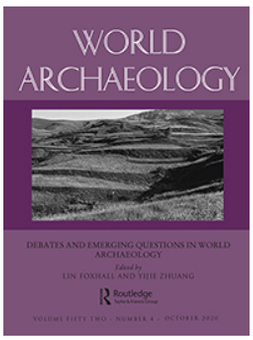

World Archaeology

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rwar20

(Im)material culture: towards an archaeology of cybercrime

Clive Harfield & John Schofield

To cite this article: Clive Harfield & John Schofield (2020) (Im)material culture: towards an archaeology of cybercrime, World Archaeology, 52:4, 607-618, DOI: 10.1080/00438243.2021.1882333

To link to this article: https://doi.org/10.1080/00438243.2021.1882333

Published online: 22 Feb 2021.

WORLD ARCHAEOLOGY
2020, VOL. 52, NO. 4, 607–618
https://doi.org/10.1080/00438243.2021.1882333

Routledge
Taylor & Francis Group

ARTICLES

(Im)material culture: towards an archaeology of cybercrime

Clive Harfield[a] and John Schofield[b]

[a]Institute of Cyber Investigations and Forensics, University of the Sunshine Coast, Sippy Downs, Australia; [b]Department of Archaeology, University of York, York, UK

ABSTRACT

Cybercrime is ubiquitous. People now inhabit a digital environment comprising permanent risk, exponential threats, and multiple virtual/physical harms, forming a global community of malefactors and the criminally exploited. The purpose of this paper is two-fold. First, through an archaeological lens, to characterize the new materiality of cybercrime (including its artefacts and architecture alongside digital/virtual manifestations). And second, to explore the potential for new perspectives on cybercrime borne out of this archaeological approach. In short: what is the archaeology of cybercrime and can new understandings emerge from an archaeological perspective? In undertaking this research we also challenge the long-held presumption that non-physical traces cannot be studied archaeologically. It is our contention that they can.

KEYWORDS

Cybercrime; cybersecurity; contemporary archaeology; new materiality; digital environment

Introduction

Traditionally, archaeology has sought to understand past human behaviours through the excavation of their material traces, taking account of those factors that transform the archaeological record between the point of deposition and discovery (e.g. Schiffer 1976). A very different archaeological approach however applies to more recent periods where a profusion in material culture exists alongside infinite other potential sources of evidence while, for the contemporary world at least, most if not all material traces exist on the surface (Harrison and Schofield 2010; Harrison 2011). A further and particular challenge exists in relation to what has been termed the 'new materiality' (DeLanda 2015; Minahan and Wolfram Cox 2007), where traces are largely if not entirely virtual, digital, fluid and intangible. Contemporary society is increasingly characterized by this new materiality and its almost infinite abundance.

In this paper we take an interdisciplinary approach to cybercrime, a particular example of this new materiality and one that is likely to affect everybody in society. Through our respective backgrounds in cybersecurity and contemporary archaeology, we first define and then outline what we consider to be the archaeology of cybercrime (comprising its 'trace' although only rarely will this be physical). We then explore the possibility of using archaeology to develop helpful new perspectives on cybercrime as a contribution to what we refer to as the philosophy of cybersecurity, being an adaptive approach to the hazards of living in the digital environment. We contend that an archaeological perspective provides unique insight on cybercrime through rendering visible or concrete what for many is invisible or abstract, and creating order and structure out of a highly complex virtual landscape. The paper also aligns with

CONTACT John Schofield John.Schofield@york.ac.uk Department of Archaeology, University of York, York YO1 7EP, UK

This article has been corrected with minor changes. These changes do not impact the academic content of the article.

current thinking around heritage, with its increased focus on the intangible elements of culture and society, on the digital archive and on the future (Harrison et al. 2020).

Over three centuries, archaeological methodologies have developed which promote the understanding of complex landscapes shaped by human interventions often over millennia. Here we extend that archaeological approach to a complex *virtual* landscape, questioning whether the same archaeological perspective might contribute to cybersecurity, comprising the countermeasures constantly being developed to mitigate and prevent cybercrime. The study forms part of a growing number of projects that demonstrate the validity and relevance of archaeology in addressing complex, multi-causal global challenges highly resistant to resolution, sometimes referred to as 'wicked problems' (APSC 2018) for which simple single-discipline solutions are unlikely to succeed. Other examples of archaeological approaches to wicked problems include marine plastic pollution (Schofield et al. 2020) and social inequality (Kiddey 2017).

Archaeologies of the contemporary past (conveniently referred to here as 'contemporary archaeology') emerged as part of the processual/new archaeology of the 1960s, with its philosophy of logical positivism: learning about the past through observed behaviours in the present, not least through use of ethnoarchaeology. Of various ethnoarchaeological encounters, Rathje's Garbage Project (e.g. Rathje and Murphy 2001; Rathje et al. 1992) stands out for its emphasis on understanding the *present* through the application of archaeological methods. This project exerted significant influence on a second wave of contemporary archaeology projects and publications in the early 21st century (summarized in Harrison and Schofield 2010), now with a clear emphasis on archaeology as contemporary practice and the archaeology *of* the contemporary world.

Two aspects of this contemporary archaeology have particular relevance here: the use of archaeology in conventional forensic investigations; and the application of archaeological methods and perspectives to the digital environment. The first of these is widely known. Examples and outcomes of archaeological work in criminal investigations regularly appear in archaeological (e.g. Crossland 2013) and criminological and forensic scientific literature (e.g. Schultz and Dupraz 2008). It is also widely known by virtue of its exposure in popular crime drama.

The second aspect comprises archaeological contributions to understanding the digital environment. Examples include Moshenska's (2014) excavation and investigation of a memory stick, Perry and Morgan's (2015) excavation of a hard-drive, Beale, Schofield, and Austin's (2018) study of the computer mouse and Cocroft and Schofield's (2019) archaeological investigation of the Cold War signals and intelligence gathering site of Teufelsberg in Berlin. A further and important area of study within this context is video gaming (e.g. Reinhard 2015; Aycock, Reinhard, and Therrien 2019). Together these contributions represent an emerging field that demonstrates the diversity of ways archaeological approaches can enhance understanding of a fast-changing digital world and people's interactions with it.

This paper builds on these various archaeological foundations, merging them with ideas and knowledge from the field of cybersecurity to construct an argument that there is an archaeology of cybercrime which can helpfully contribute to addressing the wicked problem that it presents for society. Before outlining this archaeology of cybercrime we consider, briefly, what defines cybercrime and what are its consequences, for people and for society.

Cybercrime – definitions and consequences

We define cybercrime broadly: not merely criminal deviance that exists solely in, and only because of, the characteristics of the connected and cellular digital environment (cybercrime proper) –

automated malware corrupting operating systems, for instance – but also digitized conduct that constitutes criminal deviance in non-digital environments; for example: blackmail reconfigured as ransomware; and unlawful acquisition of electronic funds or digitized intellectual property through theft or deception ('ordinary' crimes committed using a digital device). Thus an internet- or wifi-enabled digital device may be separately or simultaneously: a perpetration tool, a crime scene, and a non-biological crime-target.

Within this context, the connected digital environment parallels the physical environment. Humans co-exist in each, to different degrees by generation (Floridi 2013, 14–15; Holt, Bossler, and Seigfried-Spellar 2018, 4–5) while existence in the digital environment is triggering both psychological and physiological changes in humans (Greenfield 2015; Bhatt 2019). In terms of behaviours, digital connectivity exponentially increases the potential scope and range of deviance. Acting alone, whether at home, in a cyber-café or on a park bench, an individual can commit multiple automated crimes anywhere in the connected world (disguising their location as they do so) for as long as their digital device is powered. For those who lack the competence or sangfroid to perpetrate cybercrime themselves, 'Cybercrime as a Service' (CaaS) is available (Manky 2013; Europol 2020). The demographic profile of agents in the archaeology of cybercrime thus includes: humans; digital devices programmed to operate automatically within the limits of their programming; and artificial intelligence devices capable of self-enhancement and initiating actions beyond their original programming (see Goodman 2016). All of this is changing the character of actors, agency, and arenas in the understanding of cybercrime as a ubiquitous activity.

Cybercrime harm is multidimensional (Agrafiotis et al. 2018) and can be divided into five distinct categories:

(1) Physical harms in the form of compromised hardware, and damage caused by corrupted systems operation (Jenkins 2013; Zetter 2014); and the damage and injury arising from the criminal use of digital technology (for example, hacking driverless cars and causing crashes, Carter 2019).
(2) Virtual harms comprising compromised networks; corrupted software; crimes committed in virtual reality worlds (Goodman 2010); physical identification documents devalued through data breaches; and privacy intrusion from antisocial use of social media (Fogel and Nehmad 2009).
(3) Community and individual social harms such as the erosion of trust (Bhatt 2019), connected to the psychological damage to self-confidence through victimization; the feelings of violation, increased risk and decreased safety incurred through online identity usurpation (Goldsmid, Gannoni, and Smith 2018); and personal psychological and reputational injury (sometimes triggering victim self-harm or self-destruction) from trolling and cyber-bullying (Ballard and Welch 2015), online domestic violence (Douglas, Harris, and Dradiewicz 2019), and malicious online postings such as revenge porn (Henry and Powell 2015).
(4) Economic harms, including losses incurred falling victim to fraud, or the costs of repairing the damages of the harms itemized above (Smith 2018).
(5) Consequential harms, when non-digital crimes such as illicit commodity trafficking and service provision are facilitated by digital technology (Bartlett 2015), in turn sustaining individual and social ills such as narcotic addiction (Barratt, Ferris, and Winstock 2013), or the online exploitation of children (Carr 2010).

Digital technology exists at and cohabits the intersection of the physical and the digital environments. People explore potential within the digital environment every day, seemingly motivated as much by criminal intent as by beneficence (Schneier 2000; Bartlett 2015). The digital environment exposes more individuals to more threats and harms than they are likely to encounter in the physical environment and safety and survival necessitate adaptation founded on comprehension. Parallels exist here with past societies where people did not understand the risk of other types of contamination, for example from industrial processes, disease or water. Then, as now, people learnt from experience, and had to learn and adapt to survive. This paper takes the position that archaeology and cybercriminology could complement and supplement one another, not least in the analysis of digital environment artefacts, to help improve that comprehension. We return to this prospect in the conclusion. It is to the new materiality of cybercrime that we now turn.

The new materiality of cybercrime

A typology of cybercrime logically distinguishes physical tools from the digital (while recognizing also how the two might overlap). The physical tools – those that enable human engagement with the digital environment – may be classified under four headings:

(1) Input and interaction devices such as keyboards, mice, monitors, hand-held devices (e.g. tablets, phones, cameras) and home assistance devices (e.g. Google Home, Alexa).
(2) Storage devices (e.g. hard drives, USB thumb drives, memory cards), together with any associated peripheral devices necessary to connect a storage device to the third class,
(3) processing devices (central processing units; servers; laptops; tablets).
(4) Internet access infrastructure tools (cabling, routers, wireless access points, mobile broadband devices, wi-fi and telecommunication relay towers and their associated microwave delivery systems, including orbiting communication satellites).

This already complex communications landscape is exponentially elaborated via the so-called 'Internet of Things' [IoT]: innumerable interconnected household appliances, workplace devices, and vehicles operable from a tablet or smartphone or communicating data to other devices/vehicles, which – because security is not often a feature of their functionality – are openly vulnerable to hacking and cybercrime utilization (Schneier 2018; Blythe, Sombatruang, and Johnson 2019). Of course, and crucially, all of these physical tools are designed and routinely used for entirely legal, routine and mundane tasks.

Digital artefacts of cybercrime are no less varied. These fall under three headings:

(1) Digital tools specifically developed to commit cybercrime. This includes malware, ransomware, spyware, trojans, bots, viruses, spiders and hacking tools, all used to corrupt, compromise, or acquire control of operating systems and stored data (Cisco Security 2018; Schneier 2018).
(2) Legitimate digital tools adapted to commit cybercrime include key-loggers (Grebennikov 2007: although usually a software program, a key-logger can also be a physical device, further complicating the cybercrime artefact catalogue) and Remote Administration Tools such as an IT service help-desk might use that also enable surreptitious activation of web-cams and microphones, either peripheral or inbuilt (McMillan 2013). The construction of a false digital identity to use in committing cybercrime online may be considered an artefact, whether it

remains only virtual or whether it includes the production of forged physical identification artefacts (using a 3D printer for instance).

(3) Digital artefacts that are the product of cybercrime include aggregated data-sets of personal identification information stolen or acquired through phishing, used criminally by the data-set creator or sold on in the CaaS market (Schneier 2000; Bartlett 2015); or the creation of a digividual (digital persona or avatar) for criminal ends (the experimental invention of Ronald Pinn proving how easy this is, O'Hagan 2017).

Online or connected content or data created for, and/or unlawfully acquired by, cybercrime activity – for example, a concocted narrative founding an advance fee fraud, or stolen intellectual property in digital form – represent two other sub-categories of digital artefact capable of being used in the interpretation, analysis and understanding of human conduct within the digital environment. Simultaneous classification in different categories is conceivable: data generated via fitness self-surveillance devices (digital devices that form part of the IoT), for example, is simultaneously cultural and behavioural data created for use by the artefact wearer (Lanzing 2016); digitized information that might subsequently be amenable to archaeological scrutiny (e.g. Perry and Morgan 2015); and data that can be hacked, misappropriated, and misused by cybercriminals.

Beyond the artefacts listed above, the architecture and physical infrastructure utilized in the commission of cybercrime comprises, for example: digital communication structures (towers and satellites supporting mobile phone and wi-fi transmitters for instance); and repurposed secure buildings offering physical separation of those committing cybercrime from the community (McKay 2019). At a mundane and domestic level, are the almost infinite number of buried digital service cables, for example connecting street furniture to dwellings.

In archaeological terms, the artefacts and virtual traces we describe form a typological framework that creates some order out of immense complexity. As a framework it also allows us to position the things we find (for example through criminal investigations) relative to one another, and forms a baseline for future research. Digital connectivity can redefine dimensions and here we might helpfully refer to two dimensions that are mainstays of archaeological enquiry: the spatial dimension (noting in particular how cybercrime, unusually, is place*less*, or that 'known' fixed locations might be fake and deliberately deceptive); and a temporal dimension (in which cybercriminals are constantly trying to outwit cybersecurity, but in reality neither is fully aware of the other's capabilities). In terms of place, Follis and Fish (2020, 29) explain how the, 'absence of place has a leveling effect on the exercise of power. This fact allows solitary individuals or groups of hacktivists to act with impact on the international stage once reserved for nation-states.' As an example of the temporal dimension, digital artefact creation is possible at rates inconceivable in the physical world: for example, December 2019 witnessed 16.61 million new malware programs; January 2020, 16.76 million; February 2020, 10.62 million (AVTest 2020).

Having summarized the new materiality of cybercrime and with this redefinition of two core dimensions of archaeological inquiry in mind, we now turn to whether an archaeological approach provides fresh insight to cybercrime. What can an archaeological approach tell us that we didn't already know? First we discuss the generalities, before presenting a case study.

Archaeology and cybercrime

Archaeology has traditionally focused on the everyday and the ordinary, albeit as a contribution to wider cultural themes and questions. The archaeology of cybercrime is no exception. Indeed, this

may be its greatest advantage over other approaches and its most important contribution to the philosophy of cybersecurity, the wider themes in this case relating to technology and human adaptation. In this section we describe ways in which archaeology provides a distinctive and helpful framework for investigating cybercrime.

Hitherto, technology has characterized human interaction with the environment. Now technology *is* the environment. With cybercrime (and arguably for much of contemporary archaeology), a different relationship between people and technology prevails with implications both for the way people live and the way they should perceive their (digital) environment. While cybercrime is typically 'place*less*', we argue that this aspect of the digital world complicates and adds new dimensions to the concept of 'place' in the sense of being simultaneously in real/unreal places; or somewhere/nowhere/everywhere at the same time. Archaeological methodologies, adept at dealing with multiple conceptualizations of landscapes simultaneously, might be particularly well equipped to analyse and help to unravel these various entanglements.

Artefacts (including user-interface and data processing devices, digital products) illustrate the connectivity that renders cybercrime and the opportunities to commit it or fall victim to it ubiquitous, camouflaged by being commonplace and creating global vulnerabilities. All day every day, the means to suffer harm through digital devices intended to benefit humankind surround the digitally-connected community. It is a landscape of threats and dangers. The seemingly innocuous and the easily overlooked create an environment of convenience simultaneously characterized by hostility and uncertainty, in which not only direct users but unwitting third parties can be seriously harmed. The Australian National University data breach in late 2018, discovered and reported in 2019 (ANU 2019), which exploited decommissioned but not yet disconnected legacy hardware, is a case in point. One of the authors of this paper (CH), at ANU between 2010 and 2013, will not know for certain whether he is a victim of that crime until and unless there is corroborating evidence that his ANU identity has been usurped and used for a further criminal purpose. We explore this case study in more detail below.

An individual simultaneously occupying the physical and digital environments is much more likely to fall victim to crime in the latter than in the former. In nearly six decades, the same author (CH) has not yet suffered a robbery or burglary, but in March 2020 (for example) was the target of two dozen phishing attacks. Adaptive behaviours to sustain safety and well-being in the physical environment are insufficient to achieve the same in the digital environment. In such a hostile environment, cybersecurity cannot be merely a series of tools, apps and software add-ons. Cybersecurity must be a way of life. And because the digital environment is artificial, the survival behaviours will not be naturally instinctive but must be intuitively learned, informed by a philosophy of cybersecurity, itself founded on new perspectives on cybercrime.

In contributing an archaeological perspective to the consideration of a philosophy of cybersecurity, we might helpfully review cybercrime within three related contextual frameworks, these being evidential, technical and social.

In the evidential context, cybercrime leaves traces amenable to both physical and digital forensic investigation: the 'how' and the 'what with' being means of identifying the 'who'. For example, fingerprints, fibres, and DNA evidencing the physical presence of an individual at a location from which digital devices used in cybercrime have been recovered; paper documents linking individuals to digital records (Edwards 2020). For investigation managers, archaeological perspectives thus conceptually conjoin traditional physical scenes-of-crime examination with digital forensics, creating broader, more complex, strategic options (Shavers 2013).

In the technical context, digital stratigraphy and context relationships may offer new ways of understanding malware development, recognizing for example how systemic vulnerabilities come to be

embedded in software design processes. Before software is released on the market, such recognition could inform the 'designing out' of bugs that could be exploited criminally, a strategy consistent with the criminology concept of designing out crime (Ekblom 2005; Tilley 2005). Similarly, archaeological perspectives may produce insights into the evolution of innovative cybercrime methodologies that create new crime opportunities rather than exploit unintentional product vulnerabilities. Plotting past methodological trajectories may offer a means of anticipating emerging and future methodologies with sufficient notice to develop and implement preventive intervention.

In the social context, archaeological frameworks provide a structure for representing the cybercrime environment to the global community of ICT-users, the majority of whom are as yet unsophisticated in relation to cybersecurity. This can be achieved in ways that emphasize the totality of the threat and the personal responsibility of each user to contribute to a cybersecurity survival strategy that protects self and community members from cybercrime. For the purposes of wider community engagement and education, archaeological frameworks explicate the hostile digital environment to which people must now adapt. The threats are invisible, the vulnerabilities unrecognized, the harms unperceived and potentially catastrophic. The prism of archaeology elucidates the spectrum of cybercrime, so illuminating this risky environment, highlighting the necessity for and significance of viewing engagement with the digital environment from the perspective of a cybersecurity ecosystem (a philosophical foundation underpinning policy and practice). It also promotes well-being, safety and survival, providing a practical philosophy to juxtapose the work of moral philosophers contemplating how individuals can live a digital life worth living (Vallor 2016).

Finally, in contributing meaningfully to a philosophy of cybersecurity which explains and emphasizes the important role of ordinary users, as well as those technically-sophisticated, in sustaining a safe digital environment, archaeology draws out the important imbalance, evident in public and media representations of cybercrime between state-initiated cyberwarfare/hacking and the great majority of cybercrime. The former may be newsworthy (and important, in that this too affects everybody) but it doesn't account for most people's direct experience which more typically comprises scams and digital theft, social engineering and stalking, IP piracy and streamed sexual/physical abuse.

The Australia National University [ANU] data breach of November 2018

To date (December 2020), no other organization that has been subject of a data breach has been so candid and forthcoming in its public discussion of what went wrong and why. This is the only publicly accessible detailed case study we have of a data breach (ANU 2019).

What is particularly interesting about the ANU report is that it adopts an 'environmental' perspective in its analysis, as an archaeologist would seek to understand an artefact or a monument in its wider context. Thus, Stonehenge can be studied as a monument to learn about Neolithic masonry and construction practices, but the monument itself only makes sense, only acquires meaning for the modern audience, when viewed within its landscape. So, too, with this data breach example.

Rather than just limit themselves to understanding the technical means by which the hostile actor(s) gained access to ANU systems and data – the digital locks and bolts and how these worked or failed – ANU's analysis adopted an environment perspective that incorporated 'people and process issues' as well, concluding that this was 'an organizational issue' rather than an IT security issue, and that a key resolution strategy was the need to emphasize 'culture and security awareness among students, staff and researchers' (ANU 2019, 3).

One (non-)process that had significant implications was the failure to disconnect from the network, and dispose of in a timely fashion, decommissioned and disused digital hardware such as old desk-top

computers. This assemblage provided the hostile actor(s) with a virtual landscape of vulnerabilities that could be exploited to help disguise the presence and purpose of the intruder(s).

The analysis undertaken by ANU focused on what might be termed the occupational debris left by the intruder(s), which often comprised negative features such as the digital equivalent of a ditch cut, the wiping of event and systems logs to deny investigators evidence of precisely which data had been compromised, copied, and exfiltrated. The 'occupational debris' also provided evidence that 'the actor's dwell time on the ANU network was approximately six weeks' (ANU 2019, 2).

Piecing together the steps taken by the actor(s) – and how these related to what was or was not happening in the authorized user community and intrusion-detection systems – was not dissimilar to comprehending context chronology and relationships using a Harris Matrix.

Working in the cybersecurity arena, the lesson from this incident is the message it contains for technically-focussed colleagues about the need to view cybersecurity as an environmental system, as an archaeologist would view a site in the landscape, not simply as different types of digital locks and bolts. As much as anything, we argue that cybersecurity needs to adopt an archaeological way of thinking.

In terms of the cyber-harms we catalogue, the ANU data breach caused harms 1, 2 and 3 – and we do not yet know whether it has given rise to harms 4 and 5, but that possibility has prompted ANU to engage in constant surveillance to detect these harms as soon as they happen.

In terms of the new materiality, the ANU breach utilized all four categories, in multiple locations: the hostile actor(s) used their own hardware and internet access, as well as routing the attacks through disguised vectors and accessing the hardware and networks at ANU.

And the data breach featured all three categories of cybercrime digital artefact that we identify: Intruder-designed bespoke malware was used to compromise the ANU networks and data once systems access had been achieved through the phishing attacks (Category 1); standard email software was used to conduct social engineering attacks via phishing attacks (Category 2); and the exfiltration of data would enable the hostile actor(s) to create data-sets of copied personal identifiable information [PII] that become a criminal asset in and of themselves, and could be used to commit various other physical and digital crimes (Category 3).

Conclusion

Our archaeological framing of cybercrime builds on Perry and Morgan's (2015, 96)

> promise of an 'archaeological media archaeology', wherein the process of enquiry and interpretative outcomes trigger critical examination of both fields of practice, and heighten our capacity to think meaningfully about the past, present, and future.

We argue that archaeological techniques can 'bring a broad discussion of technology into focus through materiality' (Perry and Morgan 2015, 97), building on their citation of Buchli and Lucas (2001, 9) in translating 'an everyday perceptual language into an archaeological one'.

Archaeology provides distinct and helpful contributions to some wicked problems, many of which will only grow in scale and complexity over time, perhaps exponentially in the case of cybercrime. In characterizing the challenge for cybersecurity (admittedly with its focus more on states than individuals), Follis and Fish (2020, 204–5) suggest that,

> rather than surrender to a bleak vision of a technologically determined and dystopic future, our best strategy is to *think the future in the present*. That is, we need to think seriously about how to support and develop mechanisms of algorithmic justice; about how the legal, criminal, and ethical systems we have come to rely on will govern human and nonhuman interactions; and how to narrow the gap between our

> rapid adoption of new technologies and our slow and imperfect understanding of how these technologies are reshaping the human condition. (our emphasis)

Above all, the digitally-connected community needs to think seriously about how to help individuals understand and survive safely the digital environment they now (often unwittingly) inhabit. People need to better understand how to protect themselves – and so others – from the invisible dangers of malware and the insidious dangers of misinformation.

These are all challenges that can be viewed from an archaeological perspective that foregrounds human adaptation through its (im)material manifestations. By taking an archaeological approach to something as ubiquitous and as dangerous as cybercrime, we are proposing to follow Follis and Fish's suggestion to 'think the future in the present'. We qualify this, however, by promoting the direct use of methods and perspectives developed to investigate the *past*, notably the complex (including both spatial and stratigraphic) relationships between people and things and the ever-changing landscape in which they co-exist. In other words we suggest that, as a novel approach to the wicked problem of cybercrime and in developing a philosophy of cybersecurity, that we might helpfully think the future through the past and, in Holtorf and Hogberg's terms (2014, 351), use this aspect of 'cultural heritage for the benefit of society in the future'.

Acknowledgments

We take this opportunity to thank those staff in Archaeology at Southampton University in the early to mid 1980s who encouraged us as contemporary/fellow under- and later postgraduate students to boldly and critically explore even the unlikeliest of cross-disciplinary connections and to think about archaeological traces of the contemporary world. We each benefited from the teachings and influence of Clive Gamble, Stephen Shennan and the late Peter Ucko in this regard. We are also grateful to two anonymous referees for their helpful comments on this paper, and to Lin Foxhall for additional and helpful suggestions that have enhanced its clarity.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Clive Harfield is Associate Professor of Cybersecurity at the Institute for Cyber Investigations and Forensics, University of the Sunshine Coast, Australia. A former criminal justice sector practitioner and member of the team that established the UK's first national hi-tech crime unit, in academia he has taught criminology in the UK and criminal law in Australia. His teaching and research interests currently focus on cybersecurity policy, and investigation ethics and governance.

John Schofield is Professor of Archaeology at the University of York, UK where he is also Director of Studies in Cultural Heritage Management. Prior to joining the University of York in 2010, John spent 21 years with English Heritage working in policy and heritage protection. John has adjunct status at Griffith and Flinders universities in Australia, and is Docent in Archaeology and Museology at the University of Turku, Finland. John's current research focuses on the contributions archaeology can make to contemporary real-world problems such as environmental pollution, social justice and crime.

References

Agrafiotis, I., J. Nurxe, M. Goldsmith, S. Creese, and D. Upton. 2018. "A Taxonomy of Cyber-harms: Defining the Impacts of Cyber-attacks and Understanding How They Propagate." *Journal of Cyber Security* 4. Accessed March 24 2020. https://academic.oup.com/cybersecurity/article/4/1/tyy006/5133288

ANU. 2019. "Incident Report on the Breach of the Australian National University's Administration Systems." Accessed April 16 2020. https://imagedepot.anu.edu.au/scapa/Website/SCAPA190209_Public_report_web_2.pdf

APSC. 2018. "Tackling Wicked Problems: A Public Policy Perspective." Australian Public Service Commission. Accessed December 16 2020. https://www.apsc.gov.au/tackling-wicked-problems-public-policy-perspective

AVTest. 2020. "Malware." AVTest: The Independent IT-Security Institute. Accessed March 26 2020; website updated daily. https://www.av-test.org/en/statistics/malware/

Aycock, J., A. Reinhard, and C. Therrien. 2019. "A Tale of Two CDs: Archaeological Analysis of Full-Motion Video Formats in Two PC Engine/TurboGrafx-16 Games." *Open Archaeology* 5 (1): 350–364. doi:10.1515/opar-2019-0022.

Ballard, M., and K. Welch. 2015. "Virtual Warfare: Cyberbullying and Cyber-victimization in MMOG Play." *Games and Culture* 12 (5). doi:10.1177/1555412015592473.

Barratt, M., J. Ferris, and A. Winstock. 2013. "Use of Silk Road, the Online Drug Marketplace, in the United Kingdom, Australia and the United States." *Addiction* 109 (5): 774–783. doi:10.1111/add.12470.

Bartlett, J. 2015. *The Dark Net*. London: Windmill Books.

Beale, G., J. Schofield, and J. Austin. 2018. "The Archaeology of the Digital Periphery: Computer Mice and the Archaeology of the Early Digital Era." *Journal of Contemporary Archaeology* 5 (2): 154–173. doi:10.1558/jca.33422.

Bhatt, S. 2019. *The Attention Deficit: Unintended Consequences of Digital Connectivity*. Basingstoke: Palgrave Macmillan. doi:10.1007/978-3-030-21848-5.

Blythe, J., N. Sombatruang, and S. Johnson. 2019. "What Security Features and Crime Prevention Advice Is Communicated in Consumer IoT Device Manuals and Support Pages?" *Journal of Cybersecurity* 5 (1). doi:10.1093/cybsec/tyz005.

Buchli, V., and G. Lucas, eds. 2001. *Archaeologies of the Contemporary Past*. London and New York: Routledge.

Carr, J. 2010. "Online Crimes against Children." *Freedom from Fear* 7 (7): 26–28. doi:10.18356/8a98e865-en.

Carter, J. 2019. "Hacked Driverless Cars Could Cause Collisions and Gridlock in Cities, Say Researchers." Forbes March 5. Accessed March 14 2020. https://www.forbes.com/sites/jamiecartereurope/2019/03/05/hacked-driverless-cars-could-cause-collisions-and-gridlock-in-cities-say-researchers/#216ffa682a09

Cisco Security. 2018. "What Is the Difference: Viruses, Worms, Trojans, and Bots?" Accessed March 24 2020. https://tools.cisco.com/security/center/resources/virus_differences

Cocroft, W. D., and J. Schofield. 2019. *The Teufelsberg and Western Electronic Intelligence Gathering in Cold War Berlin*. London: Routledge (Research Focus Series).

Crossland, Z. 2013. "Evidential Regimes of Forensic Archaeology." *Annual Review of Anthropology* 42 (1): 122–137. doi:10.1146/annurev-anthro-092412-155513.

DeLanda, M. 2015. "The New Materiality." *Architectural Design*, September 1. doi:10.1002/ad.1948.

Douglas, H., B. Harris, and M. Dradiewicz. 2019. "Technology-facilitated Domestic and Family Violence: Women's Experiences." *British Journal of Criminology* 59 (3): 551–570. doi:10.1093/bjc/azy068.

Edwards, G. 2020. *Cybercrime Investigators Handbook*. Hoboken, NY: Wiley.

Ekblom, P. 2005. "Designing Products against Crime." In *Handbook of Crime Prevention and Community Safety*, edited by N. Tilley, 203–244. Cullompton, Devon: Willan Publishing.

Europol. 2020. *Internet Organized Crime Threat Assessment*. The Hague: European Union Agency for Law Enforcement Cooperation.

Floridi, L. 2013. *The Ethics of Information*. Oxford: Oxford University Press.

Fogel, J., and E. Nehmad. 2009. "Internet Social Network Communities: Risk-taking, Trust, and Privacy Concerns." *Computers in Human Behaviour* 25 (1): 153–160. doi:10.1016/j.chb.2008.08.006.

Follis, L., and A. Fish. 2020. *Hacker States*. Cambridge (Mass.): MIT Press.

Goldsmid, S., A. Gannoni, and R. Smith. 2018. *Identity Crime and Misuse in Australia: Results of the 2017 Online Survey*. Canberra: Australian Institute of Criminology. Accessed March 14 2020. https://aic.gov.au/publications/sr/sr11

Goodman, M. 2010. "Crime and Policing in Virtual Worlds." *Freedom from Fear* 7 (7): 52–59. doi:10.18356/6cced1e3-en.
Goodman, M. 2016. *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*. New York: Anchor Books.
Grebennikov, N. 2007. "Keyloggers: How They Work and How to Detect Them." *Ksapersky Secure List*. Accessed March 24 2020. https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/
Greenfield, S. 2015. *Mind Change: How Digital Technologies Are Leaving Their Mark On Our Brains*. London: Random House.
Harrison, R. 2011. "Surface Assemblages. Towards an Archaeology in and of the Present." *Archaeological Dialogues* 18 (2): 141–161. doi:10.1017/S1380203811000195.
Harrison, R., C. DeSilvey, C. Holtorf, S. Macdonald, N. Bartolini, E. Breithoff, H. Fredheim, et al. 2020. *Heritage Futures: Comparative Approaches to Natural and Cultural Heritage Practices*. London: UCL Press.
Harrison, R., and J. Schofield. 2010. *After Modernity: Archaeological Approaches to the Contemporary Past*. Oxford: Oxford University Press.
Henry, N., and A. Powell. 2015. "Beyond the Sext: Technology-facilitated Sexual Violence and Harassment against Adult Women." *Australia & New Zealand Journal of Criminology* 48 (1): 104–118. doi:10.1177/0004865814524218.
Holt, J., A. Bossler, and K. Seigfried-Spellar. 2018. *Cybercrime and Digital Forensics: An Introduction*. Abingdon: Routledge.
Holtorf, C., and A. Högberg. 2014. "Communicating with Future Generations: What are the Benefits of Preserving Cultural Heritage? Nuclear Power and Beyond." *European Journal of Postclassical Archaeologies* 4: 343–358.
Jenkins, R. 2013. "Is Stuxnet Physical? Does It Matter?" *Journal of Military Ethics* 12 (1): 68–79. doi:10.1080/15027570.2013.782640.
Kiddey, R. 2017. *Homeless Heritage: Collaborative Social Archaeology as Therapeutic Practice*. Oxford: Oxford University Press.
Lanzing, M. 2016. "The Transparent Self." *Ethics and Information Technology* 18 (1): 9–16. doi:10.1007/s10676-016-9396-y.
Manky, D. 2013. "Cybercrime as a Service: A Very Modern Business." *Computer Fraud & Security* 2013 (6): 9–13. June 9-13. doi:10.1016/S1361-3723(13)70053-8.
McKay, T. 2019. "German Police Raid Data Centre and Alleged Cybercrime Hub Based Out of Former NATO Bunker." *Gizmodo*. Accessed March 26 2020 https://www.gizmodo.com.au/2019/09/german-police-raid-data-center-and-alleged-cybercrime-hub-based-out-of-former-nato-bunker/
McMillan, A. 2013. "How Hackers Can Switch on Your Webcam and Control Your Computer." Sydney Morning Herald. April 2. Accessed March 24 2020. https://www.smh.com.au/technology/how-hackers-can-switch-on-your-webcam-and-control-your-computer-20130328-2gvwv.html
Minahan, S., and J. Wolfram Cox. 2007. "Stitch'n'Bitch: Cyberfeminism, a Third Place and the New Materiality." *Journal of Material Culture* 12 (1): 5–21. doi:10.1177/1359183507074559.
Moshenska, G. 2014. "The Archaeology of (Flash) Memory." *Post-Medieval Archaeology* 48 (1): 255–259.
O'Hagan, A. 2017. *The Secret Life*. London: Faber & Faber.
Perry, S., and C. Morgan. 2015. "Materializing Media Archaeologies: The MAD-P Hard Drive Excavation." *Journal of Contemporary Archaeology* 2 (1): 94–104. doi:10.1558/jca.v2i1.27083.
Rathje, W. L., and C. Murphy. 2001. *Rubbish! the Archaeology of Garbage*. Chicago: University of Arizona Press.
Rathje, W. L., W. W. Hughes, D. C. Wilson, M. K. Tani, G. H. Archer, R. G. Hunt, and T. W. Jones. 1992. "The Archaeology of Contemporary Landfill." *American Antiquity* 57 (3): 437–447. doi:10.1017/S0002731600054330.
Reinhard, A. 2015. "Excavating Atari: Where the Media Was the Archaeology." *Journal of Contemporary Archaeology* 2 (1): 86–93. doi:10.1558/jca.v2i1.27108.
Schiffer, M. B. 1976. *Behavioural Archaeology*. New York: Academic Press.
Schneier, B. 2000. *Secrets and Lies: Digital Security in a Networked World*. New York: Wiley.
Schneier, B. 2018. *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World*. New York: W.W. Norton.
Schofield, J., K. Wyles, S. Doherty, A. Donnelly, J. Jones, and A. Porter. 2020. "Object Narratives as a Methodology for Mitigating Marine Plastic Pollution: A New Multidisciplinary Approach, and a Case Study from Galápagos." *Antiquity* 94 (373): 228–244. doi:10.15184/aqy.2019.232.

Schultz, J. L., and T. L. Dupraz. 2008. "The Contribution of Forensic Archaeology to Homicide Investigations." *Homicide Studies* 12 (4): 399–413. doi:10.1177/1088767908324430.

Shavers, B. 2013. *Placing the Suspect behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects*. W Altham, Ma: Elsevier.

Smith, R. 2018. *Estimating the Cost to Australian Businesses of Identity Crime and Misuse*. Canberra: Australian Institute of Criminology. Accessed March 14 2020. https://aic.gov.au/publications/rr/rr15

Tilley, N. 2005. "Crime Prevention and System Design." In *Handbook of Crime Prevention and Community Safety*, edited by N. Tilley, 266–293. Cullompton, Devon: Willan Publishing.

Vallor, S. 2016. *Technology and the Virtues*. Oxford: Oxford University Press.

Zetter, K. 2014. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." *Wired*. Accessed March 13 2020. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/