Jacqueline D. Wernimont

23 Digital

Abstract: The keyword entry for ‘Digital’ explores both the etymological and disciplinary contexts for a term that has been central to the formation of a field of Digital Criminology. Considerations include the relationship of ‘digital’ to ‘cyber’ and 21st-century critiques of oversimplifications and assumptions about how ‘the digital’ operates in individual lives and broader cultural communities.

Keywords: digital, cyber-, security, communities of practice

While 21st-century invocations of ‘the digital’ tend to point toward computation and electronic devices, prior to the middle of the 20th century the term digital was intimately connected to the human hand. Borrowing from the classical Latin *digitalis*, meaning a length equal to a finger’s breadth, post-classical Latin and medieval regional languages used ‘digital’ to refer to a particular finger or to finger-like measurements. The related noun, ‘digit,’ appeared in classical Latin as *digitus* and was used in medieval Germanic and romance languages to refer to a whole number less than or equal to ten and, anatomically, to individual fingers or toes.

While the meaning of ‘digit’ has remained relatively stable and in use in mathematical and anatomical lexicons, the meaning of ‘digital’ shifted dramatically in English during the 20th century. As an adjective, ‘digital’ is important in signal and information storage and processing, where it refers to data represented by a series of discrete values, commonly 0 and 1. This usage continued with the development of computing and calculating machines that operated on data as discrete numbers and expanded to refer to many kinds of electronic technology that use data stored and processed as discrete numbers.

In 21st-century usage we tend to see ‘digital’ as an adjective modifying generalized nouns: digital photography, digital technologies, digital society/culture, digital scholarship, or digital crime. In these contexts, digital often connotes not only electronic but also more modern sociotechnical formations that are often linked to the widespread use of computation and internet connectivity (see Computation by Mazzilli Daechsel). The 2021 European Union Serious and Organized Crime Threat Assessment is deeply concerned with digital practices and technologies and opens by asserting “criminals are digital natives … virtually all criminal activities now feature some online component” (Europol, 2021).

Criminologists are particularly well-positioned to be able to define cyber and digital crime and crime control in terms of harm, ethics, historical socio-technical contexts (see Cybercrime by Holt and Holt). While most international academic institutions and research have addressed digital crime in terms of cybersecurity and located those inquiries within science, technology, engineering, and mathematics or in law programs, Brian Payne and Lora Hadzhidimova (2018) observe that criminal justice research and interventions provide important tools for understanding how human behavior shapes our approaches to justice, surveillance, and crime in our highly connected digital cultures.

Creepers and continuities

Security and privacy concerns emerged alongside early computing research and the increasing adoption of computing for commerce and, eventually, personal use. In 1972, the U.S. National Bureau of Standards (NBS) established a Computer Security Program. A year before, the first self-replicating computing program, known as Creeper, was developed by Robert Thomas in 1971 and was quickly followed by Ray Tomlinson's Reaper program, which was designed to chase and delete Creeper (Chen and Robert, 2004). Robert Morris Jr.'s infamous 1988 Morris Worm created the first known Denial of Service, or DoS, attack and disrupted roughly 10 % of the internet at the time. Despite both its impact and Morris' eventual prosecution under the 1986 Computer Fraud and Abuse Act, the Morris Worm was designed to measure the internet, not crash it. Like Creeper and Reaper, Morris Worm was not designed with criminal intent. But by the 1990s we saw an explosion of new malicious worms, viruses, and other intrusions that were created to gather personal information, access sensitive information, and for financial gain. The rise of the prefix 'cyber-' essentially follows the historical trajectory of computing-specific security, and cybersecurity curricula have been available for academic and professional education since at least the early-1980s (Parrish et al., 2018).

While harm and safety in cyberspace have been concerns for roughly fifty years, as a term 'digital' is a much older and more capacious than 'cyber-'. I will take a moment here to further unpack the term 'digital' so that we can understand its relationships to criminology before returning to security and surveillance.

A history of 'digital'

The discipline of signal processing distinguishes between digital and analog technology in terms of the duration of a signal; digital technology depends on non-continuous (discrete) signals whereas analog technology depends on continuous or wave signals. These analog signals have an infinite set of possible values, whereas digital signaling depends on a finite set of values. Examples of analog communication include landline/copper wire telephony, magnetic tapes, and classic microphones. In contrast, digital information transmission is discrete and often binary, as in the case of our familiar personal computers, in which data is encoded in 0s and 1s. But early computers like ENIAC and measurement tools like the Geiger counter use decade or base-ten encodings.

While common usage tends to conflate digital information with/in electronic devices, we have had and continue to have digital information outside of electronics. Non-electronic forms of digital information include the abacus (it's also a computer), many kinds of weaving and needlework patterns, and punched cards like those used for Bouchon and Jacquard mechanical weaving, Carpentier's melotrope music player, Hollerith's tabulating machines used for 19th-century vital statistics, and a variety of accounting machines worldwide. More modern examples of non-electronic digital information include many kinds of student testing technologies where one fills in bubbles on long cards, known as Scantron in the US, and paper voting ballets.

As we have seen, digital communication privileges the discrete and modular whereas analog signals literally make meaning through continuity. As Tara McPherson reminds us, this is a matter of both technical precision and a window into the kinds of cultural logics that digital information shares with other cultural formations (McPherson, 2012). In particular, the technical logics of digital information processing and storage are intertwined with political, social, and knowledge organizations ascendant after World War II. This includes but is not limited to late capitalism, genetics and eugenics, racializing sciences, binary understandings of gender and sexuality, universal knowledge projects, surveillance and policing practices, global migration, and modular labor practices (Chandler and Fuchs, 2019; Chun, 2021; McPherson, 2012; Abbate, 2012; Hicks, 2018; Johnson, 2018; Browne, 2015; Leurs and Smets, 2018; Gajjala, 2019; Woodcock, 2021; Richardson et al., 2019).

Imagining 'digital'

Technical practice and historical usage clearly enable the use of the term 'digital' well outside of either electronics or computing. When Europol describes 21st-century criminals as 'digital natives,' they are leveraging now well-worn rhetoric that imagines generations born into fluency with the "digital language of computers, video games and the Internet" (Prensky cited in boyd, 2014). These imaginaries depend on a slippage between digital information, rendered in discrete signals, and the electronics that have been shaping our lives since the middle of the 20th century.

There are significant socio-technical consequences of these kinds of slippages; as danah boyd so trenchantly observes, applying the term 'digital native' based on birthdate obscures uneven distributions of technological skills, media literacy, and infrastructure access within nations and across the globe (boyd, 2014). It also assumes that people born after a certain date possess uniform cultural and legal literacy when engaging across a wide variety of socio-technical contexts, including cell phone use, activity tracker wearing, biomedical device use, online research, internet banking, and even basic job and school applications. The implications are not just about access, but also about inequities in safety and security when access is possible. Digital harassment, revealing personal information without consent, and stalking are just a few of the many harms that women, people of color, queer people, and people from religious and national minorities experience when trying to engage in activities of daily living that depend on digital technologies.

In addition to problematizing the notion that young people are somehow more fluent and skilled in their engagements with digital information machines, networks, and processes, feminist scholars ask us to attend to the many ways that design choices and social narratives around 'the digital' have rendered it as something non-material. Cloud computing is a particularly salient example; the metaphor suggests an ariel, immaterial, and potentially infinite space where we can store our digital data, rather than a terrestrial network of server stacks residing in electricity and water hungry corporate warehouses. Similarly, both the internet and world wide web may seem abstract to those not familiar with the subterranean, submarine, and satellite infrastructures that connect a series of physical computers to create that web or net. Nicole Starosielski's work on submarine cables is just one example of the kind of recent scholarship that illuminates not only the physical infrastructures essential to digital life, but also their environmental impacts and roles in geopolitical power struggles (Starosielski, 2015).

Indeed, for many our modern computers and computational processes function as 'black boxes,' opaque technical systems where inputs and outputs are visible but the operations between are hidden from user and regulatory view. Unlike transparent 'glass box' operations, black boxes not only hide the technical operations within a system, but they also obscure the material, affective, embodied, labor, and situational contexts that make digital processing and information possible (Wernimont and Losh, 2018). Consequently, most people are insufficiently informed about the possible harms and affordances of digital logics and technologies when it comes time to make behavioral and policy choices.

While common usage might apply 'digital' in an overly broad manner with respect to technical usage, it is also the case that many 21st-century practices and interactions are thoroughly co-constructed alongside our epistemic dependence on discrete information and technology regimes. Consequently, we can and should understand modern 'digital' culture as part of a longer era of discrete, modular, and categorical ways of understanding the world and our societies. In many ways what we now call the digital age exists inside of an era of 'datafication' that extends back to 17th-century vital statistics and manual counting machines like the earliest pedometers and odometers (Wernimont, 2019; see also Dijck, 2014).

Digital justice and crime

Criminology and justice studies seek to understand how socio-technical contexts and human factors shape what a given culture names crime and justice, often expanding well beyond the literal letter of the law or legal precedent. In this context, the adoption of the phrase 'digital criminology' helpfully demarcates different boundaries from cybersecurity and cybercrime, both of which tend to focus on the limited domain of the computer or networks of computers and often emphasize technical processes, defenses, and resolutions (see Parrish et al., 2018; Wirkuttis and Klein, 2017).

Digital criminology is also distinctive in that it draws on longer histories of data-based crime, victimization, and justice. It offers us ways of thinking about guardianship of digital infrastructure, which can extend well beyond the computational, as well as of the many people and flows of products, services, and information in digital cultures (see Infrastructure by Grisot and Parmiggiani). As Smith et al. (2017) observe, digital criminology is "concerned with exploring the critical role performed by digital devices/infrastructures/data as intersectional and transformative mediums in the criminal justice field," as well as reckoning with the perils and possibilities introduced when digital tools are adopted in surveillance, policing, adjudicating, and determining what constitutes justice for those harmed (p. 272).

At the same time, we do well to remember the unequal distributions of power, ability, and harm embedded in modern digital life. Scholars have already enumerated a long list of irregularities and discriminatory outcomes in predictive policing and use of deeply racist or otherwise biased historical data sets (see Prediction by Gundhus, Galis, and Ķīlis; and Policing by Wilson); ethical and labor concerns in the use of synthetic images in time-based media; political and legal consequences of generated image, video, and audio recording; and intellectual property rights for scientific knowledge, artistic creation, and technical innovation (for examples see Browning and Arrigo, 2021; Egbert, 2019; Keyes et al., 2019; Pawelec, 2022; Smits and Borghuis, 2022).

Some of the harms we can point to today build on longstanding concerns about how different actors understand intellectual property, illicit content, and national security (to name just a few areas). But there is also a legacy of colonialism and imbalances in global power that underpins both the way people tend to talk about 'the digital' and people's access to digital resources and opportunities. The digital divide is very real; in 2023, 2.7 billion people (1/3 of the global population) did not have access to the internet and 53% of the world did not have access to high-speed broadband (Signe, 2023). Technological infrastructure of the sort that is now more common than not in wealthy Western nations, is clearly not the only way people can relate to one another or engage in the business of life, nor should it be. Given the psychological, social, political, and environmental costs of those resources, it is not a given that societies who do not use digital infrastructures should want to have it or must be convinced of its value so that they can become the 'next billion users' (Pichai, 2015). Nations and people must also be able to exercise self-determination in relation to socio-technical structures, rather than simply be transformed into new products and users by 21st-century mega-corporations operating as new colonial powers.

At the same time, understanding how harms are perpetuated through digital infrastructure and infostructures is necessary for protecting our most vulnerable people. To offer just a couple of examples: We need better articulations of the harms and possible remedies for women whose pregnancies are revealed without their consent through mundane technologies like loyalty programs or digital temperature monitors. Similarly, though at a different scale, we must articulate how the disruption of digital communication networks impacts survival chances of civilians caught in war. Finally, we are confronted with a double-edged sword in the proliferation of surveillance through ubiquitous computing. The experience of perpetual risk for some (Black and Brown communities in the United States, for example) has its other in the potential to document war crimes and crimes against humanity for others.

Looking forward

In 1976 the United Nations affirmed that human rights include a right to self-determination and the ability to freely pursue economic, social, and cultural development (International Covenant on Economic, Social and Cultural Rights). The history of international human rights law and of our modern computing cultures and technologies have been deeply intertwined, even if that entanglement has not always been visible. The interdisciplinary field of critical digital justice and criminology can help 21st-century scholars and practitioners maintain the focus on the interplay of sociotechnical systems and situated practices in fostering more just digital societies, more self-determination with respect to digital practices and tools, and our shared understandings of how and why digital crimes occur. These are important interventions in contexts that historically have been dominated by discussions of cybercrime and national-level security concerns. As scholars like danah boyd and others have reminded us, the notion of digital natives is fundamentally flawed even as we find so many of our lives thoroughly mediated by digital technologies. Digital and critical criminologists are essential to our efforts to develop more just futures for not just the well-connected (either in terms of politics or technology) and wealthy but also for people across the world who are seeking more just futures that include reparative modes of dealing with harms perpetuated across the spectrum from interpersonal to international. As Powell et al. (2018) note, this includes essential questions about justice: “What does it mean to be a ’just’ digital citizen? How will digital communications and social networks enable new forms of justice and justice movements?” Digital criminologists need to help us all ask and answer these questions.

Main takeaways

- The history of the term ‘digital’ extends back to antiquity where it referred to an embodied measurement.
- Digital information encoding utilizes discrete values and modular logics and can take both electronic and non-electronic forms.
- Safety and security concerns for digital technologies are as old as the technologies themselves.
- ‘Digital Criminology’ refers to a more capacious field that deals with sociotechnical cultural systems rather than the narrower technical emphasis of cyber-disciplines.

- Care must be taken when using ‘digital’ because the use of the term has often been a way to obscure material, embodied, and affective considerations for both digital infrastructure and information.

Suggested reading

Brown, M., & Carrabine, E. (2019). The critical foundations of visual criminology: The state, crisis, and the sensory. *Critical Criminology*, 27, 191 – 205.

Brown, S. (2006). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology*, 10(2), 223 – 244.

Gordon, F., McGovern, A., Thompson, C., & Wood, M. A. (2022). Beyond cybercrime: New perspectives on crime, harm and digital technologies. *International Journal for Crime, Justice and Social Democracy*, 11(1), i–viii.

Powell, A., Stratton, G., & Cameron, R. (2018). *Digital Criminology: Crime and Justice in Digital Society.* London: Routledge.

Schuilenburg, M., & Peeters, R. (eds.) (2020). *The Algorithmic Society: Technology, Power, and Knowledge.* London: Routledge.

References

Abbate, J. (2012). *Recoding Gender: Women’s Changing Participation in Computing.* Cambridge, MA: MIT Press.

boyd, d. (2014). *It’s Complicated: The Social Lives of Networked Teens.* New Haven: Yale University Press. https://doi.org/10.12987/9780300166439

Browne, S. (2015). *Dark Matters: On the Surveillance of Blackness.* Durham, NC: Duke University Press.

Browning, M., & Arrigo, B. (2021). Stop and risk: Policing, data, and the digital age of discrimination. *American Journal of Criminal Justice*, 46, 298 – 316.

Chandler, D., & Fuchs, C. (2019). *Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data.* London: University of Westminster Press.

Chen, T., & Robert, J.-M. (2004). The evolution of viruses and worms. In W. W. S. Chen, *Statistical Methods in Computer Security* (chapter 16). Boca Raton: CRC Press. 10.1201/9781420030884.ch16.

Chun, W. (2021). *Discriminating Data: Correlation, Neighborhoods, and the New Politics of Recognition,* Cambridge, MA: MIT Press.

Dijck, J. V. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance and Society*, 12, 197 – 208.

Egbert, S. (2019). Predictive policing and the platformization of police work. *Surveillance & Society*, 17(1/2), 83 – 88.

Europol. (2021). *European Union Serious and Organized Crime Threat Assessment.* https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf

Gajjala, R. (2019). *Digital Diasporas: Labor, Affect and Technomediation in South Asia.* Lexington Press, UK.

Hicks, M. (2018). *Programmed Inequality: How Britain Discarded Women Technologists and Lost Its Edge in Computing.* Cambridge, MA: MIT Press.

Johnson, J. M. (2018). Markup bodies: Black [life] studies and slavery [death] studies at the digital crossroads. *Social Text*, 36, 57 – 79. https://doi.org/10.1215/01642472-7145658

Keyes, O., Stevens, N., & Wernimont, J. (2019). *The Government is Using the Most Vulnerable People to Test Facial Recognition Software.* Slate.com. https://slate.com/technology/2019/03/facial-recognition-nist-verification-testing-data-sets-children-immigrants-consent.html

Leurs, K., & Smets, K. (2018). Five questions for digital migration studies: Learning from digital connectivity and forced migration in(to) Europe. *Social Media + Society*, 4(1). https://doi.org/10.1177/2056305118764425

McPherson, T. (2012). Why are the digital humanities so white? Or thinking the histories of race and computation. In M. K Gold (ed.), *Debates in the Digital Humanities* (pp. 139 – 160). Minneapolis: University of Minnesota Press.

Parrish, A., Impagliazzo, J., Raj, R. K., Santos, H., Asghar, M. R., Jøsang, A., Pereira, T., & Stavrou, E. (2018). Global perspectives on cybersecurity education for 2030: A case for a meta-discipline. In *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education* (ITiCSE 2018 Companion) (pp. 36 – 54). Association for Computing Machinery, New York, NY, USA. https://doi-org.dartmouth.idm.oclc.org/10.1145/3293881.3295778

Pawelec, M. (2022). Deepfakes and democracy (theory): How synthetic audio-visual media for disinformation and hate speech threaten core democratic functions. *DISO*, 1, 19. https://doi.org/10.1007/s44206-022-00010 – 6

Payne, B. K., & Hadzhidimova, L. (2018). Cyber security and criminal justice programs in the United States: Exploring the intersections. *International Journal of Criminal Justice Sciences*, 13(2), 385 – 404. doi:10.5281/zenodo.2657646

Pichai, S. (2015). Google I/O 2015 Keynote. Google also rolled out a section of their blog entitled "Next Billion Users". https://blog.google/technology/next-billion-users/

Powell, A., Stratton, G., & Cameron, R. (2018). *Digital Criminology: Crime and Justice in Digital Society.* London: Routledge.

Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *NYUL Rev. Online*, 94, 15 – 57.

Signe, L. (2023). *Fixing the global digital divide and digital access gap.* Brookings Online. https://www.brookings.edu/articles/fixing-the-global-digital-divide-and-digital-access-gap/

Smith, G., Bennett Moses, L., & Chan, J. (2017). The challenges of doing criminology in the big data era: Towards a digital and data-driven approach. *The British Journal of Criminology*, 57(2), 259 – 274,

Smits, J., & Borghuis, T. (2022). Generative AI and intellectual property rights. In B. Custers & E. Fosch-Villaronga (eds.), *Law and Artificial Intelligence.* Information Technology and Law Series, 35 (pp. 323 – 344). The Hague: T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-523-2_17

Starosielski, N. (2015). *The Undersea Network (Sign, Storage, Transmission).* Durham, NC: Duke University Press.

Wernimont, J. (2019). *Numbered Lives: Life and Death in Quantum Media.* Cambridge, MA: The MIT Press.

Wernimont, J., & Losh, L. (2018). *Bodies of Information: Intersectional Feminism and Digital Humanities.* Minneapolis, MN: University of Minnesota Press.

Woodcock, J. (2021). *The Fight Against Platform Capitalism: An Inquiry into the Global Struggles of the Gig Economy.* London: University of Westminster Press. https://doi.org/10.16997/book51

Wirkuttis, N., & Klein, H. (2017). Artificial intelligence in cybersecurity. *Cyber, Intelligence, and Security*, 1(1), 103 – 119.