Reza Montasari · Fiona Carroll ·
Ian Mitchell · Sukhvinder Hara ·
Rachel Bolton-King *Editors*

Privacy, Security And Forensics in The Internet of Things (IoT)

Springer

Privacy, Security And Forensics in The Internet of Things (IoT)

Reza Montasari • Fiona Carroll • Ian Mitchell
Sukhvinder Hara • Rachel Bolton-King
Editors

Privacy, Security And Forensics in The Internet of Things (IoT)

Springer

Editors
Reza Montasari
Hillary Rodham Clinton School of Law
Swansea University
Swansea, UK

Ian Mitchell
Computer Science
Middlesex University
London, UK

Rachel Bolton-King
Law, Policing & Forensics
Staffordshire University
Stoke on Trent, UK

Fiona Carroll
Cardiff School of Technologies, Cardiff
Metropolitan University, Cardiff, UK

Sukhvinder Hara
London, UK

ISBN 978-3-030-91217-8 ISBN 978-3-030-91218-5 (eBook)
https://doi.org/10.1007/978-3-030-91218-5

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Introduction: Critical Analysis of the Challenges Police and Law Enforcement Face in Policing Cyberspace

The digital world has transformed society enabling new ways of communication and exchanging information. This innovation simultaneously poses a plethora of new challenges as cyberspace is vulnerable to extensive misuse. Technological shifts in the criminal landscape poses a myriad of challenges for policing and law enforcement that undermine the efficacy of crime control online. In view of this, this chapter provides a comprehensive account of the challenges faced by police and law enforcement in keeping cyberspace secure. This chapter will proceed in two stages. Firstly, four key challenges of policing in the digital realm will be identified: legislation, jurisdiction, anonymity and reporting. Following analysis of the challenges, this chapter will recommend possible avenues for future research to assist both in addressing the threat of cyberspace as well as the digital investigation of cybercrime. The chapter concludes that international cooperation and multi-agency partnership between state actors, private companies, academics, architects and users will provide the most advantageous response in the fight against cybercrime.

Introduction

In the twenty-first century, the internet and associate technologies such as the Internet of Things (IoT) solutions, Cloud-Based Services (CBSs), Cyber-Physical Systems (CPSs) and mobile devices have become the defining feature of modern life (Montasari & Hill, 2019; Montasari, 2017). We live in a hyper connected world that has expanded accessibility, capability and reach. The digital age has constructed a ubiquitous environment for individuals to interact, connect and share information. Technology is fundamentally advantageous for society to fuel our ability to interact across the world. However, the internet remains a double-edged sword. As the use of technology continues to grow exponentially, so do the opportunities for criminals to exploit vulnerabilities in cyberspace.

In 2016, the Crime Survey for England and Wales introduced new victimisation questions concerning fraud and computer misuse. This data revealed the unprecedented scale and nature of the problem society faces as cyber-related crime accounted for almost half of all crimes committed (Caneppele & Aebi, 2019). The threat has evolved significantly, becoming increasingly sophisticated and multifaceted, targeting not only individuals but critical infrastructure, industries and governments. Cybercrime has become one of the fastest growing types of crime in the United Kingdom (UK) and is now recognised on the National Risk Register as a Tier 1 threat to national security (Stoddart, 2016). For the purpose of this chapter, the broad umbrella term of cybercrime will be employed to include both cyber-dependant and cyber-enabled crime. The advent of technology provides cybercriminals an opportunity to change their modus operandi, this poses significant implications for policing. Traditional models of policing and law enforcement have derived from assumptions that crime occurs in physical proximity, in limited scale with traceable evidence (Harkin et al., 2018). The digital era has disrupted conventional law and understanding of enforcement as cybercrime does not operate under the same spatial and temporal constraints. Therefore, traditional policing strategies such as localised foot patrols and hierarchically organised models are not applicable to cyberspace. Whilst adversaries proved adaptive in leveraging new technological innovation to overwhelm the capabilities of state security, law enforcement agencies were ill-prepared for this transformative shift from offline to online operations. Thus, it is apparent that the domain of cybercrime is rapidly "increasing in frequency, scale, sophistication and severity" (Harkin et al., 2018).

Drawing upon an increasing body of literature, this chapter will critically evaluate the challenges police and law enforcement endure in policing cyberspace. This chapter will explore four key policing obstacles: an archaic and time-consuming legislative process, a lack of international consensus, the anonymous nature of cyberspace, and the under-reporting of cybercrime. Following critical analysis, this chapter will provide recommendations as to how to strengthen police and law enforcement responses against cybercrime. Fundamentally, the internet is a digital environment that is changing the way criminals and law enforcement operate. Given the complexities of cybercrime, there is no one solution. Therefore, this chapter will propose that no singular agency or government can police cyberspace by itself. Instead, government, industry, engineers, users, policymakers and academics must combine efforts to tackle cybersecurity challenges.

Challenges

Addressing the challenge that cyberspace represents is fraught with difficulties as new technologies and events present a myriad of legal, policy and technical work that requires months or even years to establish. Yet the pace of innovation appears relentless and cascading, threatening to overwhelm and in many cases overtake policymakers and regulatory bodies at a national and international level. Criminals by sheer innovation are redefining cyberspace which is in turn shaping and driving current approaches to cybersecurity. The following sections will outline the key challenges police and law enforcement face in establishing a sustainable and comprehensive response to criminal activity in cyberspace.

Legislation

A key challenge in policing cybercrime in contemporary society is the apparent disconnect between legislation and technology. The penal system is an inherently retroactive and lengthy process which generates numerous obstacles in regulating the cyber domain. Technological forces are evolving at a rapid rate that is far outpacing the development of policy and legislation. Consequently, cyberspace is typically governed by a patchwork of weak, under-developed and competing legislation as illustrated by the Computer Misuse Act 1990, which is the primary piece of legislation for prosecuting cyber-related offenders (Criminal Law Reform Now Network, 2020; Montasari et al., 2016). This Act was established three decades ago with no foresight into the rapid pace of technological advancements. Therefore, the concepts embodied in the Computer Misuse Act 1990 were intended to be technologically neutral, in order to pertain to both current and future technologies. Despite attempts to future-proof, the emergence of unprecedented technology has created a number of loopholes and ambiguity in the application of the law. Consequently, Ashworth (2013) argues that legislation merely sustains a myth of control and legitimacy of the sovereign state, as legislation is often impromptu, expressive and inconsistent in an attempt to cater to public pressures with little consideration of an evidence-base and expert knowledge.

Private and public sectors are typically eager to spend money, time and resources into the enforcement of computer misuse laws in terms of the apprehension and prosecution of offenders. However, the legal foundation is sorely lacking in substance. Legislation has demonstrated an inability to target the right people and establish defences which enable private enforcement to work effectively alongside public enforcement in order to best address cyber threats. Thus, the cybersecurity industry remains constrained and inadvertently criminalised by the Computer Misuse Act (Criminal Law Reform Now Network, 2020). For this reason, critics, namely the Criminal Law Reform Now Network (2020), have claimed that the Computer Misuse Act 1990 is outdated and does not reflect the current problems police and law enforcement face. Subsequently, they deduce that cyber legislation needs to undertake radical reform. Evidently, establishing legislation to coincide with ever-evolving technology proves challenging. Despite uncertainties, it is critical to not wholly dismiss the role of law and policy on the basis that technology will always evolve more rapidly (Sallavaci, 2017). Ultimately, legislation remains a crucial component in the fight against cybercrime. An Act of Parliament provides police and law enforcement with a fundamental blueprint that guides behaviour and establishes standards and frameworks. Nonetheless, in an ever-changing highly digitised realm, substantial amendments to the rule of law are necessary to evolve in line with society.

Jurisdiction

The infrastructure of the internet is a physical construct that exists in time and space within physical borders of sovereign countries. However, the data flowing throughout this infrastructure spans across multiple national jurisdictions, which remains an inherent challenge of cyberspace. Whilst criminal activity in cyberspace penetrates effortlessly across geographical borders, law enforcement does not. As a result, nationally bounded law enforcement is required to operate within a realm that is geographically unbounded, thereby evoking a large number of complications (Kennedy & Warren, 2020). The most prominent international instrument concerning cybercrime is 'The Council of Europe Convention on Cybercrime', also known as the Budapest convention. The convention seeks to harmonise national laws on cybercrime, improve investigative techniques and increase cooperation between nations (Kennedy & Warren, 2020). However, achieving consensus proves a contentious issue as each nation possesses their own independent norms, beliefs and practices, and thus promote differing visions for cyberspace. For instance, various governments advocate for cyber sovereignty contending that national borders apply to cyberspace and each country should have the right to govern how people and businesses use the internet within their territory. Whereas other nations support internet freedom, the concept that every citizen should be free to express themselves and spread new ideas online with anyone, anywhere (Kennedy & Warren, 2020).

This fragmentation between nations renders it almost impossible to establish an international consensus concerning internet governance and regulation. However, this is not to say the Budapest Convention as a whole is obsolete. Despite its limitations, the treaty provides a fundamental framework in facilitating international cooperation and the harmonisation of legislation. Evidently, what makes cybercrime difficult to monitor and enforce is its transgressive form, one that does not respect international borders. The internet and computers have enabled individuals to steal electronic data remotely without physical proximity. Thus, criminal actors operating across borders adds a level of complexity to policing as victims, perpetrators and evidence can all reside within differing jurisdictions (Montasari, 2017). Consequently, police forces must request data preservation and access to electronic evidence residing in other jurisdictions. This reliance upon mutual assistance makes it incredibly complex, time consuming and costly to bring offenders to justice outside of the United Kingdom. As a result, recent studies, including Świątkowska's, call (2020) for more effective and synchronised international efforts to mitigate digital vulnerabilities. She determines that a lack of international consensus can offer cybercriminals a spatial safe haven whereby they operate outside the scope of law enforcement and international legislation. These safe havens provide a domain for adversaries to better evade government restrictions, detection and prosecution. Amid the global disagreement, technological innovation continues to accelerate at a tremendous speed. Therefore, international cooperation is vital to eradicate the safe haven for cyber criminals, promote information sharing and eventually enhance global investigations.

Anonymity

A further challenge the police face in the apprehension of cyber criminals is anonymity. There are many publicly available and accessible tools that allow users' internet activity to remain anonymous. The most commonly used anonymous system is the Tor browser, this is a powerful tool that offers online end-to-end encryption through masking a user's IP address (Davies, 2020). This offers the ability to protect privacy and effectively prevent governments from accessing data and tracking online activities. This freedom from censorship is therefore deemed by civil rights activists as a powerful tool to be utilised in heavily monitored and authoritarian states. Whilst encrypted communication protects the security and privacy of its users, it also presents significant disadvantages as users of illegal sites leverage this cloak of anonymity to evade police and law enforcement. There remain a series of websites hidden under a layer of protection that can only be accessed utilising specialised anonymous browsers. This realm has been deemed the dark net. Criminals can mask their identities and hide their locations by re-directing communication and activity through a distributed network of relays around the world. Whilst the dark web is not exclusively used by criminals, these hidden services can create a centralised repository of illicit marketplaces facilitating the selling and distributing of illegal goods such as firearms, drugs, counterfeit currency and child pornography (Davies, 2020). Consequently, the nature of cyberspace is problematic for policing as the risk of apprehension can be easily mitigated through utilising Tor browsers, cryptocurrency and virtual private networks.

The dark net is constantly evolving and adapting as these illicit markets operate on the fringes of the internet and are quick to adopt readily available technology in order to provide greater anonymity. This is exemplified in Ladegaard's research (2019) into the most prolific dark net investigation, Operation Onymous. Ladegaard (2019) reported that criminals will typically migrate to alternate cryptomarkets once their current darknet market is detected and removed by law enforcement. From these findings there is evidence to suggest that the cybercrime ecosystem is resilient to law enforcement takedowns as operations merely lead to a displacement of criminal activity. Arguably police crackdowns can trigger criminal innovation as infiltration forces darknet markets to enhance their security and infrastructure. Overall, anonymity in cyberspace remains a significant challenge for police investigations as criminals continue to circumvent government surveillance and detection.

Reporting

There is a vast amount of crime that goes unnoticed, unreported and undetected. This generates what scholars term, the dark figure of crime (Kemp et al., 2020). Action Fraud is the centralised reporting agency of fraud and cyber offences. However, according to the Office for National Statistics (2020) only 338,255 cases of fraud and cyber-crime were recorded by Action Fraud within a 12-month period. Whereas the Crime Survey for England and Wales recorded approximately 4.5 million incidents (Office for National Statistics, 2020). This reveals that only 7% of victims reported incidents of cybercrime and fraud to the police, as such there remains a large discrepancy between what people experience and what they report to the police. Therefore, police recorded crime does not represent the true nature and scale of the cyber problem the United Kingdom is facing. This variation between statistics highlights the advantages of victim surveys to shed light upon the dark figure of crime and the severe limitations associated with relying upon police-recorded data (Kemp et al., 2020).

There remains a significant problem with under-reporting within the realm of cybercrime as it depends upon a victim's willingness to report a crime. There are a multitude of reasons why individuals and businesses may not report a cybercrime to the police for instance, a lack of awareness of victimisation, fear of stigma, poor reporting mechanisms and potential reputation damage (Bailey et al., 2021). Cybercrime does not always have a readily identifiable victim, and it may be difficult to determine and recognise one's own victimisation, consequently computer-related crime is often referred to as 'hidden crime'. Moreover, even supposing an individual is aware of their own victimisation, they may feel too embarrassed or ashamed to report the incident. This notion is evidenced by several academics, including scholars Bailey et al. (2021), who determined that victim blaming discourse permeates cybercrime. Findings from in-depth qualitative interviews found that cyber victims frequently view themselves as partly to blame for their victimisation as participants often referred to themselves as 'gullible', 'stupid' and 'naïve'. Many participants suffered from severe psychological harm including anxiety and paranoia and experienced a breakdown of personal relationships following victimisation. Subsequently, internalised and externalised stigma may seek to explain the high levels of underreporting within cyber-related crime. It is important to note that (Bailey et al., 2021) dataset pertains to a small sample size of 80 victims; despite this methodological limitation, the study provides a rich insight into the lived experiences of cyber victimisation and the challenges of reporting cybercrime.

Official statistics that represent an accurate figure of crime are an important aspect of police operations as data can assist in detecting trends and patterns amongst criminal activity. Therefore, data analysis can help inform financial budgets and resource allocation to ensure police interventions are implemented successfully and effectively. Police ought to coordinate activity and focus their enforcement resources upon problem areas; however, with a limited dataset due to under-reporting, this proves challenging (Caneppele & Aebi, 2019).

Future Direction

Given the compounding challenges police face in cyberspace, a nodal network of regulation is required that combines private and public, state and nonstate, national and international institutions. A multifaceted threat requires a multi-layered, global, dynamic and decentralised regulatory system in order for the problem to be addressed. The following sections will offer recommendations to improve cyber protection, investigations and response.

Legistlation Reform

The Criminal Law Reform Now Network (2020) determines that legislation is "crying out for reform". In the Computer Misuse Act 1990, judicial lexicon remains broad and notoriously vague; subsequently, it permits a vast amount of flexibility in the application of the law. However, exercising prosecutorial discretion may result in inconsistent and unjust rulings. As evidenced in the case of R v Cuthbert, a computer security consultant was convicted for performing unauthorised penetration testing on a suspected inauthentic website. This ruling sparked many concerns in the penetration testing community due to fears that the law makes no distinction between good faith and malicious intent (Criminal Law Reform Now Network, 2020). Consequently, Guinchard (2021) echoes the Criminal Law Reform Now Network (2020) and proposes a radical reform of cyber legislation. Currently, an individual can be prosecuted under the Computer Misuse Act without the requirement for malicious intent; therefore, the act invertedly criminalises cyber security researchers. Most notably, the making, supplying or obtaining of hacking tools equates a computer misuse offense which inhibits vulnerability testing and threat research. Therefore, Guinchard's (2021) chapter recommends the introduction of a 'public interest' defence to allow detected vulnerabilities in systems and networks to be safely disclosed without fear of legal persecution. Guinchard's argument is persuasive as reform of the Computer Misuse Act 1990 to include a public interest defence can enable more freedom for security professionals to investigate vulnerabilities in critical national infrastructure.

The Covid-19 pandemic has highlighted the increasing need for a modernised legislative framework for law enforcement as society becomes ever more reliant upon digital technology. The pandemic saw a rapid acceleration and significant uptake of individuals around the world working from home. This greatly increased the potential pool of victims as a number of companies and individuals struggled to provide rapid security and infrastructure. Criminal organisations attempted to capitalise upon this unforeseen shift as new vulnerabilities surfaced from remote working (Buil-Gil et al., 2021). The pandemic demonstrates the need to establish adaptable and resilient judicial responses as the nature of the cyber threat is dynamic and evolving at an alarming rate.

Multi-Agency Response

Cybercrime is inherently networked and sophisticated thus the nature of the threat demands an integrated and collective regulatory response. Therefore, the policing of cyberspace calls for a multi-agency layered approach to establish a comprehensive and decentralised defence framework. Therefore, internet governance must operate seamlessly between public and private sectors, state and non-state actors, and national and international bodies. However, coordinating a sustainable and efficient collaborative effort when different organisations and administrations have differing agendas is a complex process (Leppänen & Kankaanranta, 2020). Typically, national security strategies have overlooked the role of private industry as essential stakeholders. However, private entities own and operate the infrastructure within cyberspace and are often the victim of cybercrime; therefore, it is imperative to incorporate the private sector into the policing of cyberspace. In the United Kingdom, the National Cyber Security Centre (NCSC) is a central hub of expertise that provides a significant foundation in improving public-private collaboration; however, much more work remains to be done (Stoddart, 2016). The NCSC was established to simplify the landscape for cybersecurity and devise a single point of contact. In doing so, the NCSC harmonises the way law enforcement and the private sector communicate with one another to better detect threat actors and conduct better investigations (Stoddart, 2016). Whilst the work the NCSC do has enhanced collaboration and information sharing, it is necessary to build upon this further by encouraging greater cooperation between organisations and law enforcement to better disrupt cyber criminals. This can be accomplished through a modernised legal and regulatory framework that encourages multi-agency collaboration.

The United Kingdom lives in an era whereby digital evidence is rampant in nearly every crime. Despite this, there remains tension between the transnational horizontal nature of the internet and the vertical structure of the United Kingdom's jurisdictional system based upon the geographical conception of nation states with distinct borders. Cybercrime is truly a global problem; it has no respect for traditional police force boundaries. This new era of connectivity underscores the need for international arrangements that encourage responsible cyber practices. A fundamental aspect that requires development is the capacity to exchange information amongst private and public entities across jurisdictions. Cybercriminals have the ability to operate in a flexible and agile way across borders; however, law enforcement remain restricted to local jurisdictions (Leppänen & Kankaanranta, 2020). As has already been highlighted, cybercrime is not a closed border issue, policymakers and academia must view this domain from an international perspective.

Evidence-Based Policing and Training

Police and law enforcement who attempt to solve issues of cyberspace in the sense of policymaking, legislation and enforcement often lack knowledge of the space they are regulating. Therefore, in a domain that is technologically diverse and dynamic, collaboration between police agencies and the academic sector is critical to accumulate a comprehensive evidence base. Evidence-based approaches bring a powerful tool of systematic analysis, evaluation, testing and empirical studies to policing. Evidence-based policing focuses upon knowledge that is derived from rigorous evaluations of new and existing tactics and strategies (Koziarski & Lee, 2020). Thus, this is a concept that comes from partnership between researchers and practitioners to understand the relationship between action and outcomes. Evidence-based policing has increasingly permeated UK police forces; despite this, responses to cybercrime remain an underdeveloped domain. Knowledge of 'what works' or does not work in policing cyberspace is scarce (Koziarski & Lee, 2020). As policing becomes more complex, mechanisms of oversight and scrutiny will become increasingly important to guarantee a significant degree of public trust and confidence. Therefore, it is essential for governing bodies in collaboration with researchers to evaluate and review cybercrime policing approaches in order to determine the most effective strategies for law enforcement to implement.

Cyber criminals have developed an integrated and sophisticated web of skills; therefore, investigations are complex and require specialist tools and skillsets. As a result, cybercrime requires augmenting the skill set within the police and judicial system at all levels to meet this changing environment. However, typically, law enforcement has not been well equipped to deal with emerging threats and the increasing demands placed upon it. The majority of literature concerning cybercrime and policing acknowledge training as a prevalent issue for staff; however, there remains a shortage of detailed insight. In order to expand the knowledge base, Schreuders et al. (2018) conducted in-depth interviews with officers from a United Kingdom police force. They subsequently found that officers did not possess the necessary skills or technological background required for everyday digital investigations. This chapter indicates that there must be an upskilling of police officers beyond cyber-specific agencies as cybercrime is a wider problem that intersects all types of crime. Thus, cyber knowledge and awareness needs to transpire across the core of police activity.

This claim is supported by the National Police Chief's Council (2016) in their Policing Vision 2025 report whereby they acknowledge that the advances in digital technology are presenting significant challenges and opportunities to policing. The chapter calls for transformative change and outlines a vision as to how the incorporation of technology in policing can address current and future threats in the digital era (National Police Chiefs Council, 2016). As society digitally evolves it becomes increasingly important for law enforcement agencies to be equipped with the appropriate skills, knowledge and investigative capabilities to leverage this technology. Police forces must enhance their ability to train and upskill existing personnel to meet this changing environment and capitalise upon an existing knowledge base within the workforce. Ultimately, this chapter recognises the requirement for evidence-based digital policing to permeate wider police training and tactical strategies moving forward.

Public Awareness

There is a growing role of human factors in shaping the likelihood of cyber security breaches as users are the gatekeepers of sensitive data and systems. Understanding how human error shapes the threat landscape is therefore vitally important in attempting to mitigate cybercrime (Monteith et al., 2016). In line with this notion, Williams (2016) determines that cyber defence rests upon the commitment of every citizen and thus recommends a radical overhaul of conventional reactive policing methods. Williams analysed Eurobarometer survey data and suggests that routine activity theory is applicable to the conditions of cyberspace as users' online conduct can influence the commission of an offence. Routine activity theory determines that a crime is likely to occur with the convergence of a suitable target, potential offender and absence of a capable guardian. Consequently, within cyberspace, individuals can mitigate their risk of victimisation by employing passive guardianship measures in the form of secure browsers and antivirus software (Williams, 2016). Ensuring the public are educated in how to protect their devices appropriately can increase cybersecurity, thereby decreasing the need for police intervention. However, a key challenge lies in ensuring that citizens understand the significance of cyber threats and the role individual users play in cyber security.

In order to encourage user compliance, Brenner (2007) proposes a new punitive crime-control strategy that relies upon self-policing and user 'responsibilisation'. She determines that individual users should be held liable for their own cybersecurity under criminal law. Therefore, if a victim fails to implement up-to-date security measures in order to protect one's own computer system, they will no longer be entitled to a response from law enforcement. Brenner (2007) extends this principle and determines that users who harm others as a result of their own lack of security measures should be found liable of a criminal offence under the principle of negligence. Whilst it is critical to encourage users to prevent their own victimisation, this punitive approach remains fundamentally flawed as it is rooted in notions of victim blaming. Denying cyber victims the right to a police investigation overlooks offenders' culpability and places the onus entirely upon victims. As aforementioned, there is now a considerable body of research which suggests that victims often encounter shame and stigma when reporting cybercrime; therefore, Brenner's framework (2007) perpetuates the notion that victims are to blame for not adequately protecting themselves. Instead, victims of cybercrime should be supported and offered resources to prevent any future victimisation (Monteith et al., 2016).

For future research and interventions, it is imperative to diversify cyber security beyond traditional law enforcement to consider the implications of user behaviour and action. A poor understanding of technology and its vulnerabilities puts users and companies at risk. Therefore, human factors present an opportunity for making systems safer, more robust and more resilient. Thus, there is reason to conclude that designing public awareness campaigns to educate communities on the dangers of cyberspace and develop cyber skills can help build resilience to crime in an increasingly digital world. Ultimately, a comprehensive strategy must focus not only upon the apprehension of offenders and legal pursuit but also the prevention of victimisation.

Conclusions and Recommendations

Evidently, the ecosystem of internet governance is a multifaceted issue with no singular solution. Due to the sheer volume and breadth of cyberspace, police and law enforcement efforts alone cannot fully address the challenge of cybercrime. Cybercrime is not an area that can be comprehensively tackled by an exclusive focus on cybercrime as a legal, policy or technical problem, but rather an understanding of these individual domains requires an understanding of the others. With the proliferation of new technology formulating new capabilities throughout homes, namely the advancement of artificial intelligence and the Internet of Things, it stands with good reason that cybercrime will continue to escalate in the near future. This illuminates the imminent need for policing and law enforcement practices to evolve in line with technological advances to enhance cyber-resilience within critical infrastructures. As the threat landscape is growing in complexity, there are fundamental hurdles in addressing cybercrime. This chapter has investigated the core challenges for policing cyberspace; cybercrime transgresses jurisdictional boundaries, provides anonymity, creates legislative ambiguity and experiences high levels of under-reporting. Consequently, police and law enforcement require an innovation revolution that enables the workforce to evolve with an increasingly digitised and networked society. Moving forward, preventative measures to increase community resilience and user responsibility ought to be accompanied by a skilled criminal justice taskforce to investigate and prosecute offenders at a regional and international level. Alongside this, there is a need for evidence-based cyber policing to inform and evaluate strategies and ensure practices are fundamentally rooted in an effective knowledge base. This chapter has critically evaluated the avenues for future research and work in the policing of cyberspace. Ultimately, as society moves forward, there is a need for national and international collaboration between private companies, public agencies, academia and users to ensure a robust and effective response to cybercrime.

Hillary Rodham Clinton School of Law, Aime Sullivan
Swansea University, Swansea, UK

Hillary Rodham Clinton School of Law, Reza Montasari
Swansea University, Swansea, UK

References

Ashworth, A. (2013). *Positive obligations in criminal law*. Bloomsbury Publishing.

Bailey, J., Taylor, L., Kingston, P., & Watts, G. (2021). Older adults and “scams”: Evidence from the mass observation archive. *The Journal of Adult Protection*. http://hdl.handle.net/10034/624222

Brenner, S. W. (2007). Cybercrime: Re-thinking crime control strategies. In Y. Jewkes (Ed.), *Crime online* (pp. 12–28). See ncj-218881.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during covid-19: A preliminary analysis in the UK. *European Societies, 23*(Suppl. 1), S47–S59.

Caneppele, S., & Aebi, M. F. (2019). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. *Policing: A Journal of Policy and Practice, 13*(1), 66–79.

Criminal Law Reform Now Network. (2020). Reforming the Computer Misuse Act 1990. http://www.clrnn.co.uk/media/1018/clrnn-cma-report.pdf. Accessed June 07, 2021.

Davies, G. (2020). Shining a light on policing of the dark web: An analysis of UK investigatory powers. *The Journal of Criminal Law, 84*(5), 407–426.

Guinchard, A. (2021). The criminalisation of tools under the computer misuse act 1990. The need to rethink cybercrime offences to effectively protect legitimate activities and deter cybercriminals. In *Rethinking cybercrime* (pp. 41–61). Springer.

Harkin, D., Whelan, C., & Chang, L. (2018). The challenges facing specialist police cyber-crime units: An empirical analysis. *Police Practice and Research, 19*(6), 519–536.

Kemp, S., Miró-Llinares, F., & Moneva, A. (2020). The dark figure and the cyber fraud rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research, 26*(3), 293–312.

Kennedy, S., & Warren, I. (2020). The legal geographies of extradition and sovereign power. *Internet Policy Review, 9*(3), 1–18.

Koziarski, J., & Lee, J. R. (2020). Connecting evidence-based policing and cybercrime. *Policing: An International Journal, 43*(1), 198–211.

Ladegaard, I. (2019). Crime displacement in digital drug markets. *International Journal of Drug Policy, 63*, 113–121.

Leppänen, A., & Kankaanranta, T. (2020). Co-production of cybersecurity: A case of reported data system break-ins. *Police Practice and Research, 21*(1), 78–94.

Montasari, R. (2017). An overview of cloud forensics strategy: Capabilities, challenges, and opportunities. In *Strategic Engineering for Cloud Computing and Big Data Analytics* (pp. 189–205).

Montasari, R., & Hill, R. (2019). Next-generation digital forensics: challenges and future paradigms. In *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)* (205–212). IEEE.

Montasari, R., Peltola, P., & Carpenter, V. (2016). Gauging the effectiveness of computer misuse act in dealing with cybercrimes. In *2016 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1–5). IEEE.

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2016). Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current Psychiatry Reports, 23*(4), 1–9.

National Police Chiefs Council. (2016). Policing Vision 2025. https://www.npcc.police.uk/documents/Policing%20Vision.pdf. Accessed June 07, 2021.

Office for National Statistics. (2020). Crime in England and Wales: Year ending March 2020. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2020. Accessed June 07, 2021.

Sallavaci, O. (2017). Combating cyber dependent crimes: The legal framework in the UK. In *International Conference on Global Security, Safety, and Sustainability* (pp. 53–66). Springer.

Schreuders, Z. C., Cockcroft, T. W., Butterfield, E. M., Elliott, J. R., Soobhany, A. R., et al. (2018). Needs assessment of cybercrime and digital evidence in a UK police force. *International Journal of Cyber Criminology, 14*(1), 316–340.

Stoddart, K. (2016). Uk cyber security and critical national infrastructure protection. *International Affairs, 92*(5), 1079–1105.

Świątkowska, J. (2020). Tackling cybercrime to unleash developing countries' digital potential. In *Pathways for Prosperity Commission on Technology and Inclusive Development* (p. 2020–01).

Williams, M. L. (2016). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology, 56*(1), 21–48.

Contents

Part I Privacy, Security and Challenges in the IoT

Part II Digital Forensics and Machine Learning in the IoT

Part III Cyber Terrorism and Violent Extremism in the IoT

Part I
Privacy, Security and Challenges in the IoT

Ethics and the Internet of Everything: A Glimpse into People's Perceptions of IoT Privacy and Security

Fiona Carroll, Ana Calderon, and Mohamed Mostafa

1 Introduction

The Internet of Things (IoT) can be described as an agglomeration of 'things' that are embedded with sensors and other technologies in order to connect and share data with other devices across the Internet. Nowadays, with the availability of cheap sensors, IoT enables various devices and objects around us to be addressable, recognizable and locatable (Atlam & Wills, 2020). And it is this networked scenario that is hugely impacting our society, work and life. For example, IoT has opened up a range of new opportunities and experiences for us, and it has made us more efficient in work and has made us safer in our homes and vehicles. However, as van Deursen et al. (2019) describe the daily use of IoT does not require extensive user skills (i.e. IoT operates 'on its own') and once these devices become part of an interconnected system in which they are connected to a multitude of other devices, the story gets more complex. Indeed, IoT is changing the ways people, businesses and governments interact among themselves (Economides, 2017). And as the authors of this chapter have found, it is not always a change for the greater good of society and humanity.

This chapter will take a look at users' perceptions around IoT whilst exposing the need for a trust framework to enforce ethical behaviours (i.e. ownership, trust and accountability), privacy and security and appropriate use of IoT in networked environments. The first section reviews the ethics of IoT. Following that, the chapter documents two studies: study 1 conducted a survey investigating the perceptions of personal data in the digital age which allowed for statistical as well as qualitative analyses, and study 2 utilized social networks to extract people's views of IoT and

F. Carroll (✉) · A. Calderon · M. Mostafa
Cardiff School of Technologies, Cardiff Metropolitan University, Cardiff, UK
e-mail: fcarroll@Cardiffmet.ac.uk; acalderon@Cardiffmet.ac.uk; mmostafa@Cardiffmet.ac.uk
https://www.cardiffmet.ac.uk/technologies/Pages/default.aspx

R. Montasari et al. (eds.), *Privacy, Security And Forensics in The Internet of Things (IoT)*, https://doi.org/10.1007/978-3-030-91218-5_1

privacy. The chapter concludes with a discussion on the main points of interest from the studies and then an overview of the bigger IoT picture. In particular, how IoT is not only transforming the sphere of big businesses of today but also the impact (positive and negative) it is having in people's daily lives.

2 The Ethics of IoT

We cannot deny that IoT offers great benefits to productivity; however, as Williams et al. (2018) highlights, IoT is also increasingly pervading our lives. We are seeing more and more of our critical societal services (CSSs) that provide electricity, water, heat and ways to travel, communicate and trade (i.e. vital systems) becoming part of the Internet of Things (IoT) (Asplund & Nadjm-Tehrani, 2016). And in this IoT scenario, the satisfaction of security and privacy requirements, such as data confidentiality and authentication, access control within the IoT network and privacy and trust among users and things, and the enforcement of security and privacy policies need to play a fundamental role (Sicari et al., 2015). Interestingly, in their paper, Zheng et al. (2018) highlight several recurring themes, one of which centres around users' desires for convenience and connectedness and how these desires dictate their privacy-related behaviours for dealing with external entities, such as device manufacturers, Internet Service Providers, governments and advertisers. Essentially, as IoT is built on the basis of the Internet, security problems of the Internet will also show up in IoT (Tewari & Gupta, 2020).

A core aspect of this lies in the fact that IoT collects and deals with unprecedented volumes of private, real-time and detailed data (AlHogail, 2018). But what happens with this data, what happens to our privacy and security around this data? In the midst of all this unprecedented amount of data being collected, Mashhadi et al. (2014) raise an important question: who owns this data and who should have access to it? From an end users perspective, it is hard to see and understand the scale of the full IoT picture. As van Deursen et al. (2019) describe ownership can be ascribed to a relatively limited set of devices: activity trackers, heart rate monitors, sport watches, smart thermostats and lightning systems. However, in reality, how many other million devices are collecting information on us? There is no doubt that trust management needs to play an important role in IoT for reliable data fusion and mining, qualified services with context awareness and enhanced user privacy and information security (Yan et al., 2014). However, in their research, Alraja et al. (2019) showed the trust in the IoT was also affected by both the users' risk perception and their attitudes towards using the IoT.

Thus, it creates, as Tzafestas (2018, p. 1) describes 'a new social, economic, political, and ethical landscape that needs new enhanced legal and ethical measures for privacy protection, data security, ownership protection, trust improvement, and the development of proper standards'. Indeed, the world of IoT has huge potential to enhance society, but it has all the traits that could also destroy it.