Routledge
Taylor & Francis Group

Information & Communications Technology Law

ISSN: 1360-0834 (Print) 1469-8404 (Online) Journal homepage: https://www.tandfonline.com/loi/cict20

Untangling the 'Dark Web': an emerging technological challenge for the criminal law

Matthew Robert Shillito

To cite this article: Matthew Robert Shillito (2019) Untangling the 'Dark Web': an emerging technological challenge for the criminal law, Information & Communications Technology Law, 28:2, 186-207, DOI: 10.1080/13600834.2019.1623449

To link to this article: https://doi.org/10.1080/13600834.2019.1623449

INFORMATION & COMMUNICATIONS TECHNOLOGY LAW
2019, VOL. 28, NO. 2, 186–207
https://doi.org/10.1080/13600834.2019.1623449

Routledge
Taylor & Francis Group

Untangling the 'Dark Web': an emerging technological challenge for the criminal law

Matthew Robert Shillito

Liverpool Law School, University of Liverpool, Liverpool, UK

ABSTRACT

The Dark Web, and the technology which underpins it, is fundamentally changing how crime is conducted. It is an enabler of cross-border, truly international crime where each of the major actors, evidence, and the proceeds of crime can all be in different jurisdictions. The technologies utilised mask the identity of individuals and the nature of the crimes committed. It is these complexities, and law's inability to deal with them, which this paper will focus on. It critically analyses six intersecting and overlapping themes in order to highlight the technological challenges posed by the Dark Web to the criminal law. The paper argues that the current approaches, regulatory structures, legislation and investigative methods are all unfit for purpose. There is little to suggest the law is any closer to restricting Dark Web crime, particularly given a substantial amount of the challenges posed are unsolved traditional issues, in a new form.

KEYWORDS

Dark Web; cybercrime; marketplaces; law enforcement; anonymity; regulation

1. Introduction

In today's technologically astute society, the way in which crime is conducted is evolving at an ever-increasing rate. Dark Web crime is the latest, most evolved, strain of cybercrime. The Dark Web is a 'secretive, anonymous place where shadowy users access hidden services.'[1] In particular, the marketplaces hosted there pose a significant legal challenge. These bazaars enable criminals to effortlessly purchase or sell a vast array of illicit goods and services, from the comfort of their own homes. Significantly, the impact of goods and services bought there is not purely limited to online criminal activity, it also changes the way that criminals facilitate and conduct offline crime too. As a result, the Dark Web is considered '*a hotbed for criminal activity, and an unmitigated headache for law enforcement*.'[2] Whilst at present, its usage is large enough to cause concern and spark action, there is potential for this to grow considerably in the future.[3]

CONTACT Matthew Robert Shillito m.shillito@liv.ac.uk shilts88 @Shilts88

[1]Danny Bradbury, 'Unveiling the Dark Web' (2014) 4 Network Security 14, 14.

[2]Amanda Haasz, 'Underneath it All: Policing International Child Pornography on the Dark Web' (2016) 43 Syracuse J. L. & Com. 353, 356.

[3]Evidence suggests that the Dark Web is growing year-on-year. International drug sales on the Dark Web prior to 2015 were estimated to be roughly $44 million a year, however by 2016 it was estimated that had increased to between $14 million and $25 million per month. For more, see United Nations Office on Drugs and Crime, 'World Drug Report 2018' (June 2018) UNODC Doc E.18.XI.9.

The technology which underpins the Dark Web provides a unique challenge for law enforcement around the world, and the criminal law more broadly. The use of a Virtual Private Network (VPN) in conjunction with Tor ('The Onion Router'), for encryption and security purposes, offers the potential for criminals to anonymously conduct cross-border crime and reach significantly wider audiences than usual, all from the comfort of their own home. Crucially, the use of digital currencies as a means of payment for the good and services purchased on the Dark Web further facilitates this. As a result of this, the Dark Web presents new challenges as well as reinvigorating old traditional challenges.

Law and technology are complex in different ways, which produces even more complexity when they interact. It is this complexity, and law's inability to deal with it which this paper will focus on. Following the successful takedowns of various Dark Web marketplaces, law enforcement agencies have naturally 'talked big' in asserting that they are now on top of Dark Web crime and that criminals will be successfully prosecuted. However, the low volume of shutdowns in comparison to active sites, and the large volume of users still accessing the Dark Web for illicit purposes suggests otherwise. Indeed, the United Nations Office on Drugs and Crime (UNODC) have stated '*law enforcement and the criminal justice system in many countries are still not in a position to deal effectively with the anonymous online marketplace known as the Dark* [*Web*].'[4]

The paper initially considers the Dark Web as an emerging technological challenge for the criminal law. It then outlines the broader approach to regulating emerging technology, to provide a lens for the rest of the paper. In light of this lens, the central part of the paper critically analyses six intersecting and overlapping themes which highlight the challenge posed by the Dark Web. Finally, by way of concluding remarks, the paper will consider what this type of crime, which melds online and offline worlds, tells us about the possible future of criminal law.

Crime on the Dark Web is an unparalleled new threat for the law to deal with. It has a wide reach, lack of respect for national borders, and a high evidential burden given the sophisticated technology utilised. First, it will be argued that capability is a significant issue in countering Dark Web crime, particularly when it comes to confiscating the Proceeds of Crime. Second, it will be advanced that international and regional bodies responsible for dealing with Dark Web crime have limited competences, meaning they cannot lead investigations. Third, it will be highlighted that jurisdictions struggle to work together to counter this transnational crime and that the mechanisms for facilitating cooperation have long been ineffective. Fourth, that regulatory capture by a particularly powerful nation state is inevitable where there is a lack of appetite to deal with the issue globally. Fifth, that the investigation techniques and regulatory approach adopted are not always proportionate, and that in some instances the techniques used border on being illegal. Sixth, that whilst utilising the private sector for Dark Web investigations is somewhat inevitable and brings specialised expertise, it also provides several significant risks. Finally, the paper will argue that the challenges presented by the Dark Web are evolved versions of traditional legal issues, facilitated by technology. Criminals will seek to evolve the technology in order to continue evading detection. Realistically, whilst responsive mechanisms can be put in place to deal with crime on the Dark Web, the law can never hope to prevent the evolution of technology designed to assist criminals in evading detection.

[4]UNODC, 'World Drug Report 2016' (May 2016) UNODC Doc E.16.XI.7.

2. Regulation of (emerging) technology as a research lens

In recent years, academics have become slowly attuned to the threat of the Dark Web, despite this, the literature in the area is still at an embryonic stage. As a result, it is useful when attempting to analyse the challenges that the Dark Web presents, to look beyond this literature and into a broader field. Given the technological issues that the Dark Web presents, it is appropriate to consider how law has responded to challenges presented by other technologies. Therefore, the paper will look to the wider 'regulation of (emerging) technology' literature to establish themes which will assist in untangling the challenges presented by the Dark Web.

As Weimer and Marin note, '*It is widely accepted that regulating emerging technology is a challenge due to uncertainty and limited knowledge in the management and assessment of new risks*.'[5] In particular, 'uncertainty' / 'risk' has been recognised as a key challenge throughout the literature, for many decades.[6] Further, whilst new technology might present regulators with a host of difficult questions, these are often old challenges reinvigorated by new technology rather than genuinely new issues.[7] For instance, in relation to Dark Web crime, familiar challenges emerge in relation to dealing with cross-border crime and confiscation of assets, but in a new form.

One common finding, when it comes to regulating emerging technology, is that the law fails to keep up with technological developments.[8] This finding has been framed three ways in the literature. The 'pacing problem'[9] and the 'Collingridge dilemma'[10] are two. But the third, Brownsword's concept of 'regulatory connection',[11] has emerged as the predominant way to analyse law's (in)ability to keep pace with technological developments. Dark Web and digital currency technology will continue to evolve to evade detection, it is imperative all aspects of law keep up with this by being technology neutral and connected.[12] As Brenner found, it is not uncommon for law '*designed for the technological landscape of the past*' to require reconnection.[13]

This is no different when it comes to law's efforts to tackle Dark Web crime, where there are several significant technological hurdles which means that a counter-Dark Web crime framework only just emerging. In developing a Dark Web strategy, first it must be decided

[5]Maria Weimer and Luisa Marin, 'The Role of Law in Managing the Tension between Risk and Innovation: Introduction to the Special Issue on Regulating New and Emerging Technologies' (2016) 7(3) Eur. J. Risk Reg. 469, 469.

[6]See, as examples: Graeme Laurie, Shawn H.E. Harmon and Fabiana Arzuaga, 'Foresighting Futures: Law, New Technologies and the Challenges of Regulating for Uncertainty' (2012) 4(1) LIT 1; Marjolein BA van Asselt and Ortwin Renn, 'Risk Governance' (2011) 14 Journal of Risk Research 431; and Ulrich Beck, *Risk Society: Towards a New Modernity* (SAGE Publications, 1992).

[7]Ellen Stokes and Diana M. Bowman, 'Looking Back to the Future of Regulating New Technologies: The Cases of Nanotechnologies and Synthetic Biology' (2012) 3 Eur. J. Risk Reg. 235, 235.

[8]Lyria Bennett Moses, 'Agents of Change: How the Law "Copes" with Technological Change' (2011) 20(4) GLR 765.

[9]The 'Pacing Problem' simply describes law inability to keep up with technological developments. For more, see Gary E. Marchant, Braden R. Allenby, and Joseph R. Herkert, *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight* (7th edn, Springer, 2011).

[10]The Collingridge dilemma, is that efforts to influence or control the further development of technology face a duel issue. First, an information challenge, in that impacts of a technology cannot be truly appreciated until it is developed and used. Second, a power problem, in that once a technology is widely used it is difficult to then control. For more, see David Collingridge, *The Social Control of Technology* (Pinter, 1980).

[11]For more, see Roger Brownsword and Morag Goodwin, *Law and Technologies of the Twenty-First Century: Text and Materials* (Cambridge University Press, 2012), chapter 6.

[12]Stefan Carnmel, Andreas Lbsch and Alfred Nordmann, 'A "Scanning Probe Agency" as an Institution of Permanent Vigilance' in in Morag Goodwin, Bert-Jaap Koops and Ronald Leenes, *Dimensions of Technology Regulation* (Wolf, 2010) 125.

[13]Brownsword and Goodwin (n 11).

whether regulatory intervention is required, and if so, what form it should take.[14] If the choice is to intervene, an appropriate balance must be struck between allowing enough room for innovation and establishing a sufficiently strong regulatory framework capable of countering the risks that the emerging technology presents. The literature is skewed towards the promotion of innovation, rather than the reduction of risk. However, this is because most technological innovation discussed is in the health and bioscience sectors where criminal abuse is less prevalent.[15] The Dark Web, on the other hand, presents significant risks (identified below) which make it appealing to criminals to abuse and therefore the analysis in this paper focusses primarily on the reduction of risk. Brenner supports a 'misuse' of technology approach in these circumstances.[16]

In terms of how the law responds, this too provides its own set of tough choices. On the one hand the intuitive response is to develop new regulatory responses.[17] But on the other hand, experience suggests that existing regulation will work, albeit it will most likely need some adaption.[18] This is something this paper will consider throughout, and to a large extent the answer will be informed by whether the challenges presented are genuinely new or if they represent the re-emergence of traditional challenges in a new form. If it is the latter, then it is most likely that it is regulatory adaption that is needed. Adaption is assisted by regulation being drafted in a technology neutral way.[19] Although, technology specific regulation may be needed where, for instance, there is a moral objection to the technology.[20] Meanwhile, smaller issues may be dealt with by self-regulation and guidance.[21] Alongside this, it is important to consider questions of institutional design, specifically how existing institutions '*such as law reform agencies or proposed specialised institutions might help law makers and regulators*'.[22]

Finally, for the regulation of emerging technology to be a useful 'lens' for analysing the challenge of Dark Web crime, it must '*yield insights that could not be gained by looking at the problem of regulation either more broadly (for instance regulatory theory) or more narrowly (in a particular technological or regulatory context).*'[23] For that reason, the preceding insights into emerging technology regulation will be used to critically analyse the Dark Web and digital currency threat, with the paper finishing by considering what this tells us about the future of criminal law and its application to cybercrime more broadly.

3. The Dark Web as an emerging technological challenge

Before moving into the central part of the paper, critiquing the existing Dark Web related legal framework, it must be established how and why the Dark Web is an emerging technological challenge for the criminal law.

[14]Stokes and Bowman (n 7) 235.
[15]ibid 237–38.
[16]Susan W Brenner, *Law in an Era of 'Smart' Technology* (Oxford University Press, 2007).
[17]Stokes and Bowman (n 7) 235.
[18]ibid 235.
[19]Carnmel, Lbsch and Nordmann (n 12) 125.
[20]For good discussion of the benefits and risks of technology specific regulation, see Chris Reed, 'Taking Sides on Technology Neutrality' (2007) 4(3) SCRIPT-ed 263, 283–84.
[21]Stokes and Bowman (n 7) 235.
[22]Carnmel, Lbsch and Nordmann (n 12) 125.
[23]Lyria Bennett Moses, 'How to Think about Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target' (2015) 5(1) LIT 1, 14.

The first challenge is location of the Dark Web. There are two strands to the internet; the 'surface web' and the 'deep web'. The 'surface web' is the everyday part of the internet, accessible by search engines such as Google. The 'deep web' is essentially everything else, not discoverable via a search engine, including password-protected sites and encrypted networks. The Dark Web is a small microcosm of the 'deep web' where '*content has been intentionally concealed*.'[24]

The technology individuals use to access the Dark Web provides the next challenge. From the outset, users are encouraged to mask their identity by using VPNs to create a safe and encrypted connection. They then download and use Tor to connect to the Dark Web. Tor utilises a sophisticated method of encryption which routes the user through computers of other users in order to mask identifying information.[25] Essentially, the process can be thought of like an onion, with each layer passed further obscuring an individual's identity.[26] Further, the Tor platform also provides another challenge in that the sites hosted there change locations every week, providing an evidential challenge for law enforcement in their efforts to piece together evidence. This is unlike the surface web where naming and address schemes remain static.[27] It is worth noting that anonymity gained at this stage should not be synonymous with crime, as it may simply be indicative of a desire for privacy. However, there can be no doubting the potential for widespread abuse given that a '*very conservative*' estimate suggested that '*50% of what is hosted* [*on Tor*] *is illegal and illegitimate.*'[28]

Dark Web marketplaces are reached using their specific '.onion' address.[29] They operate like an eBay for illicit goods, permitting users to trade and access a range of goods and services such as narcotics, firearms, fake identification, confidential information, card readers, child pornography, and hitmen. The challenge is that marketplaces operate across borders with sales not limited by jurisdiction. For this reason, Dark Web marketplaces are a key enabler of cross-border, truly international crime. Each of the major actors, evidence, and the proceeds of crime can be, or at least appear to be, located in different jurisdictions.

The above is further exacerbated by the use of digital currencies, such as Bitcoin, as a payment method. They facilitate funds being moved in a quick, simple and [pseudonymous[30]] way, avoiding the heavily regulated formal financial system.[31] Indeed, there may never be a need for individual to move funds back to the formal financial system, if they are content to hold their ill-gotten gains as digital currency. This is a significant challenge as digital currencies have no central body over which government can exert

[24]Gabriel Weimann, 'Going Dark: Terrorism on the Dark Web' (2016) 39(3) Studies in Conflict & Terrorism 195, 196.
[25]For a more technical and in-depth discussion of how this process works, see Kristin Finklea, 'Dark Web' *Congressional Research Service* (10 March 2017) <https://fas.org/sgp/crs/misc/R44101.pdf> accessed 26 April 2019.
[26]Adam Clark Estes, 'Tor: The Anonymous Internet, and If It's Right for You' *GIZMODO*, (30 August 2013).
[27]Should any case come to court, then it is necessary that law enforcement have time-stamped all the evidence they have gathered as it will almost certainly be different by then.
[28]Daniel Moore and Thomas Rid, 'Cryptopolitik and the Darknet' (2016) 58(1) Survival 7.
[29]For an explanation on how to access the Dark Web and use an '.onion' address. See Tor Project, 'Tor: Onion Service Protocol' <https://www.torproject.org/docs/onion-services.html.en> accessed 26 April 2019.
[30]Pseudonymity rather than anonymity is increasingly used to describe the secrecy of identifying information when it comes to most digital currencies. Anonymity infers that an individual cannot be identified, however, any transaction can be linked back to the wallet alphanumeric identifier. The challenge for law enforcement is to link the alphanumeric code with an individual. Total anonymity is possible but like with fiat currencies and traditional bank accounts it would require the use of illegitimate fraudulent means.
[31]Robert Stokes, 'Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar' (2012) 21(3) I & CTL 221, 225.

control.[32] All of this, coupled with the pseudonymity generated makes identifying criminals involved in Dark Web crime particularly difficult.[33] Further, it weakens the impact of strategies which target the proceeds of crime, a long-utilised method for controlling organised crime.[34]

The challenges being posed by the Dark Web are not limited to crime facilitated and committed on the Dark Web. It also allows criminals to plan or facilitate 'surface web' and 'offline' crime. Whilst the challenge of offline and online worlds melding is a long-standing issue for the criminal law,[35] the sophisticated technology utilised to mask identities on the Dark Web makes this an even more challenging threat to crime, at all levels.

This section has highlighted that the Dark Web and the marketplaces that are located there pose an increasingly significant technological challenge. The rest of this paper will focus on legal challenges that (re)emerge as a result of this.

4. Untangling the legal technological challenges presented by the Dark Web

This section will utilise six intersecting and overlapping themes to highlight the extent of the technological challenge that the Dark Web poses. The six thematic problems for analysis will be: capability, international, jurisdictional, regulatory capture, proportionality, and privatisation. Whilst some challenges presented are inherently new, many are issues that the law has struggled to deal with in the past which have been reinvigorated by the use of new technology. That the Dark Web presents challenges, old and new, demonstrates the scale of the challenge that actors at all levels face.

4.1. Capability problem

The capability problem encapsulates the issue of whether actors in the area have enough power, and ability, to deal with the challenges which the Dark Web presents. Given the longstanding focus on 'targeting the proceeds of crime' as a strategy for the reduction of organised crime,[36] this section will focus on the capability issues which impact law enforcement's ability to confiscate the digital currencies associated with Dark Web crime.

The first capability issue relates to law enforcement having appropriate knowledge and understanding of the Dark Web and digital currencies, so that they can investigate them. It is accepted that there is currently a lack of experience in law enforcement agencies in conducting effective investigations, and prosecutions, of crimes involving

[32] Jonathan Turpin, 'Bitcoin: The Economic Case for a Global, Virtual Currency Operating in an Unexplored Legal Framework' [2014] 21(1) Ind. J. Global Legal Studies 335–38.

[33] National Crime Agency, 'National Strategic Assessment of Serious Organised Crime' (2017) 8, <https://nationalcrimeagency.gov.uk/who-we-are/publications/32-national-strategic-assessment-of-serious-and-organised-crime-2017/file> accessed 26 April 2019.

[34] HM Treasury, 'Digital Currencies: Response to the Call for Information' (Report) (March 2015) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf> accessed 26 April 2019.

[35] See David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity, 2007); and Ralph D. Clifford, *The Investigation, Prosecution and Defense of a Computer-Related Crime* (3rd edn. Carolina Academic Press, 2011).

[36] President Nixon first declared 'war' on illegal drug cartels in the 1970's by targeting the proceeds of crime, since then legislation has grown, particularly through the 1980's, to make it a key component of the international community's strategy to tackle organised crime. For more, see; Nicholas Ryder, *Financial Crime in the 21st Century* (Edward Elgar, 2011), Chapters 1 & 6.

digital currencies.[37] First of all, law enforcement need the support of regulation in the area, this will be discussed further below. Second, there also needs to be investment in improving digital currency capabilities within law enforcement, as well as the provision of continuous training for officers in relation to emerging technological risks. The danger at present is that the risks that exist in relation to emerging technology are not disseminated to, and understood by, the individuals who are tasked with preventing these risks being abused. Increasingly, the private sector is being used to plug this law enforcement knowledge gap, however this strategy brings about its own challenges, which will be analysed in the 'privatisation problem' section below. For now, it is enough to note, that they can assist law enforcement in removing some of the anonymity afforded to criminals by the use of the Dark Web and digital currencies. The issues identified here have resulted in law enforcement staff taking matters in to their own hands, developing their own guide to identifying digital currency activity, as well as setting up their own national law enforcement cryptocurrency working group.[38]

The next challenge is evidencing that digital currencies have been used for illicit purposes, which is an incredibly difficult challenge.[39] However, the argument that Bitcoin is anonymous and therefore untraceable is a fallacy, it is in fact pseudonymous and all transactions are visible to the world on the blockchain. Therefore, once Bitcoin are linked to a crime, it is possible to identify them and link them together. Whilst LocalBitcoins facilitate the purchasing of Bitcoins without customer-due diligence, everything outlined above is still applicable once the criminal stores the Bitcoins in their wallet.[40] The challenge is that there is no personally identifiable information on the blockchain, meaning that law enforcement therefore need to link wallets to real people, which can be difficult when the transactions are simple, but is particularly tough when users operate numerous wallets.[41] This is where the lack of knowledge and understanding of digital currencies in law enforcement could really hinder them. Further, the challenge can be exacerbated by money laundering techniques we have more commonly seen in relation to fiat currency, such using fund mixing services and smurfing.[42] 'Dark wallets', which provide a high degree of anonymity, are being used by Dark Web criminals to further conceal their identity. Dark wallets encrypt and mix users' payments to make flows of money online untraceable. The effort required to source an individual or entity, if even possible, would not justify the resources it would undoubtedly take. There is also the potential that the situation will become more challenging moving forwards as criminals turn to privacy focussed digital currencies such as Monero, Zcash and Dash. They utilise 'open-source, public blockchain's, the same as Bitcoin, but the same set of identifying details are not visible.'[43] Whilst this provides a

[37]Philip Larratt and others, 'Innovation and the Application of Knowledge for More Effective Policing' (Report) (13 July 2017) <http://n8prp.org.uk/wp-content/uploads/2017/08/N8-Cryptocurrency-Report.pdf> accessed 26 April 2019.
[38]ibid.
[39]ibid.
[40]For more on the functioning of LocalBitcoins, see their website: <https://localbitcoins.com/> accessed 26 April 2019.
[41]Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Currencies* (Report) (June 2015) 11–13, <https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 26 April 2019.
[42]Smurfing is the process of breaking down large cash deposits into a number of smaller deposits in an attempt to evade detection. See Előd Takáts, 'A Theory of "crying wolf": The Economics of Money Laundering Enforcement' (2007) International Monetary Fund Working Paper 07/81 <https://www.imf.org/external/pubs/ft/wp/2007/wp0781.pdf > accessed 26 April 2019.
[43]European Parliament, *Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses* (May 2018) PE 604.970, 32.

significant challenge for the criminal law, it is worth noting that this is not the only significant challenge which exists in relation to targeting the proceeds of crime, indeed identifying cash smuggling of illicit funds is just as difficult where criminals avoid utilising the formal financial system, as seen with informal value transfer dealers.[44]

Identification and confiscation of the proceeds of crime is one of the most powerful tools, when successfully used, to disrupt and deter criminal activity. However, in order for it to be fruitful, it is essential that law enforcement is capable of bring them under their control. This is a significant challenge in relation to Dark Web crime given the use of digital currencies, where law enforcement may just struggle to identify funds are linked to crime, never mind locate them to confiscate. Where they do identify them, there are a few key challenges. The funds may be located outside the reach of the investigating jurisdiction, or worse still across multiple jurisdictions. Further, digital currencies have quick transaction times, therefore given the lack of a central body like a bank, law enforcement can be constantly chasing a moving target without the ability of asking a central body to freeze the funds. Even where they do identify the funds, and link them to a user, confiscation is then reliant on either compliance from the criminal to hand over their Bitcoin private key, or carelessness in making record of the key somewhere that law enforcement could access it. Crucially, there is no reason for a criminal to hand over their private Bitcoin key voluntarily. It is for these reasons that digital currencies have been labelled a key strategic threat[45] and noted as being 'technically challenging' to confiscate.[46] Perhaps owing to these difficulties, there is a lack of guidance, at all levels, as to how confiscation should take place when it comes to digital currencies. Although on a regional level, the European Union, through the Fifth Anti-Money Laundering Directive, is taking an active interest in tackling the use of digital currencies, though notably EU Member States have until January 2020 to implement it into national law.[47] On a national level, law is outdated globally and there is a lack of regulatory connection. There is a need for them to be updated to be clear in how they apply to digital currencies. In the UK, the government has consulted on this,[48] but has taken no further action despite the HM Treasury response to the call for information stating that they would make efforts to bring in specific digital currency legislation.[49] For this reason, law enforcement are left to interpret how the Proceeds of Crime Act, Part VII applies to digital currencies. It is hardly surprising that there is a lack of action and guidance when the confiscation of digital currencies is such a challenging prospect.

It is clear from the above, that the strategy of targeting the proceeds of crime encounters a number of significant challenges when it comes to dealing with digital currencies, some of which look insurmountable. It is also questionable whether the strategy is an appropriate one, Levi noted that the gap between the proceeds of

[44]Panagiotis Liargovas and Spyridon Repousis, 'Underground Banking or Hawala and Greece-Albania Remittance Corridor' (2011) 14(4) JMLC 313, 314.
[45]HM Government, *Serious and Organised Crime Strategy* (Report) (November 2018) Cm 9718, 14, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752850/SOC-2018-web.pdf> accessed 26 April 2019.
[46]European Parliament (n 43) 57.
[47]Directive (EU) 2018/843.
[48]HM Treasury, 'Digital Currencies: Call for Information' (3 November 2014) <https://www.gov.uk/government/consultations/digital-currencies-call-for-information/digital-currencies-call-for-information> accessed 26 April 2019.
[49]HM Treasury (n 34).

crime confiscation and the estimated proceeds of crime is so significant that '*such a gap cannot be bridged*.'[50] Whilst the fact that there is little evidence of demonstrable progress in dealing with Dark Web crime, either from reducing Dark Web usage, or from securing regular prosecutions of key Dark Web criminals, suggests that the strategy is having little impact in this area. Despite some notable takedowns, Dark Web marketplaces continue to thrive.[51]

4.2. International problem

The responsibility for dealing with this international crime has fallen on INTERPOL[52] at an international level, Europol and their European Cybercrime Centre (EC3)[53] on a regional level, as well as law enforcement agencies in individual jurisdictions. This is unsurprising given that these bodies have focussed on broader cybercrime for some time, and that clear institutional design is a key component of regulating new technology.[54]

The limit of their competence is a significant challenge when it comes to the ability of INTERPOL and Europol to deal with Dark Web crime. Both derive their competence from their membership,[55] they are not law-making bodies and have little enforcement power, in their own right. Both INTERPOL and Europol understand that they primarily have a coordinating function. In pursuit of their aims, the two bodies often work together.[56] INTERPOL's aim is to 'ensure and promote the widest possible mutual assistance between all criminal police authorities',[57] whilst Europol's is to 'improve co-operation between competent authorities in the Member States in preventing and combatting serious forms of international organised crime.'[58] To achieve this, INTERPOL and Europol facilitate law enforcement in country 'A' asking law enforcement in country 'B' to take appropriate action against a criminal, potentially leading to extradition. This assists in the smooth functioning of mutual legal assistance agreements, amongst their members. This process is orchestrated by either the INTERPOL National Central Bureau (NCB)[59] or Europol's EC3, depending on the jurisdictions involved. Further both INTERPOL and Europol provide access to their member states to databases and police services, the local INTERPOL NCB

[50]Michael Levi, 'Thinking About Organised Crime' (2014) 159(1) The RUSI Journal 6, 9.

[51]Indications are that Dark Web marketplaces such Dream Market, Wall Street, and Point Marketplace are thriving in the post-AlphaBay / post-Hansa era, after an initial ripple caution across the Dark Web community buyers and sellers have migrated to these new marketplaces. For more, see UNODC (n 3) 24; Global Drugs Survey Core Research Team, Global Drug Survey 2017 (Report) (2017) 99 <https://www.globaldrugsurvey.com/wp-content/themes/globaldrugsurvey/results/GDS2017_key-findings-report_final.pdf> accessed 26 April 2019; and Tor Project, 'Tor Metrics' <https://metrics.torproject.org/hidserv-rend-relayed-cells.html> accessed 26 April 2019; and BBC, 'Dark Web Markets Boom after AlphaBay and Hansa Busts' (1 August 2017) <https://www.bbc.co.uk/news/technology-4078826> accessed 26 April 2019.

[52]INTERPOL is the world's largest police organisation, with 192-member countries. For more, see INTERPOL, 'About INTERPOL' <https://www.interpol.int/About-INTERPOL/Overview> accessed 26 April 2019.

[53]Europol is the European Union's law enforcement agency, assisting the 28 EU Member States in their fight against terrorism, cybercrime and other serious and organised forms of crime. For more information, see Europol, 'About Europol' <https://www.europol.europa.eu/about-europol> accessed 26 April 2019.

[54]Carnmel, Lbsch and Nordmann (n 12) 125.

[55]See INTERPOL (n 52).

[56]Europol, 'INTERPOL – Europol Conference Calls for Global Response to Cybercrime' (18 September 2018) <https://www.europol.europa.eu/newsroom/news/interpol-europol-conference-calls-for-global-response-to-cybercrime> accessed 26 April 2019.

[57]ibid.

[58]Europol, 'Agreement Between Interpol and Europol' (5 November 2001) <https://www.europol.europa.eu/sites/default/files/documents/agreement_between_Interpol_and_Europol.pdf> accessed 26 April 2019.

[59]In the UK, the INTERPOL National Central Bureau is based in Manchester, as part of the National Crime Agency. See INTERPOL, 'United Kingdom' <https://www.interpol.int/Member-countries/Europe/United-Kingdom> accessed 26 April 2019.

aims to prove connectivity between the national law enforcement agency and INTERPOL services.[60]

It is an oft-stated line that an international crime requires an international response, but it is clear, at least in this area, that the international and regional bodies do not have the competence to lead Dark Web investigations. Their role is purely to assist national law enforcement agencies in working together to tackle international organised crime, by disseminating best practice and coordinating their response.[61] Therefore, there is a lot of emphasis on national law enforcement to lead the fight against crime on the Dark Web. There is no formal international mechanism for ensuring jurisdictions have and are enforcing counter measures that tackle Dark Web crime. Therefore, it leaves it to each jurisdiction to decide whether they want to engage, which raises the possibility, that will be analysed below, that one particularly powerful nation state could seize the regulatory agenda.

4.3. Jurisdictional problem

As identified at the outset of this article, one of the fundamental issues when it comes to tackling Dark Web crime is that it most often has a cross-border element. Indeed, each of the actors involved in the commission of the crime, and the proceeds of the crime, can all be in different jurisdictions. Whilst methods have changed, globalisation and cross-border crime is not a new issue. It is one that the law has long struggled to overcome.[62] To this end, the UNODC have noted that '*globalisation has outpaced the growth of mechanisms for global governance, and this deficiency has produced just the sort of regulatory vacuum in which transnational organised crime can thrive*.'[63] It has already been identified above, that the international and regional bodies have a limited mandate, therefore it is essential that national law enforcement are capable of tackling Dark Web crime, and that they can work together across multiple jurisdictions.

Traditionally, national law enforcement struggle to work together as a result of legal and cultural differences.[64] Communication and cooperation is a particularly problematic issue in this regard. In order to alleviate this, bilateral 'mutual legal assistance treaties' are used.[65] They allow states to '*seek and provide* [*transnational*] *assistance in gathering evidence for use in criminal cases or in the restraint and confiscation of the proceeds of crime*'.[66]

[60]ibid.
[61]Europol (n 56).
[62]Its origins can be dated back to the slave trade. For more, see United Nations Office on Drugs and Crime, 'The International Criminal Police' <https://www.unodc.org/unodc/en/data-and-analysis/bulletin/bulletin_1951-01-01_3_page003.html> accessed 26 April 2019.
[63]United Nations Office on Drugs and Crime, *The Globalisation of Crime* (Report) (2010) E.10.IV.6, 29, <https://www.unodc.org/res/cld/bibliography/the-globalization-of-crime-a-transnational-organized-crime-threat-assessment_html/TOCTA_Report_2010_low_res.pdf> accessed 26 April 2019.
[64]KPMG, *Cross-Border Investigations: Are You Prepared for the Challenge?* (Report) (2013) 2 <https://assets.kpmg/content/dam/kpmg/pdf/2013/12/cross-border-investigations.pdf> accessed 26 April 2019.
[65]The Vienna Convention provides that signatories should provide 'the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to criminal offences'. For more, see UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (adopted 19 December 1988, opened for signature 20 December 1988) (1988) 28 ILM 493.
[66]Kimberly Prost, 'No Hiding Place – How Justice Need Not be Blinded by Borders', in Steven David Brown, *Combating International Crime: The Longer Arm of the Law* (Routledge Cavendish, 2008) 142.

For this reason, the Council of Europe deemed it an essential tool in the fight against organised crime.[67]

However, whilst these mutual legal assistance agreements provide useful mechanisms for cooperation, they also provide their own problems. Whilst, mutual legal assistance represents around 70% of the means of international cooperation in cybercrime investigations,[68] the process is usually slow. There are several significant factors which contribute to this slowness, including: multiple follow-up enquiries[69] as a result of missing information or inadequate reporting, disparities in what is considered urgent,[70] lack of resources in the receiving jurisdiction,[71] and request being made between countries whose law's do not align,[72] and prioritising of domestic investigations over foreign requests for assistance.[73] This is a big issue in terms of Dark Web investigations, given that time is of the essence when it comes to collecting cybercrime evidence.[74]

Whilst bodies such as Europol and INTERPOL can assist in making mutual legal assistance requests more fluid between their members,[75] they cannot overcome every barrier to international cooperation. Language barriers are relatively easy to overcome, but the others outlined above are significantly more difficult, even if international and regional bodies work on harmonising laws. Approach and opinions are always likely to differ, and for that reason it is somewhat inevitable that there is always going to be difficulties when it comes to cross-border cooperation.

4.4 Regulatory capture problem

Despite the prominent position of the international agencies, outlined above, the international efforts have, as in other areas,[76] been driven by one particularly powerful nation state.[77] In this sense, 'regulatory capture' is used to describe the attempt of the US to set the Dark Web regulatory agenda and shape counter-measures in the area.

[67]Council of Europe Roma-Lyon Group, 'Addressing Requests for Mutual Legal Assistance in De Minimis Cases' (Report) (2013) <http://www.coe.int/t/dghl/standardsetting/pc-oc/PCOC_documents/Documents%202013/de%20minimis_report.pdf> accessed 26 April 2019.
[68]ibid.
[69]ibid.
[70]ibid.
[71]UNODC, *Manual on Mutual Legal Assistance and Extradition* (Report) (2012) 1 <https://www.unodc.org/documents/organized-crime/Publications/Mutual_Legal_Assistance_Ebook_E.pdf> accessed 26 April 2019.
[72]International Chamber of Commerce, 'Using Mutual Legal Assistance Treaties (MLATs) To Improve Cross-Border Lawful Intercept Procedures' (September 2012) 2 <https://www.icc-portugal.com/images/publicacoes/documentos_gratuitos/Economia_Digital/ICC_policy_statement_on_Using_Mutual_Legal_Assistance_Treaties_(MLATs)_To_Improve_Cross-Border_Lawful_Intercept_Procedures_(2012).pdf> accessed 26 April 2019.
[73]United Nations Office on Drugs and Crime, 'Informal Expert Working Group on Mutual Legal Assistance Casework Best Practice' (Report) (2001) 8 <https://www.unodc.org/documents/legal-tools/lap_mlaeg_report_final.pdf> accessed 26 April 2019.
[74]Anna-Maria Osula, 'Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data' (2015) 9(1) Masaryk University Journal of Law and Technology 43, 44.
[75]Nadia Gerspacher, 'The History of International Police Cooperation: A 150-year Evolution in Trends and Approaches' (2009) 9 (1–2) Global Crime 169, 182.
[76]The Department of the Treasury's Office of Terrorist Financing and Financial Crime, alongside other inter-agency counterparts, has been a 'driving force behind the global propagation of strong anti-money laundering standards via the FATF. For more, see Money Laundering Threat Assessment Working Group, *U.S. Money Laundering Threat Assessment* (Report) (December 2005) <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/mlta.pdf> accessed 26 April 2019.
[77]For more, on the US setting the agenda on tackling Dark Web crime, see Michael Chertoff, 'A Public Policy Perspective on the Dark Web' (2016) 2(1) Journal of Cyber Policy 26.

This attempt by the US to seize the initiative can be evidenced in two ways. First, the US have either led or assisted in all major takedowns to date,[78] whilst contributions from other states have been limited at best. Second, they are openly advocating a relaxed approach to territorial encroachment, where Dark Web investigations involve accessing digital property housed in another state.[79] It is clear, that such a power grab is a significant challenge and the consequences of which will be analysed below.

In relation to the first example, it is evident that the US have either led or assisted in all major Dark Web takedowns to date.[80] Alongside this they have also co-led on various smaller Dark Web investigations, such as 'Operation Onymous'.[81] The US position, as leaders in the area, is highlighted by Chertoff who notes '*as the United States develops and refines policy regarding the Dark Web, the international community will also be manoeuvring to put in place regulations* … '[82] This can be explained by a number of factors. First, that the US has the resources to tackle Dark Web crime. Second, that they are eager to tackle technologically advanced crime. Finally, they have a preoccupation with reducing drug-related crime, something which Dark Web marketplaces facilitate.[83] The big concern, which emancipates from these motives, is that if the US engages first, it can set the norms for engagement which the international community then codifies. This can be particularly problematic, when, for instance, the US is focussed so heavily on the 'war on drugs'. Although large volumes of the illegal activity facilitated by the Dark Web relate to drugs, it also facilitates other very serious forms of crime, identified above. It is therefore important that international efforts do not overlook Dark Web crimes such as the sale of firearms or the selling of child pornography, just because they are the focus of the US. Whilst there is evidence of some focus on broader crimes,[84] it is fair to suggest that the early focus has largely been on drug-related crime.

The open approach to territorial encroachment, discussed fully in the proportionality section below, also has ramifications in terms of regulatory capture. The US are strong

[78]For examples, see *United States of America v Ross William Ulbricht* 31 F. Supp. 3d 540 (2014); Federal Bureau of Investigation, 'Darknet Takedown, Authorities Shutter Online Criminal Market AlphaBay' (20 July 2017) <https://www.fbi.gov/news/stories/alphabay-takedown> accessed 26 April 2019; and EUROPOL, 'Massive Blow to Criminal Dark Web Activities After Globally Coordinated Operation' (20 July 2017) <https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation> accessed 26 April 2019.

[79]US Department of Justice, *The National Strategy for Child Exploitation Prevention and Interdiction* (April 2016) <https://www.justice.gov/psc/file/842411/download> accessed 26 April 2019.

[80]For examples, see *United States of America v Ross William Ulbricht* 31 F. Supp. 3d 540 (2014); Federal Bureau of Investigation, 'Darknet Takedown, Authorities Shutter Online Criminal Market AlphaBay' (20 July 2017) <https://www.fbi.gov/news/stories/alphabay-takedown> accessed 26 April 2019; and EUROPOL (n 78).

[81]Operation Onymous was an international law enforcement operation, led by Europol' Cybercrime Centre EC3, the FBI, ant the U.S. Immigration and Customs Enforcement's Homeland Security Investigations. It targeted Dark Web sites such as the Silk Road 2.0, Cloud 9, and Hydra. For more, see EUROPOL, 'Global Action Against Dark Markets on Tor Network' (7 November 2014) <https://www.europol.europa.eu/newsroom/news/global-action-against-dark-markets-tor-network> accessed 26 April 2019.

[82]Chertoff (n 77) 26.

[83]The US has long taken a leading fight in the international war on drugs indeed it was instigated by President Nixon in 1973 and have been reiterated by successive administrations. For good discussion see in particular: Ryder (n 36); and Michael Levi, 'Money Laundering and its Regulation' (2002) 582(1) The ANNALS of the American Academy of Political and Social Science 182.

[84]See U.S. v Chase 250 F.Supp.3d 1 (2017); and the 'hunt core' investigation which focussed on Dark Web forums designed for the discussion and sharing of images and videos related to rape, murder, sadism, torture, paedophilia, blackmail, humiliation and degradation. Dr Matthew Falder was found guilty of 137 charges including encouraging the rape of a four-year-old boy – see College of Policing, 'Digest: A Digest of Police Law, Operational Policing Practice and Criminal Justice' (October 2017) 20 <http://www.college.police.uk/What-we-do/Standards/Documents/Digest_October_2017.pdf> accessed 26 April 2019.

advocates of this relaxed approach,[85] but it represents a big concern. We should be deeply sceptical of any moves to informally allow territorial encroachment. Especially as the US are advocating this approach from a position of power and are more likely to be the perpetrator not the victim of encroachment. If this behaviour continues unchecked, it will pose a significant sovereignty issue for other jurisdictions.[86] As we will see below, the confusing element in all of this, is that such extra-territorial reach does not need to be accepted, there are other formal cooperation mechanisms, such as mutual legal assistance treaties, that allow the investigation to continue without granting any one state such significant influence.

Whilst, regulatory capture is perhaps an inevitable risk of powerful states being so heavily involved in the response to technological crime, it does not stand that this should be accepted, especially where other more proportionate mechanisms exist.

4.5. Proportionality problem

Despite the foregoing, where law enforcement has managed to launch Dark Web investigations, they have raised proportionality issues for those concerned. The first of these relates to the approach that should be taken to the tackling crime on the Dark Web, and in particular its marketplaces. The second issue relates to the investigative methods utilised, and specifically, whether they are proportionate to the aim being pursued.

4.5.1. Intervention

As identified above, once it is decided that intervention is required, the starting point for any debate on how to tackle an emerging crime threat is what approach should be adopted in order to restrict abuse.[87] The only resolution that could completely eradicate Dark Web crime is to get rid of the space altogether.[88] However, that is beyond the capabilities of law enforcement both legally and technically. Therefore, two approaches remain. The most risk averse approach entails denying individuals access to the Dark Web. Whilst the more proportionate but resource intensive approach is to permit access to the Dark Web, but then for law enforcement to target the leading illegitimate sites for takedown. As will be detailed below, both approaches have been tried and tested, but neither are perfect. This is largely due to the need, on one hand, to protect individuals from abuse, and on the other hand, to avoid '*interfering with innocuous activities and the existence of political freedoms.*'[89] Such a balancing act, appears difficult to achieve, and in some cases undesirable.

Several countries have sought to deny access to the Dark Web, most notably Turkey[90] and China.[91] Their approach has been to ask internet service providers (ISPs) to revoke

[85]US Department of Justice, *The National Strategy for Child Exploitation Prevention and Interdiction* (Report) (April 2016) <https://www.justice.gov/psc/file/842411/download> accessed 26 April 2019.
[86]Ahmed Ghappour, 'Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web' (2017) Stan. L. Rev. Online 1075.
[87]Stokes and Bowman (n 7) 235.
[88]Haasz (n 2) 356.
[89]Kat Hadjimatheou, 'Policing the Dark Web: Ethical and Legal Issues' (November 2017) <http://media4sec.eu/downloads/d4-3.pdf> accessed 26 April 2019.
[90]For good discussion of the measures Turkey have taken, see BBC, 'Turkey Blocks Access to Tor Anonymising Network' (19 December 2016) <https://www.bbc.co.uk/news/technology-38365564> accessed 26 April 2019.
[91]MIT Technology Review, 'How China Blocks the Tor Anonymity Network' (4 April 2012) <https://www.technologyreview.com/s/427413/how-china-blocks-the-tor-anonymity-network/> accessed 26 April 2019.

access to the Tor network.[92] However, whilst this might work to prevent the average user from accessing restricted sites, it can be advanced that the typical Dark Web user is inherently more technologically astute, and would know that VPNs are effective against such counter measures. By making the user appear to be from a different country to the one they are based in, they can then connect to Tor. As a result, China and Russia are attempting to block VPNs.[93] Despite claims this is done to prevent individuals gaining an upper hand on law enforcement, from a privacy standpoint it is a particularly problematic approach. It leaves China and Russia open to allegations of controlling internet usage, thereby preventing access to certain information and restricting citizens from expressing certain views.

It is fundamental that security and law enforcement needs are not used as subterfuge for the erosion of privacy. Indeed, as the United Nations Human Rights Council argues '*a state's obligations to respect and ensure the rights to freedom of opinion and expression, and to privacy, include the responsibility to protect encryption*.'[94] After all, encryption is not synonymous with crime and is an important part of the modern world.[95] As a result, it is not proportionate to suggest that Tor and VPN's should be blocked simply because they encrypt users identities. Encryption on the Dark Web allows journalists and nonconformists to communicate with each other, and whistle-blowers to leak information without fear of persecution. The UN is keen to ensure such platforms continue to be available: '*legislation and regulations protecting human rights defenders and journalists should also include provisions enabling access and providing support to use the technologies to secure their communications*.'[96]

It is clear from the foregoing that any argument that treats all Dark Web usage as suspicious and is used as a justification for restricting encryption services goes against an individual's privacy rights. Indeed, the general position is that Article 8 of the European Convention on Human Rights (ECHR) can be used as a defence where police have interfered in the private life of an individual.[97] This defence can be triggered when either evidence has been gained in an illegal way,[98] where an individual had not committed an offence at the material time such that no interference could be justified,[99] where powers are used for improper and unnecessary purposes,[100] and where intervention was based on erroneous beliefs or evidently wrong premises.[101] Essentially, this stems from the fact that there needs to be appropriate safeguards to prevent law enforcement abuse of investigative powers.[102] It seems then, that there needs to be demonstrable

[92]ibid.
[93]Lily Hay Newman, 'The Attack on Global Privacy Leaves Few Places to Turn' *WIRED* (8 April 2017) <https://www.wired.com/story/china-russia-vpn-crackdown/> accessed 26 April 2019.
[94]United Nations Human Rights Council, *Encryption and Anonymity Follow-up Report* (June 2018) Research Paper 1/2018, <https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf > accessed 26 April 2019.
[95]For good discussion on the everyday role of encryption, see Mark Ward, 'How the Modern World Depends on Encryption' BBC (25 October 2013) <https://www.bbc.co.uk/news/technology-24667834> accessed 26 April 2019.
[96]David Kaye, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (United Nations Human Rights Council, 22 May 2015) A/HRC/29/32 <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc> accessed 26 April 2019.
[97]Khan v United Kingdom [2000] 31 EHRR 1016.
[98]ibid.
[99]Giorgi Nikolaishvili v Georgia App no 37048/04 (ECHR, 13 January 2009).
[100]Paton v Poole BC (2010) IPT/09/01/C.
[101]Keegan v United Kingdom App no 28867/03 (ECHR, 9 August 2006).
[102]Gillan & Quinton v United Kingdom App no 4158/05 (ECHR, 12 January 2010).

evidence of a link to crime to justify police interference in an individual's private life. On this basis, a complete restriction on access to the Dark Web is disproportionate and will breach an individual's right to private life under Article 8 ECHR.

The more widely adopted approach has been to permit access to the Dark Web but shutdown sites evidenced having an illegitimate purpose. Law enforcement then use the information gained during the takedown to pursue individual prosecutions. The more widely adopted approach, though still far from successful, has been law permitting access to the Dark Web but seeking to shutdown sites evidenced as being illegitimate. Whilst there is evidence, outlined above, of the United States, United Kingdom and the Dutch adopting this approach, for the most part other jurisdictions have remained inactive in response to the Dark Web threat. Perhaps the most compelling reason for a lack of engagement by other countries is that Dark Web crimes, by their nature, are parasitic on existing 'real world' crime, and therefore their impact is less apparent until an incident is detected. But also, resource issues both in terms of finances and technical capabilities is likely to play a part too. Where adopted, the approach of law enforcement taking down Dark Web marketplaces from 'the inside' once they have taken control of their servers, has had some high-profile successes, such as the Silk Road, AlphaBay and Hansa investigations. This is clearly a more proportionate response by law enforcement, than seeking to restrict access to the technologies which permit access to the Dark Web. It only has limited incidental impact on the positive uses of the Dark Web, and individual's privacy rights, owing to the fact individuals are only targeted once they are linked to wrongdoing.[103]

However, this approach also raises its own problems owing to different applications. In the Silk Road investigation, the FBI chose to focus their efforts on the top 1% of sellers, as well as system administrators.[104] Whereas, Dutch law enforcement, in the takedown of Hansa signalled that they intended to target all users.[105] Identifying and prosecuting all individuals who use Dark Web marketplaces is substantial undertaking. At best it is a significant challenge both in terms of logistics and resources. At worst, it is an unachievable aim, owing to the sophisticated technology used, limited resources of law enforcement, and the prospect that individuals have used false identities. Indeed, it might not be possible to target as many users as the Hansa investigation owing to the special circumstances that surrounded its takedown,[106] which are critiqued in the next section. However, the US approach of targeting the top sellers and site administrators can also be criticised. The aim of the strategy is to send out a deterrent message that no one is beyond the reach of law enforcement.[107] But whether such a message could ever be successful is highly debateable given the fact that Dark Web marketplaces continue to re-emerge and grow,[108]

[103]See for instance: *United States of America v Ross William Ulbricht* 31 F. Supp. 3d 540 (2014).
[104]Kim Zetter, 'How the Feds Took Down the Silk Road Drug Wonderland' *WIRED* (18 November 2013) <https://www.wired.com/2013/11/silk-road/> accessed 26 April 2019.
[105]Over 10,000 foreign address of Hansa market buyers were passed to Europol for further investigation, whilst the Dutch law enforcement agency investigated 500 cases locally. For more, see EUROPOL (n 70).
[106]Hansa was taken under Dutch judicial cover control, allowing law enforcement to monitor the activity of users without their knowledge. Within the same time scale, AlphaBay was shut down, meaning that large volumes of these users moved to Hansa making them discoverable to Dutch law enforcement.
[107]'Attorney General Jeff Sessions Delivers Remarks at Press Conference Announcing AlphaBay Takedown' (The United States Department of Justice, 20 July 2017) <https://www.justice.gov/opa/speech/attorney-general-jeff-sessions-delivers-remarks-press-conference-announcing-alphabay> accessed 26 April 2019.
[108]UNODC (n 3) 24.

even in spite of the broader approach taken to prosecutions following the takedown of Hansa. Historically, cross-border crime is plagued with issues around the identification and prosecution of criminals,[109] nothing here suggests that it is about to change.

Once again, this section highlights the complex challenges that actors face in tackling crime on the Dark Web. The only strategy capable of success is not possible, and the other two raise significant issues relating to proportionality and privacy.

4.5.2. Investigation

Proportionality is also a substantial issue in terms of Dark Web investigations. The first issue is in relation to undercover operations and law enforcement's willingness to engage in activity which if committed by anyone other than them would result in prosecution. The second issue relates to search warrants and whether they exceed their mandates in the pursuance of Dark Web prosecutions.

Increasingly, in the course of their investigations, it is not uncommon for law enforcement to continue to operate Dark Web marketplaces after they have seized control of them, in order to gather more evidence. In this time, they utilise the 'network investigative technique' (NIT)[110] to uncover the identity of the users. However, whilst this may result in more evidential leads that law enforcement can pursue, significantly it involves them engaging in, and facilitating the commission of, crime. Whilst this may be '*considered a justifiable and sometimes necessary aspect of undercover policing*',[111] it is imperative that there are limits otherwise law enforcement will have a wide scope to abuse such freedom. The rest of this section will focus on this dilemma of ensuring law enforcement do not overstep their competence, whilst attempting to allow them enough freedom to investigate such sophisticated crime. Whilst the issues discussed are applicable to the UK, they are yet to be tested in UK courts, and so the analysis will primarily focus on US case law with elements of broader commentary on UK undercover policing. The same problems demonstrated in the US context will need resolution in the UK.

At the outset, it is important to note that it is readily accepted that the commission of crime by rogue officers in the course of undercover Dark Web investigations will be prosecuted.[112] Such conduct could never be accepted as the officers involved are acting in their own, criminal, self-interest. Further, entrapment[113] and violations of fundamental human rights[114] are not permitted in any law enforcement investigations. However, where difficulty arises, is deciding in which circumstances 'good faith' law enforcement criminality is permissible.

In two leading Dark Web investigations, law enforcement engaging in the same criminality as the individuals they were trying to identify was considered necessary and

[109]Directorate-General for Internal Policies, 'The Law Enforcement Challenges of Cybercrime: Are We Really Playing Catch-up?' (European Parliament, 2015) 44 <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536471/IPOL_STU(2015)536471_EN.pdf> accessed 26 April 2019.

[110]The NIT is a flash-based application developed by H.D. Moore, released as part of Metaspoilt. Its purpose is to provide the real IP addresses of web users, regardless of the use of Tor.

[111]Elizabeth E. Joh, 'Breaking the Law to Enforce It: Undercover Police Participation in Crime' (2010) 62(1) Stan. L. Rev. 155, 157.

[112]For more, see United States Department of Justice, 'Former Federal Agents Charged with Bitcoin Money Laundering and Wire Fraud' (30 March 2015) <https://www.justice.gov/opa/pr/former-federal-agents-charged-bitcoin-money-laundering-and-wire-fraud> accessed 26 April 2019.

[113]For more on the role of entrapment, see the judgements of Lords Hoffman and Hutton in R v. Loosely [2001] UKHL 53.

[114]International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976).

proportionate in the pursuit for prosecutions.[115] However, despite this it has been suggested by Haasz that law enforcement, in continuing to operate sites after they have seized them, are guilty of entrapment.[116] The cases have not come to such a conclusion, instead it appears that it would only be considered entrapment where law enforcement create a new Dark Web website in order to catch criminals.[117] The distinction seems to be justified on the basis that taking over a marketplace only requires maintenance whereas creating a new marketplace requires action. It appears that creating the site is considered a 'set up' whereas taking over a pre-existing site is considered a necessary evil. In reality, this is such a subtle distinction to draw and is almost indistinguishable. Maintenance of a Dark Web marketplace still requires some action by law enforcement and the facilitation of crime. It highlights a significant difficulty, in that the main investigative technique for combatting Dark Web crime is perhaps only considered legal due to the creativity of judges in interpreting what amounts to entrapment. Finally, it is clear law enforcement must be willing to detail the NIT used, otherwise potential convictions will be dropped.[118] This is challenging because whilst it ensures that law enforcement are not exceeding their mandate by utilising illegal practices, criminals would gain the upper hand if they understood how the NIT worked, and therefore they could work on countering it.

Whilst for some time, there has been an acceptance that undercover policing and everything it entails is 'the nature of the beast'.[119] In the UK, the extreme lengths that undercover police have gone to in their pursuit of criminals has come in for significant criticism recently and is subject to a public inquiry.[120] Given this, and the above discussion, it is clear that there are examples of law enforcement overstepping their competence. Despite, undercover policing often delivering results in terms of prosecutions, this should not be the primary driver, we should be more sceptical of the methods being utilised by law enforcement.

For the above investigative techniques to be utilised by law enforcement, they first require a search warrant to be issued, as essentially it amounts to a search of digital property. This also raises a significant proportionality issue, as given Dark Web crime often transcends national boundaries, it is questionable whether a search warrant permits a law enforcement agency to investigate outside its own jurisdiction.

The question of whether a search warrant is need for the execution of NITs has arisen, as it essentially amounts to a search of digital property. This raises a couple of interesting proportionality points, first, whether a search warrant is needed to execute a NIT, and second, whether a search warrant can have extra-territorial application. On the one hand, it is argued that law enforcement does not need a warrant to utilise a NIT. Judge Henry Morgan compared the situation to cases involving law enforcement peering through a suspect's broken blinds, arguing that the criminal does not have a reasonable expectation

[115]Brad Heath, *FBI ran website sharing thousands of child porn images*, (USA Today, 21 January 2016) <https://www.usatoday.com/story/news/2016/01/21/fbi-ran-website-sharing-thousands-child-porn-images/79108346/> accessed 26 April 2019; and EUROPOL (n 70).
[116]Haasz (n 2) 356.
[117]Hadjimatheou (n 89) 12.
[118]United States v. Jay Michaud CR15 5351RJB (2017).
[119]United States v. Kaminski 703 F.2d 1004, 1010 (1983). 23 March 1976) 999 UNTS 171 (ICCPR), Article 2(3).
[120]For more, see Undercover Policing Inquiry, 'Home' <https://www.ucpi.org.uk/> accessed 26 April 2019.

to expect privacy in their computer of IP address.[121] On the other hand, it is argued that a warrant issued without jurisdiction is void. Judge William Young argues that as the warrant was issued without jurisdiction, '*it follows that the resulting search was conducted as though there were no warrant at all' and therefore 'the evidence must be excluded*.'[122] A subsequent appeal[123] has, remanded the case for further hearings on the basis that '*executing officers had acted in good faith reliance on the NIT warrant*', citing the Leon 'good faith' exception.[124]

It is clear from this that there is difficulty in deciphering how to deal with this new cross-border challenge, the analogies are imperfect and the complexities very significant. The first argument that no warrant is needed cannot be allowed to stand, privacy advocates would have difficulty with such unfettered powers being handed to law enforcement. The unanswered issue is what scope a warrant has once it is granted. The options are either to permit a warrant issued in digital cases to transcend borders or to rely on mutual legal assistance between countries. Allowing a warrant to transcend a national border is unworkable as '*transborder investigations pose a risk to international relations and may potentially involve a breach of another state's sovereignty*.'[125] Ahmed adds that this may pose a threat to international relations.[126] However, the US Department of Justice have noted that the focus should be on '*triggering increased governmental cooperation rather than raising fears of territorial encroachment*'.[127] In any event, given that no state has ever objected to other jurisdiction's exercising NITs against computers within their national boundary, the norm should be seen as one of cooperation not confrontation.[128] But, that this is all based on informal understanding is slightly troubling as it does not preclude a state from deciding in the future that they do object to such behaviour. Indeed, it could also further exacerbate the regulatory capture problem discussed above. Alternatively, of course, a state could just engage in formal mutual legal assistance requests where a NIT unveils criminal activity in another country. However, this solution also raises issues as it can be slow a slow process[129] and relies on the state's having mutual legal assistance agreements in place. It is clear then that laws surrounding search warrants are imperfect, and need to be updated to provide clarity, rather than relying on judicial interpretation. The UK has recognised that search warrant law needs overhauling if it is to be applicable to digital assets.[130]

4.6. Privatisation problem

It has been established, that owing to a multitude of factors, the different actors involved in fighting Dark Web crime are ill-prepared to do so alone. As a result of technological advances, they no longer have the expertise or resources to investigate such crime

[121]United States of America v Edward Joseph Matish III 4:16 Cr. 16 (2016).
[122]United States of America v Alex Levin 1:15 Cr. 10271 WGY (2016).
[123]United States of America v Alex Levin No. 16-1567 (1st Cir. 2017).
[124]United States v. Leon, 468 U.S. 897 (1984).
[125]Law Commission, *Search Warrants* (Consultation Paper No. 235, 2018) 241.
[126]Ghappour (n 86).
[127]US Department of Justice, *The National Strategy for Child Exploitation Prevention and Interdiction* (Report) (April 2016) <https://www.justice.gov/psc/file/842411/download> accessed 26 April 2019.
[128]Orin S. Kerr and Sean D. Murphy, 'Government Hacking to Light the Dark Web: Risks to International Relations and International Law' (2017) 70 Stan. L. Rev. Online 58.
[129]UNODC (n 73).
[130]For more, see the Law Commission consultation. Law Commission, 'Search Warrants' <https://www.lawcom.gov.uk/project/search-warrants/> accessed 26 April 2019.

without assistance from private entities who are more adept at dealing with this modern crime threat.[131] But, public-private partnerships are not without issue. This section will highlight that given the increasing prevalence of technology-related crime, reliance on public-private partnerships will grow, which may cause their own problems in the future.

Public-private partnerships are not new, they have been utilised by law enforcement as a method for tackling traditional crime for some time.[132] But, their usage has become increasingly prevalent in the fight against cybercrime, as law enforcement seek outside expertise to address their deficiencies.[133] Recently, Europol's EC3 utilised such a partnership with Bitdefender to investigate the Dark Web marketplace, Hansa. The information gathered by Bitdefender directly brought about the successful takedown.[134] US law enforcement have also utilised Blockchain investigative firms, such as Chainalysis, to assist them with crimes involving digital currencies.[135] These private entities employ 'scraping techniques'[136] which serve, in most cases, to remove the anonymity afforded to criminals by the Dark Web and digital currencies.[137]

Good public-private partnerships are seen as pivotal in the fight against Dark Web crime.[138] They are '*massive force multipliers*'[139] and a more effective use of limited resources, than law enforcement trying to upskill themselves with these capabilities.[140] These partnerships have most successfully been utilised to fight financial crime,[141] where the partnerships are genuinely cooperative and focussed on the sharing of information – something Carr identifies as being significant.[142] The UK Joint Money Laundering Intelligence Taskforce has been recognised as world-leading in its endeavours to facilitate '*the exchange of tactical and strategic intelligence between law enforcement and the private sector*.'[143]

Broadly speaking, there are three models that law enforcement can choose from, when it comes to cooperation with the private sector: first, informal cooperation on specific cases and communications; second, creating common entities and Public-Private Partnerships to engage in joint actions; and third, cooperation formalised through legal

[131]National Crime Agency Strategic Cyber Industry Group, 'Cyber Crime Assessment 2016: Need for a Stronger Law Enforcement and Business Partnership to Fight Cyber Crime' (Report) (July 2016) 13 <http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file> accessed 26 April 2019.
[132]See for good discussion: Jeffrey Avina, 'Public-Private Partnerships in the fight Against Crime: An Emerging Frontier in Corporate Social Responsibility' (2011) 18 (3) JFC 282.
[133]National Crime Agency Strategic Cyber Industry Group (n 131).
[134]EUROPOL (n 78).
[135]'How Chainalysis Helps Solve Crimes: Jonathan Levin Tells All – Ep.62' Forbes (29 May 2018) <http://unchained.forbes.libsynpro.com/how-chainalysis-helps-solve-crimes-jonathan-levin-tells-all-ep62> accessed 26 April 2019.
[136]Scraping is the term used to describe the process of pulling together publicly available information from internet forums and, in this case, the blockchain. That information can then be used to help identify individuals involved in crime.
[137]Michael Felder, Michael Kester and Sudeep Pillai, 'Bitcoin Transaction Graph Analysis' (February 2015) <https://arxiv.org/pdf/1502.01657.pdf> accessed 26 April 2019.
[138]Chloe Smith MP, 'Chloe Smith speaks at Cyber Security Summit' (6 November 2012) <https://www.gov.uk/government/speeches/chloe-smith-speaks-at-cyber-security-summit> accessed 26 April 2019.
[139]Global Commission on Internet Governance, *The Dark Web Dilemma: Tor, Anonymity and Online Policing* (September 2015) 11 <https://www.cigionline.org/sites/default/files/no.21_1.pdf> accessed 26 April 2019.
[140]Smith (n 138).
[141]Tom Keatinge, 'Public-Private Partnerships and Financial Crime: Advancing an Inclusive Model' (1 December 2017) <https://rusi.org/commentary/public%E2%80%93private-partnerships-and-financial-crime-advancing-inclusive-model> accessed 26 April 2019.
[142]Madeline Carr, 'Public-Private Partnerships in National Cyber-Security Strategies' (2016) 92(1) International Affairs 43, 57.
[143]National Crime Agency, 'National Crime Agency Annual Report and Accounts 2017-18' (Report) (July 2018) 17 <http://nationalcrimeagency.gov.uk/publications/915-nca-annual-report-account-2017-18/file> accessed 26 April 2019.

instruments and guidelines.[144] Whilst all three models have been utilised by law enforcement in different areas, in relation to Dark Web crime, cooperation has been on an informal level. It either tends to involve providing knowledge and expertise to law enforcement[145] or in some cases developing / giving law enforcement access to private sector technology.[146] In this sense, the relationship is quite like the public-private partnership between a law enforcement agency and a lab that processes DNA evidence. However, the key differentiator is the level of freedom given to the private entity. A private lab is given specific DNA evidence, by law enforcement, to run tests on. Whereas, private blockchain investigative firms have a wide scope for autonomy in that their investigation is often far wider, and less focussed. It requires a lot of faith on the law enforcement side of the partnership, that the private entity is doing what they are being paid to do. This faith, may be misplaced, given that experience suggests that private entities cannot be trusted to execute their own plans and set best practice.[147] Of greater significance, is the fact that for a private blockchain investigative firms endeavours to be successful, it most likely requires law enforcement to share with them details as to what and who they are looking for. Therefore, the current public-private partnership model presents risks for law enforcement in relation to Dark Web investigations. Not only does it provide a lot of freedom for the private entity to investigate as they see fit, it also requires the sharing of potentially sensitive information between law enforcement and the private entity in order for the investigation to successfully identify the target.

It has been suggested that longer-term challenges of public-private partnership in this area, include: a lack of accountability on the part of the private entity, the risk of the private entity withholding information and capabilities, and the possibility that these firms will begin to charge more for their services.[148] Private entities work on a cost/benefit framework rather than a public good framework, therefore their actions need to be profitable.[149] This raises the possibility that a private entity could curtail their investigation based on cost factors rather than an evidential lead being exhausted. Further, given the unique expertise they have, an exclusive system might be created which empowers a small number of private entities and some countries may be overwhelmed at the prospect of developing such a system.[150]

Despite the recent announcement of investment in UK law enforcement's cyber capabilities,[151] it is clear that the constantly evolving technological landscape, and the lack of appropriate expertise and equipment in law enforcement, will result in the continuing

[144]Jean-Christophe Le Toquin, 'Public-Private Partnerships against Cybercrime' (OECD Presentation) <https://www.oecd.org/sti/consumer/42534994.pdf> accessed 26 April 2019.
[145]EUROPOL, 'EC3 Partners' <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-partners> accessed 26 April 2019.
[146]For instance, see Bitdefender, 'Bitdefender, Europol, Romanian Police, and Other Law Enforcement Release New Decryption Tool for Latest GrandCrab Ransomware' (19 February 2019) <https://www.bitdefender.co.uk/news/bitdefender-europol-romanian-police-and-other-law-enforcement-release-new-decryption-tool-for-latest-gandcrab-ransomware-3631.html> accessed 26 April 2019.
[147]David A. Powner, 'Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to be Consistently Addressed' (General Accountability Office, July 2010) 22–23 <https://www.gao.gov/new.items/d10628.pdf> accessed 26 April 2019.
[148]Keatinge (n 141).
[149]Carr (n 142) 62.
[150]Keatinge (n 141).
[151]See Home Office, 'Home Secretary Announces Law Enforcement Crackdown on Dark Web' (11 April 2018) <https://www.gov.uk/government/news/home-secretary-announces-law-enforcement-crackdown-on-dark-web> accessed 26 April 2019; and Home Office, 'Home Office Awards Over £100 Million to Police Transformation Projects' (1 August 2018)

reliance on public-private-private partnership. Significantly, there is nothing to suggest that associated risks of such partnerships are capable of being solved. Indeed, it is somewhat inevitable given that a private company is often going to have profitability as its main driver.

5. Concluding remarks – future challenges to the criminal law

It is clear, then, that modern globalised sophisticated technology presents a range of new possibilities for criminal activity. The Dark Web and its marketplaces are the current protagonists that law enforcement face. It is an enabler of cross-border, truly international crime where each of the major actors, evidence, and the proceeds of crime can all be in different jurisdictions. This is a significant investigative burden for law enforcement, testing their preparedness in terms of countering cybercrime, and stretching their resources to breaking point. But whilst the technology gives rise to new possibilities and allows people to engage in new forms of conduct, the legal challenges that it presents are not so unfamiliar. The paper has highlighted that the challenges of the Dark Web are varied, with some being new and unique, but the majority are old familiar threats in a new circumstance. That these old problems keep emerging means that law can never truly keep up with the modern world, as it struggles to deal with established issues.

The paper identified six key thematic headings to analyse the technological challenge of the Dark Web. From theses, several fundamental challenges emerge which highlight how far away law is from solving the challenge of Dark Web crime.

First, the paper identified that digital currencies provide a way for criminals to move their funds that is hard to detect, and even harder to confiscate. If criminals are unwilling to hand over their access codes to the currency, then there is no way for law enforcement to seize it due to the decentralised structure of digital currencies. Given confiscation of the proceeds of crime has long been used as a deterrent to organised crime, this provides a significant challenge for law to deal with, and one which may not have an answer. Further, even if the law does provide a solution, technology is likely to evolve in new evasive ways. Second, the paper established that the bodies at an international and regional level have limits to their competence, such that their main role is to facilitate cooperation in terms of Dark Web investigations. The third finding links to the second, given the lack of an international body with competence to lead investigations, the burden of Dark Web investigations falls on national law enforcement. Given the cross-border nature of the crime, cooperation is needed, but differences in legal structures and culture mean that this is a particularly difficult challenge to overcome. The current mutual legal assistance provisions do little to overcome this. Fourth, US regulatory capture is a substantial threat given the inadequate situation in relation to the competence of international and regional bodies, and that there has been little political will globally to fight Dark Web crime. This is undesirable as it allows them to set the agenda and regulatory initiative that the international framework will then adopt. Fifth, the paper identified proportionality issues surround investigatory techniques and regulatory approaches. A considerable threat to national sovereignty will emerge if legal mechanisms

<https://www.gov.uk/government/news/home-office-awards-over-100-million-to-police-transformation-projects> accessed 26 April 2019.

are ignored and the current approach of extra-territorial search warrants are accepted. Further, approaches which ban access to the Dark Web by restricting use of associate technologies, is a noteworthy threat to privacy. The Dark Web has good uses too, it is unsatisfactory for it to be banned outright. But similarly, too weak an approach allows the criminality to continue. Finally, issues were highlighted with regards to the use of private entities for Dark Web investigations. Whilst, their expertise means this is an inevitable development, risks such as a lack of accountability, their profit-making focus, and wide autonomy in investigations means that they may not represent value for money.

Looking to the future, although proportionately crime committed on the Dark Web is low, compared to street and normal cybercrime, the potential for growth and the subsequent difficulties it will bring are significant. Unlike traditional crime, the audience a Dark Web criminal has access to is potentially significantly greater. If the above challenges are not addressed, and this potential for growth is realised by criminals the Dark Web could become an unparalleled threat to the criminal law. The challenge is a significant one and requires a fundamental change in how law enforcement deal with crime. The need to become more willing to rely on the private sector to assist them in investigations, more open to assisting cross-border investigations, and more willing to think in a global and connected way. The traditional architecture of crime, confined by borders, is lost forever. It will become increasingly rare for one law enforcement agency to single handedly follow a crime from start to finish. The criminal will continue to seek ways to exploit the weaknesses of predominantly local focussed law enforcement. Finally, law needs to become tech neutral, adaptation of law is traditionally focussed on addressing new technology, which is something criminals have learned to exploit. Instead, law needs to be broad and new tech applicable rather than narrow and focussed on a specific new technology, otherwise we will consistently need new updated law. However, the reality is that this is difficult to achieve, and even where it is, it then requires interpretation to be applied, which can present further challenges.

Disclosure statement

No potential conflict of interest was reported by the author.

ORCID


Matthew Robert Shillito http://orcid.org/0000-0001-5816-2895