POLICE USE OF TECHNOLOGY TO FIGHT AGAINST CRIME

Tombul Fatih, PhD
Turkish National Police, Batman City Police Department
Cakar Bekir, PhD
Turkish National Police, Kars City Police Department

Abstract

Traditionally, law enforcement agencies have had an unfriendly relationship with technology. However, there is no way one can ignore and/or resist the adoption of new technologies any longer since recent developments in information technology have changed the attitudes and perceptions of police forces as well as criminals. The technological advances over the years have provided law enforcement agencies new perspectives and considerations beyond the traditional methods and opportunities to utilize a wide range of innovations in different contexts. The recent innovations and implementations which increase the efficiency and effectiveness of policing including network analysis, GIS, crime mapping, biometrics, fingerprints, DNA research, facial recognition, speech recognition, social media policing, shotspotter detection system, and CCTV are detailed in this study.

Keywords: Police, law enforcement, fight against crime, police and technology

Introduction

Recent technologic developments have changed the way people in society live as well as their work routines. Developments evaluated as impossible previously are now seen as possible through the development of new technologies. Today, technology has become intrinsic to society and seems to be a natural component of our personal lives. On the other hand, criminal behaviors and routine habits have changed parallel to these technological developments. Criminals have started to use technology tools when committing crimes. With advanced software and hardware forms of technology they can commit crimes readily, and crimes have now shifted from their previous more observable methods of operation to the digital realm. This means that whoever realizes the importance of information technology and has enough knowledge about its recent developments can

take ownership of a situation to a greater extent today than in the past. In this regard, what should law enforcement agencies do to fight against the new application of digital technology as regards committing crimes and the criminals who use technology? How can they be better prepared to overcome the challenges associated with this issue? Of course, law enforcement agencies should give high priority to the importance of the developments in the new technologies more than simply to criminals and fighting against such crimes. This article focuses on the role of law enforcement authorities in the context of limiting digital or technologic crimes and discusses some technological tools that are being used in police organizations around the world.

The importance of the use of technology by police in fighting crimes

Information technologies have recently been utilized extensively in law enforcement agencies around the world both for the processes of general administration work (Personnel, Payroll etc.), as well as for core policing work, such as preventing crimes. Law enforcement agencies are now using a variety of newly developed technologies to fight against those criminals who are employing the advantages of these technologies for negative purposes. However, law enforcement agencies may need to seek out more highly developed software and technologies to overcome these application of technology by criminals which may be very sophisticated (Addarly & Musgrove 2001, p. 100). Organizations also need to begin to adapt their daily routines and procedures to the available computer technology in order to remain competitive in their various environments. However, organizations can face difficulties in taking advantage of new technologies to boost an organizations' performance due to the lack of effective technology utilization and the resistance of organization managers and professionals to apply these technologies in the workplace (Fred, Bagozzi, & Warshaw, 1989, p. 982).

Crimes can occur at any time and can take place anywhere and in varied forms. Police forces categorize crimes according to crime type and whether the crime is major or not and whether it is a volume crime or not. While murder, armed robbery and rape are evaluated as major crimes, crimes such burglary and shoplifting are categorized as volume crimes. These crimes can be committed individually or in serial fashion. If the crime is committed in serial fashion finding the offender is easier than the individual case alone due to the possible availability of having a common description of an offender who has committed different crimes in different places. Law enforcement agencies often employ crime analysts who are experts on information technologies and different types of discipline. They assist the police force by showing them the links among crimes, detecting the crime

patterns and trends, and developing programs that expose those criminals who commit serial crimes. Law enforcement agencies also utilize information technology and can create different software and hardware tools that can analyze data such as crime recordings and Geographic Information System (GIS) data (Addarly & Musgrove 2001, p.100).

The public's expectations as regards law enforcement agencies is that they should have advanced technologies and use these in order to prevent crimes, respond to crises and conduct appropriate investigations. In addition, technology should enable the police to analyze different types of information so as to achieve appropriate results. The public also expects that even if law enforcement agencies have quantities of sensitive personal information they have enough technology and security tools to protect these pieces of information. It is a fact that police forces have some policies in place to handle the information they have on hand. All the information such as the owner of the information and acquiring the time of the information is legally stored in databases and that allows police to analyze related sections of that information. Managing the information legally, acquiring the related information from different databases and providing this with efficiency is the most difficult part of law enforcement (Johnston, 2007, p. 68).

According to the study reported by Garicano and Heaton (2010, p. 196) although there is no significant relationship between general IT and crime fighting and deterrence, the productivity of the police increases when the adaptation to using IT rises. Like other companies, police organizations acquire advantages in using IT when they merge these technologies and their organizational practices to yield appropriate results.

Colvin and Goh (2005) emphasized the fact that the use of IT is an important factor affecting the performance of police work. In their study it was proven that information quality and timeliness are two important components that are effective in terms of achieving the acceptance by patrol officers. Wright (1978, p. 306) commented that the aim of technology as used in law enforcement is to facilitate and provide efficiency in policing. Technology has also shifted the perception of the police and changed the character of traditional policing. Using technology in law enforcement also represents a change in police management and organization. In other words, there is a positive relationship between police management and adaptation to the new technologies.

Hughes and Jackson (2004, p.65) explained that knowledge is the driving force for an organization in terms of competition with other organizations in the world. By using knowledge strategically, organizations can produce effective outputs that lead to customer satisfaction. It can be said that organizational knowledge is so important that investing in knowledge assets in an organization is much more profitable than investing

in material assets. Thus law enforcement agencies spend considerable effort on knowledge management in order to have a learning organization that can best characterized by the principles of innovation, sharing and analysis. In explaining why law enforcement agencies give importance to the learning organization, Luen (2001, p. 312) cited two reasons for investing in knowledge management; one of them was that police forces need accurate and timely information. The second was that police forces have to deal with vast amounts of data and contacts.

George (2005) explained that law enforcement agencies should utilize all available information technologies when creating portals to merge decentralized databases since agencies may strongly demand a database that allows them to share crime data in cooperation with other institutions in the judicial area. The interesting thing is that criminals are professional enough to utilize IT for purposes of committing more crimes and defining more targets. For example drug dealers were the early users of cell phones and pager technologies.

According to a study by Ellahi and Manarvi (2010, p. 22) if an organization takes into consideration the user characteristics of their employees, the utilization of Information technology (IT) can increase. Otherwise no organization can achieve the expected performance level of utilization of IT. The study also revealed that the attitude of police officers in relation to computer usage is very important as it affects the use of IT as a tool in policing. An awareness program explaining the positive aspects of using computers in policing should be conducted in order to assist officers to have a more positive attitude about IT usage in policing.

Custers (2012) enlightens us that law enforcement agencies do try to optimize the use of technology in criminal investigation and prosecution processes, but many of the users are not satisfied. Owing to their lack of insight about new technology, users might prefer to continue to use the current technology rather than the new technology. Furthermore, Custers (2012, p. 67) claims it is not clear which technologies are more usable and effective in the context of a police organization. Thus, it is impossible to know precisely which obstacle, lack of budget, or knowledge or experience, is a barrier to the use of new technology. A critical review and clear understanding is important for learning about these obstacles. In order to tackle this issue, a large paradigm shift is required to arrive at a decision about which technologies should be used.

In sum, a successful fight against crime can be provided with proactive strategies and tactics. For that reason, technology supported crime prevention programs and strategies are vitally important methods and actions in combating crime. The technological advances over the years have provided law enforcement agencies new perspectives and considerations

beyond the traditional methods and opportunities to utilize a wide range of innovations in different contexts.

Recently Developed Technologies used in Policing

There are many recent advances and changes in both the hard and soft technologies of policing used by law enforcement departments in a wide range of contexts. The recent innovations and implementations which increase the efficiency and effectiveness of policing including network analysis, GIS, crime mapping, biometrics, fingerprints, DNA research, facial recognition, speech recognition, social media policing, shotspotter detection system, and CCTV are detailed below:

Network Analysis: Sutherland (1947) claimed that the social networks of an individual can serve as the source for crimes and delinquency. According to this author if a person is subject to criminal activities and criminals then the probability of his learning to carry out criminal and delinquency activities will be high as criminal behaviors are learned. Network analysis is an important tool for law enforcement purposes and one can demonstrate the nature of any an emerging relationship between two persons in this regard. Knowing who knows who in social network sites like Facebook and MySpace may help police forces to shed light on a given criminal case. On the other hand, the information from traffic data on telephones and email may represent an important clue to solving a criminal activity (Custers, 2012).

In particular, social network analysis (SNA) is a powerful tool for law enforcement that can help police to analyze, discover and envision the actions of criminal suspects. Besides using SNA it is possible to map the relationship of a criminal when police forces have sufficient data to analyze. The manual examination of social networks is time consuming and ineffective compared to the use of SNA which increases the effectiveness and efficiency of law enforcement agencies. It is known that social networks sometimes cause the spread of illegal behaviors. They can cause young people to carry out illegal behaviors such as juvenile delinquency. Thus, to reduce criminal behavior, the use of SNAs by law enforcement agencies is essential in the context of having an effective crime fighting strategy (Johnson, Reitzel, Norwood, McCoy, Cummings, & Tate, 2013).

Geographical Information System GIS and *Crime Mapping* are new technologies that have been well used within policing. GIS is a spatial decision support system (SDSS) that focuses on decision making and problem solving processes (Crossland & Wynne, 1994). "GIS is not simply another alternative data display tool. It is a comprehensive set of tools for collecting, storing, retrieving, analyzing and displaying spatially referenced information" (Crossland & Wynne, 1994 p. 542). In GIS, implementations,

automated computerized pin mapping and hot spot analysis are the most widely used applications among law enforcement departments. Crime mapping provides an informative output and mental representation that increases the accuracy of decisions on decision making process. Hence, the system minimizes the effort and enhances the decision maker's (law enforcement) existing capacity (Vessey, 1991; Smelcer & Carmel, 1997).

Crime mapping applications enable law enforcement agencies to analyze crime incidents and affect factors within any geographic area. It is worth noting here that "a picture is worth a thousand words" (Vessey, 1991, p. 219). In other words, mapping allows officers to see the big picture on a single snapshot and it helps agencies to determine high-crime points, crime types, and the best way to respond. It also helps them to identify high risk and hazardous points in a geographical area. Hence, the system enables agencies to create more effective crime prevention strategies and methods in the policing context.

It should be emphasized that a GIS application does not aim to predict specific events and their offenders in a certain time. It is very difficult to predict certain time, point, and event to occur, but the applications can help to identify the most likely areas where they may occur and which crimes may occur in a jurisdiction. Regarding this issue, Risk Terrain Modeling (RTM) is a good example that can be created in GIS. RTM is a method of representing risk assessment which was developed by the Rutgers University School of Criminal Justice (Caplan, 2014). RTM provides an approach to analysts that helps them to identify risk terrains which represent actionable meaning related to crime outcomes. This approach can help planners to predict where crimes are more likely to happen. The RTM process occurs in three steps; First, based on theoretical grounding, analysts use criminological theories which provides an overview of the social and environmental risk factors influencing crime patterns. In the second step, RTM use technical methods that employ ArcGIS software to represent risk terrains. In the final step, analysts present their ideas and forecasts to decision makers developing strategic and tactical decision making in the future (Caplan & Kennedy, 2010). In short, RTM provides meaningful and measurable information and interpretations that can address the most vulnerable areas in a jurisdiction for decision makers at all levels.

Biometrics: Biometrics refers to technologies based on an individuals' unique characteristics, such as their finger prints, their DNA make up, and their voice patterns (Custers, 2012). Biometrics has been used for many years in police forces and intelligence agencies around the world. Biometrics are used to identify the individual. In addition they are used to figure out who the suspects or criminals are who are responsible for

committing a crime (For example finding the criminals who left their fingerprints on the gun) (FBI, 2014).

Biometric technology is utilized in law enforcement for matching sensitive information by comparing this with different regional and national databases that have a superior authentication ability. Portable biometric identity management technologies also enable police forces to verify drivers' licenses and mug shots over fingerprint readers.

A fingerprint is one of the most important forms of biometrics that is utilized in law enforcement agencies around the world. Fingerprints vary depending and are unique to different persons and do not change over the time. Thus, fingerprint analysis is a very useful tool for law enforcement agencies in terms of identifying the suspect and providing useful evidence related to verifying the suspect of any crime. The Integrated Automated Fingerprint Identification System used by FBI does not store fingerprints, but keeps a record of criminal histories such as mug shots, scars, and hair and eye color. That system has the fingerprints of 70 million suspects and 34 million civil prints in its database (FBI, 2014).

*DNA research. B*esides using fingerprints, law enforcement agencies have obtained lots of advantages with the application of DNA research. The popularity of using DNA increased when forensic scientists took part mostly in many TV documentaries and others items of various channels. It is a fact that no other investigative tool has changed the view point in justice system as much as the use of DNA tests and analysis. DNA analysis gives direction to police forces in investigation process. First of all, DNA analysis can solve lots of difficult cases, especially those that have failed when using other techniques. Secondly, even if there are no witnesses, DNA analysis can provide some additional crime clues of importance. In addition, it also reduces arrests that were implemented wrongly with the use of old techniques. Besides, it improves the reliability of the evidence. Last, but not least, it can depict the connection of one crime case with other cases (Prime & Newman, 2007).

Facial recognition is another form of technology that helps law enforcement agencies to obtain the profile of individuals and to analyze it from different databases. Speech recognition technology is also useful for law enforcement purposes to identify audio samples of criminals and to compare these with known criminal profiles (Findbiometrics, 2014).

Social Media: Social media has influenced millions of people and become indispensable in the everyday lives of people around the world. Its attraction face caused the different networking sites to erupt on the internet. However those networking sites although using the same technologies, have different establishment aims While some of them serve the purpose of politics, others emphasize the shared interests of many people. In this

respect, criminals are taking advantage of using technology including social media to commit crimes.

According to Stuart (2013), social media is a crucial tool for law enforcement agents, because it can help them connect with the general public. With social media, the general public can send and receive real time information and provide related documents such as pictures and audio records that can help to solve crimes. Social media allow law enforcement agents to remain in contact with local communities thus providing a useful source of information in an effective way.

Many law enforcement agencies also use social media to some extent. In particular, social media is an important key tool in crisis situations such as earthquakes, tsunamis, and riots etc. For example, in 2011, investigators from Kentucky State Police posted photos of jewelry and a facial composite of an unknown person found ten years ago and after that the police identified the deceased person as a result of receiving some evidence from users of social media (Highland, 2011). The Boston Police Department also used social media following the bombings at the 2013 Boston Marathon. After the attacks the department actively used social media as a means of sharing information with the community to find suspects. The Vancouver riots provides another important example of the use of social media in policing. After the Vancouver team lost at the 2011 Stanley Cup Playoffs, a riot started in downtown Vancouver and the rioters destroyed stores and cars. Within an hour of the riot, social media users organized themselves and cooperated with the police. They started to submit photos and videos through Facebook and mobile technologies. People created a kind of surveillance on their own suing social media and this process resulted in direct and rapid cooperation between the community and the police. The Vancouver police obtained and benefited from thousands of pieces of digital evidence related to the events (Trottier, 2012). Hence, social media can provide one of the easiest and cheapest ways for law enforcement agencies to obtain and access evidence in any event. The problem that the law enforcement agencies face is how to obtain accurate information in any communication with the public. As seen in the Vancouver example, social media and mobile technologies can help to solve crimes by providing an effective means of communication between public members and law enforcement agencies.

ShotSpotter Detection System: This system is very useful for law enforcement agents in the context of detecting gunfire. These sensors can be located on rooftops and can be used for monitoring the sounds made by a gun. The system can log hundreds of gunfire incidents in a given period of time. For example, approximately 39000 separate incidents of gunfire have been documented with 300 acoustic sensors across 20 square miles of the Washington DC. The system can be installed at sites where the most violent

crimes occur to provide information on the specific location of the crime. ShotSpotter detection systems also enable police to report all gunfire incidents, as not all gunfire incidents may have been reported in the past due to an assumption the sound was not gunfire (Petho, Fallis, & Keating, 2013).

CCTV: The factors that make a society feel unsafe such as higher crime rates, increased terrorist attacks, and school and workplace shootings have led law enforcement agencies to install closed-circuit television (CCTV) security monitoring systems in many locations. Some of these video cameras are installed inside police vehicles and are used to monitor stops and vehicle movement. With the development of technology, the cost of CCTV equipment has declined. Thus many security managers have started to install and implement security monitoring systems in the locations they are responsible for. As well, wireless technology has enabled law enforcement agencies to monitor security cameras from their laptops and mobile phones. Crime investigation units of law enforcement agencies can also take advantage of CCTV. Crucial evidence captured by CCTV is often helpful for enlightening a crime case and providing evidence to the court. Videos are utilized mostly in police departments for patrol vehicle in-car cameras, training, public affairs, robbery investigation, crime scene processing, undercover surveillance, tactical operations, vehicle collision investigation, interrogation, and video lineup (Fredericks, 2004).

Conclusion

Traditionally, law enforcement agencies have had an unfriendly relationship with technology. However, there is no way one can ignore and/or resist the adoption of new technologies any longer since recent developments in information technology have changed the attitudes and perceptions of police forces as well as criminals. Undoubtedly, the technologically sophisticated types of crimes related to these perceptions and attitudes will increase and continue. However, the effective use of technological advancements and the implications of utilizing IT for policing will be helpful in combating crimes.

For pro-active policing solutions, information technologies can undoubtedly serve an important role in policing. It is no longer a luxury for law enforcement agencies to have large amounts of information and to be able to analyze them an automated way (Johnston, 2007). It is clear that the traditional and age-old methods and strategies neither provide for better control and decision making nor do they help in effective crime fighting. This also results in a lower performance level by a law enforcement agency. For that reason, the only solution to achieving successful policing lies in following current technological developments more closely, understanding

the effective use of information technology, and applying this in a wide range of policing contexts.

References

Adderley, R. W., & Musgrove, P. (2001). Police crime recording and investigation systems–A user's view. Policing: An International Journal of Police Strategies & Management, 24(1), 100-114.

Caplan J. M. (2014). Risk Terrain Modeling for Strategic and Tactical Action. Crime Mapping and Analysis News, A police Foundation Publication.

Caplan, J. M. & Kennedy, L. W. (2010). Risk Terrain Modeling Manual. Newark, NJ: Rutgers Center on Public Security.

Colvin, C. A., & Goh, A. (2005). Validation of the technology acceptance model for police. Journal of Criminal Justice, 33(1), 89-95.

Crossland, M., & Wynne, B. (1994). Measuring and testing the effectiveness of a spatial decision support system. Proceedings of the Twenty- Seventh Hawaii International Conference on System Sciences, 27(4), 542-551.

Custers, B. (2012). Technology in policing: Experiences, obstacles and police needs. Computer Law & Security Review, 28(1), 62-68.

Ellahi, A., & Manarvi, I. (2010). Understanding attitudes towards computer use in the police department of Pakistan. The Electronic Journal of Information Systems in Developing Countries, 42(1), 1-26.

FBI (2014). Fingerprints & Other Biometrics.
http://www.fbi.gov/about-us/cjis/fingerprints_biometrics

FindBIOMETRICS, (2014). Justice and law enforcement biometrics.
http://findbiometrics.com/applications/justicelaw-enforcement/

Fred, D., Richard, P., Bagozzi, and Paul R. Warshaw. "User acceptance of computer technology: A comparison of two theoretical models." Management science 35.8 (1989): 982-1003.

Fredericks, G. (2004). CCTV: A law enforcement tool. Police ChiefMagazine.http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=disp layarch&article_id=359&issue_id=82004

George, N. (2005). Hip Hop America. PenguinHighland, D. (2011). KSP Turns to Facebook as Investigative Tool, Bowling Green Daily News,http://www.bgdailynews.com/news/ksp-turns to- facebook-as-investigative-tool/article_00d04894-3a41-59b5-96f5-631ac03ed070.html.

Johnson, A. J., Reitzel, D. J., Norwood, F. B., McCoy, M., Cummings, B.,& Tate, R. R. (2013). Social Network Analysis: A Systematic Approach for Investigating.
http://www.fbi.gov/statsservices/publications/law-enforcement-bulletin/2013/March/social-network-analysis

Johnston, R. (2007). Law enforcement Fusion Centers: Where information, technology and Policy intersect. Sheriff Magazine, 67-70.
http:/www.lexisnexis.com/government/solutions/casestudy/lefusion.pdf
Garicano, L., & Heaton, P. (2010). Information technology, organization, and productivity in the public sector: evidence from police departments. Journal of Labor Economics, 28(1), 167-201.
Hughes, V., & Jackson, P. (2004). The influence of technical, social and structural factors on the effective use of information in a policing environment. The Electronic Journal of Knowledge Management, 2(1), 65-76.
Luen, T. W., & Al-Hawamdeh, S. (2001). Knowledge management in the public sector: principles and practices in police work. Journal of information Science, 27(5), 311-318.
Petho, A., Fallis, S. D., & Keating, D. (2013). ShotSpotter detection system documents 39,000 shooting incidents in the District http://www.washingtonpost.com/investigations/shotspotter-detection-systm-documents-39000-shooting-incidents-in-the- district/2013/11/02/055f8e9c-2ab1-11e3-8ade-a1f23cda135e_story.html
Prime. R. J., & Newman, J. (2007). The impact of DNA on policing: Past, Present, and Future. The PoliceChief.
http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_d=1320&issue_id=112007
Smelcer, J. B., & Carmel, E. (1997). The effectiveness of different representations for managerial problem solving: Comparing tables and maps. Decision Sciences, 28(2), 391-420.
Stuart, D. R. (2013). Social media: Establishing criteria for law enforcement use. http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/2013/february/social-media-establishing-criteria-for-law-enforcement-use.
Sutherland, E.H. (1947). Principles of Criminology. Fourth edition, Chicago:J.B. Lippincott.
Vessey, I. (1991). Cognitive fit: A theory-based analysis of the graphs versus tables literature. Decision Sciences, 22(2), 219-240.
Wright, S. (1978). New police technologies: an exploration of the social implications and unforeseen impacts of some recent developments .Journal of Peace Research, 15(4), 305- 322.