the phenomenon – situational and dispositional, psychological and social-cultural –the study of cyber-bullying has yet to receive an integrated approach that could address its various patterns and dimensions. It has also been suggested that the young people typically surveyed in cyber-bullying research may in fact view many of the behaviours under consideration as unexceptional and routine elements of life online. This in turn has led critically minded scholars to suggest that public and political alarm about the harms wrought by such experiences may be overplayed, and that it might warrant exploration through the lens of moral panic theory (Cesaroni et al., 2012). These problems notwithstanding, it is likely that cyber-bullying (alongside the other kinds of harmful interpersonal communications noted) will continue to be a focus for law- and policy-makers, regulators, educators and researchers both within and beyond criminology.

MAJID YAR

Associated Concepts: cybercrime, social media, trolling, virtual criminology

KEY READINGS

Broll, R. and Huey, L. (2015) '"Just being mean to somebody isn't a police matter": Police perspectives on policing cyberbullying', *Journal of School Violence*, 14 (2): 155–176.

Cesaroni, C., Downing, S. and Alvi, S. (2012) 'Bullying enters the 21st century? Turning a critical eye to cyber-bullying research', *Youth Justice*, 12 (3): 199–211.

Holt, T.J., Bossler, A.M. and Seigfried-Spellar, K.C. (2015) *Cybercrime and Digital Forensics: An Introduction*. New York, NY: Routledge.

Li, Q. (2006) 'Cyberbullying in schools: A research of gender differences', *School Psychology International*, 27 (2): 157–170.

Patchin, J.W. and Hinduja, S. (2006) 'Bullies move beyond the schoolyard: A preliminary look at cyberbullying', *Youth Violence and Juvenile Justice*, 4 (2): 148–169.

Smith, P.K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S. and Tippett, N. (2008) 'Cyberbullying: Its nature and impact in secondary school pupils', *Journal of Child Psychology and Psychiatry*, 49 (4): 376–385.

Willard, N.E. (2007) *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats and Distress.* Champaign, IL: Research Press.

CYBERCRIME

DEFINITION

Cybercrime is a term that has come to be widely applied to a range of crimes and deviant behaviour facilitated, enabled or mediated by computers connected to the Internet. Originally a more restricted set of crimes, the list of possible activity that can come under the description of cybercrime has expanded considerably with the advent of cloud computing, where your computer becomes an input device and the data are stored on third party computers, and the Internet of Things, where a diverse range of everyday devices, such as fridges, watches and doorbells, are connected to the Internet. A non-exhaustive list of cybercrimes is hacking, Distributed Denial of Service (DDoS) attack, spreading malware and viruses, credit card fraud (carding), ransomware attacks, cyber-stalking and phishing.

DISTINCTIVE FEATURES

The prefix *cyber* derives from the term cybernetics, itself made up from Ancient Greek κυβερνητικός (kybernetikos), meaning to steer, pilot or guide. The first use of the term cybernetic was in Norbert Weiner's 1948 book, *Cybernetics: Or Control and Communication in the Animal and the Machine.* The prefix's attachment to the word crime is a rather awkward mix of two terms that each have a contentious definition rendering their coupling doubly vexatious. David Wall distinguished three distinct ways that cybercrime could be understood, expressed sequentially as generations. The first generation describes crimes that take place *within* an internal computer network, unconnected to computers outside of the internal network. Stealing or altering company data are examples of this. The second generation of cybercrimes are those that are facilitated by networked computer technology. Such crimes could take place without networked computers, but would be limited in their scope, the manner of its enactment or the speed that can be achieved using computers. Digital piracy, cyber-stalking, hacking, hacktivism and credit card fraud would come under this category. The third generation of cybercrimes are those that are wholly mediated by networked computer technology, regarded by Wall as true cybercrimes. Crimes such as the spread of malware or computer viruses could not take place without such technology. This generational approach is useful for understanding the development of different forms of crime over time that have already become described and prohibited, but less useful for risk-assessing novel technologies and applications.

The alternative is to engage in horizon scanning the future innovations and crimes that might be imagined to be enabled or facilitated by it. For example, apps like Snapchat, which allow the sending of text or images which are deleted after viewing, would seem innocent without the knowledge of how they might be used to spread indecent images of children who are encouraged to upload pictures of themselves. The inducement that the images will be deleted provides a false sense of security. But any phone image can be captured, and not necessarily by a complicated piece of software, just another camera taking a picture of the image before it deletes. Understanding the criminal opportunities of different applications is a key feature of this form of horizon scanning. But this also highlights the truly unique quality, and threat, of networked computers linked to almost unlimited cloud data storage. The possibility that data, such as pictures, text, geographical movement, likes and dislikes, and criminal behaviour, can never be erased. It has allowed our online identities to become akin to adhesive accumulating layers of data-detritus, a sticky identity, that cannot be escaped and that can allow the creation of vast data-pictures of who we are and what we do. Our data are now a resource to be captured, controlled and possibly manipulated and stolen. These data collections were ostensibly created to better target advertising to consumers who may be receptive of it. However, it is now a huge resource for a new form of methodology termed Big Data analytics. Such data might include credit card usage, GPS-enabled map apps, websites used and data left behind as cookies, comments or emojis. It is why many of the social media sites we use are free because we have signed up to have our data harvested, and then sold on to advertising companies and others interested in finding out about us. These data form a unique picture of one's life. Consequently, they also become a major source of investigation in criminal cases. The irony of much cybercrime is that anonymity seems to be the overriding feature since for the most part the offender is at least a couple of screens away from the target of the offence. Yet, the possibility of leaving a data trail of incriminating information that could lead to the location of the originating screen, and so the human in front of it, has become exponentially more detailed and informative. Big data analytics has become, therefore, a hugely important resource for investigators, and a pitfall that offenders are having to negotiate and avoid.

EVALUATION

Smartphones, tablets and the Internet of Things have all shown how cybercrime is now ubiquitous. Indeed, ubiquitous computing is a term that has been coined to describe the way that computing is hyper mobile and embedded in our lives to such an extent that our health, location, emotions (likes, dislikes and emojis) and intentions can be constantly monitored. Automated technology from cars to drones and the decreasing costs associated with these innovations have meant that opportunities for novel forms of crime have proliferated. Which raises the question about whether or not the term cybercrime is even relevant anymore? If everything we do has a 'cyber' or computer-networked element, then isn't every crime a cyber-enabled crime? Moreover, very few cybercrimes are solely ever anchored to networked computers, and drift offline to the world of face-to-face interactions.

But more problematic are those arguments that maintain cybercrime is a moral panic, a new and unique crime that has been exaggerated, in Stan Cohen's classic formulation, or that cybercrime is not as big of a problem as presented by the various cheerleaders arguing for greater protections against its harm. The simple answer is that we do not know the scope of the crime, and perhaps never will. But this is not unique to this form of offending and is equally true of crime that is not computer or network-enabled. One issue that is very clear, as at the time of this writing, cybercrime does not attain the level of coverage in criminological texts as traditional crime. This is in spite of its increasing appearance in the popular imagination, and in the increasing resources put into protections against it, and the legal regulations being built to form the legislative framework for prosecuting it. This absence is all the more surprising given huge international cybercrime cases, such as the WannaCry ransomware attack on the National Health Service in the UK in 2017 or the leaks by Edward Snowden showing the level of international state-sponsored surveillance, and the often unwitting complicity of international companies, such as Google, in its facilitation. Whether or not we regard cybercrime as a moral panic, a danger to national and international infrastructure, or an everyday crime that we will need to build defences against in the same way we lock doors or use alarms, criminology has been slow to incorporate it into its canon of topics that we routinely research, teach about and include in the textbooks and journal articles of our discipline.

CRAIG WEBBER

Associated Concepts: big data, cyber-bullying, cybersecurity, moral panic, social media

KEY READINGS

Glenny, M. (2011) *Darkmarket: Cyberthieves, Cybercops and You*. London: The Bodley Head.

Holt, T.J., Bossler, A.M. and Seigfried-Spellar, K.C. (2015) *Cybercrime and Digital Forensics: An Introduction*. London: Routledge.

McGuire, M. (2012) *Technology, Crime and Justice: The Question Concerning Technomia*. London: Routledge.

van Hardeveld, G.J., Webber, C. and O'Hara, K. (2017) 'Deviating from the cybercriminal script: Exploring tools of anonymity (mis)used on cryptomarkets', *American Behavioural Scientist*, 61 (11): 1244–1266 .

Wall, D.S. (2007) *Cybercrime: The Transformation of Crime in the Information Age*. Malden: Polity Press.

Yar, M. (2013) *Cybercrime and Society* (2nd edn). London: Sage.

CYBERSECURITY

DEFINITION

Cybersecurity is generally understood to be the protection of the cyber environment (including cyberspace, its providers and its users), through risk analysis, policy, practice and prevention, from all types of attacks that create insecurity, which are initiated by insiders and outsiders driven by a range of motivations to destroy, damage, disrupt, disable or steal the hardware, software (code) or the data which together constitute the cyber environment.

DISTINCTIVE FEATURES

The problem with such complex and absolute definitions which amalgamate many different definitions, is that cybersecurity is one of those concepts, like cybercrime, where everybody