

Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact

Cahiers Politiestudies
Jaargang 2011-3, nr. 20
p. 17-40
© Maklu-Uitgevers
ISBN 978-90-466-0412-0



James Byrne¹ and Gary Marx²

New technological innovations have been developed to prevent crime and to improve the performance of the police, but we know remarkably little about how and why certain innovations are adopted, and the consequences –both intended and unintended—of technology-driven solutions to the problem of crime. This article provides an examination of a wide range of new technological innovations that have applications in the areas of crime prevention generally, and crime control (by police) in particular. We provide a description of recent technological innovations, summarize the available research on the extent of adoption in the United States, and then review the available research on the impact – both intended and unintended – of each form of new technology on crime prevention and police performance. We also discuss three key issues – (1) militarization of crime prevention and policing, (2) coercive vs. non-coercive technology, (3) public vs. private sector control over crime prevention and policing – raised by both proponents and critics of what has come to be known as the second technology revolution.

1. Introduction

Even a cursory review of the historical development of our efforts to prevent crime underscores the point that technology – or more precisely, technological innovation – has been the driving force leading to reform of crime prevention and crime control strategies, both by individual citizens and concerned groups, and by formal police agencies (Reichert, 2001; Chan, 2001; Harris, 2007). There are two general types of technological innovations that can be identified: information-based technologies (which we will refer to here as soft technologies) and material-based technologies (which we will refer to here as hard technologies). Both types of technological innovation have been linked to “dramatic changes in the organization of police” (Reichard, 2001:1), particularly at the turn of the last century, while similar linkages can be offered to more general crime prevention strategies employed by individuals and groups of residents.

According to a recent review of police technology by Harris (2007), the first technology revolution in the United States that changed the way police were organized and how

1 James M. Byrne is Professor of Criminal Justice and Criminology, University of Massachusetts, Lowell

2 Gary T. Marx is Professor Emeritus at MIT (Massachusetts Institute of Technology).

they operated centered around three technological innovations that were incorporated into policing: the telephone, the two-way radio, and the automobile:

“With the proliferation of telephones in the early twentieth century, policing changed. Citizens called – and in fact were encouraged to call – the police to deal with a multitude of problems, and the police responded to those calls from dispatch via a two-way radio, and sped quickly to locations via patrol cars. These technological advances, along with changes in police administrative procedures, helped to create the police as we know them today” (Harris, 2007: 153).

Several commentators have argued that we are in the beginning stages of a second technological revolution, which will once again dramatically change police organization and administration (Chan, 2001; Stroshine, 2005; Harris, 2007). A recent review of the use of information technologies by law enforcement agencies highlighted the role of the Federal government in funding these new technology innovations. Between 1995 and 2002, Goff and McEwen (2008: 8) noted that the Office of Community Oriented Policing Services (COPS) program gave grants that *“helped more than 4,500 law enforcement agencies acquire and implement technology in support of efficient police operations. The grants totaled more than 1.3 billion and funded crime fighting technologies that helped redeploy the equivalent of more than 42,000 full-time law enforcement professionals into community policing activities”*. While the specific types of technologies acquired in this program varied from agency to agency, the most commonly acquired technologies were mobile data centers (MDCs) or laptops, followed by automated field reporting systems (AFRS), record management systems (RMS), personal computers, computer-Aided Dispatch (CAD) Systems, and Automated Fingerprint Identification Systems (AFIS). Of course, these technology expenditures only tell part of the technology implementation story. In a recent review, Hummer (2007) has documented the acquisition of a wide range of additional hard technology innovations during the last two decades, including new weapons, less-than-lethal force technologies, body armor, CCTV systems, gunshot location technology, and new patrol car technology. If this investment in new technology does result in fundamental changes in the way we prevent crime and/or respond to crime, then perhaps the second technology revolution is here. However, there are critical questions that need to be considered about the design, development, implementation, and impact of crime prevention and police technology innovations.

We identify a range of new technological tools in the following review, separating *hard* material based technological innovations from *soft* information based innovations in two areas: crime prevention, and policing³. For each type of innovation, we describe the

3 There are many ways of classifying the material. More analytic concerns focus on ways of controlling the environment (target removal, devaluation, or insulation, offender weakening or incapacitation, exclusion and offense/offender/target identification (Marx 2007) or on basic functions (Nogala 1995). However since our goal here is merely descriptive, the simple hardware-software as broadly defined is sufficient. Of course, those are often intertwined as well (Byrne and Rebovich, 2007). Our focus here is on new technological innovations, but we recognize that it is critical to understand how technology is used to support specific crime prevention and law enforcement strategies. Byrne(2008), for example, has pointed out that under the guise of community-oriented policing, a wide range of coercive policing strategies have been introduced, typically in areas of high minority concentration. The same technologies used to design coercive policing strategies could be used in the development of non-coercive policing strategies. In addition, while we have focused primarily on state and local police use of technology in this review, there has been recent literature on the impact of various technologies on the investigative work of detectives (see, e.g. Braga, et.al., 2011). In addition, our review only briefly touches on the impact of technology on the activities – and the performance – federal law enforcement agencies, but it is worth noting that in next year’s FBI Budget, 20.5 million dollars has been

extent of current adoption, and then review the available empirical research on the impact of these innovations on crime prevention and police performance. We then consider some broader social and ethical implications of recent technological innovations.

We devote most attention to policing in its narrow sense, exploring the notion that technological innovation can be viewed as one of the four elements of a new professionalism in policing, along with accountability, legitimacy, and national coherence, that distinguishes “*the policing of the present era from that of 30, 50 or 100 years ago*” (Stone and Travis, 2011: 1). Stone and Travis argue that those departments with a commitment to innovation will also have an understanding and appreciation for developing evidence-based policies and practices, a premise that will likely be challenged (Manning, 2003). However, our broader interest is in technology and social control, a topic central to understanding the different aspects of norms and rule enforcement – whether this involves the prevention and discovery of violations or subsequent actions involving arrest, prosecution, sanctioning and rehabilitation.

2. Hard versus Soft Technology Innovations

Innovations in criminal justice technology can be divided into two broad categories: hard technology (hardware or materials) and soft technology (computer software, information systems). Hard technology innovations include new materials, devices, and equipment that can be used to either commit crime or prevent and control crime. An initial distinction can be made between criminal justice innovations that have a *hard* material base as against a less tangible information *soft* base (even if in practice these are often interwoven). We increasingly see hard technologies intended to *prevent* crime – the ubiquitous CCTV cameras, metal detectors in schools, baggage screening at airports, bullet proof teller windows at banks, and security systems at homes and businesses. Note also the use of personal protection devices (tasers, mace, lifeline/emergency call mechanisms) and ignition interlock systems with alcohol-sensor devices to prevent an individual from starting a car while intoxicated. We can also identify hard technology innovations being used by police, including, new weapons, less than lethal force devices, new technology-enhanced patrol cars, and new police protective gear.

Soft technologies involve the strategic use of information to prevent crime (e.g. the development of risk assessment, and threat assessment instruments) and to improve the performance of the police (e.g. predictive policing technology, and recording/video streaming capabilities in police vehicles). Soft technology innovations include new software programs, classification systems, crime analysis techniques, and data sharing/system integration techniques. Table 1 highlights the types of hard and soft technology innovations in crime prevention, and policing (adapted from Byrne & Rebovich, 2007). Although this listing of new hard and soft technologies is not meant to be exhaustive, we suspect that it captures the range of technological innovations currently being applied in police settings, both in this country and abroad.

requested to support development of the Data Integration and Visualization System (DIVS). For a description of DIVS, see Mueller (2011).

Table 1: The Application of Hard and Soft Technology to Crime Prevention and Police

	HARD Technology	SOFT Technology
Crime Prevention	<ul style="list-style-type: none"> - CCTV - street lighting - citizen protection devices(e.g. mace, tasers) - metal detectors, - ignition interlock systems(drunk drivers) 	<ul style="list-style-type: none"> - Threat assessment instruments - risk assessment instruments - Bullying ID protocol - sex offender registration - risk assessment prior to involuntary civil commitment - profiling potential offenders - facial recognition software used in conjunction with CCTV
Police	<ul style="list-style-type: none"> - Improved police protection devices(helmets, vests, cars, buildings) - Improved/new weapons - less than lethal force (mobile/ riot control) - computers in squad cars - hands free patrol car control (Project 54) - offender and citizen ID's via biometrics/ fingerprints - mobile data centers - video in patrol cars 	<ul style="list-style-type: none"> - Crime mapping (hot spots) - Crime analysis (e.g. COMPSTAT) - Criminal history data systems enhancement - Info sharing w/in CJS and private sector - New technologies to monitor communications(phone, mail, internet) to/from targeted individuals - Amber alerts - Creation of watch lists of potential violent offenders - gunshot location devices

3. The New Technology of Crime Prevention

Crime prevention is a concept that has been applied in a number of different ways to the problem of crime: it has been used to refer to both *activities* (e.g. crime prevention programs and/or strategies) and *outcomes* (e.g. lower levels of crime in communities and/or lower levels of offending/re-offending by individuals). In the name of crime prevention, researchers have examined the influence/role of *formal* social control mechanisms (e.g. the deterrent effects of police, courts, and corrections) and *informal* social control mechanisms, with a focus on the influence (through mechanisms such as attachment, commitment, and involvement) of family, peers, school, work, community and the role of shame and belief systems/religion). In addition, crime prevention strategies have been targeted on different levels of prevention (primary, secondary, tertiary) and on the need for individual (i.e. private actions), parochial (group actions by neighborhood residents), and public actions (i.e. decisions to call the police) to prevent crime.

Understanding crime prevention requires studying intentions, as well as consequences. A broad array of measures needs consideration beyond the traditional number of criminal events or offenders. Additional factors include the amount of harm prevented or the number of victims harmed or harmed repeatedly (Sherman, et al, 1997; Hirschi 1987, Reiss & Roth 1993, Farrell 1995). An even broader definition of crime prevention can be seen in the concern with newer factors such as reduction of risk factors for crime (e.g., gang membership or failure to complete high school). While crime prevention currently is used as a ubiquitous, catch-all phrase that can be applied to both criminal justice-based and non-criminal justice-based initiatives, our focus is on strategies that utilize new technological innovations to either prevent crime (in particular places) or prevent re-offending by targeted groups of offenders (e.g. sex offenders, mentally ill offenders,) that do *not* rely exclusively on traditional actions by the police (arrest), courts (prosecution), and/or corrections(punishment, control, reform).

3.1. Hard Technology Crime Prevention Innovations

According to a recent review of crime prevention technology by Brandon Welsh and David Farrington (2007: 81), “*Technological advances over the years have had a profound influence on the way we think about crime and the efforts that are taken to prevent it. Hard technologies to prevent crime cover a wide range of applications in different contexts, including metal detectors in schools, baggage screening at airports, bullet proof teller windows at banks, and security systems at homes and businesses*”. There are other hard technology applications that quickly come to mind, including the use of personal protection devices (tasers, mace, lifeline/ emergency call mechanisms) and ignition interlock systems with alcohol-sensor devices to prevent an individual from starting a car while intoxicated, and the various types of “social engineering strategies” described by Marx (e.g. target insulation, target devaluation, target removal, offender incapacitation, offender exclusion, etc) and advocates of crime prevention through situational crime control and/or environmental design manipulations (Marx, 2007; Clarke, 1997).

Unfortunately, it is difficult to offer an accurate estimate of the extent to which each of these hard technology crime prevention innovations have been adopted. For example, several large U.S. cities have recently begun deploying CCTV cameras, including Boston, New York, Los Angeles, Chicago, and Newark New Jersey, and it was estimated that there were approximately 1 million CCTV cameras being deployed across the United States by year end 2006 (Nestlel, 2006), but more current estimates are not available. While no cost estimates have been calculated, it is apparent that the expansion of video surveillance from private to public spaces will require substantial funding by local government (Hier, 2004; Greenburg and Roush, 2009). Indeed, what began as a technology to monitor “*private retail interests and traffic flows*” in the late 1950s has morphed into a police-managed and/or government funded open visual surveillance system today (Hier, 2004: 542).

CCTV surveillance systems are constantly being upgraded to include new soft technology features. In several cities (e.g. Boston, Newark), the addition of gunshot location technology allows rapid deployment of emergency medical personnel, and police, to the locations where gunshots are identified (Mazerolle, et.al., 1998). Shentzhen, China is currently testing a 200,000 camera CCTV system with the capability of alerting police when inordinate numbers of individuals cluster at one location. In addition, software has been developed utilizing China’s national identification data base and facial recognition software that will allow the police to identify individuals under video surveillance. In China, over 3.4 billion dollars was spent in 2006 alone on the development and implementation of CCTV systems (Klein, 2008).

Estimates of the extent of use (and projected cost) of several other hard technology crime prevention innovations – metal detectors in schools, baggage screening at airports, bullet proof teller windows at banks, and security systems at homes and businesses, protection devices (tasers, mace, lifeline/emergency call mechanisms), and ignition interlock systems are difficult to obtain, but it is obvious that crime prevention technology is a growth industry, both in the United States, and internationally. For example, it is estimated that approximately 2% of all U.S. schools deploy metal detectors, typically in conjunction with security guards (Hankin, Hertz and Simon, 2011), while a recent report revealed that a dozen airports received a total of a billion dollars in federal stimulus

funds in 2009 for upgraded baggage screening and checkpoint technology (Homeland Security Press Release, 2010).

There are only two hard technology crime prevention innovations that have *known* effects on crime: closed circuit television cameras (CCTV) and improved street lighting. For the other types of hard technology we describe, the necessary research is either inconclusive (see the recent review on the impact of metal detectors on school violence by Hertz and Simon, 2011) or has not been conducted. To identify the crime prevention effects of CCTV and street lighting, Welsh and Farrington (2007) conducted a systematic review of the research on both forms of hard technology, which they have continually updated (Welsh and Farrington, 2002, 2004, 2006, 2007). They found that “*CCTV and improved lighting were more effective in reducing property crimes than in reducing violent crimes, with CCTV being significantly more effective than street lighting in reducing property crime*” (2007: 94). Of course, the majority of the evaluations reviewed by these authors focused on parking lots and/or garages; we simply do not have adequate empirical research to know whether these crime prevention effects will be found in other public places.

One additional caveat is in order when considering these findings. Both CCTV and improved street lighting strategies were found to be “*far more effective in reducing crime in the U.K. than in the U.S.*” (Welsh and Farrington, 2007: 95). The obvious question is: why? The authors consider a number of possibilities for this differential effect, including length of follow-up (shorter follow-ups show better results), the actual date the study was conducted and the specific technology used (newer studies/technologies do better), whether the strategy was implemented as a stand-alone innovation or used in conjunction with another initiative (stand-alones do worse), and cultural context/public support (more public support for CCTV in U.K. than in U.S.). We agree with the authors that while these two strategies meet the review criteria established for identifying programs/strategies that *work* (this standard has been described by some as the bronze standard, since it only requires a minimum of two level 3 (quasi-experiments) research studies to support this assessment (Byrne & Hummer, 2008). Assuming you accept this standard of proof, it is clear that that these new technologies only work in one setting (parking lots/garages) and for very specific categories of crime (i.e. property). Welsh and Farrington conclude with a typical refrain: “*there is still much to be learned about the optimal conditions under which CCTV and improved street lighting are most effective in reducing crime*” (2007: 96). Given the limited evidence of success it is interesting that adoption has been so widespread. It appears that CCTV advocates have successfully marketed limited evidence of success in very specific areas (parking lots) as an effective crime prevention strategy for both violence and property crime prevention in ALL public places (Haggerty, 2008). As we will note for other technologies, the availability of evidence documenting a tactic’s effectiveness (or advantages and disadvantages relative to other tactics) generally plays a minor role in the decision to adopt or to continue.

3.2. Soft Technology Crime Prevention Innovations

In addition to the various hard technology applications we have just described, a wide range of new soft technology innovations have been developed in recent years and used as a crime prevention tool. Recent technology innovations include the latest generation of offender risk classification tools, the emergence of threat assessment protocols, bullying identification tools, software programs developed to prevent identity theft, and to protect

data privacy, new tools for monitoring the location and movement of at-risk populations, such as mentally ill offenders and sex offenders, and most recently, new assessment tools designed to identify individuals who are likely homicide offenders (or victims) within a specified timeframe. While the extent to which each of these new technologies has been adopted is difficult to assess, we can offer the following preliminary assessment.

The United States has invested considerable resources in the soft technology of crime prevention. For example, we monitor the location and movement of the approximately 800,000 registered sex offenders in the United States using a national sex offender registration system with the capability to provide community notification for any newly arriving sex offender, and law enforcement notification for sex offenders who fail to register or who violate location restrictions. The risk of recidivism among this group of offenders will typically be classified (high, moderate, low) based on the completion of one of the myriad of risk assessment tools that have been introduced in recent years (e.g. RRASOR, Static-99, SORAG, MnSOST, SONAR, SVR-20 for sex offenders). We can also use GIS mapping programs, in conjunction with the national and individual state registry data bases, to examine offender locations and assessing the impact of sex offender residency restrictions on crime prevention (Mandelstam & Mulford, 2008).

A second area of heavy financial investment is risk assessment. The management of the 7.5 million offenders currently under correctional control in the United States relies on the use of actuarially based risk classification systems (Pattavina & Taxman, 2007; Byrne & Pattavina, 2007). The prevention of crimes committed by offenders when they leave prison, or when placed on parole, has received considerable attention and financial support in recent years. According to a recent review, *“a majority of the serious crimes are committed by a small fraction of people, in a small number of crime-ridden neighborhoods, during the first few months of probation or parole”* (Byrne, 2009: 1). Risk assessment tools are designed to identify this subgroup of offenders accurately, allowing corrections systems to target resources and supervision/surveillance on high risk, people, times, and places (Byrne, 2009). It should be noted that these assessment tools have generally been developed as proprietary instruments, in the private sector and represent one example of the privatization of crime prevention.

A third area of soft technology innovation related to crime prevention that has received considerable attention – and funding – post 9/11 is threat assessment. In less than a decade, an industry has been created based on a simple notion: it is possible to identify the threat (i.e. probability) of a terrorist attack and/or a serious violent event occurring at one of the following sites: airports, nuclear power plants, schools, train stations, government buildings, and private companies. In conjunction with threat assessment is vulnerability assessment: what can and should we be doing to prevent this threat from being realized? The average cost of these assessments varies from vendor to vendor and from site to site; one recent report indicated that an individual school threat/vulnerability assessment can cost between \$25,000 and \$50,000, with colleges costing considerably more.

A fourth area where information technology has been used to prevent crime is in the use of newly developed computer software and creation of devices to monitor individual transactions and communications, on the cell phone, over the internet, and on various web-based social media sites (Saghoian, 2011). This new technology has changed the

way police investigate financial crimes, drug crimes, internet-related human trafficking, and sex crimes. In a recent review of electronic surveillance by policing agencies in the United States, Soghoian (2011) found that there has been a recent movement away from surveillance practices for which there are specific reporting requirements such as wiretaps, roving intercept orders, pen registers, and trap and trace devices and emergency voluntary disclosures) and toward surveillance methods that do not have reporting requirements, such as requests to view “*stored communications and subscriber records. This includes stored emails, instant messages, web browsing history, search engine records, as well as documents stored in the cloud*” (Soghoian, 2011:20). It should come as no surprise that Facebook and other social media sites would be examined by investigators attempting to solve crimes and monitor the activities of known suspects. In 2009, for example, Facebook representatives revealed they were receiving about 10-20 requests weekly from law enforcement agencies (*Newsweek*, May 18, 2009). However, it is surprising that there appears to be little oversight or even reporting requirements associated with these requests.

Given our reliance on information technology to manage offender populations via risk classification and other soft technology-based strategies, such as sex offender registration, it is surprising that we do not know more about the effectiveness of these new technologies. A similar assessment can be made about the effectiveness of the other innovations we have mentioned, including the recent development of threat assessment protocol. Both risk assessment and threat assessment represent examples of how soft technology innovations can be applied to the prevention of crime by targeted individuals (sex offenders, mentally ill) or at targeted places (schools, workplace, airports). The problem is that whether we ‘profile’ high risk people or high risk places, we simply do not have the necessary information to make accurate predictions; and as a result, false positives are subject to unnecessary – and potentially harmful – surveillance and control. In our quest to prevent a small number of high stakes, but low risk, crimes (e.g. school shootings, terrorist attacks, sex offending), we may be trading personal freedom for the undocumented promise of crime prevention. To the extent that the *actuarial assumption* inherent in the newest generation of risk prediction devices results in the identification of minority group members as the potential ‘at-risk’ group, the use of these risk instruments may institutionalize disparities by race and class (Gandy, 2007). Perhaps equally important is the notion that we may be wasting crime prevention resources on unproven strategies, many of them coercive in nature; a more prudent course would be to reallocate resources to non-coercive strategies with *known* crime/violence prevention effects (e.a. education, jobs, poverty reduction) and fewer ethical concerns (Byrne & Roberts, 2007; Stemen, 2007).

Harris and Lurigio (2007) point out that one of the major paradoxes related to the development and expansion of risk-assessment technology in the area of violence prevention is that practitioners seem obsessed by the need to assess risk in groups of individuals (e.g. sex offenders) with very low failure rates. For some offender groups, risk appears much less important than stakes; for sex offenders in particular, it appears that the *possibility* of re-offending is more important than the *probability* of re-offending (Byrne, 2009).

In addition to their examination of risk assessment technology, Harris and Lurigio (2007) examined the development of new threat assessment protocols, and observe the

following: *“threat assessment involves instruments or protocols to prevent violent incidents that rarely occur (e.g. an individual’s risk of being a murder victim in a school shooting is less than one in a million), but nonetheless create great fear and anxiety in the general population, such as terrorism and violence in the school and workplace. The purpose of threat assessment strategies is to prevent events of targeted violence (e.g. at schools and in the workplace) in which assessing a particular individual’s inherent risk of violence is secondary the trajectory of behaviors leading up to the planned attack”* (Harris & Lurigio, 2007: 104). Harris and Lurigio’s review revealed that threat assessment is only in its early stages of development and that the risk assessment field has a much sounder empirical base. We conclude from the available research that whether high risk people or high risk places are profiled, the data to make accurate predictions is lacking and there may be other unwanted outcomes.

4. The New Technology of Policing

Changes in both the hard and soft technology of policing appear to be transforming local, state, and federal policing departments in a number of fundamental ways; but some scholars have raised questions about how much has really changed (Manning, 2003). Two recent reviews (Hummer, 2007; Harris, 2007) of technology and the police describe this transformation process, review the evidence of its impact on police practices and outcomes, and discuss the implications of technological changes in policing for the public. Both Hummer (2007) and Harris (2007) reach similar conclusions: police technology has not been found to significantly improve police performance. Similar assessments of the limited measurable impact of police technology on police performance have been reached by others who have reviewed the available research on the impact of recent technological innovations on police performance (NRC, 2006; Manning, 2003).

4.1. Hard Technology Police Innovations

There are several recent advances in the hard technology of policing that can be identified, including: (1) non-lethal weaponry (chemical irritants, electric shock immobilizing technology, rubber, plastic, wooden bullet guns, beanbag shotguns, strobe and acoustical weaponry), (2) various non-electric immobilizing devices (water pressure, trap nets, sticky foam), (3) technology to reduce the number of vehicular pursuits (barrier strips, vehicle disabling and tracking devices), and (4) technology designed for officer safety (improved bullet-proof vests, new body armor technology, improved patrol car protection technology). There are several other hard technology applications in policing that can be identified, including new gunshot location devices, cameras to detect speeders and red light violations, the use of biometrics/ improved fingerprint identification and the hands-free communications systems being tested in patrol cars.

Based on recent reviews of technology adoption by police departments in the United States, it is clear these new technologies are being adopted at a rapid pace, due in large part to significant financial support from the federal government. Consider the taser, a less-than-lethal force weapon. It is estimated that 345,000 tasers have been sold to date (Taser, 2011), with 4,500 police agencies worldwide distributing them to their entire department. In the United States, over 12,000 police agencies have purchased tasers, and recent research on the effectiveness of the taser (White and Ready, 2009; Alpert, Smith, Kaminski, Fridell, MacDonald, and Kubu, 2011) will likely increase the

adoption of this technology. A second hard technology that has been rapidly acquired is the laptop, or mobile data center, used by officers on patrol in cars. 67% of the police agencies receiving COPS funding acquired laptops with their funds (an average of 30 laptops per agency). Groff and McEwen (2008) reported that over 1.3 billion was distributed for technology-related hardware and software between 1995 and 2002, including enhancements to police cars (e.g. the hands-free police vehicle), new police protective gear, and other acquisitions. However, few independent evaluations of the impact of these technological innovations on police performance have been conducted, which makes an assessment of the effects of the COPS technology enhancement strategy difficult (Groff and McEwen, 2008).

Focusing on the link between new technology and officer safety, it appears that “[w]hile there are many factors in a complex dynamic associated with the significant decline in officer deaths over the past thirty years (Batton & Wilson, 2006), it seems reasonable to state that these innovations have played more than a negligible role” (Hummer, 2007: 146). Apart from significant improvements in officer safety linked (generally) to advances in body armor, Hummer argues that there is little empirical evidence available to assess the impact of the other hard technology innovations on police performance. Our own view is that while hard technology may account for significant improvements in officer safety, a more likely explanation is their improvements in officer safety are linked to a general reduction in violence across the country over the past several decades.

Given the cost of acquiring and maintaining these new hard technologies, it certainly appears that we need to conduct much more – and higher quality – research on the impact of these new technological innovations on police performance. Consider tasers, for example: recent research suggests that the taser (referred to as a conducted energy device or CED) may “significantly reduce injuries to suspects and the use of CEDs can decrease injuries to officers” (Alpert, et.al., 2011). Positive findings on the impact of pepper spray were also reported by the authors of this study, which is currently being highlighted by the U.S. National Institute of Justice, *Research In Brief Series*. However, it should be noted that this was a non-experimental study of 962 CED cases across six police departments; both the rate of injury to suspects and officers varied greatly across sites. Perhaps most importantly, there is no evidence that the introduction of this form of non-lethal technology has resulted in fewer instances where police will decide to draw and use their weapons; it appears that tasers and other non-lethal weaponry are actually being used to control individuals who would not – in the past – have been viewed as a threat necessitating a weapon-based response. As the authors of the evaluation note: CEDs can be used too much and too often. A critical question focuses on the officers becoming too reliant on CEDs. Some officers may turn to a CED too early in an encounter and may be relying on a CED rather than relying on the officer’s conflict resolution skills or even necessary hands-on applications. (Alpert, et.al. 2011: 16). It is in this context that it can be argued that we may have *widened the net* of coercive police control with the introduction of this new technology. Further research is needed to determine whether this net-widening applies to the introduction of a variety of other hard technology applications. There is currently no body of research evidence that spending money on the types of hard technology innovations described here will *improve* police performance. One has to ask: why are we so enamored with these innovations?

4.2. Soft Technology Police Innovations

There have also been a number of recent reviews of the design, implementation, and impact of soft, information technology in the policing area (Pattavina, 2005; Manning, 2006; National Research Council, 2006). Harris (2007) identified a number of new, technology-driven advances, including innovations related to (1) data collection and management (new record management systems, mobile data terminals, computer-aided dispatch (CAD) systems, information sharing via the internet, and (2) new data-driven police strategies (including Compstat, the use of computerized crime analysis and crime mapping software, and early warning/ early intervention systems targeting police misconduct). Recent reviews of technology adoption by police agencies highlight the extent that these new technological innovations are being used. For example, Groff and McEwen (2008:12) report that a wide range of soft technology was acquired by COP funding recipients between 1995 and 2002, with 29.6% of the agencies reporting that they purchased automated field reporting systems (AFRS), 24.3% record management systems (RMS), 20.4% personal computers, 16.9% computer aided dispatch (CAD) systems, 9.6% Automated Fingerprint Identification Systems (AFIS), 7.5% arrest and booking systems, 4.9% crime analysis systems, 4.9% mapping systems, and 32.4% reporting other technology acquisitions.

Since 2002, federal and state governments have continued to fund new police technology innovations, and new policing strategies with names like community-oriented policing, problem-oriented policing, intelligence-led policing, and most recently, predictive policing. A recently released report from the Police Executive Research Forum (PERF, 2011) revealed that 70% of survey respondents reported using predictive policing analytics, including crime mapping software and data analysis techniques, to stop serial offenders and to develop crime prevention strategies for their agency. Survey respondents also noted that their agencies had purchased in-car video recording capability, with 25% of respondents indicating that 100% of their cars had this technology. Other technologies reported being used included wireless video streaming from fixed surveillance cameras to police vehicles (23%), license plate readers (71%), the use of GPS technology to track suspect movements (83%), track police vehicles (69%), and track on-duty officers (4%), monitor social media to identify investigative leads (86%).

A review of the available research on the effectiveness of these innovations underscores a recurring theme in this review: the necessary research on most of these innovations has not been conducted. However, there are two separate systematic, evidence-based reviews that have been completed: an assessment of hot spot policing by Braga (2006); and an assessment of problem-oriented policing by Weisburd and colleagues (2010). Both these reviews point to significant, albeit modest, improvements in police performance that can be linked to the introduction of these technology-enhanced strategies, using a variety of outcome measures. Despite the existence of these reviews, there is debate over the design, implementation, and effectiveness of hot spot policing strategies, and problem-oriented policing/community-oriented policing strategies (Skogan and Frydl, 2004; Rosenfeld, Fornango, and Baumer, 2005; Manning, 2003; Weisburd, Mastrofski, Greenspan, and Willis, 2003, 2004).⁴ Interestingly, it is not the technology that is the

4 Many of the alternative measures of police performance suggested by Marx (Marx 1976) four decades ago are now in use.

focus of this debate; it is the strategies that are developed using new technology that are examined and critiqued.

Harris (2007) is cautious in his appraisal of the long-term impact of the IT revolution on police organization and administration. He concludes his review by placing these recent soft technology enhancements in their proper historical context: “*While IT has the potential to enhance police work, and perhaps fundamentally alter traditional police practices, there is little evidence that IT has revolutionized policing when compared to the earlier eras of policing and the adoption of the telephone, two-way radio, and automobile. To the extent that newer IT has contributed to policing, it appears to have largely enhanced traditional practices*” (Harris, 2007:181).

Perhaps unsurprisingly evidence on both crime prevention and police performance generally offer only modest support, in light of the frequently immodest claims of proponents. Of course, police performance involves multiple dimensions and some are much easier to measure than others and there is little agreement on how competing values should be weighed. But what is most easily measured quantitatively and in financial terms should not necessarily be equated with what is most important.

5. Innovations in Criminal Justice Technology: Issues to Consider

The ideas offered regarding rational policy development in schools of public administration suggest that research and evaluation should determine policy. In the field of criminal justice, there has been a recent emphasis on the importance of conducting quality evaluation research, and to develop new programs – and remodel existing ones – based on evidence-based practice (Welsh & Farrington, 2006; Braga, 2010). That is hardly the case for the various types of hard and soft technology innovations considered above, which challenges the *new professionalism* model of policing we mentioned at the outset of this review (Stone and Travis, 2011). The present review of an under-researched area of great significance – the implementation and impact of crime prevention and police technology – raises many questions. One issue involves the role of evidence in setting public policy. Given the limited evidence of success for new crime prevention and police technologies, it is interesting that adoption has been so widespread. Research documenting a tactic’s effectiveness (or advantages and disadvantages relative to other tactics) generally plays a minor role in the decision to adopt or to continue to use a technology.

Given the weak empirical foundation for these innovations and potentially detrimental side effects, what drives change? In the U.S. the pressure to innovate is *not* related to an objectively worsening crime problem (perceptions are of course another matter). There is a long term downward trend in crime, with violent crime rates down over twenty percent since 1995 and the overall crime rate is back to where it was in 1970. However, more likely factors are declines in several measure of effectiveness. For example, police clearance rates for homicide have dropped from over 90% in the late 1960’s to 60% today, with similar precipitous drops for other categories of violent crime. Over the last two decades court’s developed reforms to address long standing problems of race and class bias such as actuarial-based pretrial and sentencing decision making tools (e.g. sentencing guidelines). These reforms appear to have simply institutionalized race and class based disparity rather than eliminating it (Taxman, Byrne, and Pattavina, 2005) .

The institutional correctional system has been criticized in a number of performance related areas (note a comprehensive review by the National Commission on Safety and Abuse in America's Prisons (Gibbons & Katzenbach, 2006). There is an emerging consensus that our prison system 'makes offenders worse' in critical areas, such as mental and physical health. Offenders leaving prison and being supervised in the community are failing at a much higher rate today than in 1980, with parole success rates dropping from 60 to 40 percent and probation failure rates dropping from 80 to 60 percent (Byrne, 2008).

But apart from the difficult to define factor of needs, the United States in particular has a fascination with the new and with technology (Police Executive Research Forum, 2011). Techno-fallacies noted several decades ago with respect to the rapid spread of electronic monitoring technology are still present today (Corbett & Marx 1991; and for an extension across control technologies: Marx 2007). For example, the *fallacy of novelty* brings the assumption that new means are invariably better than the old. The appeal is in the novelty rather than in data suggesting that the new will work (or work better than the traditional). When nothing works very well, the *vanguard fallacy* supported by the power of fads and fashion is a related cultural element. The assumption is if the leading players are doing it, it must be the way to go. The actions of the larger or more prestigious organizations are copied in an effort to appear modern.

Corbett & Marx (1991) observed: "*New technology is inherently attractive to an industrial society. It's risky to be against new technology, however mysterious its operations or recondite its underlying engineering. Technical innovation becomes synonymous with progress. To be opposed to new technology is to be a heretic, to be old-fashioned, backwards, resistant to change, regressive, out of step.*" Administrators looking for ways to distinguish their careers and agencies may be drawn to new technologies. Reputations may be enhanced by introducing new technology-enhanced programs rather than on maintaining the old. The ambitious professional is unlikely to want to be regarded as a caretaker. Related to the above is the *fallacy of intuitive appeal or surface plausibility*. A policy may be adopted because, "it sure seems as if it would work." The emphasis is on commonsense "real-world" experience and a dash of wish fulfillment in approaching new programs. In this ahistorical and anti-empirical world, evaluative research has little currency. A central factor driving the fads and fashions of new technologies is the private sector through its lobbying and sales efforts. With the reduction of cold war spending since 1990, the private sector has sought non-military applications for its products. There is an intertwining of militarization and privatization in criminal justice as discussed below. But even if the evidence for a tactic's effectiveness was more closely linked to decisions to adopt and there was greater awareness of the rampant, too facile, unexamined assumptions about technology, there are questions that are not easily answered by research such as the broader implications for policing in a democratic society. A key feature here is the role of people as against machines and of changing persons as against coercively controlling them. The increased militarization and privatization of policing are also relevant here.

Any new technological innovation is likely to have both intended and unintended consequences for crime and social control that are important to understand. Three critical issues come immediately to mind. First, perhaps the most salient issue related to the new technological innovations is whether –over time – we will replace *people* (police officers, court officers, judges, corrections officers, and community corrections

officers) with various forms of *thing* technology (CCTV, cameras that detect speeders, wired courts, electronic monitoring, supermax prisons, etc.). For example, why do we need police officers patrolling the streets (and highways) when we have the technological resources (via cameras to detect speeders and red light violations, and CCTV to monitor public places) to remotely monitor activities and deploy a smaller number of police to address crime problems that are detected? The downsizing of police force manpower may be an inevitable consequence of this type of technological innovation, which is one reason that technological change may be viewed suspiciously by line personnel and the unions that represent their interests. Similar scenarios can be offered about the likely impact of various technological innovations in the courts (electronic filings, sentencing software) institutional corrections (the techno-prison, new identification and prisoner tracking devices), and community corrections (electronic monitoring with real time tracking/ location restrictions). What do we lose when we rely on technology rather than people to perform essential criminal justice tasks? Corbett and Marx's admonition – written about electronic monitoring over twenty years ago – is right on target: there is no soul in the new machine.

It is certainly possible that our increased reliance on technology will lead us further down a potentially treacherous road: an increased reliance on both coercive surveillance and coercive control strategies. For those who draw parallels between domestic policing and military strategy (e.g. Kraska, 2001), it may be helpful to consider a recent shift in the approach of the military to the question of troop strength/deployment strategy: we are now considering reducing our reliance on large, standing forces of military personnel and instead creating a number of small, highly trained, and technology-rich quick strike Ranger- style units that can move to (and from) various “hot spot” areas as needed. This strategy may represent a possible deployment model for local, state, and federal police agencies that use various forms of hard technology (e.g. cameras, gunshot location devices, CCTV) and soft technology (e.g. crime mapping, hot spot analysis) to monitor areas (and analyze crime patterns) from a central location.

Critics of the second technological revolution in policing argue that we are “transforming policing” not by linking science to practice (Manning, 2008a,b; Marx, 2008), but rather by developing strategies that utilize science/technology as a means to an end (coercive social control). Of course if such control-based technologies *improved* police performance, then such innovations would be on firm scientific ground, despite the obvious ethical/ moral issues. That is not the case here. Only a handful of quality research studies of technology-based crime prevention and police innovations have been conducted to date; and careful reviews of this body of research suggest only a modest overall positive impact (see the evidence-based reviews by Welsh and Farrington, 2006 on CCTV and street lighting; by Braga, 2006 on hot spots policing; and by Weisburd, et.al., 2010 on problem-oriented policing).

While it is certainly possible that further research on various technology-based crime prevention and policing strategies may reveal strategies that increase police performance initially, it is important to consider exactly how this effect will be achieved. Weisburd et.al. (2010) recently observed that POP (problem-oriented policing) is more accurately described as a process, rather than a specific program. If coercive police strategies are being employed, the longer term effects may not be so positive, due to the distrust of the police in high crime, poverty pocket areas that will likely be fostered by such strategies.

Braga (2006:190) recently commented about the hot spots policing strategies included in his review: “*Proactive patrols, raids, and crackdowns do not specifically address the site features and facilities that cause specific locations to generate high volumes of crime. Perhaps a greater focus on changing these criminogenic situational characteristics would result in longer lasting crime reductions at crime places.*” Before we move too far in this direction, we may need to consider the alternative: the development of non-coercive crime prevention and crime control strategies (Cole & Lobel, 2007; Byrne, 2009). We can spend money on the latest unproven technological innovation in our search for an effective crime prevention and/or crime control strategy, but it is worth considering whether similar – or greater – crime prevention/control effects can be realized by using this money on *proven strategies* to improve education systems, create job training programs, improve housing, relocate families living in high crime areas, reduce poverty, or hire more police to walk, talk, and problem solve in these “at risk” communities (Stemen, 2007; Byrne & Roberts, 2007).

A second related issue is whether our fascination with the new technology of offender control will result in the continued development and expansion of criminal justice policies that minimize the possibility – and undermine the prospects – for individual (offender) and community change (Byrne and Taxman, 2006; Byrne, 2009). One doesn’t have to look any further than our recent prison build-up to find a good example of how our reliance on offender control in institutional settings. We spent 60 billion on corrections last year alone with over three quarters of that total allotted to prison management. This has undermined our ability to provide treatment to offenders (for substance abuse, mental health, education/skill deficits) that might actually change their (criminal) behavior, both while in prison and upon reentry to the community (Gibbons and Katzenbach, National Commission on Safety and Abuse in American Prisons, 2006). To the extent that new technological innovations reinforce what David Garland has aptly labeled a culture of control, technology may be moving our criminal justice system in the wrong direction. Perhaps we need to think in terms of a correctional paradigm that emphasizes the new technology of offender change, would represent a departure from our current emphasis on control technologies; in doing so, we would recognize a simple lesson of history: more often than not, “brute force” fails (Kleiman, 2005).

And finally, out of necessity rather than by design, we certainly need to consider the long-term consequences of privatization of key criminal justice system functions, including information management, offender/place-based monitoring, and offender control). In large part because the line staff and management in most criminal justice agencies do not currently have the necessary technology-based skill sets, we are forced to rely on the private sector today more than at any point in our history, particularly in the area of information technology. It is certainly possible to envision a *Brave New World* of crime prevention and control, where the private sector’s helping, short-term support role (e.g. in the areas of information technology, system integration, electronic monitoring, CCTV, private security, and prison construction and management) expands to the point where private sector crime control ultimately replaces public sector crime control in several critical areas (crime prevention, offender monitoring, place-based monitoring, and various forms of offender control). If this occurs, our concern would be that the moral performance of the criminal justice system will suffer, because a concern for the economic bottom line by the private sector will have negative consequences in a number of critical areas (privacy protections, resource availability and quality, fairness, procedural justice).

To some observers, advances in new, hard technology, and the involvement of the private sector, are the inevitable consequence of the militarization of domestic law enforcement (Kraska, 2001). Hummer(2007:133) observes that “While some of these devices were created exclusively for law enforcement use (Silberman, 2005), many of these technological advances originated from the U.S. military, NASA, DARPA (the Defense Advanced Research Projects Agency), other national research laboratories, and private sector corporations (Alexander, 2001; Hubbs & Klinger, 2004; Nunn, 2001). It is important to keep in mind the profit factor: hard technology police innovations are the direct result of the private sectors need to find lucrative, non-military (post war) applications for military hard technology.

6. Concluding Commentary: Understanding the Context and Consequences of Technological Change

Technological innovation has the potential to dramatically improve both the efficiency and the effectiveness of the criminal justice system; but it also has the potential to divert critical resources away from more traditional crime prevention and police strategies that may actually make us safer, without the negative side effects (e.g. erosion of personal freedom, increased public distrust, emphasis on coercive control, etc). Recent changes in the technology area generally – and in the area of information technology in particular – have been so dramatic and profound that they deserve special attention and critical review. As we demonstrate in this article, it is important to consider new technology developed to support crime prevention generally and crime control by police, because by focusing on innovations in only one area, we would likely miss the consequences – both intended and unintended – of our investment in police technology for individuals and groups interested in alternative crime prevention strategies.

Any modern society needs police who can make good use of technology (if for no other reason because criminal adversaries with an alternative code will find ways of using technology). But there are, of course, many other reasons to embrace technology in the areas of crime prevention and the police, including the potential for increased efficiency and effectiveness. Information technology, for example, “*increases our ability to store and process large volumes of data, improving intelligence and investigative capabilities, and providing ready access to criminal records and other kinds of relevant data*” (Reichert, 2001: 1). But also of great importance is the need to sustain democratic values through a criminal justice system under law that is just, fair, accountable and goes beyond the often self-defeating aspects of punishment and responding after the fact. The effective use of DNA in various innocence projects is illustrative, as is the accountability of videotaping in social control settings⁵.

5 Key here is how widely available technologies are for uses beyond government or deputized private users. A case in point is the contentious citizen use of cell phone (or other cameras) in recording police who are filming them. In the U.S. there have been cases where citizens have been arrested for doing that in public places, in some cases ironically charged with violating a state’s wiretapping laws. This is one strand of a larger freedom of information issue. For example should police video records be seen as public documents available to anyone who requests them? Should they be automatically posted on the internet (as has been done after some demonstrations as police sought the public’s help in identifying participants). What are the implications for grey policing? Accountability is vital but this needs to be thought about carefully with respect to visibility. We must ask visible to whom and under what conditions. The restrictions of that slope however may be mega-slippery (Hoogenboom 2010).

Any argument in favor of increasing the power of those in positions of authority through technology must be tempered by an awareness of all that can go wrong and by the advantages increased power can offer to those in positions of authority. One factor here is the too easy effort to create legitimacy through promoting the aura of science and technology as infallible. This ignores the role of humans (and particular interests) in shaping what technologies are developed and how they are designed and applied.

One issue with privatization and the profit seeking goals of the sellers is whether the technology is honestly presented rather than being oversold. Is there sufficient attention to the ability of more clever offenders to thwart control? In conflict settings (whether the conflicts are seen to be socially legitimate or not) control is always imperfect and dynamic. New technical solutions are usually only partially effective and with time may become less effective. Tools for neutralization become available –whether legally or on the black market Marx (2009).

Criminal justice changes are often put forth as desirable because they are seen to be more humane and less coercive. But such claims must be carefully examined. The reflective observer must be ever on patrol for unexpected outcomes, trade offs and related value and goal conflicts (Marx, 2007). The glut of information provided may overwhelm agents in a sea of data. And they may be unwilling to share it. Chan (2001) in an empirical study reports on officers feeling information overload. If the technology is effective –at least at identifying offenders and offenses, is there a danger of flooding control systems such that they can't process the amount of violations uncovered? That may bring the risk of unfairness regarding who gets processed and leave control agents feeling overwhelmed. As with the case of the tasers mentioned above will this widen the deviance catchment nets in the absence of policy directives to do this?

Bars on homes that keep thieves out may also prevent those inside from fleeing in the event of a fire. Encrypting information offers security, but at increased expense and increasing the time required for a transaction, not to mention worry over losing the keys. Technologies directed at offenders may backfire and also effect agents (tear gas or crowd control devices that lead to loss of bowel control, remote cell phone and other electronic signals that can be tell-tale but also can impact other devices such as pace-makers or garage doors).

Having cars or electronic devices that can only be activated by a biometric control or a code from their owner may lead to an increase in violent confrontations between victims and offenders (not the new crime of car-jacking). Video cameras in parking lots may simply displace car theft to areas where there are no cameras. A dynamic struggle may escalate –police use of body armor may lead to offenders using more powerful weapons and wearing armor as well. Bank barriers may reduce theft but make customers feel less welcome and lead to their using banks that don't install them. Documenting ever more of the behavior of criminal justice practitioners may increase accountability but make for more timid, less energized or innovative workers fearful of using discretion. Discretion is central and there are many grey areas that should not automatically be subject to rigid rules, nor immediate publicity (Hoogenboom 2010).

Risk prediction technology, as in the case of profiling, may be statistically accurate across many cases, but inaccurate with respect to a given case (this is the issue of aggregate

rationality vs. individual cases). Even if accurate in the individual case it may conflict with the rights of the individual who is to be judged on the basis of actual behavior, not a prediction of future behavior. That issue is at the core of films such as *Minority Report*. A risk manager pushing hard wired, technical solutions said, “if we could control ourselves, we wouldn’t need any of this technology.” Ok, but then what kind of a society do we have if people are only and increasingly controlled by their physical environment? In the conflict settings of law enforcement what happens if (or better when), the technology breaks or the electric power simply goes out? A society that is based on external control is unreliable and has morally failed.

The special issue of this journal is devoted to “technology led policing”. But do we really want technology to lead society? Where will it lead? Who will be in control? Will we have time to know that before it is too late? A well-known expression suggests that, “where there is a will there is a way.” Certainly human are distinct from most organisms because of their reason. However in an age unduly fevered by technology the phrase may be reversed to, “where there is a way there is a will” reversing the traditional relationship between means and ends. But even granted that, it is important to maintain, if not a doubtful attitude, at least a skeptical attitude toward claims for the new, – at least until there is some evidence for the claims and voices beyond those who will profit from the introduction of a technology are heard.

Our age has two rather distinct fears of technology. One, ala George Orwell, is that it will work too well creating a manipulated, totalitarian society naively taking pride in how free it is. The other fear, reflective of Franz Kafka, is that it won’t work well enough. This suggests a crazily complex, out-of-control, rubric, interdependent, opaque, non-fail safe society steeped in technological errors and *catch-22* absurdities. The myth of Frankenstein alerts us to be ever vigilant to be sure that we control the technology rather than the reverse. Jacques Ellul’s (1964) warning about the danger of self-amplifying technical means silently coming to determine the ends or even becoming ends in themselves, separated from a vision of, and the continual search for, the good society needs to be continually repeated.

Bibliography

- ALEXANDER, J. (2001). An overview of the future of non-lethal weapons. *Medicine, Conflict, and Survival*, 17:180-193.
- ALPERT, G., SMITH, M., KAMINSKI, R., FRIDELL, L., MACDONALD, J. AND KUBU, B. (2011). “Police use of force, tasers and other less-lethal weapons” *NIJ Research in Brief* 1-19 (May, 2011). Washington, D.C.: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.
- BATTON, C. and WILSON, S. (2006). *Police murders: An examination of historical trends in the killing of law enforcement officers in the United States, 1947-1998*. *Homicide Studies*, 10:79-97.
- BRAGA, A. (2006). “Policing crime hot spots” in B. Welsh and D. Farrington, eds. *Preventing Crime: What works for Children, Offenders, Victims, and Places*, 179-193. Great Britain: Springer.

- BRAGA, A., FLYNN, E., KELLING, G., AND COLE, C. (2011) "Moving the Work of Criminal Investigators Towards Crime Control" *New Perspectives in Policing*. Cambridge: Harvard Kennedy School.
- BYRNE, J. (2009). *The New Generation of Concentrated Community Supervision Strategies: Focusing Resources on High Risk Offenders, Times, and Places*. (Washington, DC: A Report for the Public Safety Performance Project, the Pew Charitable Trusts).
- BYRNE, J. (2008) "Editorial Introduction-The social ecology of community corrections: understanding the link between individual and community change". *Criminology and Public Policy*, p. 263-274.
- BYRNE, J. and REBOVICH, D. (2007). *The New technology of Crime, Law and Social Control* Monsey, NY: Criminal Justice Press.
- BYRNE, J. and REBOVICH, D. (2007). "Introduction. The New Technology of Crime, Law and Social Control." In: BYRNE, J. and REBOVICH, D.(2007). *The New technology of Crime, Law and Social Control*, Monsey, NY: Criminal Justice Press, p. 1-21
- BYRNE, J. and PATTAVINA, A. (2007). "Institutional Corrections and Soft Technology". In BYRNE, J. and REBOVICH, D. (2007). *The New technology of Crime, Law and Social Control*, Monsey, NY: Criminal Justice Press, p. 245-286.
- BYRNE, J. and TAXMAN, F. (2006). "Crime Control Strategies and Community Change" *Federal Probation* June: 3-12.
- BYRNE, J. and TAXMAN, F. (2005). "Crime (Control) is a Choice: Divergent Perspectives on the Role of Treatment in the Adult Corrections System" *Criminology and Public Policy*, p. 291-310.
- CHAN, J. (2001). "The Technology game: How information technology is transforming police practice" *Journal of Criminal Justice*, 1:139-159.
- CLARKE, R. V. (1997). *Situational crime prevention: Successful case studies*. Albany, NY: Harrow and Heston.
- COLE, D., and LOBEL, J. (2007). *Less safe, Less Free: Why America is Losing the War on Terror*. New York: The New Press.
- CORBETT, R. and MARX, G. (1991) "Critique: No Soul in the New Machine: Technofal-lacies in the Electronic Monitoring Movement". *Justice Quarterly*, 8(3):359-414.
- ELLUL, J. (1964). *The technological society*. New York: Vintage Books.
- FARRELL, G. (1995). Preventing Repeat Victimization. In Michael Tonry and David P. Farrington, Eds., *Building a Safer Society. Crime and Justice*, Vol. 19. Chicago: University of Chicago Press.
- FARRINGTON, D., and WELSH, B. (2005). "Randomized Experiments in Criminology: What Have We Learned in the Last Two Decades?" *Journal of Experimental Criminology* 1:1-29.
- FEDERAL BUREAU OF INVESTIGATION (2004). *FBI Strategic Plan: 2004-2009*. Washington, D.C., Federal Bureau of Investigation .
- FELSON, M and CLARKE, R. V (1998). *Opportunity makes the thief: Practical theory for Crime Prevention*. Police Research Series Paper 98. London: Home Office.

- GANDY, O. (2007). *Race and Cumulative Disadvantage: Engaging the Actuarial Assumption* (The B. Aubrey Fisher Memorial Lecture, Department of Communication, University of Utah, October 18, 2007).
- GARLAND, D. (2002). *The Culture of Control: Crime and Social Order in Contemporary Society*. New York: Oxford University Press.
- GIBBONS, J. and KATZENBACH, N. (2006). *Confronting Confinement: A Report of the Commission on Safety and Abuse in America's Prisons*. Vera Institute of Justice, New York, NY.
- GILLIGAN, J. (1996). *Violence: Reflections on a National Epidemic*. New York: Random House.
- GREENBURG, D. and ROUSH, J. (2009). "The Effectiveness of an electronic security management system in a privately owned apartment complex" *Evaluation Review* 33(1): p. 3-26.
- GROFF, E. and MCEWEN, T. (2008). *Identifying and measuring the effects of information technologies on law enforcement agencies: The making officer redeployment effective program*. Washington, D.C U.S. Department of Justice, Office of Community Oriented Policing Programs.
- HAGGERTY, K. (2008). "Book Review: Evidence-Based Crime Prevention" *Theoretical Criminology*, p. 121-126.
- HARRIS, A. and LURIGIO, A. (2007) "Crime Prevention and Soft Technology: Risk Assessment, Threat Assessment, and the Prevention of Violence", P 103-132, in BYRNE, J. and REBOVICH, D.(2007). *The New technology of Crime, Law and Social Control* (Monsey, NY: Criminal Justice Press).
- HARRIS, C. (2007) "Police and Soft Technology: How Information Technology Contributes to Police Decision Making" In: BYRNE, J. and REBOVICH, D.(2007). *The New technology of Crime, Law and Social Control*, Monsey, NY: Criminal Justice Press, p. 153-183.
- HANKIN, A., HERTZ, M., and SIMON, T. (2011). "Impacts of metal detector use in schools: insights from 15 years of research" *Journal of School Health*, 81(2), p. 100-106.
- HIER, S. (2004). Risky spaces and dangerous places: Urban surveillance, social disorder and CCTV. *Social and Legal Studies*, 13(4):541-554.
- HIRSCHI, T. (1987). On The Compatability of Rational Choice and Social Control Theories of Crime. In Derek CORNISH and Ronald CLARKE, Eds., *The Reasoning Criminal*. NY: Springer-Verlag.
- HOOGENBOOM, B. (2010). *The Governance of Policing and Security: Ironies, Myths and Paradoxes*. Palgrave Macmillan.
- HOMELAND SECURITY PRESS RELEASE (2010). Secretary Napolitano Announces Additional Recovery Act Funding for Airport Security Technologies. Available at: http://www.dhs.gov/ynews/releases/pr_1275500818702.shtm
- HUBBS, K. and KLINGER, D. (2004). *Impact munitions use: Types, targets, effects*. Washington, D.C.: Department of Justice, Office of Justice Programs, National Institute of Justice.

- HUMMER, D. (2007). "Policing and "Hard" Technology" In: BYRNE, J. and REBOVICH, D.(2007). *The New technology of Crime, Law and Social Control*, Monsey, NY: Criminal Justice Press, p. 133-152.
- HUXLEY, A. (1932). *Brave New World* New York: Bantom Books.
- KLEIMAN, M. (2005). *When Brute Force Fails: Strategic Thinking for Crime Control*. Final report to the National Institute of Justice(ncj: 211204)
- KLEIN, N. (2008). *China's All Seeing Eye*. Rolling Stone, May 14, 2008, available at www.naomiklein.org?articles/2008?05/chinas-all-seeing-eye
- KRASKA, P.B.(2001) *Militarizing the American Criminal Justice System: The Changing Role of the Armed Forces and the Police*. Boston, Ma.: Northeastern University Press
- LEMAN-LANGLOIS, S. (2008). *Technocrime: Technology, crime, and social control*. Cul-lompton, Devin: Willan Publishing
- LAUB, J. and SAMPSON, R. (2001). "Understanding Desistance from Crime". In: TONRY, M. *Crime and Justice: A Review of Research, vol.28*, University of Chicago Press.
- MANDELSTAM, J. and MULFORD, C. (2008). Unintended consequences of sex offender residency laws: Can GIS mapping help? NIJ Update. Washington, D.C.: National Institute of Justice.
- MANNING, P. (2003). *Policing Contingencies*. Chicago: University of Chicago Press.
- MANNING, P. (2008a). "Surveillance: From them to us and back to them". Presentation at the 2008 Hixon-Riggs Forum on Science, Technology, and Society, Roger Mudd College, Claremont, Ca: March 28.
- MANNING, P. (2008b). "A view of surveillance", In: LEMAN-LANGLOIS, (ed) *Techno-Crime: Technology, Crime, and Social Control*, Willan Publishing: Collompton, Devon, p. 209-242.
- MARX, G. (2008). "Windows into the soul: Surveillance and society in an age of high technology" Keynote Presentation at the 2008 Hixon-Riggs Forum on Science, Technology, and Society, Roger Mudd College, Claremont, Ca: March 27.
- MARX, G. (1976) "Alternative Measures of Police Performance" in VIANO, E. (ed.) *Criminal Justice Research*. Lexington Books.
- MARX, G. (1988). *Undercover: Police Surveillance in American Society*. Berkeley: Univ. of California Press.
- MARX, G. 2009. "A Tack in the Shoe and Taking off the Shoe: Neutralization and Counter-neutralization Dynamics" *Surveillance and Society*.
- MARX, G. (2001). "Technology and Social Control: The Search for the Illusive Silver Bullet" *International Encyclopedia of the Social ad Behavioral Sciences*.
- MARX, G. (2007). "Rocky Bottoms and Some Information Age Techno-Fallacies". *Journal of International Political Sociology*, vol. 1, no. 1.
- MARX, G. (2007). "Engineering of Social Control: Intended and Unintended Consequences" P In: BYRNE J. and REBOVICH, D. (eds) *The New Technology of Crime, Law and Social Control*, Monsey, NY: Criminal Justice Press, p 347-371.

- MARX, G. (2008) "Windows into the soul: Surveillance and society in an age of high technology". Keynote Presentation at the 2008 Hixon-Riggs Forum on Science, Technology, and Society, Roger Mudd College, Claremont, Ca: March 27, 2008.
- MAZEROLLE, L. WATKINS, C., ROGAN, D., FRANK, J. (1998). Using gunshot detection systems in police departments: the impact on police response times and officer workloads. *Police Quarterly* 1(2): 21-49.
- MUELLER, R (2011). "FBI budget for fiscal year 2012" Statement before the Senate Committee on Appropriations, Subcommittee on Commerce, Justice, Science, and Related Agencies (April, 7, 2011) downloaded 4/8/2011 from www.fbi.gov/news/testimony/fbi-budget-for-fiscal-year-2012-1.
- NESTEL, T. (2006). Using Surveillance camera systems to monitor public domains. Master's Thesis, Naval Postgraduate School (March). <http://www.chds.us>.
- NOGALA, D. (1995). "The future role of technology in policing". In: BRODEUR, JP. (ed) *Comparisons in Policing: An International Perspective*, Avebury, UK: Aldershot, p. 191-210.
- NUNN, S.(2001). Police technology in cities: Changes and challenges. *Technology in Society*, 23:11-27.
- PATTAVINA, A. (2005) *Information Technology and the Criminal Justice System*. Thousand Oaks, Ca: Sage.
- PATTAVINA, A. and TAXMAN, F.(2007). "Community corrections and soft technology" BYRNE, J. and REBOVICH, D. (ed). *The New Technology of Crime, Law, and Social Control*. Monsey, N.Y. Criminal Justice Press, p 327-346.
- Police Executive Research Forum (2011) "Use of technology in Policing: The chief's perspective" *Critical Issues in Policing Series*. Washington, D.C. Police Executive Research Forum (April 4, 2011).
- REAVES, B. (2010). *Local Police Departments, 2007*. Washington, D.C.: Bureau of Justice Statistics.
- REBOVICH, D. and MARTINO, A. (2007). "Technology, Crime Control and the Private Sector in the 21st Century" P 49-79, BYRNE, J. and REBOVICH, D. (ed). *The New Technology of Crime, Law, and Social Control*. Monsey, N.Y. Criminal Justice Press, p 327-346.
- REICHERT, K. (2001). "Use of information technology by law enforcement". *Promising Approaches to Addressing Crime Series*. University of Pennsylvania, Jerry Lee Center of Criminology, Forum on Crime and Justice.
- REISS, A. and ROTH, J. (1993). *Understanding and Preventing Violence*. Washington, DC: National Academy of Sciences.
- ROSENFELD, R., FORNANGO and BAUMER, E. (2005). Did CEASEFIRE, COMPSTAT, AND EXILE reduce homicide? *Criminology and Public Policy*, 4(3):419-450.
- SHERMAN, L.W., GOTTFREDSON, D.C., MACKENZIE, D.L., ECK, J.E., REUTER, P., and BUSHWAY, S.D. (1997). *Preventing Crime: What Works, What Doesn't, What's Promising*. Washington, DC: National Institute of Justice, U.S. Department of Justice.
- SKOGAN, W. and FRYDL, K. (2004). *Fairness and Effectiveness in Policing: The Evidence*. Washington, D.C.: National Academies Press, National Research Council.

- SOGHOIAN, C. (2011). "The Law Enforcement Surveillance Reporting Gap" unpublished report, Center for Applied Cybersecurity Research, Indiana University, Bloomington (April 10, 2011). Available at SSRN: <http://ssrn.com/abstract=1806628>
- STONE, C. and TRAVIS, J. (2011). "Toward a New Professionalism in Policing". *New Perspectives in Policing*. Cambridge: Harvard Kennedy School.
- STROSHINE, M. (2005). "Information technology innovations in policing". In R. DUNHAM and G. ALPERT, eds., *Critical issues in policing*(5th ed.) Longrove, Il.: Waveland Press.
- SUMMERS, N. (2009). "Walking the cyberbeat" *Newsweek*, May, 18, 2009. Available at <http://www.newsweek.com/id/195621>.
- TASER (2011). About Taser. available at <http://www.taser.com/about-taser>
- TAXMAN, F., BYRNE, J. AND PATTAVINA, A. (2005). "Racial Disparity and the Legitimacy of the Criminal Justice System: Exploring Consequences for Deterrence" *Journal of Health Care for the Poor and Underserved* 16, p. 57–77.
- TAYLOR, R., CAETI, T., LOPER, D., FRITSCH, E., AND LIEDERBACH, J. (2006). *Digital Crime and Digital Terrorism* . Upper Saddle River, New Jersey: Prentice Hall.
- TAYLOR, R.B. & GOTTFREDSON, S. (1986). "Environmental design, crime and prevention: An examination of community dynamics". In: REISS, JR. & TONRY, M. (Eds.), *Communities and Crime. Crime and Justice: A Review of Research*, Vol. 8. Chicago: University of Chicago Press.
- WEBSTER, C., DOOB, A., and ZIMRING, F. (2006). "Proposition 8 and Crime Rates in California: The Case of the Disappearing Deterrent" *Criminology and Public Policy*, p. 417-448.
- WEISBURD, D., TELEP, C., HINKLE, J., and ECK, J. (2010). "Is problem-oriented policing effective in reducing crime and disorder? Findings from a Campbell systematic review" *Criminology and Public Policy*, 9(1), p. 139-172.
- WEISBURD, D., MASTROFSKI, S. D., GREENSPAN, R., and WILLIS, J. J. (2003). Reforming to preserve: Compstat and strategic problem solving in American policing. *Criminology & Public Policy*, 2, p. 421-455.
- WEISBURD, D., MASTROFSKI, S. D., GREENSPAN, R. and WILLIS, J. J. (2004). *The growth of Compstat in American policing*. Washington, D.C.: Police Foundation.
- WELSH, B.C. and FARRINGTON, D.P. (2002). *Crime Prevention Effects of Closed Circuit Television: A Systematic Review*. Home Office Research Study, No. 252. London: Home Office.
- WELSH, B.C. and FARRINGTON, D.P. (2004). Surveillance for crime prevention in public space: Results and policy choices in Britain and America. *Criminology & Public Policy*, 3, p. 497-526.
- WELSH, B.C. and FARRINGTON, D.P. (Eds.). (2006). *Preventing Crime: What Works for Children, Offenders, Victims, and Places*. New York: Springer.
- WELSH, B.C. and FARRINGTON, D.P. (2007). "Crime Prevention and Hard Technology: The Case of CCTV and Improved Street Lighting", In: BYRNE, J. and REBOVICH,

D. *The New Technology of Crime, Law and Social Control*, Monsey, NY: Criminal Justice Press, p. 81-102.

WHITE, M. and READY, J. (2009). Examining fatal and nonfatal incidents involving the TASER: Identifying predictors of suspect death reported in the media. *Criminology and Public Policy*, 8(4):863-889.