession is an offence under Section 58 of Terrorism Act 2000.	– First result is direct link to PDF on Wordpress "the muslim issue". – Third result is a new document on the "Safety and security guidelines for lone world mujahedeen and small cells" on the field of encryption, translated from Arabic. ***Google autopredicted search.***	– First result is a PDF on wordpress site "investigative project". – Contents are copied and pasted on various chat forums and blogs. ***Autopredicted search from "muhajid" onwards.***
Miracles in Syria	Contains information on how to get to the *caliphate*, and photographs of what are referred to as "smiling corpses": photographs of corpses of fighters with their faces set to smile, to indicate their happiness about their "eternal reward".	– First result a direct link to PDF on Ummah.com. – Comment on the forum with a link to the PDF has been up since 06/02/2014 (more than four years).	– First result ebook. *Problematically, also leads to other extremist literature:* 'Black flags for the Islamic State'; 'Syria: Two years, two long' (Islamic Relief); 'Muslim Gangs: Ebook 1: How to Survive the West – the Future of Muslims in the West'; 'Heroes of Syria: Shahada stories from al-Sham' *"Ya*

[308] Content descriptions based on *London Borough Tower Hamlets v. B*, UK Royal Courts of Justice [2016] EWHC 1707 (Fam).

			Allah, take from my blood until you are pleased". 'Martyrs of Syria' (2014); 'Martyrs of Rome' (Europe); 'Black Flags from Palestine' (includes mujahid fitness training); – Third result a direct link to PDF.
Hijrah to Islamic State	Contains information and advice on hiding from airport security, and advice for females wanting to join IS territory through Turkey	– First result a direct link to Wordpress, "the jihad project". – Second result is full text from archive.org. – Third result is Dabiq Issue 2. – Fourth result is Dabiq Issue 3.	– First result is a review on the text: "A call to hijrah: The Islamic state publishes a beautiful magazine to entice recruits and terrify the West…I cannot urge you enough to read the magazine." Third result a direct link to PDF on wordpress site "chainsoff's blog".
The Dust Will Never Settle Down	Audio lecture by radical Islamist preacher Anwar Al-Awlaki in 2008.	Direct PDF links available: – First result direct PDF on Kalamullah.com. – Second result a transcription. – Third result is the clip on soundcloud. ***Translations in Bangla for Bangladeshi community.*** ***Transcripted on blogs.*** ***Google autopredicted.*** ***All results on first page of search.***	– First result Kalamullah.com. Available on: Archive.org Word of Islam Islamic Knowledge Free MP3
The Book of Jihad	Audio lecture by radical Islamist preacher Anwar Al-Awlaki in 2003.	– First result full transcription of text on Archive.org. *Bangla version available.* – Available on Blogspot "a Study on Jihad". – Sixth result direct pdf to lecture series. – Eighth result "A call to jihad".	– Second result is a Direct PDF.
44 Ways to Support Jihad	Practical suggestions on supporting terrorist activity by radical Islamist preacher Anwar Al-Awlaki.	– First result direct PDF download. Directs result to forum with links to "authentic tawheed".	Videos on supporting jihadist financing and sympathising with jihadists.
For the Sake of Allah		Lyrics in Arabic. Nasheed videos.	– First result MP3.

Upon the Prophetic Methodology		***Google autopredicted "methodology, English, nasheed, video".*** Second result live leak video with Hindi and Urdu subtitles.	– First result on liveleak

TERROR IN THE DARK
How Terrorists use Encryption,
the Darknet and Cryptocurrencies

By: Nikita Malik

£9.95 price
ISBN: 978-1-909035-45-4

The Henry Jackson Society
Millbank Tower
21-24 Millbank
London SW1P 4QP

Registered charity no. 1140489

Tel: +44 (0)20 7340 4520
www.henryjacksonsociety.org

CRT
Centre for the Response to
Radicalisation and Terrorism
At The Henry Jackson Society

THE HENRY JACKSON SOCIETY
DEMOCRACY·FREEDOM·HUMAN RIGHTS