Crime in the Age of the Smart Machine: A Zuboffian Approach to Computers and Crime

Kevin F. Steinmetz
Kansas State University, United States

Abstract

This analysis ruminates on the quintessential qualities that underpin the relationship between computers and crime by drawing from the foundational work of Shoshana Zuboff, a scholar whose work has to date been largely ignored in the study of crime. From this perspective, computers are best described as "informating" machines that require "intellective skills" in both licit and illicit forms of work. The first part of this analysis describes the role of such skills in the commission of computer-related crimes and considers factors that affect the degree to which such skills are necessary for perpetration. The second part considers how a Zuboffian approach can inform examinations of other subjects that have historically been considered important for criminological inquiries, including learning and subculture, the emotional experience of crime, and perceptions held by offenders and victims.

Keywords

Computer crime; cybercrime; Zuboff; informate; Smart Machine.

Please cite this article as:
Steinmetz KF (2022) Crime in the age of the smart machine: A Zuboffian approach to computers and crime. *International Journal for Crime, Justice and Social Democracy* 11(1): 225-238. https://doi.org/10.5204/ijcjsd.2136

ISSN: 2202-8005

Introduction

Over the past half a century, computers have become a fixture of everyday life. An increasing share of the workforce regularly uses computers for their jobs, many people in developed countries carry smartphones everywhere, and internet use has become a necessity for social and civil life (Pew Research Center 2019). Likewise, crimes mediated through or targeting computers have similarly proliferated (Furnell 2017). Scholars have made significant strides during this period to understand the new topography of crime introduced by computers and networking technologies (e.g., Holt and Bossler 2014; Powell, Stratton, and Cameron 2018; Wall 2007; Yar and Steinmetz 2019). Among other changes, research has found that computer technologies have significantly affected the scope and scale of crimes, reshaped the social relationships involved in crime commissions, rearranged the political economy of crimes and control, and introduced new challenges for law enforcement and security regarding criminal detection, prevention, and investigation.

Criminologists have utilized a diverse assortment of approaches to dissect the complexities that computers have introduced to criminal enterprises. For instance, some criminologists have chosen to adapt standard criminological theories (e.g., routine activities theory, social learning theory, and self-control theory) for computer-related crimes (Yar and Steinmetz 2019). Others have forged novel approaches tailored for digital contexts like extension theory (Brey 2017), actor–network theory (Brown 2006; Latour 2005; van der Wagen 2018; van der Wagen and Pieters 2015), digital drift (Goldsmith and Brewer 2015), and digital criminology (Powell, Stratton, and Cameron 2018). The breadth and depth of theorizing and scholarship to date in the area have been laudable. Amidst such advances, however, it is worth pausing to ruminate on the quintessential qualities that underpin the relationship between computers and crime—qualities from which all other considerations of such crimes proceed. Such an endeavor can provide a unifying and parsimonious base to ground computer crime scholarship and theorizing.

This analysis applies Shoshana Zuboff's (1988) treatise on computer technologies and work, *In the Age of the Smart Machine: The Future of Work and Power* (*Smart Machine*), to accomplish this task. While widely influential in the fields of science and technology studies, *Smart Machine* has been largely ignored by criminologists. In this work, Zuboff (1988) examined multiple worksites during a historical period of significant industrial changes as computers, then new and novel devices, were increasingly integrated into the workplace. She considered the effects of computers on the experience of labor, the skills required to accomplish occupational tasks, the structure of the workforce within an organization, and the role of authority in the workplace. While her study was detailed and thorough, two foundational concepts comprised the fulcrum of her analysis. The first concerned the characteristic that, according to her, distinguishes computers from other machines—they "informate." In addition to automating tasks, computers process data and provide textual feedback to the user. Thus, computers mediate work, adding a layer of abstraction to the labor process. Second, "intellective skills" or abstract reasoning and processing skills are necessary to conduct informated work. As her analysis revealed, these deceptively simple concepts bear significant implications for the nature of work in a computerized era.

This analysis argues that the same concepts that Zuboff (1988) applied to the transformation of legitimate work are equally applicable to illegitimate forms of labor. Just as Zuboff (1988: 13) discarded the "natural attitude" that takes for granted the role of computers in work and everyday life, this analysis requires taking on an "attitude of strangeness" to examine the subtle yet profound ways that computers affect the relationship between criminals and their crimes—to reconsider the very notion of what computers *do* to crime (Neuman 2007: 284). Additionally, the application of *Smart Machine* to the study of crimes necessitates a willingness to view crime itself as a kind of work. Letkemann (1973: 6) noted decades ago that the "various dimensions of work appear to be as applicable … to the illegitimate as the legitimate worker." In other words, crime is a form of labor, criminals are laborers, and both can be understood in terms like those applied to legitimate enterprises (Fagan and Freeman 1999; Letkemann 1973; Steinmetz 2016; Sutherland 1937). Just as information technologies fundamentally reconfigured legitimate work, similar changes are evident as crime is computerized (Wall 2007: 42-44).

The current analysis builds from Zuboff's (1988) conceptual work to reframe the issues of computer crime and criminality in two parts. Part 1 elaborates on the concepts of informating and intellective skills. It also describes their immediate application for understanding the relationship between computers and crime. Regarding informating, this analysis contends that criminologists should consider examining computer crimes not as a distinct type of crime but simply variants of preexisting forms of crime shaped by the *degree* to which they are informated or reliant on computers. For intellective skills, this essay traces the transition of these skills from "action-centered" skills and the criminological implications of such changes. Further, it argues that though intellective skills are important for computerized work, not all tasks are equally dependent on computers, nor are all criminals equally willing to utilize such technologies. As such, the factors that affect the extent to which intellective skills are required in crime commissions are considered, including *centrality*, *availability*, and *engagement*.

Part 2 of this analysis considers how a Zuboffian approach can inform examinations of other subjects that have historically been considered important for criminological inquiry. It begins by considering the role of information technology and intellective skills for knowledge transmission, addressing criminological concerns like social learning and subcultures. Further, Zuboff's (1988) insights are applied to the emotional experience of crime, a domain of longstanding fascination for criminologists. Finally, the implications of the distance between what Zuboff (1988: 84) described as a "symbol and reality" for perceptions held by both criminals and their victims are explored. These dynamics are considered in turn.

Part 1: Zuboff, the Informating Machine, and Intellective Skills

Informating Explained

Technology restructures production processes and the relationships that workers have with the means of production (Marx 1867). Computers have further transformed work by handling mental tasks previously performed by human workers like logistics and supervision, as well as increasing the efficiency and effectiveness of automated physical processes. In her observations of eight organizations, Zuboff (1988) noted that the introduction of computers into the workplace meant that workers' experiences of the production process fundamentally changed: their experience of their action contexts—the actual work done by production processes—became mediated through the symbolic interface of the computer.[1]

According to Zuboff (1988), changes in the labor process and worker experience occur because of a defining characteristic of computers that separate these machines from others.[2] While machines of various sorts had long been revolutionizing work by expanding human production capacities through automation (Braverman 1974; Marx 1967), computers further revolutionized work by automating *and* informating tasks (Zuboff 1985, 1988). As she explained:

> Information technology … not only imposes information (in the form of programmed instructions) but also produces information. It both accomplishes tasks and translates them into information. The action of a machine is entirely invested in its object, the product. Information technology … introduces an additional dimension of reflexivity: it makes its contribution to the product, but it also reflects back on its activities and on the system of activities to which it is related. Information technology not only produces action but also produces a voice that symbolically renders events, objects, and processes so that they become visible, knowable, and shareable in a new way. (Zuboff 1988: 9)[3]

As machines displace the physical labor of workers, computers transform such physical processes into data. These machines perform the mental labor previously reserved for human intelligence. Human labor's role in the process becomes the handling of data interpretation and decision-making that has yet to be embedded into the logic of the machine. The machine, in this sense, "is active, reactive, it talks back" (Turkle 1984: 211). Zuboff (1988) was not the first to recognize the informating potential of machines (see Noble 1991: 133), but the language she used to frame the phenomenon is useful.

Conceptualizing Informated Crimes

In his oft-cited book *Cybercrime: The Transformation of Crime in the Information Age*, Wall (2007: 10) defined computer crimes or "cybercrimes" as "the transformation of criminal or harmful behavior by networked technology." He attributed such transformation to the networked qualities of such technologies, the connection between value and information, and the link between computer networks and globalization (Wall 2007: 34-39). While these dimensions of computers and networking technologies are important, Zuboff's (1988) analysis made it clear that the antecedent characteristic driving such change—giving life to such transformative characteristics—is the informating capacity of computers.

On a lexical level, the concept of informating bears implications for contemporary conceptualizations of "cybercrime," "e-crime," "technocrime," or other terms used to describe computer-related crimes. It challenges taxonomic approaches that often distinguish, for instance, between "computer-assisted" crimes (those that existed prior to the advent of computers and the internet but can make use of such technologies) and "computer-focused" crimes (those that emerged alongside the development of these technologies and cannot exist independent of them) (Furnell 2002: 22; 2017; McGuire 2020: 14-15; Wall 2007). Instead, a Zuboffian perspective is more aligned with arguments that computers themselves create no new forms of crimes, that "the number of ways in which humans can harm other humans is ultimately rather limited—so genuinely novel harms are therefore rare" (McGuire 2018: 144; see also Brown 2006: 236; Lusthaus 2018: 60).[4]

From a Zuboffian perspective, computer crimes are simply informated variants of preexisting forms of crime. For instance, so-called cyberstalking could just as easily be understood as "informated stalking" because stalking behaviors existed before the internet—computers simply informate the process to varying degrees. Similarly, illicit computer hacking, often considered the computer crime par excellence (Wall 2008: 47), can easily be considered an amalgamation of informated variants of familiar crimes. For instance, computer intrusions are informated forms of trespass where the premises encroached upon are digital rather than physical. If data is stolen during a trespass, then the crime can be described as informated burglary or theft. Systems alteration or destruction would be informated vandalism or sabotage. Malware becomes a tool not so dissimilar from a burglar's lockpicks, a carjacker's shim, or a safecracker's stethoscope used to trespass, surveil, pilfer, and damage or alter systems (Sutherland 1937; Tobias 1971).[5] Such programs have the capacity to automate and informate tasks, but they are tools, nonetheless. Perhaps, then, "informated crime" would be a more precise term than any others that have proliferated to describe computer-related offenses (McGuire 2019).[6]

Intellective Skills

The second key concept of importance for this analysis concerns how the laborer responds to the informating capacities of computers. Specifically, the unique informating quality of the computing machine requires workers to utilize different skills in the laboring process. For Zuboff (1988), there are two skill domains that distinguish informated from non-informated forms of labor. Non-computerized work often involves action-centered skills, including the interpretation of information "derived from physical cues" and the execution of skills through "physical performance" (Zuboff 1988: 61). These skills only have meaning "within the context in which its associated physical activities can occur" and involve a "felt linkage" between the laborer and the labor process (Zuboff 1988: 61). Such knowledge tends to be situational and tacit in nature (Zuboff 1988: 186). Mastery of the labor process is apparent in the bodily sensations experienced and the outcomes witnessed (the relationship between sensations, experiences, and computers is explored in greater detail later in this analysis).

When work involves computers, it "becomes the manipulation of symbols" and, as Zuboff (1988: 23) explained, "when this occurs, the nature of skill is redefined." In particular, she contended that computer technologies require the use of "intellective skills," involving the interpretation of data presented through a "symbolic medium" like a computer interface, and then making decisions based on these interpretations (Zuboff 1988: 75, 95). Abstraction, inferential reasoning, and systematic and procedural thinking are all examples of intellective skills (Zuboff 1985, 1988). Abstraction involves the ability to understand data

representation (what data corresponds to in the physical world) (Zuboff 1985: 11). Inferential reasoning includes both inductive and deductive ("bottom-up" and "top-down") approaches to identifying the relationships and patterns among abstracted, computer-generated data and interpreting their overall significance for the work being done. Importantly, such reasoning involves the ability to generate and test hypotheses, build working models in the mind of the processes at hand, and apply theoretical understandings of the processes governed by the informated machine. Systematic and procedural thinking refers to the ability to sift through the data and arrive at interpretations of the data in a structured and stepwise manner.

These intellective skills are particularly useful for generating what Zuboff (1988: 92) referred to as "insight." The process of producing insight involves the use of:

> the symbolic medium to ascertain the condition of "reality" in ways that cannot be reduced to correspondence with physical objects (for example, the ability to discern states, trends, underlying causes, relations, dynamics, predictions, sources of suboptimization, opportunities for improvement, et cetera). (Zuboff 1988: 96)

Thus, insights involve the derivation of latent relationships and processes that may not be evident from the feedback garnered from immediate action contexts. Required is the ability to mentally envision relationships between data points and the systems they represent, separate from any physical context, to form architecture in the mind (Turkle 1984: 168; Zuboff 1988: 86).

Much has changed in the thirty-plus years since *Smart Machine*'s publication. Computers have become more pervasive and integrated into everyday life, and efforts are underway to deskill computerized labor (Harvey 2014: 120). Yet such changes have, at least to date, not altered the fact that work with computers requires different skill sets than non-computerized labor. The reader should note that associating intellective skills with informated work is not to say that such skills are not applicable to action-centered contexts, only that the more a laborer relies on computers, the more important such intellective skills become (Zuboff 1988: 95).

Action-Centered Versus Intellective Crimes

As crimes become informated with the introduction of computers, intellective skills become increasingly relevant for crime commission. To demonstrate this argument, it is useful to describe the role of action-centered skills in an archetypal street crime and then describe the skills required for its informated equivalent. Consider, for instance, burglary. Burglaries are often crimes of opportunity based on snap decision-making by offenders to invade the physical space of another to commit theft or some other crime (Hough 1987; Manaugh 2016; Wright and Decker 1994). Though some scholars have asserted that such crimes are unskilled and unsophisticated (Gottfredson and Hirschi 1990), burglars and related home invaders rely on a constellation of skills often grounded in experience in the physical parameters of action contexts. For instance, perpetrators often physically traverse architecture by climbing, crawling, cutting, boring, and crashing their way into buildings (Manaugh 2016). Once inside, they need to move through the space, find valuable items, and carry only as much as can be physically carried. They may employ physical tools to breach a building that rely on bodily action and feedback, such as lockpicks and prybars (Manaugh 2016). Thus, burglary involves a series of decisions made using knowledge and skills rooted in physical experience, intuition, bodily sensations, and tacit understandings of their job that may be difficult to translate into words.

Reference to the use of action-centered skills is not to say that such legitimate or illegitimate workers are not creative or knowledgeable (Zuboff 1988: 40). In the case of burglars, offenders frequently find creative uses for everyday objects and the environment for breaching a building's security (Manaugh 2016). It also does not preclude a robust knowledge of their trade, like the details concerning various locks, safes, doors, cameras, and other security devices (Manaugh 2016; Sutherland 1937). The difference lies in the context in which such knowledge is curated and deployed and the types of skills involved. Action-centered skills refer to the fact that such knowledge and creativity cannot be separated from physical situations and

bodily actions. Further, both skill domains emphasize different kinds of intelligence, where action-centered skills may emphasize "bodily and spatial intelligence" while the intellective skills developed in a "computer-mediated environment" correspond with "logical-mathematical competence" (Zuboff 1988: 194).

By that token, computer intrusions and data theft conceptually involve similar action contexts to burglary—the perpetrator enters a system without authorization and absconds with goods (i.e., data). The types of skills brought to bear by perpetrators, however, are more intellective in nature. In fact, the intellective skills described by Zuboff (1988) parallel the kinds of skills celebrated by computer hackers (Holt 2010; Steinmetz 2016; Taylor 1999; Turkle 1984). The development of such skills, along with coding abilities, is a key source of social and cultural capital among hackers (Holt 2010; Steinmetz 2016; Taylor 1999; Turkle 1984). From this vantage, hacking involves interpreting computer-generated outputs, understanding their structure, envisioning their relationships to other points of data, identifying weaknesses in the underlying structures represented by these outputs, and manipulating the systems to either solve or exploit said weaknesses. Required is the mental mapping of relationships among abstract data points to draw connections and inferences, derive and test hypotheses, and develop working models of the systems.

Intellective Skills and Crime: The Role of Centrality, Availability, and Engagement

The degree of intellective skills required to execute crimes like computer intrusion is easily established because computers are clearly vital for crime commissions. Not all crimes, however, are so reliant on computers. For some crimes, computer use is more incidental, and, as a result, fewer intellective skills may be required of the perpetrator. The person using social media to stalk a victim employs more intellective skills than the person who does not use such technologies to perpetuate their harassment. The latter requires a degree of computer savvy, like the ability to navigate the abstract spaces of the web to locate their victim's digital traces. More robust intellective skills would be necessary, however, for the stalker who uses malware and other software against their victim; more still for the offender who conducts a breach and intrusion into a victim's computer systems and online accounts.

Despite the thoroughness of her analysis, Zuboff (1988) never fully considered factors that influence the degree to which an individual may rely on computers to do their work and the level of intellective skills that must be brought to bear. In her study, computers were generally imposed on workers, and they were forced to adapt. While such impositions may occur in the context of crimes, participation in such activities is often undertaken on a more voluntary basis. At this point, the current analysis expands upon *Smart Machine* to argue that the development of what Zuboff (1988: 181) called "competence" in intellective skills is principally a function of three interrelated factors: the *centrality* of computers to the crime, the relative *availability* of computers to the criminal actor, and the level of *engagement* with technology embraced by the perpetrator.

Centrality refers to the frequency and duration of involvement of a computer in the commission of a crime. It is a function of the proportion of time spent on a computer to execute a criminal event. In other words, to what extent is the computer necessary for criminal execution? The use of a smartphone to coordinate a drug drop-off, for instance, is largely incidental to a crime and only requires basic knowledge of cellular phone user interfaces. Conversely, administering a dark web forum to buy and sell drugs necessitates spending a greater proportion of time in front of a computer, making it a pivotal component of criminal execution. The more an act requires the use of a computer, the greater the intellective skills needed.

Availability refers to the fact that the use of intellective skills with computers requires that such technologies be available to the perpetrator. It also concerns the degree to which such technologies are open to manipulation by the end user. Zittrain (2008: 2) distinguished between "generative" devices, which "invite innovation," and "sterile" devices, which only allow the user to use the device according to the parameters erected by the device designer or manufacturer. Smartphones, for instance, typically restrict the user to limited interactions with programs and functions preapproved by the manufacturer while many desktop computers give users more control to create, customize, manipulate, and otherwise

alter machine hardware and software, allowing users to get "under the hood," so to speak. The more "under the hood" a user can get with informating technologies, the more chances they develop to curate and deploy intellective skills.

Technology needs not only to be available and open, but perpetrators also need to be willing to capitalize on available computers—to exercise their agency and choose to engage with computers. The deeper the *engagement*, the more important intellective skills become. An internet stalker, for example, may spend hours scrolling through a victim's social media profiles and sending harassing messages, but such use does little to take full advantage of the freedoms afforded to them by the technology at hand (e.g., scripting malware and exploring the victim's computer network). A user who seizes on the potential of such technology—engaging in what Levy (1984: 40) called the "hands-on imperative"—will need to bring greater intellective skills to bear. In this sense, engagement correlates to a kind of "symbolic closeness" to the machine (Turkle 1984: 178).[7] The development of intellective mastery requires a certain degree of access to computers and their internal mechanisms, as well as committed engagement with technology through such opportunities (Turkle 1984).

An additional matter to consider is that centrality, availability, and engagement relate to what Zuboff (1988: 80) described as a "crisis of trust" introduced by computer technologies. This is not the trust between users connecting over computer networks—though computer technologies certainly affect social trust in this sense (Rainie and Wellman 2012: 270-271). Instead, she referred to the trust between workers and the computers (Zuboff 1988: 80). The computer acts as a kind of "black box" that processes data to present to the user. In this manner, "before, knowledge was immediate. Now, any slender sense of certainty is prey to a hundred invisible dependencies" contained within the machine (Zuboff 1988: 81). Therefore, there is a fundamental paradox introduced by computer technologies to the laboring process.

These machines are supposed to create efficiency and predictability. Yet because so much of their operations are hidden away from the user in the various operating systems, programs, and protocols cobbled together to run the machine, there is an innate level of uncertainty introduced to the laboring process. The computer user is confronted with a dilemma. Perpetrators who have limited opportunities or desire to engage with computer technologies on a more meaningful level must trust the machine as a matter of "faith" in the expert systems that comprise the technology (Giddens 1990). Those who take advantage of available machines and commit to computer use can develop the skills necessary to determine when the machine functions as intended or create or modify technologies that conform with their desires and expectations. In this manner, the worker must become adept at the interpretation of data yielded by the computer system to develop a sense of mastery over their trade (Zuboff 1988: 80-81). The choice between faith and mastery is dependent on centrality, availability, and engagement with technology.

Part 2: Further Criminological Applications of the Zuboffian Approach to Crime

Up to this point, this analysis has primarily demonstrated that Zuboff's (1988) concepts of informating and intellective skills are useful for making sense of the relationship between computers and crime. The subsequent sections shift gears, focusing on how these concepts can be extended to other areas of criminological inquiry. In particular, the current analysis applies insights from *Smart Machine* to topics considered historically and contemporarily important by criminologists, including (1) criminal learning and subculture, (2) the emotional experience of crime, and (3) the subjective perceptions of crime, criminality, and victimization.

Zuboff and Criminal Knowledge: Intellective Skills, Social Learning, and Subculture

A chief concern among criminologists is the role of social relations in the production of crime and criminality. Here too, *Smart Machine* proves informative for the study of computer crimes. In particular, Zuboff (1988) considered the implications of the intellective skills required by informating machines for group social dynamics, particularly in terms of how knowledge is shared among members. For her, knowledge dissemination among group members varies based on the type of culture present, and that

culture is intimately connected with prominent technologies used in work and communication. In other words, Zuboff (1988) discussed one of the most robust areas of criminological inquiry to date: learning and subculture.

According to Zuboff (1988), computers and intellective competence affect group dynamics, particularly in terms of how knowledge is shared among members. She argued that non-informated work and action-centered skills are associated with oral culture, which tends to be situational and inseparable from physical activity that demands "present-tense engagement in the immediate world of objects and people" (Zuboff 1988: 175-178). Knowledge is rooted in physical experience, and it relies on repetition, observation, and practice. Informated work and its intellective skills, however, emphasize knowledge creation and transmission via the written word, predominantly through electronic text. Knowledge is more easily preserved, external to the author, and is distant from situational context, serving as a standalone document to be encountered by the reader.

The "oral" and "written" cultures associated with action-oriented and intellective labor are applicable to criminal learning and subcultural transmission (Burgess and Akers 1966; Ferrell, Hayward, and Young 2015; Sutherland, Cressey, and Luckenbill 1995). Sutherland (1937: 21), for instance, referred to learning in the context of professional thieves, reflecting a reliance on the in-person transmission of skills involved in the various rackets and trades consistent with oral culture:

> A person can become a professional thief only if he is trained by those who are already professionals. It is ridiculous to imagine an amateur deciding to become a pickpocket, con man, penny-weighter (jewelry thief), or shake man (extortioner) without professional guidance. He knows nothing of the racket, its technique or operations, *and he can't learn these things out of books*. [emphasis added]

The point is that learning principally occurs among such criminal actors in physical contexts through observation of others and direct tutelage.

While mentorship and group learning dynamics can occur through information technologies, scholars have noted the role of indirect knowledge transmission in criminal learning through secondhand artifacts created and posted by others online (Goldsmith and Brewer 2015; Steinmetz 2016: 86-91). Goldsmith and Brewer (2015: 120), for instance, described changes in the learning of criminal values, techniques, and behaviors when social relations are mediated through computers and the internet, affecting "how knowledge is acquired that enables criminal behavior to occur as well as the sources of reassurance that one will not get caught." For example, as in the case of "lone wolf terrorists," an individual does not have to interact directly with others to be politically radicalized. Instead, knowledge transferal can occur through interactions with archived and preserved textual artifacts, occurring through a kind of "self-instruction" or, in the case of the transferal of political values, "self-indoctrination" (Goldsmith and Brewer 2015: 121).

Of course, ethnographers would be quick to highlight the false dichotomy at play between "oral culture" and "written culture" among criminal groups. Cultural criminologists have highlighted the effects of media and popular culture on shared criminal meanings, for instance, which cut across action-oriented or intellective contexts (Ferrell, Hayward, and Young 2015). The distinction offered in this analysis is not one of kind but of degree and situational context. Action-centered activities are more likely to necessitate learning in shared group contexts where physical actions are performed, practiced, and passed on while learning in contexts of the electronic text are more likely to require "geeks," including those involved in illicit affairs, to engage in self-directed study and practice (Holt 2010: 474; Reagle 2016).

Written culture and intellective skills also interact with the aforementioned crisis of trust introduced by informating technologies. In particular, the level of "faith" one is willing to embrace in the criminal enterprise may affect social standing among illicit technological subcultures. Among highly skilled hackers, the ability to create one's own programs or "scripts" is a marker of social status (Furnell 2002; Holt 2010;

Lusthaus 2018; Steinmetz 2016). It is increasingly common for people interested in compromising a system, however, to purchase premade malware (Lusthaus 2018: 61). A certain degree of intellective skills is still necessary for the person to purchase and deploy the software, but not the same degree necessary for an individual to craft malware to breach a system. The latter is more likely to involve knowledge of the architecture of the target system or software, formulating and testing hypotheses about which functions may exploit the system, and developing theoretical knowledge to formulate new understandings inductively of the problem at hand. For the purchaser of these scripts, they must place a certain degree of faith or trust in the expertise of the script author. There are reputational mechanisms built into many dark web marketplaces to fortify such faith, but faith is still required (Dupont et al. 2017; Holt 2013; Holt, Smirnova, and Hutchings 2016; Lusthaus 2018). Thus, these communities simultaneously bolster faith in technology while encouraging robust intellective skills through mechanisms governing social status.

To summarize, the degree to which an activity is informated likely corresponds with changes in the learning of criminal values and techniques, the organization of subcultures, and the types of skills curated, transmitted, and valued in such contexts. Therefore, computers become actors within these social networks (Latour 2005). They not only affect the relationship between the illicit worker and their work but similarly shape the social relations that comprise peer groups and subcultures in fundamental ways (Goldsmith and Brewer 2015).

Informating the Criminal Experience

Though not fully articulated by Zuboff (1988), the insights provided by *Smart Machine* speak directly to the emotional experience of labor, particularly in how the use of informated technologies alters the relationship between actions, skills, and embodiment. Criminologists have long been fascinated with the role of emotions in crime, with the effects prominently factoring into major criminological theories such as rational choice theory, general strain theory, and cultural criminology (Agnew 1992; Ferrell, Hayward and Young 2015: 74; Jacobs and Cherbonneau 2017). Thus, Zuboff's (1988) analysis holds value for the examination of the emotions experienced during criminal engagements and their relationship to computers.

Both informated and non-informated behaviors can result in intense emotional satisfaction (Katz 1988). One source of satisfaction shared is derived from "playing with the issue of control" (Turkle 1984: 210). For instance, non-informated crimes may involve a quest for adrenaline rushes found by taking risks with one's own health and safety—a pursuit cultural criminologists describe as "edgework" (Lyng 1990). As Ferrell, Hayward, and Young (2015: 74) explained, for edgework, "these skills matter in distinctly dangerous ways, spiraling participants every closer to an edge others can't know … and the more risk one takes, the more polished those skills must become." The kinds of skills one needs to approach the edge are action-centered in nature. For instance, the motorcyclist careening down the highway at 120 miles per hour feels the counters of the road through the machine, responding to the physical feedback while anticipating possible obstacles and other dangers (Lyng 1998). Thrill, requisite skills, embodiment, and situational experiences are inseparable.

However, most informated crimes do not involve putting one's body in danger but deal with the issue of control just the same. This control is not achieved through the demonstration of action-oriented skills but through intellective mastery. For instance, Steinmetz (2016) described how hackers might derive intense pleasure in their activities from achieving flow—a psychological state of engrossment in one's activities where time loses meaning (Csikszentmihalyi 1975; Hayward 2004). Accomplishing a task from this flow state can result in an intense feeling of satisfaction, euphoria, or excitement. Importantly, the ability to achieve flow is directly connected to the level of skill one has in the activity (Csikszentmihalyi, Abuhamdeh, and Nakamura 2005). In this manner, the informating qualities of computers directly affect the relationship between crimes, emotions, physicality, and skills. The distinction is not to suggest that embodiment does not matter (Brown 2006); a hacker's pulse may elevate and sweat may dribble down their back as they accomplish a hack. Instead, the argument is that the embodied element of emotions is separate from physical performance and action-centered skills.

The Distance Between Symbol and Reality

The final contribution of a Zuboffian approach to the study of computers and crime explored in this analysis concerns Zuboff's (1988: 84) argument that the informating qualities of computers coincides with a perceived distance between "symbol and reality"—that the abstraction occurring through an informating medium creates a perceptual disconnect between what is experienced by the end user of the system and the action context. For instance, in the computer-focused brewery, the worker no longer feels the heat of the machines, hears the singing of the pipes, or feels the strain of their muscles as they move materials and handle tools (Zuboff 1988: 62-63). The immediacy of their labor is intercepted by the informating machine. While it is perhaps an obvious point now for most computer users, such a disconnect is important to bear in mind as an important part of what a computer does—it *mediates*, but it does so imperfectly. It does not communicate the arrangement of stimuli one might encounter in the physical world but instead converts such data into a more narrowly defined set of outputs, typically textual or graphical representations.

While computer output capabilities are improving, they have yet to mirror the embodied sensations of non-computer-mediated experiences. Of course, the distancing effects of computers and the internet is not an observation unique to Zuboff. It is effectively a truism that while electronic communications can connect people across vast spaces instantaneously, the dromoscopic dimensions of the medium (that the fullness of experience diminishes with acceleration) can also create a profound perceived social distance between individuals (McGuire 2007; Meyrowitz 1997; Virilio 1984). The contribution of Zuboff (1988) is that this social distance is a fundamental by-product of the informating qualities of computers.

The distance between symbol and reality has important implications for crime and victimization. Essentially, the offender of informated crimes is deprived of the (sometimes visceral) immediacy of their actions (Suler 2004). The informated burglar does not hear the glass shatter as they walk in the door, feeling its crunch beneath their feet as they step over the vestibule. They do not smell the prior meals lingering in the kitchen. They also do not see framed photos of smiling faces and family vacations. The immediacy of the situation may affect the sensations experienced, but it may also illuminate the fact that they are ultimately affecting people. For the informated burglar, victims are often reduced to text on a screen, reducing possible feelings of guilt for any transgressions. Thus, computers encourage a kind of alienation that disconnects the criminal laborer from their target in ways that significantly affect the experiences of the perpetrator (Marx 1967). Further, the disconnect affects the experiences of victimization by abstracting the perpetrator and obfuscating the nature of the crime, though that disconnect does not diminish the potential harm such crimes can cause (e.g., Cross, Dragiewicz, and Richards 2018).

Conclusion

Zuboff's (1988) work illuminates foundational elements of computers and work that are all too easily taken for granted in the information society. In such vertiginous times, adopting an "attitude of strangeness" is necessary to find common ground on which scholars can orient themselves when grappling with a disorienting subject matter (Neuman 2007: 284; Young 2007). A Zuboffian approach provides a foundation for such an attitude that, as detailed here, stands to make important contributions to the study of computers and crime.

Specifically, the Zuboffian approach makes it clear that computer crimes are not a distinct type of crime. Instead, criminologists should be more concerned about the extent to which criminal acts are informated or mediated via computers. Further, the informating capacity of computers affects several factors pertinent to criminological inquiries, including the type of skills necessary for crime commissions, depending more on intellective rather than action-centered skills. Further, the degree of intellective skills required depends significantly on the *centrality* of computers to crime commissions, the *availability* of computers to the criminal, and the perpetrator's *engagement* with technology.

This analysis has also demonstrated that the informating machine and its corresponding intellective skills bear direct implications for other prominent areas of criminological inquiries. First, the role of computers

and intellective skills in criminal learning and subcultural dynamics were considered. Second, Zuboff's (1988) insights were also applied to the emotional experiences of crime, useful because many criminological theories consider emotions important for explaining criminality. Finally, the analysis explored the distance between symbol and reality introduced by computers, a gap of significance for the study of perceptions of criminal acts, victims, and offenders, as well as the role of shame or guilt. In this sense, the variegated influences of computers on crime can all be traced back to the defining characteristic of computers—that they are informating machines.

A key utility of approaching cybercrime issues as informated criminal labor is that such an approach provides a focal point for connecting the individual to the situational and the structural. For example, this analysis lends itself readily to a broader consideration of the role of technology and crime within the machinations of contemporary information capitalism. Future criminological analyses can trace the connections between informated labor, intellective skills, and the increasing industrialization and professionalization of cybercrime activities (Banks 2018; Dyer-Witheford 1999; Huws 2014; Lusthaus 2018). Alternatively, Zuboff's ideas can be used to inform examinations of computerized work and institutions of social control. Indeed, Zuboff (2019) herself has been engaged in such work in her recent book *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* Similarly, such an approach may be useful for the burgeoning field of digital criminology by helping draw connections between the essential elements of informated illicit labor, digital society, or "fundamental nature of the technological, structural, and social changes in the contemporary society in which we live" and technosociality or "the processes, cultures and practices that characterize our day-to-day lives" (Powell, Stratton, and Cameron 2018: 4). As such, detailing the essential dimensions of the relationship between computers and labor provides a fruitful avenue for examining the intersection of structure, situation, and agency regarding computers and crime.

Relatedly, the applications of Zuboff's (1988) work can be useful for understanding the role of social stratification in the perpetration of informated crimes as well as their associated forms of victimization. One's position vertically or horizontally within social hierarchies may affect the availability of access to information technology and opportunities to develop and display intellective skills. For instance, while not explicitly detailed in her work, other scholars have noted that Zuboff's (1988) approach may be useful for understanding the connections between gender, technology, and work—conclusions that might be extended to examine gender disparities in informated crimes (Halberstam 1991: 457-458). There also exists ample room to consider how social class, race, and ethnicity differentially affect involvement in informated and non-informated crimes considering the "digital divide" that exists in the United States and other countries regarding technology and training access (Hill 2001; Pontell and Rosoff 2009; Steinmetz 2016).

The objective of this analysis was to demonstrate the value of Zuboff's insights to criminological inquiry. In doing so, it has highlighted how the identification of the essential qualities of computerized labor can have ripple effects across many domains of criminological inquiries. Thus, future criminological research and theorizing would be well-served by using these ideas as a central mooring point for understanding the relationship between computers and crime moving forward.

Correspondence: Kevin Steinmetz, Department of Sociology, Anthropology, and Social Work, Kansas State University, Manhattan, KS 66506, United States. kfsteinmetz@ksu.edu

[1] While her arguments can be construed in this manner, Zuboff (1988) is not a "technological determinist" because she has recognized that the social and technical interplay reciprocally, reflecting what is commonly referred to as the "technosocial" (Davis 1990: 285; Powell, Stratton and Cameron 2018).

[2] Though not explicitly stated, the process Zuboff (1988) used to arrive at the defining characteristic of computers mirrors the phenomenological process of eidetic reduction whereby an object's defining essence or eidos is determined (Palermo 1978).

[3] In most cases, Zuboff has appeared to use "information technology" in a way that is interchangeable with "computers." Such usage may create confusion for people who consider the two to be related by separate concepts.

[4] Furnell (2017) himself has considered how the distinction between "computer-assisted" and "computer-focused" crimes becomes blurred when the motivations of the criminal are considered and the shared vectors that both crimes might employ, like email. For him, the distinction rests upon "the means of attack, rather than the motivation and intended outcome" (Furnell 2017: 67). The approach adopted in this analysis, however, is that the defining characteristic of a crime is the action context—what the crime ultimately does.

[5] Though it is beyond the scope of this analysis, it is worth noting the role of social advantage or class in the perpetration of informated variants of crime like computer hacking; one needs access to technology and time to develop such skills, which is made easier if one is a member of the middle- or upper-classes (Pontell and Rosoff 2009; Steinmetz 2016).

[6] McGuire (2020) likely provided the most robust overview to date regarding the litany of definitional issues surrounding computer crimes and should be a go-to source for scholars in the area.

[7] The phrase "symbolic closeness" was derived from Turkle's (1984: 178) description of computer work in machine language as "the closeness of the contact is symbolic—you are talking the only language that the machine can 'understand' directly."

References

Agnew R (1992) Foundation for a general strain theory of crime and delinquency. *Criminology* 30(1): 47-88. https://doi.org/10.1111/j.1745-9125.1992.tb01093.x

Banks J (2018) Radical criminology and the techno–security–capitalist complex. In Steinmetz KF and Nobles MR (eds) *Technocrime and criminological theory*: 102-115. New York: Routledge.

Braverman H (1974) *Labor and monopoly capital: The degradation of work in the twentieth century.* New York: Monthly Review Press.

Brown S (2006) The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology* 10(2): 223-244. https://doi.org/10.1177%2F1362480606063140

Brey P (2017) Theorizing technology and its role in crime and law enforcement. In McGuire MR and Holt TJ (eds) *The Routledge handbook of technology, crime and justice*: 17-34. New York: Routledge.

Burgess RL and Akers RL (1966) A differential association-reinforcement theory of criminal behavior. *Social Problems* 14(2): 128-147. https://psycnet.apa.org/doi/10.1525/sp.1966.14.2.03a00020

Cross C, Dragiewicz M and Richards K (2018) Understanding romance fraud: Insights from domestic violence research. *British Journal of Criminology* 58(6): 1303-1322. https://doi.org/10.1093/bjc/azy005

Csikszentmihalyi M (1975) *Beyond boredom and anxiety.* San Francisco: Jossey-Bass Publishers.

Csikszentmihalyi M, Abuhamdeh S and Nakamura J (2005) Flow. In Elliot AJ and Dweek CS (eds) *Handbook of competence and motivation*: 598-608. New York: Guildford Press.

Davis A (1990) Zuboff, Shoshana 1998: In the age of the smart machine, the future of work and power. New York: Basic Books [Book Review]. *Review of Radical Political Economics* 22(2-3): 285-287. https://doi.org/10.1177%2F048661349002200215

Dupont B, Côté A-M, Boutin J-I, and Fernandez J (2017) Darkode: Recruitment patterns and transactional features of "the most dangerous cybercrime forum in the world." *American Behavioral Scientist* 61(11): 1219-1243. https://doi.org/10.1177%2F0002764217734263

Dyer-Witheford N (1999) *Cyber-Marx: Cycles and circuits of struggle in high-technology capitalism.* Chicago: University of Illinois Press.

Fagan J and Freeman RB (1999) Crime and work. *Crime and Justice* 25: 225-290. https://www.journals.uchicago.edu/doi/abs/10.1086/449290

Ferrell J, Hayward KJ and Young J (2015) *Cultural criminology: An invitation*. 2nd ed. Los Angeles: SAGE Publications.

Furnell S (2002) *Cybercrime: Vandalizing the information society*. London: Addison-Wesley.

Furnell S (2017) The evolving landscape of technology-dependent crime. In McGuire MR and Holt TJ (eds) *The Routledge handbook of technology, crime and justice*: 65-77. London: Routledge.

Giddens A (1990) *The consequences of modernity.* Stanford: Stanford University Press.

Goldsmith A and Brewer R (2015) Digital drift and the criminal interaction order. *Theoretical Criminology* 19(1): 112-130. https://doi.org/10.1177%2F1362480614538645

Gottfredson MR and Hirschi T (1990) *The general theory of crime*. Stanford: Stanford University Press.

Halberstam J (1991) Automating gender: Postmodern feminism in the age of the intelligent machine. *Feminist Studies* 17(3): 439-460. https://doi.org/10.2307/3178281
Harvey D (2014) *Seventeen contradictions and the end of capitalism*. New York: Oxford University Press.
Hayward K (2004) *City limits: Crime, consumer culture, and the urban experience.* New York: Taylor and Francis.
Hill L (2001) Beyond access: Race, technology, community. In Nelson A, Tu TLN, and Hines AH (eds) *Technicolor: Race, technology, and everyday life*: 13-33. New York: NYU Press.
Holt TJ (2010) Examining the role of technology in the formation of deviant subcultures. *Social Science Computer Review* 28(4): 466-481. https://doi.org/10.1177%2F0894439309351344
Holt TJ (2013) Examining the forces shaping cybercrime markets online. *Social Science Computer Review* 31(2): 165-177. https://doi.org/10.1177%2F0894439312452998
Holt TJ and Bossler AM (2014) An assessment of the current state of cybercrime scholarship. *Deviant Behavior* 35(1): 20-40. https://doi.org/10.1080/01639625.2013.822209
Holt TJ, Smirnova O and Hutchings A (2016) Examining signals of trust in criminal markets online. *Journal of Cybersecurity* 2(2): 137-145. https://doi.org/10.1093/cybsec/tyw007
Hough M (1987) Offenders' choice of target: Findings from victim surveys. *Journal of Quantitative Criminology* 3(4): 355-369. https://doi.org/10.1007/BF01066836
Huws U (2014) *Labor in the global digital economy: The cybertariat comes of ages.* New York: Monthly Review Press.
Jacobs BA and Cherbonneau M (2017) Nerve management and crime accomplishment. *Journal of Research in Crime and Delinquency* 54(5): 617-638. https://psycnet.apa.org/doi/10.1177/0022427817693037
Katz J (1988) *Seductions of crime: Moral and sensual attractions in doing evil.* New York: Basic Books.
Latour B (2005) *Reassembling the social: An introduction to actor-network-theory*. New York: Oxford University Press.
Letkemann P (1973) *Crime as work*. Englewood Cliffs: Prentice-Hall.
Levy S (1984) *Hackers: Heroes of the computer revolution*. London: Penguin.
Lusthaus J (2018) *Industry of anonymity: Inside the business of cybercrime*. Cambridge: Harvard University Press.
Lyng S (1990) Edgework: A social psychological analysis of voluntary risk taking. *American Journal of Sociology* 95(4): 851-886. https://psycnet.apa.org/doi/10.1086/229379
Lyng S (1998) Dangerous methods: Risk taking and the research process. In Ferrell J and Hamm MS (eds) *Ethnography at the edge: Crime, deviance, and field research*: 221-251. Boston: Northeastern University Press.
Manaugh G (2016) *A burglar's guide to the city*. New York: Farrar Straus Giroux.
Marx K (1867/1967) *Capital: a critique of political economy*. Vol 1. New York: International Publishers.
McGuire MR (2007) *Hypercrime: The new geometry of harm*. Milton Park: Routledge-Cavendish.
McGuire MR (2018) Cons, constructions misconceptions of computer related crime: From a digital syntax to a social semantics. *Journal of Qualitative Criminal Justice & Criminology* 6(2): 1-27. https://doi.org/10.21428/88de04a1.505d151e
McGuire MR (2020) It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime. In Leukfeldt R and Holt TJ (eds) *The human factor of cybercrime*: 3-28. London: Routledge.
Meyrowitz J (1997) Shifting worlds of strangers: Medium theory and changes in "them" versus "us." *Sociological Inquiry* 67(1): 59-71. https://doi.org/10.1111/j.1475-682X.1997.tb00429.x
Neuman WL (2007) *Basics of social research: Qualitative and quantitative approaches*. 2nd ed. Boston: Pearson Education.
Noble DD (1991) In the cage with the smart machine. *Science as Culture* 2(1): 131-140. https://doi.org/10.1080/09505439109526296
Palermo J (1978) Apodictic truth: Husserl's eidetic reduction versus induction. *Notre Dame Journal of Formal Logic* 19(1): 69-80. https://doi.org/10.1305/ndjfl/1093888208
Pew Research Center (2019). Mobile fact sheet. https://www.pewresearch.org/internet/fact-sheet/mobile/
Pontell HN and Rosoff SM (2009) White-collar delinquency. *Crime, Law and Social Change* 51(1): 147-162. https://doi.org/10.1007/s10611-008-9146-0
Powell A, Stratton G and Cameron R (2018) *Digital criminology: Crime and justice in digital society*. New York: Routledge.
Rainie L and Wellman B (2012) *Networked: The new social operating system.* Cambridge: MIT Press.
Reagle J (2016) The obligation to know: From FAQ to feminism 101. *New Media & Society* 18(5): 691-707. https://doi.org/10.1177%2F1461444814545840
Steinmetz KF (2016) *Hacked: A radical approach to hacker culture and crime*. New York: NYU Press.
Suler J (2004) The online disinhibition effect. *CyberPsychology & Behavior* 7(3): 321-326. https://psycnet.apa.org/doi/10.1089/1094931041291295
Sutherland EH (1937) *The professional thief*. Chicago: University of Chicago Press.
Sutherland EH, Cressey DR, and Luckenbill D (1995) The theory of differential association. In Herman NJ (ed) *Deviance: A symbolic interactionist approach*: 64-68. Lanham: Rowman & Littlefield Publishing Group.

Taylor PA (1999) *Hackers: Crime in the digital sublime*. London: Routledge.
Tobias MW (1971) *Locks, safes, and security: A handbook for law enforcement personnel*. Springfield: Charles C. Thomas Publisher.
Turkle S (1984) *The second self: Computers and the human spirit*. New York: Simon and Schuster.
van der Wagen W (2018) The cyborgian deviant: An assessment of the hacker through the lens of actor-network theory. *Journal of Qualitative Criminal Justice & Criminology* 6(2): 1-24. https://doi.org/10.21428/88de04a1.6a5d95c2
van der Wagen W and Pieters W (2015) From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks. *British Journal of Criminology* 55(3): 578-595. https://doi.org/10.1093/bjc/azv009
Virilio P (1984/2005) *Negative horizon: An essay in dromoscopy*. Degener M (trans). New York: Continuum.
Wall DS (2007) *Cybercrime: The transformation of crime in the information age.* Malden: Polity Press.
Wall DS (2008) Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology* 22(1-2): 45-63. https://doi.org/10.1080/13600860801924907
Wright R and Decker SH (1994) *Burglars on the job: Streetlife and residential break-ins*. Boston: Northeastern University Press.
Yar M and Steinmetz KF (2019) *Cybercrime and society*. 3rd ed. Los Angeles: SAGE Publications.
Young J (2007) *The vertigo of late modernity.* Los Angeles: SAGE Publications.
Zittrain J (2008) *The future of the internet and how to stop it*. New Haven: Yale University Press.
Zuboff S (1985) Automate/informate: The two faces of intelligent technology. *Organizational Dynamics* 14(2): 5-18. https://psycnet.apa.org/doi/10.1016/0090-2616(85)90033-6
Zuboff S (1988) *In the age of the smart machine: The future of work and power*. New York: Basic Books.
Zuboff S (2019) *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: Public Affairs.