Chapter 4

Policing Virtual Spaces: Public and Private Online Challenges in a Legal Perspective

Tine Munk

1 Introduction

The scope and complexity of the global Internet infrastructure show that no single actor can manage cyberspace on its own. Cyberspace requires a pluralistic approach to policing where different actors are involved in the process of monitoring, detecting, and investigating online crime in virtual spaces. The overarching challenges for policing derive from the fact that the virtual world is extra-territorial without fixed boundaries applying to legal or illegal online activities in the same way as the rules and regulations developed to manage real-time crimes. Cyberspace offers creative hackers the opportunity and freedom to obtain control over interconnected spaces[1]

Responding and managing the growing number of cybercrimes requires another approach compared with offline crimes. Yet, the ambition is to enhance the different security actors' role online on both the strategic and the practical level. The complexity of cyberspace calls for new techniques to be introduced which are not applicable to traditional crimes in the same format. Currently, there is an international legislative gap that needs to be assessed in order to create a better preventive and investigative consensus worldwide.

The online challenges as well as the rise of the Darknet have created severe obstacles to traditional police investigation and it is no longer possible to trace cyber offenders by their online footprints. To be effective, law enforcement has been called upon to actively monitor and secretly infiltrate virtual spaces such as the Darknet and different social media forums. Moreover, the growing use of encryption of data makes it difficult to obtain access to the material during an investigation. Private actors are also increasingly involved in the monitoring and investigatory processes, and mega Internet businesses and Internet service providers are enhancing their monitoring systems.[2] New initiatives were launched in the aftermath of the 2017 terrorist attacks in the United Kingdom (UK), where the focus has been on the role of large Internet companies and their responsibility to monitor illegal activities online.[3]

[1] J Avina, 'Public-private partnerships in the fight against crime: An emerging frontier in corporate social responsibility' (2011) 8(3) *Journal of Financial Crime* 282, 286; L Strate, 'The varieties of cyberspace: Problems in definition and delimitation' (2009) 63(3) *Western Journal of Communication* 82; M Yar, 'Cybercrime and society' (2nd ed, Sage 2013), 13.

[2] G Corera, 'Facebook reveals measures to remove terrorist content' *BBC News* (15 June 2017).

[3] T Munk, 'Is preventing online extremism only the responsibility of big internet companies?' (*MDX Minds*, 06 June 2017); A Asthana, 'Theresa May calls on tech firms to lead fight against online extremism' *The Guardian* (25 May 2017).

Policing virtual spaces with several public and private actors is compatible with the restructuring of police forces in recent years where traditional police work increasingly merge with private security actors (see Egan infra).[4] The interaction between public policing and private security presents new challenges as the different actors from the private and public sector have different agendas and methods to monitor the Internet, which means that there are different questions regarding ethical, moral and legal questions, for instance in relation to police investigation methods.

This chapter investigates and explains the online legislative framework and policing practices developed to manage virtual spaces. This is an under-researched area, and data regarding law enforcement operations is limited. However, there is ample supply of research that has been published on legal issues concerning the policing of online child sex offenders. Economic cybercrime is also an area where a number of empirical research projects have analysed the bitcoin industry and the online purchases of drugs in the aftermath of demolition of the online illegal marketspace, the 'Silk Road'.[5] Therefore, this chapter will draw on the relevant findings which assist in reconstructing the emergence of a complex policing framework. First, this chapter sets out the framework for the ensuing discussion by defining crucial areas such as virtual spaces, cybercrime, the Darknet and cybercrime legislation. Second, this chapter focuses on and transnational and cross-sectoral legislative problems which creates limitations to policing. Thirdly, this chapter will include different private and public policing challenges as well as outline some of the complications of online public and private policing, such as technological regulation and operational limitations.

2 Defining Virtual Spaces and Cybercrime

Cyberspace is defined by its global interconnectivity. It is defined as "the notional environment in which communication over computer networks occurs".[6] Cyberspace can be explained as 'as the diverse experiences of space associated with computing and related technologies'.[7] Deibert and Rohozinski have supported this definition by claiming that cyberspace includes both a material and a virtual realm of things and ideas, structure and content.[8] Virtual spaces consist of several elements, and they are based on physical infrastructures and telecommunications devices (SCADA devices, smartphones/tablets, computers, servers,

[4] A Crawford, 'Plural policing in the UK: Policing beyond the police' in T Newburn (eds) *Handbook in policing* (Willan 2008), 147.
[5] J Martin, *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs.* (Palgrave Macmillan 2014). *See also:* R Stokes, 'Virtual money laundering: the case of Bitcoin and the Linden dollar' (2012) 21(3) *Information & Communication Technology Law* 11. L J Trautman, 'Virtual currencies; Bitcoin and what now after Liberty Reserve, Silk Road, and Mt. Gox?' (2014) 20(4) *Richmond Journal of Law and Technology* 1, 108. M C Van Hout and T Bingham, 'Silk Road', the virtual drug marketplace: A single case study of user experiences' (2013) 24(5) *International Journal of Drug Policy* 385.
[6] Oxford Dictionaries, 'Living Oxford dictionaries' (28 July 2017).
[7] Strate 2009 (note 1 above), 383.
[8] R J Deibert and R Rohozinski, 'Risking security: Policies and paradoxes of cyberspace security' (2010) 4(1) *International Political Sociology* 15, 16.

etc.); connected networks systems and organisational networks of networks systems; the access nodes of users and intermediaries routing nodes and essential data.[9]

Virtual spaces are associated with positive as well as negative values, for instance with freedom, but also with a threat. Virtual spaces can be interpreted in a broad sense as they concern computer technologies, communication platforms and specific areas, which can be attacked. For example, cybercrime can be something that threatens the personal integrity of individual's online activities. Other areas are transferred from offline offences to cyberspace, such as fraud, theft, threats, manipulations, bullying and discrimination.[10] These are part of the contemporary world along with child pornography, voyeurism and xenophobia. Moreover, cyberspace can be used as a platform for freedom and of political activism, where the online platforms open up to new forms of political participation and organisation of democracy.[11]

The Internet, the Darknet and other non-traceable networks and forums creates a significant challenge to policing. Law enforcement actors are forced to develop and introduce very intrusive ways of policing based on surveillance, covert operations where police officers interact with cybercriminals in an unprecedented form. Yet, this does not signify that law enforcement should be allowed to intervene indiscriminately in people's online and offline lives. There are limits to police powers offline which also should apply to online policing, such as use the existing warrant routes to access online user's data. However, there are also various exceptions to these normative standards. Police investigators are generally allowed to access to chat rooms, to monitor conversations and pose as potential victims and sexual offenders online to identify predators as well as sellers or buyers on illegal markets.[12] Law enforcement agencies are also using the same tools to infiltrate the Darknet to follow illegal activities, and prosecute terrorists and organised online criminals. The Snowdon revelations in 2013 showed that state agencies have extended their powers to monitor online users, crack encryption codes and build backdoors into software.[13] Allowing law enforcement to circumvent encryption and build backdoors into systems was raised again after the San Bernardino attack in 2016, where the US Federal Bureau of Investigation (FBI) wanted Apple to break the encryption code on an iPhone.

[9] M Mayer et al, 'International politics in the digital age: Power diffusion or power concentration?' (*SISP Conference*, 2013), 8.
[10] *See also* J Van Buuren, 'Doelwit Den Haag?: Complotconstructies en systeemhaat in Nederland 2000-2014' *PhD thesis, Leiden* (2016).
[11] J Kremer 'Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace' (2014) 23(3) *Information & Communications Technology Law* 220, 226.
[12] E E Jardine, 'The dark web dilemma: Tor, anonymity and online policing' (2015) 21 *Global Commission on Internet Governance Paper Series*, 9.
[13] J Ball et al, 'Revealed: how US and UK spy agencies defeat internet privacy and security. *The Guardian* (05 September 2013); E MacAskill et al, 'Mastering the internet: how GCHQ set out to spy on the world wide web' *The Guardian* (21 June 2013).

Similar methods and powers have also been suggested in the United Kingdom in the aftermath of the 2017 terrorist attacks.[14]

These hidden networks, forums, and communication platforms are based on attribution, anonymization and encryption. Facilitated by a combination of the Internet and encryption technologies, the Darknet trade is possible and will increase in the future as it will continue to create difficulties for law enforcement to break the encryption codes.[15] Together with new computer technologies and virtual spaces, the secret underworld makes policing difficult because law enforcement's limited powers to follow criminal leads online. Currently, a number of new legal instruments in the field of cybercrime are being drafted to address the changes in online criminal behaviour. For example, The Netherlands has been active in adopting new legislation and is progressing its adoption of the Third Computer Crime Legislation.[16] The legislation was passed in Parliament but was awaiting endorsement by the Senate at the time of writing. This cybercrime legislation allows police officers to actively infiltrate computer data of individuals who are suspected of specified crimes as well as crimes that may undermine the legal order (i.e. terrorism). Moreover, in this 3rd generation legislation, a new article has been added which gives police the power to prevent the crime, allowing the Public Prosecutor the possibility to make the relative content inaccessible in order to end or prevent new criminal offences.[17] This also means that the Netherlands is in the second phase of implementing the Council of Europe Cybercrime Convention

However, the actual challenge of policing the Internet is not only linked to the increasing use of the Darknet, the TOR network, proxy servers, secure hosting and encrypted communication apps. There is a range of products and services that cover user's activities, and identities are readily available online. In the mind of law enforcement communities these create obstacles for the effective policing of online criminal activity.[18] Europol has highlighted that communities of offenders mature and learn from their own mistakes as well as their assets that have been seized by law enforcement. Thus, it becomes very difficult to infiltrate cyberspace, and the increase of online policing has pushed offenders to switch to the untraceable dark-

[14] E Nakashima, 'Apple vows to resist FBI demand to crack iPhone linked to San Bernardino attacks' *Washington Post* (17 February 2016). A Hamilton, 'INTERVIEW: Telegram and terror: How data encryption shapes our lives' (*Digit*, 13 June 2017).

[15] M J Barratt, 'Silk Road: Ebay for Drugs' (2012) 107 *Addiction* 683, 107.

[16] *"Aan artikel 126cc worden twee leden toegevoegd, luidende: 5. Indien bij een onderzoek in een geautomatiseerd werk gegevens worden aangetroffen met betrekking tot welke of met behulp waarvan het strafbare feit is gepleegd, kan de officier van justitie bepalen dat die gegevens ontoegankelijk worden gemaakt voor zover dit noodzakelijk is ter beëindiging van het strafbare feit of ter voorkoming van nieuwe strafbare feiten. Het bepaalde in artikel 125o, tweede en derde lid, is van overeenkomstige toepassing. 6. Zodra blijkt dat gegevens die zijn vastgelegd tijdens een onderzoek in een geautomatiseerd werk van geen betekenis zijn voor het onderzoek, worden zij vernietigd. Artikel 125n, tweede lid, is van toepassing."* Eerste Kamer der Staten-Generaal, 'Computercriminaliteit III (34.372); gewijzigd voorstel van wet (EK, A)' (20 December 2016).

[17] Eerste Kamer der Staten-Generaal (note 18 above).

[18] Europol, 'The internet organised crime threat assessment (IOCTA) 2015' (2015), 9. Europol, 'The Internet organised crime threat assessment (IOCTA) 2016' (2016a), 17, 57; Europol, 'The relentless growth of cybercrime' (27 September 2016b).

networked underground.[19] Many criminal tools and services cut across several different cybercrime areas. Disrupting one network has a significant impact on a larger number of cyber-enabled crime due to the interconnectivity. To disrupt, dismantle or take down these networks, a greater level of cooperation is required between investigators from, for example, cyber-attacks, payment fraud and online child sexual extortion units to efficiently prioritise and coordinate investigations and prevent conflicts of interest between the different units.[20] The fact is that cybercrime units need to work across the narrowly defined cyber-crime types and spread knowledge and techniques about cybercriminal's methods and profile. Together, policing units are forced to develop norms and practices which can cover more than one cybercrime area. This cooperation involves developing useful operational methods to infiltrate and investigate the hidden networks and forums, where cyber criminals can manoeuvre undetectably. Currently, there is a lack of a unified legislative framework that ties together public and private policing means and methods at national as well as international level.

2.1 Policing virtual spaces: a public and private challenge

The policing of virtual spaces tends to have a highly proactive character. Several measures have been introduced to monitor and prevent cybercrime. Policing today is practiced as a pluralistic enterprise where public and private security actors co-operate and secure the Internet. A variety of surveillance techniques and monitoring software has been developed which influence policing of virtual spaces spanning from law enforcement investigation tools to Internet providers and social media use of monitoring, filtering and blocking software.[21] The terrorist attacks in France and the UK has put a substantive pressure on Internet companies such as Twitter, Facebook and YouTube to increase their private policing of extremist content uploaded on their platforms).[22] Facebook (2017) claims that it has increased its specialist team working on counter-terrorism specifically. This includes academic experts on counterterrorism, former prosecutors, former law enforcement agents and analysts, and engineers. In addition, Facebook highlights that it applies algorithms to identify groups of accounts, messages or images.[23] This illustrates that the role of private actors in the policing of virtual spaces is rapidly on the rise. Activities such as filtering, blocking and intrusive undercover policing operations have transformed from the original idea concept of cyberspace being a cyberspace for communication to a monitored and regulated space. Surveillance techniques and tools are

[19] Europol 2015 (see note 18), 31.
[20] Europol 2016a (see note 18), 15.
[21] A A Gillespie, '(2008) Cyber-strings: Policing sex offenders on the internet' (2008) 81(3) *The Police Journal: Theory, Practice and Principles* 196. R Cohen-Almagor, 'Online child sex offenders: Challenges and counter-measures' (2013) 52(2) *The Howard Journal on Crime and Justice* 190. M Rowe and R King, 'An investigation into the performance of UK internet providers' (Lancs.ac.uk, 02 November 2015).
[22] BBC News, 'US official: Russia 'hacked' 21 US states in election' *BBC News* (21 June 2017a).
[23] Corera 2017 (note 2 above).

widely used and the use of undercover police operations have spread from the United States to the European mainland – yet with some national limitations.[24]

The focus on terrorists' use of the Internet has increased the Charlie Hebdo attack in 2015.[25] The European attacks are indirectly linked to online spaces as the attackers draw inspiration from each other and propaganda and extremists' material are widely broadcasted and streamed online.[26] In 2010, the UK introduced the Counter-Terrorism Internet Referral Unit (CTIRU), which is a national police unit that works together with online companies to address the growing number of online content that violate legal prohibitions against glorifying or inciting acts of terrorism.[27] In 2015, the European Union created a similar Internet Referral Unit[28] and France adopted legislation that expanded the government's surveillance authorities to counter terrorist threats.[29]

The EU has launched different initiatives and forums to tackle online radicalism. The Radicalisation Awareness Network (RAN) was established in 2011.[30] In 2015, the EU established an Internet Forum which brings together the online industry, Member States, law enforcement and civil society partners to discuss how to manage the growing challenge of online extremist propaganda and create a voluntary cooperation, which at the same time protects fundamental rights, such as freedom of expression. The Commission has worked together with social media businesses, such as Facebook, Twitter, YouTube and Microsoft, to establish a code of conduct to combat the spread of illegal hate speech online in Europe.[31]

One of the most significant challenges to managing virtual spaces is the jurisdictional dilemma where cyber legislation is defined differently in jurisdictions worldwide. Legislation differs considerably in the various geographical jurisdictions and an act can be legal in one state but illegal in another.[32] Unfortunately, the harmonisation or development of cybercrime legislation is hindered by a range of obstacles. Given the technological, legal and cultural diversity of the world's nations, the risk perception differs strongly. States have different priorities; some recognise that different forms of regulation are needed to cover the extensive cybercrime types – and therefore, they have developed a comprehensive framework. There are states who do

[24] Kruisbergen et al, 'Undercover policing: Assumptions and empirical evidence' (2011) 51(2) *The British Journal of Criminology* 394, 3; J E Ross, 'Undercover policing and the shifting terms of scholarly debate: The United States and Europe in counterpoint' (2008) 4 *Annual Reviews* 239, 241; C Fijnaut and G T Marx, 'The normalization of undercover policing in the west: Historical and contemporary perspectives' in C Fijnaut et al (eds) *Undercover: Police surveillance in comparative Perspective* (Klüwer 1995), 15-16.
[25] BBC News, 'Charlie Hebdo attack: Three days of terror' *BBC News* (14 January 2015); Munk, 2017 (note 3 above).
[26] Ibid (note 3 above). Hamilton 2017 (note 14 above).
[27] Europol, 'Europol Internet Referral Unit One Year On' (22 July 2016c). Sky News, 'Police unit removes 250,000 terror items from internet' *Sky News* (23 December 2016).
[28] Europol, 2016c (note 27 above).
[29] D P Fidler, 'Countering Islamic State exploitation of the internet' (*Council on Foreign Relations*, 18 June 2015).
[30] European Commission, 'FAQ: The Radicalisation Awareness Network' (28 January 2013).
[31] European Commission, 'Supporting the Prevention of Radicalisation Leading to Violent Extremism' *COM(2016) 379 final* (14 June 2016), 6.
[32] M Cross, *Scene of the cybercrime* (2nd ed, Syngress 2008), 3.

not recognise cyber-offences and regard them as falling under the scope of existing offline regulations and thereby, they are rejecting the whole framework of cyber-dependent crimes. Moreover, some states are focusing on online theft of intellectual property where other states are prioritising online blasphemous or seditious communications.[33] A different interpretation of acceptable online behaviour puts strains on policing and the way they are deployed to the online community.[34]

Cybercrimes are by nature transnational but because of the lack of comprehensive international treaties and cooperation, the effort to manage cybercrime is largely left in the hands of national law enforcement. So far, obstacles for ensuring efficient management derive from judiciary limits, insufficient intelligence gathering/sharing capabilities, technical difficulties, disparate investigative and forensic capacities, lack of trained staff, and inconsistent cooperation with other stakeholders.[35]

3 Characteristics of Cybercrime

It is widely recognised that cybercrime has two overall characteristics. Cyberspace opens up new ways of committing a crime, or new ways of committing offline crimes. This forces governments around the world to introduce new laws to respond to the new threats.[36] Europol (2016) has highlighted a new platform for crime based on an increasing cybercriminal economy based on the inclusion of cyberspace in everyday life and the low level of digital security. These cybercrimes mirror traditional crimes (cyber-enabled crime) where cyber-space is a mean to an end; they are only different in their practice.[37] These traditional crime types have emerged in forums where criminals and potential criminals exploit cyberspace to commit crime, i.e. online paedophilia, cyber terrorism, identity theft, online fraud, ransomware, the criminal use of data, payment fraud, online child sexual abuse, abuse of the Darknet, social engineering and virtual currencies.[38]

[33] P Grabosky, 'Requirements of prosecution services to deal with cyber-crime' (2007) 47(4-5) *Crime, Law & Social Change* 201, 207.

[34] European Commission, 'Protecting Europe from large scale cyber-attacks and disruptions: Enhancing preparedness, security and resilience' *COM(2009) 149 final* (30 May 2009); European Commission, 'Achievements and the next steps: Towards global cyber-security' *COM(2011) 163 final* (31 March 2011a), 2, 4; European Council and the High Representative of the European Union for Foreign affairs and Security Policy, 'Cybersecurity strategy of the European Union: An open, safe and secure cyberspace' *JOIN(2013) 1 final* (7 February 2013).

[35] European Council and the High Representative of the European Union for Foreign affairs and Security Policy 2013 (note 34 above); European Commission, 'Tackling crime in our digital age: Establishing a European Cybercrime Centre' *COM(2012) 140 final* (28 March 2012).

[36] G S Jackson, 'Types of cybercrime and their penalties' (It Still Works, 28 July 2017). M Theoharis, 'Computer and Internet Crime Laws' (*CriminalDefenceLawye*r, 28 July 2017). Eurojust 'Eurojust Annual Report 2011 (2012), 34.

[37] M McGuire and S Dowling 'Cyber crime: A review of the evidence. Chapter 2: Cyber-enabled crimes' (*Home Office*, October 2013a), 4.

[38] *See:* D S Wall, 'Policing cybercrimes: Situating the public police in networks of security within cyberspace. Police practices and research' (2007) 8(2) *Police Practice and Research*, 186; D S Wall, 'The Internet as a conduit for criminals' in A Pattavina (eds) *Information technology and the criminal justice system* (Sage 2005), 77; B R Jones, 'Comment: Virtual neighbourhood watch: Open source software and community policing against cybercrime' (2007) 97(2) *The Journal of Criminal Law and Criminology* 601, 602; Jackson 2017 (note 36 above); Theoharis 2016 (note 36 above); Europol 2016a (note 18 above); Europol 2016b (note 18 above); M McGuire and S Dowling, 'Cyber crime: A review of the evidence. Chapter 1: Cyber-dependent crimes' (*Home Office*, October 2013b).

Other cybercrimes (cyber-dependent crimes) are specific related to cyberspace using computer technology to develop new forms of crime, i.e. malware infections, viruses, spam, denial of service attacks.[39] These types of cybercrime are based on the technological development and the online interconnectivity, and they can only be carried out using cyber-space. Therefore, these cyber-dependent crimes are distinct from real-time offences even though they share some parameters with real-time crimes.[40]

Today, online and offline criminal activities are entangled due to the rapid technological development which puts pressure on policing in a non-physical domain which has merged with the real world on multiple levels.[41] Cyber-dependent crimes are harder to deal with because there is no offline crime legislation which can be used analogue until cyber legislation is developed. Yet, it is not only in relation to cyber-dependent crimes that a legislation framework is underdeveloped. In other areas, such as cyber-terrorism, specific legislation has not been developed and it has not been considered to be a distinct offence. Instead, cyber-terrorism is considered to be covered by the counter-terrorism legislation and/ or cybercrime, depending on the offence. However, the growing use of the Internet to recruit and spread propaganda by IS and large-scale attacks, such as the Dyn[42] attack in 2016 calls for a rethinking of cyber-terrorism as a cybercrime type separated from offline crime rather than keep the offences floating between counter-terrorism and cybercrime legislation.

A classic example of transnational cybercrime is the 'love bug' worm from 2000. This worm was developed in the Philippines and infected computers worldwide. Yet, the investigation in the Philippines was hindered because of malicious development and spreading of damaging software, at the time, was not criminalised in the country.[43] This bug was a global eye-opener which instigated the development of cybercrime legislations. Yet, the problem of international cybercrime stays unsolved. Some interesting cases have caught the world by surprise, such as the suspicion about Russian spyware during the United States of America (USA) Presidential election in 2016, where Russian hackers made repeated attempts before the election to get into important US institutions.[44] Moreover, it has been claimed that Russian hackers tried to hijack the US election by targeting the election systems in 21 US states.[45] In 2017, large scale attacks have increased which have had a significant impact worldwide. The WannaCry Ransomware attack worldwide showed the

[39] Wall 2005 (note 38 above), 77; I Walden, *Computer crime. Computer law* (Oxford University Press 2007); Jones 2007 (note 38 above); Home Office, *Cyber Crime Strategy* (Strategy, Cm 7842, March 2010), 12-16; Wall, 2007 (note 28 above), 186; A Klimburg, 'Mobilising Cyber Power' (2011) 53(1) *Survival* 41, 43.
[40] Wall 2007 (note 38 above), 186.
[41] Europol, 'Massive blow to criminal Dark Web activities after globally coordinated operation' (30 July 2017); Munk 2017 (note 3 above); Hamilton 2017 (note 14 above).
[42] *Dyn is a company which controls most of the internet's domain name system (DNS) infrastructure.* N Woolf 'DDoS attack that disrupted internet was largest of its kind in history, experts say' *The Guardian* (26 October 2016).
[43] United Nations, 'Twelfth United Nations Congress on crime prevention and criminal justice' (United Nations, 12-19 April 2010), 5; BBC News, 'Police close in on Love Bug culprit' *BBC News* (06 May 2000).
[44] L Hardin, 'What we know about Russia's interference in the US election' *The Guardian* (16 December 2016).
[45] BBC News, 'UK and France to work together to tackle online extremism' *BBC News* (13 June 2017b).

problems with the online interconnectivity and the problems investigating the attack – especially as it is presumed that the hackers belonged to the Lazarus Group; a group that works from both China and North-Korea.[46] Later in 2017, another international ransomware attack, PetrWrap, brought down banks, government IT systems and energy firms in Poland, Italy, Germany, France, Denmark, the USA, the UK, Russia and Ukraine.[47]

4 The Criminalisation of Online Conduct in National Jurisdictions

States worldwide have developed legislation which criminalises cybercrimes and different online behaviours. The punishments might increase the level and the severity of sentences. However, they have limited effect on making virtual spaces safer, and it is difficult to get a precise overview over the conviction rates as most cybercrime data are not separated from offline offences. For example, in the UK, data about the conviction rate of online grooming and online sexual child abuse was not divided between online and offline offences and only a small number of offences falls under the scope of the UK Computer Misuse Act 1990.[48] Harsh punishment might dissuade some people, but the cybercriminals with the intent to misuse computer systems are likely to continue their criminal pathway online and they are seldom caught and prosecuted.[49] Cybercriminals can easily move their enterprise to safe havens that have little or no cybercrime legislation in place. Moreover, the online underground represented by the Darknet and the extended use of encryption create a unique opportunity to continue to offend and be inspired by other cybercriminals. This requires that law enforcement directs their efforts to these networks and they need to adjust the practices to the new circumstances in this untraceable area.

4.1 Legal Frameworks on Cybercrime

One of the problems related to the online policing is the lack of a standard definition which can be used universally. The definitions as well as legislation developed is fragmented and content-related rather than

[46] D Lee, 'WannaCry ransomware cyber-attack 'may have N Korea link'' *BBC News* (16 May 2017).
[47] BBC News, 'Global ransomware attack causes turmoil' *BBC News* (27 June 2017c); Sky News, ''Powerful' cyberattack on Ukraine goes global' *Sky News* (27 June 2017).
[48] National Statistic 'Criminal justice system statistics quarterly: December 2016. Criminal justice statistics outcomes by offence tool' (GOV.UK, 18 May.2017). In the UK (2016) the total number of cautions issued and convictions amounts to: 103.353 persons were issued a caution and 1.240.271 were convicted. Under *the UK Computer Misuse Act 1990 S1(3*) - Unauthorised access to computer material, 26 persons were issued a caution and 32 persons were convicted. *The UK Computer Misuse Act 1990 S2 - Unauthorised access with intent to commit further offences, etc.* 21 persons were issued a caution and 21 persons were convicted. *The Computer Misuse Act 1990 S3 - Unauthorised acts with intent to impair, etc*, 0 person was issued a caution and 2 persons were convicted. *The UK Computer Misuse Act 1990 S3A - Making, supplying or obtaining articles for use in offence under Sections 1 or 3*, 0 persons was issued a caution and one person was convicted. *Fraud by false representation: cheque, plastic card and online bank accounts;* 1.345 persons were issued a caution and 5.367 were convicted. *The UK Computer Misuse Act 1990 S.1;* 8 persons were issued a caution and four persons were convicted. National statistic, 2017.
[49] The European 'EU gets strict with cybercrime penalties' (*The European*, 10 July 2013).

providing general guidelines and powers that can be transferred to the different crime forms. At the Tenth United Nation Congress on the Prevention of Crime and Treatment of Offenders (2000) cybercrime was defined as "cybercrime in a narrow sense (computer crime): Any illegal behaviour directed at employing electronic operations that targets the security of computer systems and the data processed by them".[50] Moreover, the definition also covers the second strand by including: "Cybercrime in a broader sense (computer-related crime): Any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network".[51]

Currently, there is only one global cybercrime convention developed in place. The Council of Europe's Convention on Cybercrime from 2001 opens for a global framework.[52] This Convention establishes a more harmonised approach to policing by offering definitions and criminalisation of certain online behaviours.[53] Additionally, the Convention is wide-ranging, and it includes illegal access, illegal interception of data, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and online offences related to infringements of copyright and related rights.[54] The Convention also provides a common-law enforcement framework for dealing with cyber criminals, foster sharing of information among all signatory states, and it gives powers to security actors. Significantly, the Convention allows for intrusive monitoring systems for offline collection of online data.[55]

Nevertheless, only a limited number of states have signed up to this convention which leaves the area significantly unregulated in a global context.[56] One the most severe limitations to tackle the global phenomenon of cybercrime is the lack of signature states – which weakens the global effect of the Convention.[57] By 2017, only 55 states signed up for the Convention, and only 51 states ratified it (Colombia, Ghana, Paraguay, and Peru have not ratified the Convention). Surprisingly, four-member states of the Council of Europe have not signed up for this treaty (Ireland, Russia, San Marino and Sweden).[58] For example, Sweden needs a constitutional change in order to ratify the Convention and its additional

[50] United Nations, 'The United Nations Convention against transnational organized crime' *UNODC* (2000(b)).
[51] P Rivera, 'United Nations' definition of cybercrime' (Innovative Dynamics Network, 07 December 2016); Cross 2008 (note 32 above); United Nations, 'The Tenth United Nations Congress on the prevention of crime and treatment of offenders' (*United Nations*, 10 April 20008a)).
[52] Council of Europe, 'The European convention on cybercrime' European Treaty Series - No. 185 (23 November 2001); P Pawlak, 'A Wild Wild Web? Law, Norms, Crime and Politics in Cyberspace' (*EUISS*, 12 July 2017), 4.
[53] Council of Europe 2001 (note 52 above).
[54] D Emm, 'Cybercrime and the law: a review of UK computer crime legislation' (*Securelist*, 29 May 2009); Council of Europe 2001 (note 52 above).
[55] Council of Europe 2001 (note 52 above).
[56] Council of Europe 2001 (note 52 above); Pawlak 2017 (note 52 above), 2, 4.
[57] Emm 2009 (note 54 above); Council of Europe 2001 (note 52 above).
[58] Council of Europe, 'Chart of signatures and ratifications of Treaty 185' (*Treaty Office*, 28 July 2017)

protocols.[59] This is the same problem Ireland is facing. However, the Department of Justice in Ireland published in 2016 the Criminal Justice (Offences Relating to Information Systems) Bill which makes it possible to ratify the Council of Europe's Convention on Cybercrime.[60] However, Russia chose not to sign the treaty due to cultural and political objections to international treaties, cybercrime investigative cooperation and the definition of cybercrime.[61] Yet, this is a state-centric convention based on an agreement between states without any input from other actors, and non-state actors will still have very little influence on a new Convention, should it be negotiated. Moreover, due to the growing state concern of online activities and scepticism of private actors' ability to monitoring online spaces, the outcome could change the multi-stakeholder format of the Internet to a purely state-centric regulatory model.[62]

Meanwhile, the European Commission (2007) proposed a three-fold definition which covers traditional forms of crime committed by means of electronic communication networks and information systems, publication of illegal content over electronic media and crimes unique to electronic networks.[63] Other organisations include specific offences: The Council of Europe Convention (2001) uses the term cybercrime to refer to offences ranging from criminal activity against data to content and copyright infringement.[64] The United Nations Manual on the Prevention and Control of Computer-Related Crime (1994) definition includes fraud, forgery, computer sabotage, unauthorised access, and copying computer programmes as examples of cybercrime. However, neither most national legislations appear concerned with a strict definition of the word cybercrime. Instead, legislation is commonly referred to 'computer crimes', 'electronic communications', 'information technologies' or 'high-tech crime'.[65] Surprisingly, nor does the Council of Europe Convention on Cybercrime (2001) offer a precise definition of cybercrime.[66] The lack of an internationally recognised definition creates a definitional lacuna which creates obstacles for legislators and law enforcement and others involved in policing. However, most states accept that cybercrime is related to illegal online activities or behaviour, unauthorised access to a computer system or interference with a computer system or data. Moreover, the Tallinn Manual 2.0 from 2017 claims that in the pre-cyber era international law has been applied to cyber operations, both conducted by and directed against states.[67] In relation to interstate online

[59] Statens Offenliga Utredningar 'Europarådets konvention om it-relaterad brottslighet' *Betänkande av Utredningen om it-brottskonventione* (2013).
[60] C Morrissey, 'The Cybercrime Bill is here' (*Ireland IP & Technology Law Blog*, 20 January 2016)
[61] K Giles, 'Russia's public stance on cyberspace issues' in C Czosseck, R Ottis and K Ziolkowski (eds) 4th International Conference on Cyber Conflicts (NATO CCD COE, 2012).
[62] Pawlak 2017 (note 52 above), 4.
[63] Commission of the European Communities, 'Towards a general policy on the fight against cyber crime' *COM(2007) 267 final* (22 May 2007); Home Affairs Committee, 'What is e-crime?' (*www.Parliament.uk*, 30 July 2013)
[64] Council of Europe 2001 (note 52 above).
[65] UNODC, 'Comprehensive study on cybercrime (draft)' *(UNOCD*, February 2013), 11-12.
[66] Council of Europe, 2011 (see note 52); UNDOC 2013 (note 65 above), 12.
[67] NATO Cooperative Cyber Defence Centre of Excellence, 'Tallinn Manual 2.0.' (*CCDCE*, 28 July 2017).

conflicts, cyber events do not occur in a legal vacuum as states both have rights and obligations under international law.[68]

Fragmented attempts and agreements are developed to manage the area, but it is challenging to ensure transnational commitment from states as well as cross-sectoral parties. The United Nations (UN) Convention against Transnational Organized Crime covers some areas of cybercrime in relation to organised crime groups – but it does not cover the activities of individual hackers.[69] In 2007, the International Telecommunication Union (ITU) launched the Global Cybercrime Agenda (GCA) for a framework to coordinate the international response to the growing cybersecurity challenge built on five pillars: Legal measures, technical and procedural measures, organisational structures, capacity building and international cooperation.[70] There are several reasons for the lack of commitment to an international agreement. For instance, Russia and China have blocked UN attempts of creating an international cybercrime treaty. In 2010, the issue was discussed but ended in a stalemate because Russia, China and a number of developing countries failed to reach an agreement with the United States, Canada, the United Kingdom and the EU over national sovereignty issues and concerns for human rights.[71]

There is a lack of consensus about the development and harmonisation of legislation and policing practices. Some countries do not acknowledge the scale of the problem and they are still under the impression that offline legislation covers online offences sufficiently. Other countries have a different interpretation of cyber-risks and the level of the problem. This differentiated focus on cybercrime blocks legislative consensus and it creates significant obstacles to developing governance and policing forms. These problems are not only related to transnational cooperation on the strategic level; the same barriers are visible on the operational level. For instance, Russia refused to cooperate with foreign law enforcement in the Estonia-case (2007) to investigate the cyber-attack.[72] The same occurred in the Lithuania-case (2008) and the Georgia-case (2008).[73]

4.2 Harmonisation of Cybercrime Legislation

The existence of fragmentary and divergent legislation may contribute to an unbalanced approach towards online security. For example, negotiations between Russia and Western partners on cyberspace issues are not progressing due to a lack of mutual comprehension and flexibility. National jurisdictions have different

[68] Pawlak 2017 (note 52 above), 2.
[69] United Nations 2000(b) (note 50 above).
[70] ITU, 'Global Cybersecurity Agenda (GCA)' (*ITU*, 28 July 2017).
[71] G Masters, 'Global cybercrime treaty rejected at U.N.' (*SC Media*, 23 April 2010).
[72] E Tikk et al, 'International cyber incidents: Legal considerations' (*CCD COE*, 2010), 27; L Hansen and H Nissenbaum, 'Digital disaster, cyber security and the Copenhagen school' (2009) 53 *International Studies Quarterly* 1555, 1170.
[73] Tikk et al 2010 (note 71 above), 51-53, 89.

norms and values which are seen as threatening to the other part. Moreover, there is a lack of collective understanding of cyberthreats as well as defined concepts which stall the development[74] Even though China and Russia vetoed UN agreements, Russia presented in 2011 a "Draft Convention on International Information Security" which pre-dated the "International Code of Conduct for Information Security" annex presented by Russia and China, Tajikistan and Uzbekistan to the United Nations addressed to the UN Secretary-General in 2015.[75] China and Russia signed a bilateral agreement in 2015, in which they agreed not to hack each other, as well as on law enforcement cooperation and exchange of cybersecurity technologies.[76] Nevertheless, these countries' positions are not clear in relation to cybercrime and the stakeholders involved. i.e. law enforcement cooperation and exchange of cybersecurity technologies. But the Code of Conduct and the Bilateral agreement do not specify if these laws apply to cyber space.[77] China's International Strategy of Cooperation in Cyberspace from 2016 includes a commitment to 'study the application on international law in cyberspace. This should be done from the perspective of maintaining international security, mutual trust and preventing cyber-conflicts.[78] There is a will to develop an agreement, but the UN parties and the Russian-China group have opposite views of the threat and what an agreement should contain.

Policing online crimes reveals a legislative gap where states have different legislation in place which creates structural and cultural limitations upon legislations and this has resulted in an online security deficit.[79] Online offending is significantly technical and legally complex. Continuous development in the functionality of information communication technologies (ICTs) and disparities between legal systems worldwide present a growing challenge to everyone involved in policing virtual spaces, such as first responders, investigatory authorities, forensic interrogators, prosecution services and criminal justice authorities.[80]

The UN (2017) has provided an overview over the cybercrime legislation worldwide. The UN states that 138 states have enacted cybercrime legislation. Of these, 95 states are developing and transition economies. Yet, 30 countries still have no cybercrime legislation in place. The data provided by the UN shows that 72% of the states have legislation in place. 9% of the states have developed draft legislation, 19% of the states have

[74] Giles 2012 (note 61 above), 64.
[75] United Nations Information Service, 'Cybercrime' (*United Nations Information Service*, 12-19 April 2015); Pawlak 2017 (note 52 above), 2.
[76] I Kilovaty and I Mann, 'Towards a cyber-security treaty' (*Just Security*, 3 August 2016).
[77] Pawlak 2017 (note 52 above), 2.
[78] Ibid.
[79] J Nhan and L Huey, 'Policing through nodes, clusters and bandwidth: The role of network relations in the prevention of and response to cyber-crimes' in S Leman-Langlois (eds) *Technocrime: Technology, crime and social control* (Willan 2008).
[80] C S D Brown, 'Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice' (2015) 9(1) *International Journal on Cybercrime* 55.

no legislation in place and finally, 1% of the states have not provided any data regarding their cybercrime legislation.[81]

It is widely recognised that the compatibility of criminal offences and investigative measures across jurisdictions is the most efficient way to policing cyberspace and this goes through enhanced cooperation across jurisdictions. Different international organisations, such as the UN, the Internet Governance Forum, the Council of Europe and the EU have taken steps to manage cybercrime and develop a general cyber-security framework to address the constant changing cyber-threats.[82] However, the lack of recognition and harmonisation of legislation and practices can cause problems where cybercrime is carried out from states with more accommodating governance standards. This creates safe havens with opportunities to cybercriminals to avoid detection, prosecution and imprisonment.[83]

The need for cross-jurisdictional harmonisation has been acknowledged in the European Union. Most EU Member States have expanded their national criminal code to include cybercrime because of the CoE Convention and the number of EU directives developed. Moreover, new EU legislation refers to criminalisation and penalties. The Treaty of Lisbon provided the European Union with a stronger mandate to harmonise legislation on computer-related crime.[84] For example, the EU Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography[85] includes 20 different offences, creates minimum levels for criminal penalties and facilitates reporting, investigation and prosecution.[86] The EU Directive (2011) provides intrusive powers to law enforcement to prevent and prosecute offenders online, i.e. interception of communications, covert surveillance including electronic surveillance, monitoring of bank accounts or other financial investigations. The Directive states that tools should also include the possibility for law enforcement authorities to use a concealed identity on the Internet. Yet, these powers ought to be developed in accordance with national law.[87] The problem is that there is no clear cybercrime legislation in place in most of these areas. Tackling cybercrime is implicit in legal EU instruments, such as the EU Directive on Money Laundering.[88] Moreover, there is a legislative lacuna in relation to cyber-terrorism which is caught up between national counter-terrorism and cybercrime legislation without

[81] UNCTAD, 'Cybercrime legislation worldwide' (*UNCTAD*, 01 June 2017)
[82] Home Office 2010 (note 39 above), 10-11.
[83] UNCTAD 2017 (note 81 above); United Nations Information Service 2015 (note 75 above).
[84] Council of Europe 2001 (note 52 above); United Nations, 2010 (note 43 above), 6; European Union, 'Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community' *2007/C 306/01* (17 December 2017).
[85] European Union, 'Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA' *L335/1* (13 December 2011).
[86] European Commission, 'European Parliament supports stronger legislation against child sexual abuse' (27 October 2011b); European Commission, 'Child sexual abuse' (*Migration and Home Affairs*, 27 July 2017).
[87] European Union 2011 (note 85 above).
[88] European Union, 'Directive (EU) 2015/849 on preventing the use of the financial system for money laundering or terrorist financing (4th Anti-Money Laundering Directive)' *L 141/73* (15 June 2015). *See also*: The Council of the European Union (2001) Council Framework Decision 2001/413/JHA on Combating fraud and counterfeiting of non-cash means of payment' *L 149/1* (02 June 2001).

addressing the growing problem of encryption tools, the Darknet, broadcasting and streaming of extremist propaganda, as seen in relation to Telegram and WhatsApp communication apps.[89]

The lack of consensus between transnational and cross-sectoral legislation and practices complicates the policing of virtual spaces. Moreover, the lack of transparency and openness regarding the strategies and measures imposed worldwide creates a problem regarding the problems and different measures and operations are often only discussed in the Western countries. Therefore, it is only possible to investigate the issue from a European-American public-private perspective.

5 Plural Investigation and Monitoring of Virtual Spaces

The evidence of cybercrime is mostly in electronic or digital form, such as computer files, transmissions, logs, metadata, or network data. Obtaining online evidence combines traditional and new policing techniques. Traditional policing techniques covers interviewing victims or undercover visual surveillance of suspects. New policing techniques covers computer-specific measures, such as viewing, and seizing or copying computer data from devices from the suspect or third parties (such as ISPs) and intercepting electronic communications.[90]

Technical measures and monitoring techniques is now a part of a wider surveillance regime where new processes, practices and software has been developed to police cyberspace. Surveillance introduced to monitor Internet traffic is now a common technique which normalises, or legitimises, Internet control. Surveillance has been defined as "any collection and processing personal data, whether identifiable or not, for the purpose of influencing or managing those whose data has been garnered".[91] This definition covers any collection and processing personal data through new policing processes, practices and software.[92] Nevertheless, Internet censorship is a controversial topic. On one hand, these techniques have the ability, for example, to limit available content, such as child pornography and hate speech. On the other hand, the same techniques can be used to suppress individuals and it is considered a significant threat to human rights and fundamental freedoms.[93] Unwarranted spying on states and citizens creates concerns about fundamental freedoms of online users and the extent to which state actors can/ should monitor citizens. These freedoms are not only linked to the right to privacy, freedom of speech and freedom of expression but also the data protections rights incorporated in international and regional treaties and conventions creates safeguards

[89] Hamilton 2017 (note 14 above).
[90] UNODC 2013 (note 65 above), 122.
[91] D Lyon, *Surveillance society: Monitoring eveyday life* (2001 Open University Pres), 2; *See also:* D Lyon, *Surveillance studies. An overview* (2007 Polity Press), 13-16.
[92] Lyon 2007 (note 91 above), 13-16.
[93] J Dalek et al, 'A method for identifying and confirming the use of URL filtering products for censorship' (2013) *The 2013 conference on Internet measurement*, 23; Y Mou, K Wu and D Atkin, 'Understanding the use of circumvention tools to bypass online censorship' (2016) 18(5) *New Media & Society* 837, 838; W Wu and S H Koo, 'Perceived effects of sexually explicit internet content: the third-person effect in Singapore' (2001) 78(2) *Journalism & Mass Communication Quarterly* 260.

against and over-intrusive and controlling state.[94] Yet, tools to circumvent censorship have been developed and are being deployed by Internet users.[95] Moreover, it has had a displacement effect on users, who are not cybercriminals, to use the Darknet and encryption tools.

Some online areas are blocked by national legislation, and national and international ISPs are forced to introduce automatic filtering software. In the UK, there are four areas of information where filtering is in use, i.e. child abuse images, material which can infringe copyright, extremist material, and general illegal content. Yet, no system is 100% secure. On the one hand, this automatic filtering can cause over-blocking of data, where sites are blocked despite not falling directly into these four groups. For example, sexual health advice blogs, charity web pages, addiction support sites, political related sites and opinion blogs. On the other hand, the filtering systems are not without loopholes which allows for an under-blocking of data as the filtering systems cannot comprehend everything and data which should be blocked are exchanged unhindered.[96]

Social media companies, such as Facebook, Twitter, Google, MTV Networks/Viacom, etc. have developed their own monitoring software.[97] Society today merges online and offline activities as well as public and private activities and therefore, it is impossible to separate the different actors' involvement in policing the Internet. Both the public police and private security actors, ISPs and online companies have a role to play to enhance online safety.[98] Social media companies have been criticised in relation to extremist content and propaganda uploaded by IS – especially after the second London attack in 2017, where UK Primer Minister Theresa May accused big online companies of not doing enough to prevent online extremist material to spread and for creating safe areas for terrorists.[99] Moreover, social media companies, such as Twitter, Facebook and Google, have also been critiqued by British Members of Parliament for not taking tougher action to tackle hate speech online.[100] As a response to criticism of the failure of social media companies to remove terrorism and extremist material online, Facebook, Google, Microsoft and Twitter joined forces in 2017 to counter online terror content by developing technology to identify expressions of violent extremism.[101]

Yet, the criticism is not entirely fair. Social media companies have acted over the years and invested in better monitoring systems, but they are struggling to create a balance between security and censorship. Facebook

[94] Kremer 2014 (note 11 above), 232.
[95] Mou 2016 (note 90 above).
[96] Rowe and King 2015 (note 21 above), 2.
[97] Cohen-Almagor 2013 (note 21 above), 8.
[98] Munk 2017 (note 3 above); Hamilton 2017 (note 14 above).
[99] Council of Europe 2001 (note 52 above); A Sullyman, 'Whatsapp Encryption: What is it, how does it work and why is the Governments so worried about it?' *The Independent* (27.03.2017).
[100] A Travis 'Face-off between MPs and social media giants over online hate speech' *The Guardian* (14 March 2017)
[101] M Murgia and D Robinson, 'Social media groups join forces to counter online terror content' *Financial Times* (05 December 2016).

has received numerous complaints which have forced them to change their filtering systems and allowing content which normally would have been blocked, such as the iconic image of a girl fleeing a Napalm attack during the Vietnam war was removed because of nudity, and the same happened to cartoon breast cancer awareness video. In both cases, Facebook made a U-turn, apologised, and reinstalled the material.[102] Flagging up content is another technique developed by social media and online companies. This system allows users to express their concerns by reporting offensive content in the comment fields on news sites and blogs, yet, this has also been criticised as it can be misused.[103]

Although only a limited number of Internet users are cybercriminals, all Internet users are being subjected to these software systems without having any choice to opt out, and there is always the chance that fully legitimate communication is subject to blocking or filtering because the software systems are applied indiscriminately.[104] Additionally, the blocking and filtering systems are not reporting back the IP addresses of people who try to enter blocked sites, so the tools do not collect evidence which can be used to a formal investigation. Thus, private online monitoring techniques do not have the same effect as the tools deployed by law enforcement. In relation to the Darknet, these techniques are not useful as this space is beyond the control of states, ISPs, social media, and companies behind Internet search engines.

5.1 Monitoring Data Traffic and Proactive Online Policing

It is important to be able to police the Internet and identify cybercriminals while they are online on the basis of both online and offline intelligence. However, this can involve that the police officers may transgress the line of criminal activities which are committed by cybercriminals. This creates an ethical, moral and legal dilemma concerning how far law enforcement agents can go to detect, investigate and prosecute cybercriminals. In relation to the investigation of cybercrime, each investigative measure must be assessed in its own legal and practical context. This needs to be done to determine whether its interference with the privacy, family, home or correspondence of its subject can be justified. The nature of covert operations and/or electronic surveillance may raise privacy challenges. Almost all states have privacy safeguards incorporated in relation to investigating computer data and electronic communications. However, the way in which such protections are incorporated in law differs, and this can create obstacles to transnational covert operations in the online arena.[105]

[102] Z Kleinman, 'Fury over Facebook 'Napalm girl' censorship' *BBC News* (09 September 2016); H Kaminsky 'Facebook has re-approved a breast cancer awareness ad after initially blocking it for its content' (*Digital Trends*, 23 October 2016); K Crawford and T Gillespie, 'What is a flag for? Social media reporting tools and the vocabulary of complaint' (2016) 18(3) *New Media and Society* 410; A France-Presse 'Facebook bans 'offensive' Swedish breast cancer awareness video' *The Guardian* (20 October 2016); BBC News, 'Facebook U-turn over 'Napalm girl' photograph' *BBC News* (09 September 2016).
[103] Crawford and Gillespie 2016 (note 100 above), 2.
[104] Wall 2007 (note 38 above), 200.
[105] UNODC 2013 (note 50 above), 135.

In the United States, the gradual transition from reactive to proactive policing has resulted in a more expansive use of undercover operations mostly linked to the so-called buy-bust operations where the police create opportunities for someone to commit a crime, i.e. an undercover agent pose as someone who wants to buy drugs.[106] Thus, undercover police become engaged in apparently illegal activity to gather evidence or to uphold their fabricated identities. For example, the FBI and Interpol have established trap sites, web pages or bulletin boards which either present genuine child pornography material – or allow contributors to supply images or information about authentic web pages or URLs.[107] Yet, these activities are not considered to be crimes unless they are committed by 'rough' police officers not authorised to participate in the illegal activity. Instead, they are justified internally in law enforcement as a 'necessary evil' to carry out the operation. This practice of authorised criminality, developed by law enforcement, is conducted in secret, it is unaccountable, and it conflicts with the foundation of democratic policing based on the Rule of Law and its associated values, such as accountability and transparency. Circumventing democratic policing sends a mixed message to the public about moral standards which can undermine the social support for the police.[108]

5.2 Balancing Proactive Policing and Criminal Activities.

Proactive online policing cooperation is growing due to the transnational nature of virtual spaces. Undercover policing allows covert police officers to engage in activities that otherwise would be considered criminal.[109]. A number of these activities are seen in relation to online child abuse and economic cybercrime where it is impossible to investigate the illegal activities through the ordinary policing practices. Although the Darknet imposes significant challenges to policing different initiatives to crack the Tor router and Darknet code have been launched as well as policing operations which include a number of states. There are successful operations where law enforcement manages to break the Darknet codes or the encryption for several reasons.

These operations can involve a lengthy operation where law enforcement is monitoring the Darknet and the offender makes a mistake as seen in relation to the 'Silk Road'. The online 'Silk Road' was a busy black market for drugs which neither governmental legislation nor drug wars could control[110]. However, the

[106] Fijnaut and Marx 1995 (note 24 above), 15-16; Ross 2008 (note 24 above), 241; Kruisbergen et al 2011 (note 24 above), 3.
[107] Cohen-Almagor 2013 (note 21 above), 13; P Jenkins, Beyond Tolerance: Child Pornography on the Internet' (New York University Press 2001), 159.
[108] E E Joh, 'Breaking the law to enforce it: Undercover police participation in crime' (2009) 62 *Stanford Law Review* 155, 157.
[109] Jenkins 2001 (note 104 above), 157.
[110] A Greenberg, 'The Silk Road's dark-web dream is dead' (Wired, 14 January 2016); Jardine 2015 (note 12 above). *See also*: J Martin, 'Lost on the Silk Road: online drug distribution and the 'cryptomarket'' (2014) 14(3) *Criminology & Criminal Justice* 351; J Martin 'Informal security nodes and force capital' (2012) 23(2) *Policing & Society* 145; J Martin and N Christin, 'Ethics in Dark Net Research' (2016) 35 *International Journal of Drug Policy* 84; J McCulloch and J Martin, 'Policing the Globe: International Trends and Issues in Policing', in B Arrigo and H Bersot (eds) *International*

Darknet online market has been subjected to a number of disruptions of the illegal online trade starting with FBI taking down the 'Silk Road'. Sites such as Evolution and its competitor Agora has gone offline due to the change of security following attacks on Tor's hidden services, as well as the FBI's mass takedown of Darknet markets in late 2014.[111] So, it is possible to trace the sites and the people involved in the illegal online trade. However, it is very time consuming, and law enforcement has so far only managed to scratch the surface of the Darknet. According to Europol (2016), the use of encryption by criminals to protect their communications creates a significant challenge for law enforcement which creates obstacles to obtain access to essential intelligence and evidence.[112]

Some of these activities have been successful and improvements have been introduced. The Danish Police managed to arrest drug traffickers after a surveillance investigation of the blockchain on the Darknet market places. The Blockchain technology makes it possible to trace the bitcoin translations on the Darknet and the evidence obtained using this technology was used in court. Moreover, the experience has been shared with states which participate in Europol, (FBI) and the Drug Enforcement Agency (DEA).[113] Companies, such as Elliptic and Chainalysis, area also working with law enforcement agencies like the FBI, Interpol, Europol and Anti-Money Laundering (AML) and Know Your Customer (KYC) platform providers to investigate the Darknet.[114] In 2017, months of covert monitoring, preparation and coordination have resulted, in the takedown of two of the largest criminal Dark Web markets, AlphaBay and Hansa in a joint cooperation led by FBI, the DEA and the Dutch National Police, with the support of Europol.[115] Yet, these are only minor operations when set off against the wide range of illegal activities carried out on the Darknet. Naturally, these operations can successfully remove some actors and platforms, but the fact is that new and less traceable techniques would be deployed or the activities will be displaced to other virtual hotspots, such as WhatsApp and Telegram.[116]

5.3 Undercover Operations

Working with police forces around the world, the FBI and their special agents fronted an investigation that ended in 2008 with 59 arrests and prevented an estimated US$70 million in bank fraud.[117] During the two-

Handbook of Crime and Justice (Routledge 2013); J Martin 2014 (note 12 above), D D Robinson, 'Social media groups join forces to counter online terror content' *Financial Times* (05 December 2016).

[111] Greenberg 2016; (note 106 above); Jardine 2015 (note 12 above).

[112] Europol 2016a (note 18 above).

[113] J Redman, 'Danish Police surveil the blockchain to make arrests' (*Bitcoin.com*, 22 February 2017); K Bjørnholt, 'Dansk politi har knækket bitcoin-koden' *Dansk Politi Bladet*. (20 April 2017); Berlingske Tidende, 'Dansk gennembrud: Narkohandlere kan ikke længere gemme sig bag bitcoins' *Berlingske Tidende* (21 February 2017); J Markussen, '22-årig fik 2,3 kilo amfetamin leveret med posten' *Holstebro Struer Dagbladet* (25 April 2016).

[114] Redan 2017 (note 110 above).

[115] Europol, 'Massive blow to criminal Dark Web activities after globally coordinated operation' (30 July 2017).

[116] Hamilton 2017 (note 14 above).

[117] E Mills, 'Q&A: FBI agent looks back on time posing as a cybercriminal' (*CNet*, 30 June 2009); R McMillian 'Three years undercover with the identity thieves' (*PCWorld*, 20 January 2009).

year longer operation, the FBI agent (Master Splyter) was undercover and became an active member of DarkMarket as well as the site's administrator. The Spamhouse Project helped the FBI by creating a false identity for the FBI agents as a successful spammer prevented him from committing criminal.[118] Putting 'Master Splyter' on the list of the worst cyber-offenders created an opportunity for the police to investigate and prosecute members of the forum.[119]

In 2010, the FBI created a fake carding forum called 'Carder Profit' allowing the FBI to collect information on cybercriminals. During this two-year long operation, the FBI recorded the IP addresses of users' computers who accessed the site which resulted in a number of arrests in different states.[120] The problem is to what extent the FBI was involved in criminal activities by allowing cards and card details to be sold on the fake web page while they were monitoring the criminal activities. As mentioned above, one of the most fundamental policing principles is that the police officers should never incite the commission of a crime. If this principle is not respected by the law enforcement or their informant, the court can claim that the investigators have acted as agent provocateurs and the evidence would not be permissible (Harfield, *infra*).[121] It can be questioned whether the FBI overstepped that line when they created this criminal forum. It is also questionable whether other states can build a case on the FBI evidence unless they have been involved in the operation and acted within the limit of the national law. Otherwise, they need to carry out their own investigation by seizing the computer devices and trace the offender's actions.

Other successful operations have been carried out on the Darknet in the aftermath of the success with the 'Silk Road'. For example, "Operation Hyperion" was started by U.S. Federal Law Enforcement, the Five Eyes Law Enforcement Group (Australia, Canada, New Zealand, the United Kingdom and the United States) together with Europol. This operation is considered to be a step towards developing a more unified global law enforcement response to the growing usage of the Darknet by cybercriminals. The main target is to focus on individuals seeking to buy and sell illicit drugs and other illegal goods and services.[122] However, information is published about the actual operation and whether it has been based on a lengthy undercover operation as outlined above. The lack of information is to some extent understandable as it can jeopardize other operations. However, the strategic powers available for police forces should be made public to ensure transparency and accountability – and the public can debate whether they believe that these measures are acceptable.

[118] J Lusthaus, 'Trust in the world of cybercrime' (2012) 13(2) GC 71, 83; Mills 2009 (note 114 above).
[119] Ibid (note 115 above).
[120] T Smith, 'FBI locks up 24 people in undercover card hacking operation' (*CBR*, 27 June 2012).
[121] E Martellozzo 'Policing online child sexual abuse' (2015) 3(1) *European Journal of policing Studies* 32, 40; C Harfield and K Harfield, *Covert investigations. Blackstone's practical policing* (Oxford University Press 2005).
[122] ICE Newsroom, 'Law enforcement agencies around the world collaborate on international Darknet marketplace enforcement operation' (*U.S. Immigration and Customs Enforcement*, 31 October 2016).

6 Conclusion

The most considerable challenge to online police derives from a lack of consensus worldwide in how to manage cybercrime and exchange knowledge across border. At present, there are too many safe places for cybercriminals to hide and carry out their illegal activities from a distance. The lack of international and national harmonised legislative frameworks can over time lead to mission creep in areas where accountability and transparency are insufficiently guaranteed. The normalisation of exceptional policing norms can create grey zones where these norms are adopted without any legislative foundation. Moreover, the limits of and between public and private policing need to be defined. Without any doubt, private policing has a role to play in a pluralistic policing system of virtual spaces and a number of private actors can help law enforcement to develop software, technical security measures, monitor content uploaded and report offensive behaviours.

There is a pressing need for developing a new global cybercrime Convention which update and harmonise the criminalisation of online offences to reflect the current threat. States worldwide need to find a common stance and develop a universal treaty, which is long overdue to manage the growing types of cyber threats and different virtual platforms, such as the Darknet and impenetrable encryption tools which create obstacles for the policing of different communication tools used by cybercriminals. Moreover, a new Convention needs to set out global legal standards to prevent the creation of safe havens for cybercriminals. This chapter has demonstrated that there is an imbalanced approach to the criminalisation and the management of online offences. The way cybercrime is being policed at present is fragmented and does not keep in pace with developments. Hence, the policing effort fails to proportionately reflect the pervasiveness of the threat and the huge number of victims who suffer from a wide range of Internet crimes.

Meanwhile, problems are exacerbating with the use of the Darknet and encryption tools, making it very difficult to investigate and prosecute online offenders. In this context, it is important to recognise the role of private policing actors (see Shearing and Stenning *infra*) and the work that ISPs and online businesses are doing to manage the data flow – yet, they can improve their work; and initiatives has been taken to create better-monitoring systems. Moreover, it is important that relevant actors improve their mutual communication, and pool their capabilities and resources in joint operations to manage the growing misuse of cyberspace. In this context, it is important that private actors are consulted and involved in creating a new Convention as they have a significant role to play in policing the Internet.

The Darknet constitutes a challenge for police officers as means and methods developed to police the Internet are unusable due to the architecture of the Internet. Active covert police operations focused on the dismantling of criminal networks and catching offenders are becoming more widespread. Nevertheless, these activities are a balancing act. On the one hand, it is important to be able to police the Internet and the Darknet. On the other hand, on-line policing the transgression of formal lines for the collection of evidence.

This creates an ethical, moral and legal dilemma concerning how far law enforcement agents can go to detect, investigate and prosecute cybercriminals and cyberterrorists.

7 References

Asthana, A, 'Theresa May calls on tech firms to lead fight against online extremism' *The Guardian* (25 May 2017). <https://www.theguardian.com/politics/2017/may/25/theresa-may-calls-on-tech-giants-to-lead-fight-against-online-extremism> accessed 27 July 2017.

Avina, J, 'Public- private partnerships in the fight against crime: An emerging frontier in corporate social responsibility' (2011) 8(3) *Journal of Financial Crime* 282 <https://doi.org/10.1108/13590791111147505> accessed 27 July.2017.

Ball, J, J Borger and G Greenwald, 'Revealed: how US and UK spy agencies defeat internet privacy and security. *The Guardian* (05 September 2013) <https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security> accessed 27 July 2017.

Barratt, M J 'Silk Road: Ebay for Drugs' (2012) 107 *Addiction* 683 <http://onlinelibrary.wiley.com/doi/10.1111/j.1360-0443.2011.03709.x/epdf> accessed 27 July 2017.

BBC News, 'Charlie Hebdo attack: Three days of terror' *BBC News* (14 January 2015) <http://www.bbc.co.uk/news/world-europe-30708237> accessed 27 July 2017.

BBC News, 'Facebook U-turn over 'Napalm girl' photograph' *BBC News* (09 September 2016) <http://www.bbc.co.uk/news/technology-37318040> accessed 27 July 2017.

BBC News, 'Global ransomware attack causes turmoil' *BBC News (27 June 2017c)* <http://www.bbc.co.uk/news/technology-40416611> accessed 27 July 2017.

BBC News, 'Police close in on Love Bug culprit' *BBC News* (06 May 2000) <http://news.bbc.co.uk/1/hi/sci/tech/738537.stm> accessed 27 July 2017.

BBC News, 'UK and France to work together to tackle online extremism' *BBC News* (13 June 2017b) <http://www.bbc.co.uk/news/uk-politics-40258799> accessed 27 July 2017.

BBC News, 'US official: Russia 'hacked' 21 US states in election' *BBC News* (21 June 2017a) <http://www.bbc.co.uk/news/world-us-canada-40357357> accessed 27 July 2017.

Berlingske Tidende, 'Dansk gennembrud: Narkohandlere kan ikke længere gemme sig bag bitcoins' *Berlingske Tidende* (21 February 2017) <https://www.b.dk/nationalt/dansk-gennembrud-narkohandlere-kan-ikke-laengere-gemme-sig-bag-bitcoins> accessed 27 July 2017.

Bjørnholt, K, 'Dansk politi har knækket bitcoin-koden' *Dansk Politi Bladet*. (20 April 2017) <http://www.dansk-politi.dk/artikler/2017/maj/dansk-politi-har-knaekket-bitcoin-koden> accessed 27 July 2017.

Brown, C S D, 'Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice' (2015) 9(1) *International Journal on Cybercrime* 55 <http://www.cybercrimejournal.com/Brown2015vol9issue1.pdf> accessed 27 July 2017.

Cohen-Almagor, R, 'Online child sex offenders: Challenges and counter-measures' (2013) 52(2) *The Howard Journal on Crime and Justice* 190 <http://onlinelibrary.wiley.com/doi/10.1111/hojo.12006/abstract> accessed 27 July 2017.

Commission of the European Communities, 'Towards a general policy on the fight against cyber crime' *COM(2007) 267 final* (22 May 2007) <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52007DC0267&from=EN> accessed 27 July 2017.

Corera, G, 'Facebook reveals measures to remove terrorist content' *BBC News* (15 June 2017) <http://www.bbc.com/news/technology-40290258> accessed 27 July 2017.

Council of Europe, 'Chart of signatures and ratifications of Treaty 185' (*Treaty Office*, 28 July 2017) <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=V5sshFBZ> accessed 27 July 2017.

Council of Europe, 'The European convention on cybercrime' *European Treaty Series - No. 185* (23 November 2001) <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561> accessed 27 July 2017.

Crawford, A, 'Plural policing in the UK: Policing beyond the police' in T Newburn (eds) *Handbook in policing* (Willan 2008).

Crawford, K and T Gillespie, 'What is a flag for? Social media reporting tools and the vocabulary of complaint' (2016) 18(3) *New Media and Society* 410 <http://journals.sagepub.com/doi/full/10.1177/1461444814543163> accessed 27 July 2017.

Cross, M, *Scene of the cybercrime* (2nd ed, Syngress 2008)

Dalek, J, B Haselton, H Noman, A Senft, M Crete-Nishihata, P Gill and R J Deibert, 'A method for identifying and confirming the use of URL filtering products for censorship' (2013) *The 2013 conference on Internet measurement* <http://www3.cs.stonybrook.edu/~phillipa/papers/imc112s-dalek.pdf> accessed 27 July 2017.

Deibert, R J and R Rohozinski, 'Risking security: Policies and paradoxes of cyberspace security' (2010) 4(1) *International Political Sociology* 15 <http://onlinelibrary.wiley.com/doi/10.1111/j.1749-5687.2009.00088.x/full> accessed 27 July 2017.

Eerste Kamer der Staten-Generaal, 'Computercriminaliteit III (34.372); gewijzigd voorstel van wet (EK, A)' (20 December 2016) https://www.eerstekamer.nl/behandeling/20161220/gewijzigd_voorstel_van_wet_9/info accessed 18 July 2017.

Emm, D, 'Cybercrime and the law: a review of UK computer crime legislation' (*Securelist*, 29 May 2009) <https://securelist.com/analysis/publications/36253/cybercrime-and-the-law-a-review-of-uk-computer-crime-legislation/> accessed 27 July 2017.

Eurojust 'Eurojust Annual Report 2011 *Eurojust* (2012) <http://eurojust.europa.eu/doclibrary/corporate/eurojust%20Annual%20Reports/Annual%20Report%202011/Annual-Report-2011-EN.pdf> accessed 27 July 2017.

European Commission, 'Achievements and the next steps: Towards global cyber-security' *COM(2011) 163 final* (31 March 2011a) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF> accessed 27 July 2017.

European Commission, 'Child sexual abuse' (*Migration and Home Affairs*, 27 July 2017) <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/child-sexual-abuse/index_en.htm> accessed 27 July 2017.

European Commission, 'European Parliament supports stronger legislation against child sexual abuse' (27 October 2011b) <http://europa.eu/rapid/press-release_IP-11-1255_en.htm> accessed 27 July 2017.

European Commission, 'FAQ: The Radicalisation Awareness Network' (28 January 2013) <http://europa.eu/rapid/press-release_MEMO-13-40_en.htm> accessed 27 July 2017.

European Commission, 'Protecting Europe from large scale cyber-attacks and disruptions: Enhancing preparedness, security and resilience' *COM(2009) 149 final* (30 May 2009) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF> accessed 27.07.2017.

European Commission, 'Supporting the Prevention of Radicalisation Leading to Violent Extremism' *COM(2016) 379 final* (14 June 2016) <http://ec.europa.eu/dgs/education_culture/repository/education/library/publications/2016/communication-preventing-radicalisation_en.pdf> accessed 27 July 2017.

European Commission, 'Tackling crime in our digital age: Establishing a European Cybercrime Centre' *COM(2012) 140 final* (28 March 2012) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:PDF> accessed 27 July 2017.

European Council and the High Representative of the European Union for Foreign affairs and Security Policy, 'Cybersecurity strategy of the European Union: An open, safe and secure cyberspace' *JOIN(2013) 1 final* (7 February 2013) <https://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf> accessed 28 July2017

European Union, 'Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA' *L335/1* (13 December 2011) <http://eur-lex.europa.eu/legal-ccontent/EN/TXT/PDF/?uri=CELEX:32011L0093&from=EN> accessed 28 July 2017.

European Union, 'Directive (EU) 2015/849 on preventing the use of the financial system for money laundering or terrorist financing (4th Anti-Money Laundering Directive)' *L 141/73* (15 June 2015) <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2015_141_R_0003&from=ES> accessed 28 July 2017.

European Union, 'Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community' *2007/C 306/01* (17 December 2017) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:306:FULL:EN:PDF> accessed 28 July 2017.

Europol, 'Europol Internet Referral Unit One Year On' (22 July 2016c) <https://www.europol.europa.eu/newsroom/news/europol-internet-referral-unit-one-year> accessed 29 July 2017.

Europol, 'Massive blow to criminal Dark Web activities after globally coordinated operation' (30 July 2017) <https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation> accessed 29 July 2017.

Europol, 'The internet organised crime threat assessment (IOCTA) 2015' (2015) <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015> accessed 28 July 2017.

Europol, 'The Internet organised crime threat assessment (IOCTA) 2016' (2016a) <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016> accessed 28 July 2017

Europol, 'The relentless growth of cybercrime (27 September 2016b) <https://www.europol.europa.eu/newsroom/news/relentless-growth-of-cybercrime> accessed 28 July 2017.

Fidler, D. P, 'Countering Islamic State exploitation of the internet' (*Council on Foreign Relations*, 18 June 2015) <https://www.cfr.org/report/countering-islamic-state-exploitation-internet> accessed 28 July 2017.

Fijnaut, C and G T Marx, 'The normalization of undercover policing in the west: Historical and contemporary perspectives' in C Fijnaut, C and G T Marx (eds) *Undercover: Police surveillance in comparative Perspective* (Kluwer 1995).

France-Presse, A, 'Facebook bans 'offensive' Swedish breast cancer awareness video' *The Guardian* (20 October 2016) <https://www.theguardian.com/technology/2016/oct/20/facebook-bans-swedish-breast-cancer-awareness-video-for-being-offensive> accessed 28 July 2017

Giles, K, 'Russia's public stance on cyberspace issues' in Czosseck, C, R Ottis and K Ziolkowski (eds) *4th International Conference on Cyber Conflicts* (NATO CCD COE, 2012) <https://ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf> accessed 28 July 2017.

Gillespie, A A, '(2008) Cyber-strings: Policing sex offenders on the internet' (2008) 81(3) *The Police Journal: Theory, Practice and Principles* 196 <http://journals.sagepub.com/doi/abs/10.1350/pojo.2008.81.3.415> accessed 28 July 2017.

Grabosky, P, 'Requirements of prosecution services to deal with cyber-crime' (2007) 47(4-5), *Crime, Law & Social Change* 201 <https://link.springer.com/content/pdf/10.1007%2Fs10611-007-9069-1.pdf> accessed 28 July 2017.

Greenberg, A, 'The Silk Road's dark-web dream is dead' (*Wired*, 14 January 2016) <https://www.wired.com/2016/01/the-silk-roads-dark-web-dream-is-dead/> accessed 28 July 2017.

Hamilton, A, 'INTERVIEW: Telegram and terror: How data encryption shapes our lives' (*Digit*, 13 June 2017) <hhttp://www.digit.fyi/whatsapp-telegram-terror/ > accessed 28 July 2017.

Hansen, L, and H Nissenbaum, 'Digital disaster, cyber security and the Copenhagen school' (2009) 53 *International Studies Quarterly* 1555 <http://onlinelibrary.wiley.com/doi/10.1111/j.1468-2478.2009.00572.x/abstract> accessed 28 July 2017.

Hardin, L, 'What we know about Russia's interference in the US election' *The Guardian* (16 December 2016) <https://www.theguardian.com/us-news/2016/dec/16/qa-russian-hackers-vladimir-putin-donald-trump-us-presidential-election> accessed 28 July 2017.

Harfield, C and K Harfield, *Covert investigations. Blackstone's practical policing* (Oxford University Press 2005).

Home Office, *Cyber Crime Strategy* (*Strategy, Cm 7842*, March 2010) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf> accessed 28 July 2017.

Home Affairs Committee, 'What is e-crime?' (www.Parliament.uk, 30 July 2013) <http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/7004.htm

ICE Newsroom, 'Law enforcement agencies around the world collaborate on international Darknet marketplace enforcement operation' *(U.S. Immigration and Customs Enforcement*, 31 October 2016) <https://www.ice.gov/news/releases/law-enforcement-agencies-around-world-collaborate-international-darknet-marketplace> accessed 28 July 2017.

ITU, 'Global Cybersecurity Agenda (GCA)' (*ITU*, 28 July 2017) <http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx> accessed 28 July 2017.

Jackson, G S, 'Types of cybercrime and their penalties' (*It Still Works*, 28 July 2017) <http://techin.oureverydaylife.com/types-cyber-crimes-penalties-1808.html> accessed 28 July 2017.

Jardine, E E, 'The dark web dilemma: Tor, anonymity and online policing' (2015) 21 *Global Commission on Internet Governance Paper Series* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2667711> accessed 28 July 2017.

Jenkins, P, *Beyond Tolerance: Child Pornography on the Internet*' (New York University Press 2001)

Joh, E E 'Breaking the law to enforce it: Undercover police participation in crime. (2009) 62 *Stanford Law Review* 155 <http://heinonline.org/HOL/Page?handle=hein.journals/stflr62&div=7&g_sent=1&collection=journals> accessed 28 July 2017.

Jones, B R, 'Comment: Virtual neighbourhood watch: Open source software and community policing against cybercrime' (2007) 97(2) *The Journal of Criminal Law and Criminology* 601 <http://www.jstor.org/stable/40042835?seq=1#page_scan_tab_contents> accessed 28 July 2017.

Kaminsky, H, 'Facebook has re-approved a breast cancer awareness ad after initially blocking it for its content' (*Digital Trends*, 23 October 2016) <http://www.digitaltrends.com/social-media/facebook-reapprove-breast-cancer-awareness-ad-blocking-censor/> accessed 28 July 2017.

Kleinman, Z 'Fury over Facebook 'Napalm girl' censorship' *BBC News* (09 September 2016) <http://www.bbc.co.uk/news/technology-37318031> accessed 28 July 2017.

Klimburg, A, 'Mobilising Cyber Power' (2011) 53(1) *Survival* 41 <http://www.tandfonline.com/doi/abs/10.1080/00396338.2011.555595> accessed 28 July 2017.

Kilovaty, I and I Mann, 'Towards a cyber-security treaty' (*Just Security*, 3 August 2016) <https://www.justsecurity.org/32268/cyber-security-treaty/> accessed 28 July 2017.

Kremer, J, 'Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace' (2014) 23(3) *Information & Communications Technology Law* 220 <http://www.tandfonline.com/doi/abs/10.1080/13600834.2014.970432> accessed 27 July 2017.

Kruisbergen, E W, D. de Jong and E R Kleemans, 'Undercover policing: Assumptions and empirical evidence' (2011) 51(2) *The British Journal of Criminology* 394 <https://academic.oup.com/bjc/article-abstract/51/2/394/601777/Undercover-PolicingAssumptions-and-Empirical> accessed 28 July 2017.

Lee, D, 'WannaCry ransomware cyber-attack 'may have N Korea link'' *BBC News* (16 May 2017) <http://www.bbc.co.uk/news/technology-39931635> accessed 28 July 2017.

Lusthaus, J, 'Trust in the world of cybercrime' (2012) 13(2) *Global Crime* 71 <http://www.tandfonline.com/doi/abs/10.1080/17440572.2012.674183> accessed 28 July 2017.

Lyon, D. *Surveillance society: Monitoring eveyday life* (2001 University Press).

Lyon, D, *Surveillance studies. An overview* (2007 Polity Press).

MacAskill, E, J Borger, N Hopkins, N Davis and J Ball, 'Mastering the internet: how GCHQ set out to spy on the world wide web' *The Guardian* (21 June 2013) <https://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet> accessed 28 July 2017.

Markussen, J, '22-årig fik 2,3 kilo amfetamin leveret med posten' *Holstebro Struer Dagbladet* (25 April 2016) <http://dagbladet-holstebro-struer.dk/holstebro/22-aarig-fik-23-kilo-amfetamin-leveret-med-posten/artikel/83961> accessed 28 July 2017.

Masters, G, 'Global cybercrime treaty rejected at U.N.' (*SC Media*, 23 April 2010) <https://www.scmagazine.com/global-cybercrime-treaty-rejected-at-un/article/557657/> accessed 28 July 2017.

Martellozzo, E, 'Policing online child sexual abuse' (2015) 3(1) *European Journal of policing Studies* 32 <http://eprints.mdx.ac.uk/18271/>accessed 28 July 2017.

Martin, J, *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs.* (Palgrave Macmillan 2014).

Martin, J, 'Lost on the Silk Road: online drug distribution and the 'cryptomarket'' (2014) 14(3) *Criminology & Criminal Justice* 351 http://journals.sagepub.com/doi/abs/10.1177/1748895813505234?journalCode=crjb accessed 22 September 2017.

Martin, J, 'Illuminating the Dark Net: The Ethics and Methods of Cryptomarket Research' in Adorjan, M and R Ricciardelli (eds) *Engaging with Ethics and Method in Criminological Research* (2016), Routledge

Martin, J, 'Informal security nodes and force capital' (2012) 23(2) *Policing & Society* 145 http://www.tandfonline.com/doi/abs/10.1080/10439463.2012.671821 accessed 22 September 2017.

Martin, J and N Christin, 'Ethics in Dark Net Research' (2016) 35 *International Journal of Drug Policy* 84 http://www.ijdp.org/article/S0955-3959(16)30160-8/fulltext> accessed 22 September 2017.

Mayer, M, N de Scalzi, L Martino and I Chiarugi, 'International politics in the digital age: Power diffusion or power concentration?' (SISP Conference 2013) <http://www.academia.edu/14336129/International_Politics_in_the_Digital_Age> accessed 28 July 2017.

McCulloch, J and J Martin, 'Policing the Globe: International Trends and Issues in Policing', in Arrigo, B and H Bersot (eds) International Handbook of Crime and Justice (Routledge 2013).

McGuire, M and S Dowling, 'Cyber crime: A review of the evidence. Chapter 1: Cyber-dependent crimes. (*Home Office,* October 2013b) <http://www.justiceacademy.org/iShare/Library-UK/horr75-chap1.pdf> accessed 28 July 2017.

McGuire, M and S Dowling 'Cyber crime: A review of the evidence. Chapter 2: Cyber-enabled crimes' (*Home Office,* October 2013a) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf> accessed 28 July 2017.

McMillian, R, 'Three years undercover with the identity thieves' (*PCWorld,* 20 January 2009) <http://www.pcworld.com/article/158005/article.html> accessed 28 July 2017.

Mills, E, 'Q&A: FBI agent looks back on time posing as a cybercriminal' (*CNet,* 30 June 2009) <https://www.cnet.com/uk/news/q-a-fbi-agent-looks-back-on-time-posing-as-a-cybercriminal/> accessed 28 July 2017.

Morrissey, C, 'The Cybercrime Bill is here' (*Ireland IP & Technology Law Blog,* 20 January 2016) <http://www.irelandip.com/2016/01/articles/cyber-risk-data-privacy/the-cybercrime-bill-is-here/> accessed 29 July 2017

Mou, Yi, K Wu and D Atkin, 'Understanding the use of circumvention tools to bypass online censorship' (2016) 18(5) *New Media and Society* 837 <http://journals.sagepub.com/doi/abs/10.1177/1461444814548994> accessed 28 July 2017.

Munk, T, 'Is preventing online extremism only the responsibility of big internet companies?' (*MDX Minds*, 06 June 2017) <https://mdxminds.com/2017/06/06/preventing-online-extremism-only-responsibility-big-internet-companies/> accessed 28 July 2017.

Murgia, M, and D, Robinson, 'Social media groups join forces to counter online terror content' *Financial Times* (05 December 2016) <https://www.ft.com/content/ff15c750-bafd-11e6-8b45-b8b81dd5d080> accessed 28 July 2017.

Nakashima, E, 'Apple vows to resist FBI demand to crack iPhone linked to San Bernardino attacks' *Washington Post* (17 February 2016) <https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html?utm_term=.1ed909cf855b> accessed 28 July 2017.

National Statistic 'Criminal justice system statistics quarterly: December 2016. Criminal justice statistics outcomes by offence tool' (*GOV.UK*, 18 May.2017) <https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-december-2016> accessed 28 July 2017.

NATO Cooperative Cyber Defence Centre of Excellence, 'Tallinn Manual 2.0.' (*CCDCE*, 28 July 2017) <https://ccdcoe.org/tallinn-manual.html> accessed 28 July 2017.

Nhan, J and L Huey, 'Policing through nodes, clusters and bandwidth: The role of network relations in the prevention of and response to cyber-crimes' in Leman-Langlois, S (eds) *Technocrime: Technology, crime and social control* (Willan 2008).

Oxford Dictionaries, 'Living Oxford dictionaries' (*Oxford*, 28 July 2017) <https://en.oxforddictionaries.com/> accessed 28 July 2017.

Pawlak, P, 'A Wild Wild Web? Law, Norms, Crime and Politics in Cyberspace' (*EUISS*, 12 July 2017) <https://www.iss.europa.eu/content/wild-wild-web-law-norms-crime-and-politics-cyberspace> accessed 28 July 2017.

Redman, J, 'Danish Police surveil the blockchain to make arrests' (*Bitcoin.com*. 22 February 2017) <https://news.bitcoin.com/police-surveil-the-blockchain/> accessed 28 July 2017.

Rivera, P, 'United Nations' definition of cybercrime' (*Innovative Dynamics Network*, 07 December 2016) <http://idn-wi.com/united-nations-definition-cybercrime/> accessed 28 July 2017.

Ross, J E, 'Undercover policing and the shifting terms of scholarly debate: The United States and Europe in counterpoint' (2008) 4 *Annual Reviews* 239 <http://annualreviews.org/doi/abs/10.1146/annurev.lawsocsci.4.110707.172416> accessed 28 July 2017.

Rowe, M, and R King, 'An investigation into the performance of UK internet providers' (*Lancs.ac.uk*, 02 November 2015) <http://eprints.lancs.ac.uk/76435/> accessed 28 July 2017.

Sky News, 'Police unit removes 250,000 terror items from internet' *Sky News* (23 December 2016) http://news.sky.com/story/police-unit-removes-250000-terror-items-from-internet-10706526> accessed 09 September 2017.

Sky News, ''Powerful' cyberattack on Ukraine goes global' *Sky News* (27 June 2017) <http://news.sky.com/story/ukraine-cyberattack-cripples-government-website-and-banks-10928915> accessed 28 July 2017.

Smith, T, 'FBI locks up 24 people in undercover card hacking operation' (*CBR*, 27 June 2012) <http://www.cbronline.com/news/fbi-locks-up-24-people-in-massive-card-hacking-operation-270612> accessed 28 July 2017.

Statens Offenliga Utredningar 'Europarådets konvention om it-relaterad brottslighet' *Betänkande av Utredningen om it-brottskonventione* (2013) <http://www.regeringen.se/contentassets/b7ef66bff0b94040b781df446546c745/europaradets-konvention-om-it-relaterad-brottslighet-sou-201339> accessed 29 July 2017.

Stokes, R, 'Virtual money laundering: the case of Bitcoin and the Linden dollar' (2012) 21(3) *Information & Communication Technology Law* 11. <http://www.tandfonline.com/doi/abs/10.1080/13600834.2012.744225> accessed 28 July 2017.

Strate, L, 'The varieties of cyberspace: Problems in definition and delimitation' (2009) 63(3) *Western Journal of Communication* 382 <http://www.tandfonline.com/doi/abs/10.1080/10570319909374648> accessed 28 July 2017.

Sullyman, A, 'Whatsapp Encryption: What is it, how does it work and why is the Governments so worried about it?' *The Independent* (27.03.2017) <http://www.independent.co.uk/life-style/gadgets-and-tech/features/whatsapp-encryption-what-is-it-how-does-it-work-why-ban-it-backdoor-access-secret-messages-a7652396.html> accessed 28 July 2017.

The Council of the European Union (2001) Council Framework Decision 2001/413/JHA on Combating fraud and counterfeiting of non-cash means of payment' *L 149/1* (02 June 2001) <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32001F0413> accessed 28 July 2017.

The European 'EU gets strict with cybercrime penalties' (*The European*, 10 July 2013) <http://www.the-european.eu/story-3437/eu-gets-strict-with-cyber-crime-penalties.html> accessed 28 July 2017.

Theoharis, M, 'Computer and Internet Crime Laws' (*CriminalDefenceLawyer*, 28 July 2017) <http://www.criminaldefenselawyer.com/crime-penalties/federal/computer-crimes.htm#> accessed 28 July 2017.

Tikk, E, K Kaska and L Vihul, 'International cyber incidents: Legal considerations' (*CCD COE*, 2010) <www.ccdcoe.org/publications/books/legalconsiderations.pdf> accessed 28 July 2017.

Trautman, L J, 'Virtual currencies; Bitcoin and what now after Liberty Reserve, Silk Road, and Mt. Gox?' (2014) 20(4) *Richmond Journal of Law and Technology* 1, 108 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2393537> accessed 28 July 2017.

Travis, A, 'Face-off between MPs and social media giants over online hate speech' *The Guardian* (14 March 2017) <https://www.theguardian.com/media/2017/mar/14/face-off-mps-and-social-media-giants-online-hate-speech-facebook-twitter> accessed 27 July 2017.

United Nations, 'International code of conduct for Information Security' *A/69/723* (13 January 2015) <https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf> accessed 28 July 2017.

United Nations, 'The Tenth United Nations Congress on the prevention of crime and treatment of offenders' (*United Nations*, 10 April 2000(a)) <http://www.un.org/press/en/2000/20000410.soccp216.doc.html> accessed 28 July 2017.

United Nations, 'The United Nations Convention against transnational organized crime' *UNODC* (2000(b)) <https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf> accessed 28 July 2017.

United Nations, 'Twelfth United Nations Congress on crime prevention and criminal justice' (*United Nations*, 12-19 April 2010) <http://www.un.org/en/conf/crimecongress2010/> accessed 28 July 2017.

United Nations Information Service, 'Cybercrime' (*United Nations Information Service*, 12-19 April 2015) <http://www.unis.unvienna.org/unis/en/events/2015/crime_congress_cybercrime.html> accessed 28 July 2017.

UNCTAD, 'Cybercrime legislation worldwide' (*UNCTAD*, 01 June 2017) <http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx> accessed 09 September 2017.

UNODC, 'Comprehensive study on cybercrime (draft)' (*UNOCD*, February 2013) <https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> accessed 28 July 2017.

Van Buuren, J, *'Doelwit Den Haag?: Complotconstructies en systeemhaat in Nederland 2000-2014'* PhD thesis, Leiden, 2016 (Supervisors: E Bakker; B A de Graaf, Co-Supervisors: P Nieuwenburg; P Abels) <https://openaccess.leidenuniv.nl/handle/1887/43818> accessed 29 July 2017.

Van Hout, M C and T Bingham, 'Silk Road', the virtual drug marketplace: A single case study of user experiences' (2013) 24(5) *International Journal of Drug Policy* 385 <http://www.sciencedirect.com/science/article/pii/S0955395913000066> accessed 29 July 2017.

Walden, I, *Computer crime. Computer law* (Oxford University Press 2007) <http://kavehh.com/my%20Document/KCL/Internet%20Law/Internet%20Material/Computer%2520Crime%2520%25286th%2520ed.%2529.pdf> accessed 29 July 2017.

Wall, D S, 'Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police practices and research,* (2007) 8(2) *Police Practice and Research* <http://www.tandfonline.com/doi/abs/10.1080/15614260701377729> accessed 29 July 2017.

Wall, D S, 'The Internet as a conduit for criminals' in Pattavina, A. (eds) *Information technology and the criminal justice system* (Sage 2005).

Woolf, N, 'DDoS attack that disrupted internet was largest of its kind in history, experts say' *The Guardian* (26 October 2016) https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet> accessed 24 September 2017.

Wu, W and S H Koo, 'Perceived effects of sexually explicit internet content: the third-person effect in Singapore' (2001) 78(2) *Journalism & Mass Communication Quarterly* 260 <http://journals.sagepub.com/doi/abs/10.1177/107769900107800204> accessed 29 July 2017.

Yar, M, '*Cybercrime and society*' (2nd ed, Sage 2013)