Technology-enabled Crime, Policing and Security

Sam McQuade

Abstract

Crime, policing and security are enabled by and co-evolve with technologies that make them possible. As criminals compete with security and policing officials for technological advantage perpetually complex crime, policing and security results in relatively confusing and therefore unmanageable threats to society. New, adaptive and ordinary crimes emerge over time to create technology crime waves, the magnitude of which can theoretically be measured, compared and predicted. These principles underscore a new theory of technology-enabled crime, policing and security pertinent for understanding contemporary threats posed by emerging forms of cybercrime, transnational crime and terrorism networks that defy traditional methods criminal justice and security measures for preventing and controlling crime.

Introduction

Few things are as fundamental to human history and ongoing development of society as technology. Readers of this article know full well that technology may be variously conceptualized, categorized and defined; is ubiquitous and serves seemingly infinite purposes; and evolves in its design, engineering, materials, components, manufacturing processes, adoption, implementation, systems integration and diffusion. When coupled with science, which in its broadest meaning denotes systematized learning across scholarly fields of research, technology and the interactive forces which make these possible (e.g., imagination, processing of raw materials, economics, and political processes) accommodate human preferences and enable societal functions in astounding ways. It is also well understood that synergistic science and technology may result in good or evil as determined by how they are used in relation to social norms, ethics and laws. Hence, the notion that technology has always and inevitably been used for socially abusive or criminal purposes as determined through processes of social construction and thereafter (hopefully) arrested via the administration of justice when not prevented is not surprising. Indeed this is expected and generally regarded as the way in which technology functions in and affects society.

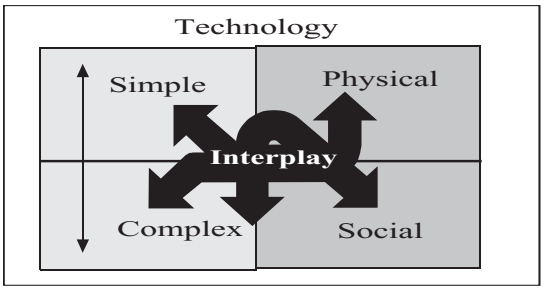
Given the obvious role that technology has in the enablement and evolution of crime, and in countervailing policing and security functions of society, it is surprising however, that criminologists who have long sought to explain causes and correlates of crime and corresponding victimization have not significantly considered technology-related principles, processes and theories. Theories of the Classical School of criminology for example, examined 18th-century legal structures and criticized arbitrarily-designated criminal behavior and punishment imposed without regard for human rights, justice, or fairness (Williams and McShane, 1993) but did not consider the theoretical role of technology in crime. Similarly, 19th-century Positive School theories ignored the role of technology even when considering criminal behavior, "use of scientific methodology, assumption of pathology, classification of criminal types, prediction of criminality, and treatment of criminals" (Williams & McShane, 1993). And while Sutherland's (1947) Differential Association Theory identified simple-to-complex techniques as an aspect of criminal learning processes later specified by Akers along with other scholars (see e.g., Akers 1998; 1985; Burgess & Akers, 1966; Burgess et al., 1966), even as Cohen and Felson (1979) referenced technology when observing that crimes are more likely to be committed by motivated offenders who have suitable targets in the absence of capable guardians, no unifying theory about criminal use of technology, and countervailing use of technology for policing and security purposes, has been developed. This paper contributes to that process.

Physical and Social Technology Interplay

Technology can be defined as the application of hard and/or soft science knowledge, methods, and materials to practice arts and skills. This definition implies a distinction between hard "physical technologies" and soft "social technologies." Whereas physical technologies are tools enabling accomplishment of tasks, social technologies are methods or techniques which pertain to how human activities, behaviors, and interactions occur. Physical and social technologies range from being simple-to-complex, and

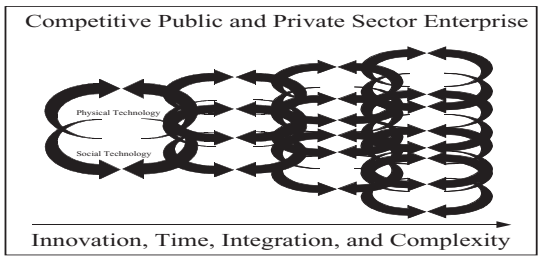
complexity often has to do with the number of components or systems involved in technological functions or processes. As used here, complexity refers to the use of technology which cannot be explained by an investigative or security expert to similar experts across time and distance. This operationalization is adapted from the original definition developed by Kash and Rycroft (1997) to address complex technology-related issues and processes in organizational settings. In practice technologies are used conjunctively. It is also notable that both physical and social technologies facilitate research and theory-building in the hard and social sciences such as criminology. As shown in Figure 1, combinations of interplay between simple-to-complex physical and social technologies that enable knowledge-building and other human accomplishments are conceivably infinite with respect to inputs, processes, outputs and outcomes. Complete technology intertwining, and thus maximum complexity, occurs as all parties involved concurrently employ myriad technologies which combine components, systems, interactive processes and effects to defy understanding among experts. Over time complexity diminishes as the uses and effects of technology are better understood and become more manageable.

Figure 1. Dynamic intertwining and substitution of simple to complex, physical and social technologies. Perpetually Complex Technology-enabled Competition



When technologies establish reliability they tend to be adopted. This is because human enterprises generally seek to improve, and because nobody likes to get worse at anything. Even those persons or organizations preferring to remain static in their use of technology may be forced to adapt to market or other forces, and thereby adopt new tools or processes. "Perpetual innovation" (Kash, 1989; Kash and Rycroft, 1996) is a concept pertaining to synthetic analysis of tacit knowledge and skills residing in individuals, groups and organizations that enable continual discovery and adoption of new tools and techniques. Essentially, it is the notion that people involved in competitive enterprises are always trying to do things just a little bit better. Perpetual innovation applies to the interplay of physical and social technologies used by public and private enterprises operating in competitive environments. Perpetual improvement of products and services developed within organizational environments may lead to new discoveries, spin-off inventions and innovation of these. Hence, combinations of tools and techniques may be transformed into new technologies in their own right. The overall effect is creation of invention-to-obsolescence cycles in which physical and social technologies become more integrated and complex with time as shown in Figure 2.

Figure 2. Perpetual innovation-to-obsolescence cycles



Note that new technologies designed to achieve competitive advantage may constitute state and/or trade secrets, each having crime-related competitive implications (e.g., development or acquisition of weapons of mass destruction by terrorist organizations and/or theft of proprietary information by corporations). Thus, as previously acknowledged, new technologies are adopted for illicit purposes as well as countervailing policing and security purposes. Further, although perpetual innovation is intended to improve matters such as organizational processes, products, services, and profits etc., actual improvements are often unclear or subjective. Not everyone agrees for example, that a new gadget or way of doing things is better, or that these will result in greater benefits when compared to costs at the level of the organization much less within broader society. At the time of its adoption, a given technology might be just too complex to understand or operate, or not cost effective given extant states of research and development in varying scientific, technological, organizational, economic, and political environments. Even if technology is affordable to develop, adopt, implement and master by personnel involved it may nonetheless result in more harm than good and be considered economically inefficient in the grand scheme of outcomes. And

because perpetual innovation only and necessarily occurs under conditions of competition, winners and losers will eventually emerge unless a technological balance is struck and maintained among competitors. For this to occur, all parties involved must believe that achieving technological advantage is either futile or undesirable, and that their would-be opponents are not secretly trying to resurrect or invent new threatening capabilities. Crime versus policing and security are inherently competitive and distrusting enterprises, and there is nothing novel about these technology-related principles, although considering them explicitly in theoretical terms as integral aspects of crime, policing and security is long overdue.

Technology as Crime, Policing and Security

Cunning criminals have always taken advantage of new technologies often as the result of learning how to do so from other people including fellow criminals. Periodically they experiment with existing tools or techniques in order to develop a satisfactory *modus operandi* with which they are comfortable and believe gives them reasonable advantages over the security technologies of intended targets, as well as police who may be prowling about physical and cyber environments for signs of crime. Upon establishing their M.O., successful criminals are disinclined to change either their preferred tools or techniques, although on rare occasions enterprising criminals may concoct new ways in which to commit their illicit activities. As a natural byproduct of perpetual technology innovation and criminal adoption and adaptation, methods of committing crime can change at the societal level. Thus crime consisting of myriad methods of gaining technological advantage for illicit purposes can be conceived of as social technology with its own innovation-to-obsolescence cycles. Graycar and Grabosky for instance, referred to the evolution of the technology of money laundering (1996, p. viii). Today we are also witnessing systemic changes in the technological nature and technology-enabled organization of transnational crime networks, terrorist cell operations, and cybercrimes.

Crime as social technology will almost always involve use of physical technologies (i.e., tools), although rape, assault, and murder committed without the use of weapons or other instruments such as those used to penetrate body cavities are notable exceptions. Conceiving of crime as social technology incorporating use of physical technologies allows for construction of a matrix similar to that used by Kash and Rycroft (1997), but differentiating as depicted in Figure 3 between: (1) simple crime committed using simple tools; (2) simple crime committed using complex tools; (3) complex crime committed using simple tools; and (4) complex crime committed using complex tools. As indicated above, complex crime occurs to the extent combinations of relatively complex physical and social technologies are employed.

Just as various types of crime (e.g., money laundering) can be considered a social technology, so can various methods of policing.

Figure 3. Simple-to-complex crimes committed with simple-to-complex tools.

1. Simple Crime Committed Using Simple Tools	3. Complex Crime Committed Using Simple Tools
Single suspect using a manual instrument to unlawfully threaten, harm, damage, or gain entry to a vehicle or structure.	Traditional racketeering, vice, and corruption using relatively simple physical technologies.
2. Simple Crime Committed Using Complex Tools	**4. Complex Crimes Committed Using Complex Tools**
A marijuana grower who uses a cellular phone and pager to facilitate his own frequent drug sales, and a computer to store digitized records of his transactions, expenses, and income.	Combined drug smuggling, gang violence, and money laundering of victims across multiple jurisdictions using a variety of digital devices to generate, transmit, and store encrypted crime-related information.

Figure 4. Categories, interplay, and examples of simple-to-complex policing methods and physical technology.

A. Simple Policing Using Simple Tools	B. Complex Policing Using Simple Tools
An officer on foot patrol conducting building checks at night with a flashlight.	A community Police officer issuing citizens Neighborhood Block Watch stickers in the course of conducting crime prevention seminares and "hot spot" problem-solving within a community.
C. Simple Policing Using Complex Tools	**D. Complex Policing Using Complex Tools**
Random preventative patrol using a modern, well-equipped police cruiser.	Undercover store-front sting operation using electronic surveillance equipment and GIS tracking technology to investigate cellular phone theft and fraud.

Community policing for instance, often described as a philosophy that emphasizes problem-solving in partnership with community members to enhance crime prevention methods may be conceptualized as a social technology. Obviously security and policing technologies are also physical and range from being relatively simple to complex. Thus, analogous to crime as technology, the interplay of simple-to-complex policing or security methods and tools such as described by the examples in Figure 4 are also social technologies that are bound only by human ingenuity.

Perpetually Complex Crime and Policing

It follows that crime and policing/security co-evolve with technology invented or adapted for these purposes and that as the result of competition in a manner akin to a civilian arms race is limited only by available resources broadly defined (e.g., imagination, knowledge, skills, money, time.). Figures 3 and 4 represent conceptual analogues of crime and policing/security which combine tools and techniques (or methods) into practical functions that are subject to change as new technologies are developed, learned, adopted and implemented by individuals, groups, organizations and even entire regions or societies. Referring only to crime for the moment, we may conceptualize its evolution sequentially and at the micro level of an individual. For example, a young thief might first learn to shoplift using her purse for concealment, and later graduate to stealing from multiple victims using a computer. Thus, and in reference to Figure 3, a Category 1 crime (i.e., simple crimes committed with simple tools) might evolve into Category 2, then into Category 3, and eventually Category 4 crimes with corresponding increases in technological complexity. Figure 3 depicts this interplay and provides an example of hypothetical crime(s) in each category, while Figure 2 depicts technology as intertwining physical and social technologies that may used to commit crime , and thus crime itself being innovated, integrated, and becoming more complex over time.

A more realistic conception of technologically evolving crime would involve all four categories of the matrix in Figure 3 co-evolving with increases in resources coupled with intensity of motive (i.e., the drive) of criminal groups and organizations as well as individuals, and in environments consisting of various levels of policing/security where detection avoidance by criminals is also required. After all, individual criminals and organized networks of criminals use various levels of simple-to-complex technology to commit various types of crimes while learning from one another, all the while also avoiding police and security officers and/or overcoming crime prevention, detection and apprehension technologies.

Some crooks however, may prefer to remain operating in relatively simple ways they deem satisfactory, or they may be incapable of advancing their knowledge and skills beyond a certain level of technological complexity. Collectively

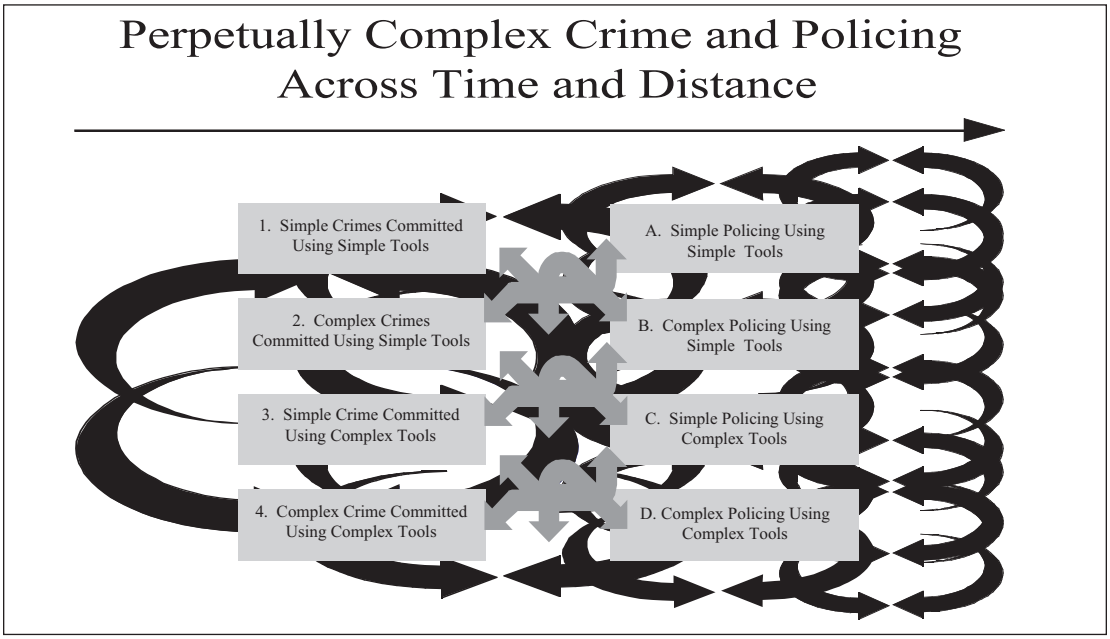
however, competitive society (and therefore, crime as well as policing/security) perpetually innovates even if individual criminals or criminal organizations become static in their own invention, adoption and use of particular technologies. As criminals become more sophisticated in their use of technology, forms of crime committed by them also become increasingly complex and difficult to understand and manage. Thus police and security officials must stay current in their knowledge and understanding of emerging crime, and both well resourced and expert regarding their own technological capabilities.

Crime and policing/security are technologically competitive enterprises that are inextricable, dynamic and co-evolving. Criminal innovations drive policing and security innovations, and by extension each perpetually co-evolves the other throughout time and society. As intentionally shown in the hopelessly complicated Figure 5 below, the gamut of simple-to-complex physical and social technologies used by these enterprises are dynamically intertwined, and they become more complex over time and distance subject to broad social, cultural, political and economic conditions and constraints.

Thus, crime and methods for preventing it via security and policing evolve together as a function of these factors plus human ingenuity. And as crime in a given geographic location or cyber realm emerges in a new way, police and security officials inclusive of technology developers respond accordingly. Who in computerized societies does not continually experience the technological competition surrounding creation and release of malware (i.e., computer viruses, worms, Trojans, spyware and adware) for which firms are continually writing prevention, detection and removal code? Conversely, if security or police officials in a given realm develop new tactics and/or employ new tools, criminals will adjust their activities to reclaim technological advantages. This insidious cat and mouse game may involve considerable financial and other resources, and periodically may also culminate in significant destruction of property, physical injury or even death. But as long as the security officials and police are winning the overall game, there is relatively little cause for alarm. After all, these processes are inevitable — crime, however socially constructed and legislated against, occurs naturally given human nature. Yet, when it comes to preserving a safe, secure and orderly society, security and police forces using their technological capabilities must ultimately triumph over criminals.

What matters most is not the type or amount of crime measured in incidence or prevalence within a given geographic location or cyber realm, rather reasonable innovation and perpetuation of relatively sophisticated security and policing which is capable of deterring, preventing, interdicting, suppressing or otherwise displacing existing capabilities of criminals regardless of the relative complexity of crimes committed. In other words, policing and security officials should stop obsessing with crime rates, and

Figure 5. Dynamic crime and policing technology co-evolution



with the help of researchers, develop practical ways in which to measure how level the playing field really is. This requires systematic rethinking, education, training, equipping, and organizing of police and security forces to some extent so that they may continually anticipate and recognize crime threats, and then formulate and implement forward-looking prevention and control strategies consistent with their resource limits.

Happily, in the game of perpetually complex crime and policing/security, the "good guys" (and girls!) usually have many advantages. For example, they are generally well trained, equipped, and organized, and they often lend interagency assistance and work in inter/multi-agency task forces in order to address complex crime problems, etc. Historically, the Federal Government has created huge new policing and security organizations in order to address emerging technology-enabled crime problems. For example, in 1909 a new unit officially named the Bureau of Investigation as the FBI was then known began investigating emerging interstate prostitution under authority granted by the White Slave Traffic (Mann) Act. This is how the Federal Government became involved in policing organized interstate crime which, until onset of the automobile combined with ubiquitous long distance telephone service, was conceived of in the press and by the public as merely local crime.

Following the terrorist attacks of September 11, 2001, against the World Trade Center towers and Pentagon, Congress acted with unprecedented speed to authorize creation of the new Department of Homeland Security to combat, prevent, and interdict terrorism in all its forms in concert with intelligence and military components of the federal government, as well as in cooperation with state and local policing agencies and private sector security firms. Problems arise however when during the emergence of new forms of crime, security and police capabilities within society loose their competitive advantage. On this point there is no substitute for informed and supportive policy makers who are willing in the midst of uncertainty (i.e., lack of understanding about complex crime problems) to make fiscal investments and pass adequate crime legislation before the onset of crises. The danger lies in providing police with too little technology relative to crime-fighting needs, or with too much technology relative to adequate controls on their power.

Ordinary, Adaptive, and New Forms of Crime

Since crime is technologically dynamic and can become increasingly complex over time and distance in accordance with supporting resources such as money or culture versus constraining factors such as lack of money or culture, it is useful to categorize the evolution of perpetual innovation as it applies to potential crime and security breaches in three ways, each denoted with a technical term. *Ordinary crimes* are conventional. They routinely occur in many places, are recognized and well understood in their variations, and are actively prevented, investigated, and prosecuted. A clear indication that crime is ordinary is the existence of statutes defining criminal behavior, an accompanying body of case law to reference when developing prosecution strategies and making arguments before a court, and police or security record-keeping systems which track frequency and location of occurrences. For example, all crimes tracked by the FBI's Uniform Crime Reporting (UCR) system are, technologically speaking, ordinary crimes (e.g., common varieties of theft, burglary, and robbery).

Adaptive crimes are new technological variations of ordinary crime. They are manifested through incremental and innovative use of technology. As such they subsume one or more existing forms of crime or security threats, and they occur relatively frequently even though they may not initially constitute legally defined criminal behavior. As such, adaptive crime can be prosecuted in its essence under existing crime legislation supported by a body of case law albeit with varying precision and success. It may not be necessary to prosecute technologically adaptive crimes via an untested legal strategy because adequate statutory and case law will afford clear authority if not ample precedence based on similar case facts.

New crimes involve radical innovative use of technology to commit an act of social abuse which is not necessarily illegal at the time of first occurrence. Truly new forms of social abuse (i.e., new crimes) happen rarely and may initially go undetected or even unrecognized because police and security officials will typically have little or no training and no basis of experience to understand what is happening. Since new crime does not conform to broader social experiences it seems mysterious and complex to other government officials, the media and members of the

public. Mysterious because it is not understood; complex because it may: (a) involve relatively complicated technologies; (b) involve many suspects, victims, and considerable amounts of harm and/or loss; (c) subsume varieties of ordinary and/or adaptive crime; (d) not be explainable by investigative experts to other investigative experts across time and distance sufficiently to formulate prevention and control strategies; (e) generate intensity in the form of public outrage not only against the act and its perpetrators, but also against police or security officials for not responding adequately to the crime or security threat; and (f) diffuse at varying rates across many geopolitical jurisdictions or cyberspace. New crimes cause considerable public amazement, perhaps even shock, disbelief, and/or outrage once they are discovered. They are also often labeled in sensational albeit confusing terms such as "data rape" (Szwak, 1995). Such terms are often created by the media which understandably is always seeking something new to report and thereafter create headlines to promote profits through direct sales of publications or advertising of air time. While new crimes are socially abusive, because they are not initially defined as being criminal, the consummate act (or significant portions thereof) may be extremely difficult if not impossible to prosecute. For instance, many states and the federal government were unable to successfully prosecute early computer abuse. Even prosecution of Robert Morris Jr. for his releasing of the first Internet worm in 1988 was difficult under the then newly passed Computer Fraud and Abuse Act. Today however, the federal government and all fifty states have at least one and in many cases several specific computer crime laws under which cybercriminals can be prosecuted for specific acts.

Obviously new crimes via the copycat crime phenomena (Pease & Love, 1984) become adaptive crime and eventually ordinary crime. Table 1 distinguishes between the three stages of crime evolution with respect to their occurrence, innovative use of technology, social cognizance (i.e., observe-ability and understanding), and legal sanctions. Note that the suicidal terrorist airliner bombings of September 11, 2001, may be considered examples of new crime because although the crime itself, murder, previously existed, the technological means (crashing hijacked airliners into buildings) involved radical innovation, societies (not limited to the United States) did not immediately comprehend the nature of the terrorist threat, and there existed no specific crime laws against the consummate act of hijacking an aircraft in order to simultaneously commit suicide, mass murder and incredible amounts of property damage for political or religious purposes. Similarly, in 1971 when bomb-strapped D. B. Cooper commandeered a Northwest Airlines 727 in Portland, commanded it to land in Seattle, and thereafter parachuted (possibly to safety) over the Columbia River gorge on the border of Washington and Oregon, there existed no term or label, much less a crime law against hijacking. Obviously that all changed as Cooper's original form of social abuse was copied and modified technologically to become adaptive crime and eventually ordinary crime committed by terrorists. Note that although hijacking incidents were always extremely serious and upsetting, they eventually occurred with sufficient frequency that they were not featured by many media sources as sensational events.

Table 1. Aspects and examples of ordinary crime, adaptive crime, and new crime.

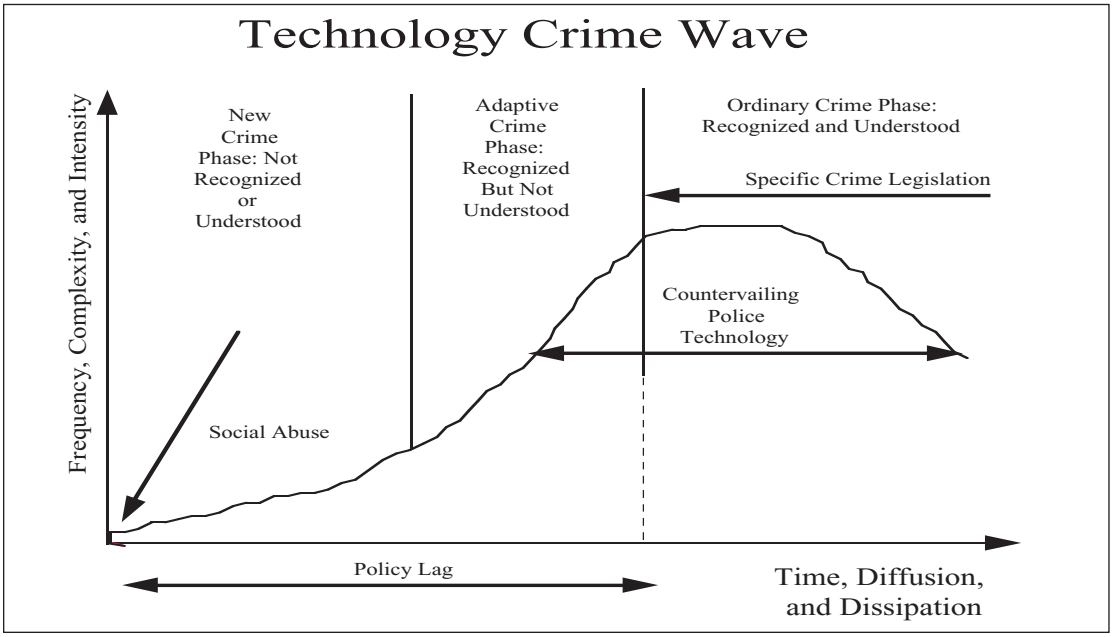
Feature/ Crime Type:	Occurrence	Use of Technology	Social Cognizance	Legal Sanctions and Prosecution Strategy	Contemporary Examples
Ordinary Crime	Routinely	No innovation	Recognized and well understood	Clearly violates existing crime law	Common theft, burglary, etc.
Adaptive Crime	Relatively frequently	Incremental innovation	Recognized but not well understood	Violates existing laws in some respects and does not require innovative prosecution	Releasing a new computer virus onto the Internet
New Crime	Rarely	Radical innovation	Not widely recognized and not understood	Consummate act does not violate existing laws; Impossible to prosecute as an explicit overarching criminal offense	Human Molotov missiles of Sept. 11, 2001

Criminal Purposes and Technology Crime Waves

People who commit crime use technology for ten core technology-enabled purposes: surveillance, planning/record-keeping, communication, transportation, coercion, protection, concealment, value storage, to inflict harm and to expand their operations. These purposes should not be confused with legal intent or personal motives for committing crime, which are different. Whenever radical new and socially abusive use of technology occurs for any of these core purposes, new crime emerges. When an increasing minimum (and arbitrary) number of the same kind of new crime occurs within a certain period of time (e.g., seven slight variations of a new crime within thirty months) a new *technology crime wave* begins to form (see Figure 6). Such waves occur periodically, strike across geopolitical jurisdictions and with varying levels of force, and spread and dissipate at rates inversely related to development of countervailing understanding and implementation of security and policing technologies. Other factors including social, cultural, economic and political conditions, coupled with media attention and perhaps other forces may also contribute to the spread or dissipation of a technology crime wave. Here also, do not confuse the concept of a technology crime wave with the conventional expression "crime wave" which typically refers to a rash of similar crimes in a particular location (e.g., a rash of burglaries in a neighborhood). In contrast, a technology crime wave comes about as the result of unique technology abuse that is not understood rather than numbers of conventional crimes. The time period between the emergence of a new crime and development and implementation of countervailing security and police technologies as signaled by formulation of crime legislation prohibiting the consummate illegal act represents policy development and implementation lag time.

As shown in Figure 6, technology crime waves always begin with an original incident of unusual social abuse and increase in the frequency of technologically similar incidences over time. As the number of similar and still-unusual incidents increase, the intensity of the emerging wave (i.e., social concern, disdain, or outrage surrounding radical innovative use of technology for abusive purposes) also increases. In the long term, three technology stages each corresponding to cognitive phases further corresponding to the continuum of new crime, adaptive crime, and ordinary crime results. Each of these stages/phases varies in duration depending on the number and frequency of incidences, complexity of technology involved, intensity generated, and rate of diffusion and dissipation. Like waves in the ocean, technology crime waves start small and develop more energy, travel at different rates, overlap, and collide. In the real world, multiple smaller waves exist within larger waves, such that only general wave patterns are measurable. Figure 6 depicts how a single technology crime wave originates with social abuse, forms into a new form of crime, picks up energy via copycatting becoming adaptive crime, and

Figure 6. Technology crime wave



eventually transforms into ordinary crime as security, policing, prosecution and other forces for law and order prevail.

Research exploring the nature of technology crime waves could contribute to criminology and to criminal justice and security policies and practices involving technology invention, innovation, adoption, procurement, implementation, routine use and diffusion. As a point of departure it may be useful to determine how different technology crime waves defined on the basis of core criminal purposes and simple-to-complex tools and techniques used by criminals for innovative purposes vary initially and over time and distances. Determining the magnitude of a technology crime wave relative to various contributing and constraining factors, and under varying circumstances which combine to affect its emergence and dissipation would be extremely challenging. How technologically complex is a given type of crime? The answer matters because crimes which are complex relative to security and policing understanding and technological capabilities are less manageable. Thus, determining the extent to which new forms of technology-enabled social abuse and crime are more complex, less manageable and also potentially harmful to society is useful from the standpoint of allocating security and policing resources.

To this end consider that estimates of the number of suspects, victims, and geopolitical jurisdictions, and some measure of technological systems relied upon by criminals in given incidents are calculable and therefore theoretically capable of being used to establish a *complexity factor*. Similarly, an *intensity factor* estimating harm (i.e., death, injuries, and property loss in terms of dollars) and the extent of public outrage based potentially on the amount of media coverage could also be developed. Finally a *diffusion factor* consisting of frequency of incidences, across different jurisdictions, and within a specified period of time could also be determined. Data on each of these factors could possibly be gathered and/or estimated from combinations of police and media reports describing incidences of social abuse (operationally defined as new crime). Obviously such data, to the extent it exists or could be generated, would empirically demonstrate the existence of technology crime waves, although determining when new crime ends and adaptive crime begins within a wave would necessarily be subjective and need to be controlled for in research studies. Nonetheless, when combined and quantified such data could be used to measure and compare the magnitude of technology crime waves representing different types of emerging social abuse, in which: (Mw) is the overall magnitude of the crime wave (area under the curve), and complexity (C), intensity (I), diffusion (D), recognition of new crime (R), and understanding (U) are combined into the following general formula (McQuade, 1998):

$$Mw = (C * I * D)/(R * U).$$

Thus, the area under the curve (see Figure 6) represents the magnitude of a single technology crime wave for a specified place (or cyber realm) and period of time. Depending on the number of separate or integrated waves examined, formulation of a prediction model for potential crime or known emerging crime, along with estimates of the magnitude of new crime/security-related threats to society may also be possible. Analysis of crime legislation enactment and media accounts of new crime could provide external validity to these concepts thereby bolstering support for a formal theory of technology-enabled crime, policing and security. By analogy, if we can predict the onset and intensity of earthquakes and volcanic eruptions although imprecisely, as well as model potential new strains of disease and their negative public health impacts, perhaps it is also possible to estimate (albeit initially unreliably) the onset and magnitude of social abuses that are inherently illicit if not initially illegal and threaten society.

Summary: General Theoretical Propositions[1]

Technologies are combinations of tools and techniques ranging from simple-to-complex in their design, materials, construction and manufacturing processes, adoption, social implementation, technical/systems integration and applications. Criminals, police and security professionals employ a full range of technologies that are available to them for similar and countervailing purposes.

New forms of deviance, social abuse or crime, that is new crimes, are committed through innovative use of technology. Initially new crime is not well understood, and is therefore relatively complex, because investigative experts tend not to be able to explain how criminals are using technologies to other investigative experts across time and distance. Faced with relatively complex crime and attendant management problems,

police, security professionals and prosecutors innovate with countervailing technologies and legal strategies to overcome and if possible stay ahead of technological gains made by criminals.

With increased understanding and law enforcement interdiction, new crimes transform into better-understood adaptive crimes, and laws making criminally adaptive behaviors explicitly illegal begin to be enacted. The process of formulating and enacting new crime laws and regulations raises public awareness of crime problems threatening society. Combined with media attention about these issues, attitudinal and behavioral changes emerge in ways that precipitate arrest and prevention of adaptive crimes. Eventually, adaptations of laws are widely adopted and diffused as a form of legal/social technology that leads to increased investigation and prosecution. When this happens, once new and then adaptive crime transforms into ordinary crime that is much better-understood, routinely recognized and responded to, and may be systematically targeted for prevention. New crime, adaptive crime and ordinary crime emerge sequentially to form a technological crime wave in which technological complexity increases across time and distance unless and until countervailing awareness, knowledge and understanding and attendant security/policing technology capabilities are developed to afford greater manageability of the crime problem. Enhanced enforcement, combined with continual technological advances in society, compel smart criminals intent on getting away with ordinary crime to adopt new technologies. This begins anew the cycle of technological competition between criminals and the police (i.e., the emergence of deviance/social abuse, new crime, adaptive crime, and ordinary crime). Criminals that do not adopt new technologies are at greater risk of being caught unless and until their technological capabilities exceed those of law enforcement and security professionals. Similarly, law enforcement and security professionals must consistently develop, adopt, and diffuse new technologies or risk falling behind in their crime fighting capabilities.

Over time, recurring criminal and police innovation cycles have a ratcheting-up effect akin to a civilian arms race. Crime and policing become increasingly complex as a function of increasingly complex tools and/or techniques available in society and employed by criminals, police or security professionals. The result is perpetually complex, technology-enabled crime, policing and security management — a never-ending competition in which police and security professionals will, in general, react to criminological innovation. Tools and techniques once developed, adopted, and understood tend to remain in use by criminals, police and security professionals because of their continuing functionality and/or constraints to technology development or adoption. The result is a full range of relatively simple (ordinary) to relatively complex (new) forms of crimes and countervailing investigation and protective methods. Concerned criminals and police are always wondering about their adversary's activities, and each group may not fully understand the consequences of their own operations (i.e., use of technology). This can result in unintended positive and negative spin-off effects. Over time, technology employed in crime, policing and security management is better understood, thus relatively less complex, and in the case of crime (hopefully) more manageable, except to the extent that criminal innovations disrupt relatively stable technological competitions between law abidance and violating forces of society.

Conclusion

Concepts of technology-enabled crime, policing and security, along with perpetually complex aspects of these concepts, and technology crime waves have been described as a way of understanding how technology-enabled innovative social abuse and criminal behavior emerges, impacts society and then diffuses. Technology-enabled social abuse and crime are usually inevitable negative spin-offs of technology R&D, and initially new crimes are relatively more complex and less manageable because investigative and other experts tend not to be able to explain what is happening across time and distance to other experts. The result is a series of new, adaptive and ordinary crimes grounded in technological capabilities of criminals versus those of security and policing officials. General hypotheses concerning a formal theory of technology-enabled crime, policing and security were advanced that incorporate the concepts of technological complexity and technology crime waves. These concepts are intended to complement, but not supplant, existing theories of crime causality and technology development and diffusion. Indeed, many of the concepts described in this paper are not new and draw upon long-held views and conventional wisdom of experienced practitioners as well as various research findings having to do with crime, security, technology and

competition within many sectors of society. Accordingly, this paper did not focus on why crime occurs, but rather how it may occur with respect to innovative use of technology. These issues are relevant for assessing the technological nature, extent and potential threats posed by crime and terrorism, and potentially for allocating resources for deterring, preventing, interdicting, displacing or otherwise controlling these socially undesirable behaviors. Important considerations in taking the topic further are: (a) whether the somewhat amorphous concepts preliminarily presented here can be more theoretically, conceptually, and methodologically bound in order to logically and convincingly make the case for the existence and utility of technology crime waves thereby supporting a more general theory of technology-enabled crime, policing and security; and (b) the ability to collect or generate sufficient data on complexity, intensity, and diffusion factors for testing hypotheses related to new, adaptive and ordinary crime stages and cognitive phases.

Dr. Sam McQuade is an Assistant Professor of Criminal Justice at the Rochester Institute of Technology.

References

Akers, R. L. (1985). *Deviant behavior: A social learning approach (3rd ed).* Belmont, California: Wadsworth.

Akers, R. L. (1998). *Social learning and social structure: A general theory of crime and deviance.* Boston: Northeastern University Press.

Burgess, R. L., & Akers, R. L. (1966). A differential association-reinforcement theory of criminal behavior. In Joseph E. Jacoby (Ed.), *Classics of criminology,* 2nd, 1994 *edition,* (pp. 228-235). Prospect Heights, Illinois: Waveland Press, Inc.

Cohen, L. E., & Felson, M. (1979). Social change and crime: A routine activity approach. In Joseph E. Jacoby (Ed.), *Classics of criminology*, 2nd, 1994 *edition,* (pp. 66-74). Prospect Heights, Illinois: Waveland Press, Inc.

Graycar, A., & Grabosky, P. (1996). *Money laundering*. Sidney: Australian Institute of Criminology.

Kash, D. E. (1989). *Perpetual innovation : The new world of competition.* New York: Basic.

Kash, D. E. (1996). Complexity. Chapter 4, unpublished manuscript.

Kash, D. E., & Rycroft, R. (1997). Technology policy in the 21st century: How will we adapt to complexity? Presented at the annual meeting, American Association for the Advancement of Science, Seattle, Washington, February 13-18.

McQuade, S. (1998). *Towards a theory of technology enabled crime.* Unpublished manuscript. George Mason University, Fairfax, Virginia.

McQuade, S. (2001). *Cops versus crooks: Technological competition and complexity in the co-evolution of information technologies and money laundering*. George Mason University, Fairfax, Virginia

McQuade, S. (2005). Theoretical and social perspectives of cybercrime. Chapter 5 in, *Understanding and managing cybercrime.* Boston: Allyn & Bacon.

Pease, S. E., & Love, C.T. (1984). Copycat crime phenomenon. In, Ray Surette (Ed) *Justice and the media* (pp. 199-211). Springfield, Illinois: Charles C. Thomas.

Sutherland, E. H. (1947). Differential association theory. In, Frank P. Williams III and Marilyn D. McShane (Eds.), *Criminology theory: Selected Readings*, (pp. 54-59). Anderson: Cincinnati.

Szwak, D. A. (1995). Data rape: High tech theft of credit identities. *National Law Journal*, 17, (20), 18.

U.S. Department of Justice (1980). *Computer crime: Legislative resource manual.* (BJS Contract No. J-LEAA-007-80). Washington, DC: Bureau of Justice Statistics.

Williams, F. P. & McShane, M. D. (1993). *Criminology theory: Selected classic readings*. Cincinnati: Anderson.

Notes

[1] (McQuade, 1998; McQuade, 2001; McQuade, 2005)