**Synergistic Effect of Technology in Combating Crime**

Abdulateef A. Khalefa

The National Ribat University

Khartoum, Sudan

profashmaig@hotmail.com

Mohamed H. Sayed

The National Ribat University

Khartoum, Sudan

M.hassan@ribat.edu.sd

**ABSTRACT:** Recently, crime has become one of the biggest threats to the survival of mankind on the planet. It is evidently a challenge to national security for all countries, a sure enemy to national development and stability. No doubt, Information and Communication Technology (ICT) has pervaded every facet of human endeavor, and crime groups too are taking advantage of its potentials to commit crimes. This paper present and highlight crime and the Synergistic Effect of Technology in combating crimes using digital skills of security agencies and proffer recommendations that can help mitigate crimes such as crime mapping technology, Smartphone applications, web reporting, social media, sharing information, and mobile technology. In spite of abuse of technology in committing crime, it does more good than harm in the fight against crime.

Key words: security, crime, internet technology, digital skills, crime detection, sharing information, mobile technology, managing crime, capacity building.

1. **Introduction:**

The term criminal can and has been applied to many types of behavior, some of which nearly all of us have been guilty of at some time in our lives. We can all think of acts that we feel ought to be criminal but are not, or acts that should not be criminal but are. The list of acts that someone or another at different times and at different places may consider to be crimes is very large, and only a few are defined as criminal by law at this time. Despite these difficulties, we need a definition of crime in order to proceed. The most often-quoted definition is that of Paul Tappan [1], who defined crime as “an intentional act in violation of the criminal law committed without defense or excuse, and penalized by the state”. A crime is thus an act in violation of a criminal law for which a punishment is prescribed; the person committing it must have intended to do so and must have done so without legally acceptable defense or justification.

Tappan’s definition is strictly a legal one that reminds us that the state, and only the state, has the power to define crime.

Technology has been considered a significant driver to law enforcement strategies and tactics for as long as can be remembered. In the 20th century, the introduction of the telephone, the automobile and two-way radios created seismic shifts in what police do, pushing departments toward a strategy of rapid response to citizens’ request for police assistance [2]. These technological capabilities provided closer connections and information sharing between police and the citizens they serve. Now, in the 21st century, powerful technological advancements have emerged, including closed-circuit television, automatic license plate readers (LPRs), in-car cameras, and body-worn cameras (BWCs), Predictive policing software, and social media communication and monitoring tools. The proliferation of computer technology, communication technology and other major technological advancements over the last several decades have made numerous technologies available to law enforcement officers that were virtually unheard of by their predecessors. Many departments are implementing these and other technologies to increase efficiency and improve outcomes, especially in times of diminished resources and enhanced public attention on and scrutiny of law enforcement tactics and outcomes.

1. **Conventional and cyber crimes:**

Cyber crime is not quite the same as conventional crime in different ways, yet two noteworthy contrasts are that, In cyber crimes, the culprit is regularly significantly harder to find, distinguish, and in the end get [3]. Numerous individuals utilize the web, content informing, and online networking to take cover behind a virtual character which, basically, can be anything and anybody they need. With the new capacities we have nowadays, anybody can figure out how to utilize the web further bolstering their good fortune and thus utilize it to hurt others. Hacking, which basically was outlandish (or exceptionally unrealistic) until of late, has turned out to be shockingly simple on the off chance that somebody can get the correct data. With conventional crime, the culprit doesn't have an indistinguishable capacity from inside cyber crime. While still difficult, cyber crime is a significantly less demanding approach to get what somebody needs. Some X person via web-based networking media could be your nearby neighbor and you'd never know it. With expanding information of PCs and how to utilize and control them, cyber crimes are more probable than at any other time. Programmers from different nations are disturbing atomic power plants, individuals are having their personalities and whole lives stolen from them. Cyber crime, while entirely different from conventional crime, is as yet an appalling offense. So conventional crimes can be defined as those traditional, illegal behaviors that most people think of as crime. Most crime is conventional crime. Non-conventional crime, may be [Organized Crime](http://sociologyindex.com/organized_crime.htm), [White-Collar Crime](http://sociologyindex.com/white_collar_crime.htm), [Blue-collar Crime](http://sociologyindex.com/blue_collar_crime.htm), [Pink-collar Crime](http://sociologyindex.com/pink-collar-crime.htm), [Political Crime](http://sociologyindex.com/political-crime.htm), [Corporate Crime](http://sociologyindex.com/corporate-crime.htm), [Occupational Crime](http://sociologyindex.com/occupational_crime.htm). Conventional crime includes murder, rape, assault, robbery, burglary and theft. Cybercrime is just a conventional crime committed with high-tech devices.

**3. The role of technology in committing crimes:**

The electronic age of personal computers and various devices have all been used as portals for information and various ways of communicating with others [4]. However, there are many individualsthroughout the world who have utilized these machines for committing crimes of a myriad of types.   
These crimes range from the theft of information from a person’s computer in his or her home to corporate secrets used as a competitive edge and to fraud and espionage. Digital crimes are wide-ranging and sometimes difficult to prosecute successfully. Without proper laws in place, these violations may perpetuate for decades with little to no repercussions.

Individual hacking may be utilized through the use of a personal computer, anonymous device or some type of handheld machine. The most effective types of hacks involve code generated for specific means. These may be to steal information, change programs or systems, obtain something to seek financial gain or to commit other crimes. It is often the big corporations that contain the information a hacker may use the most to provide a way of greater monetary advantage. The use of software may be utilized to copy usernames and passwords to access private or protected information. This permits these individuals to peruse systems, websites, databases and other areas of a company or area of the internet.

**4. Digital skills in policing:**

Internationally, criminals are harnessing digital technology to expand the reach and increase the impact of their crimes. But advances in technology also present law enforcement agencies with an enormous opportunity to transform how they tackle crime. To fully benefit from the technology and to keep up with the proliferation of technology and networked devices, it is critical that police officers have the requisite digital skills to be effective [5].

The Strategy acknowledges the growing significance that digital sources play in police investigations. And it commits the Home Office to use money from the Police Transformation Fund to:“enable the Digital Investigation and Intelligence (DII) programmers to further develop police capability in relation to the skills and technology required to effectively police a digital age and protect victims of digital crime”. In order to achieve this goal, the Home Office and Law Enforcement Agencies will need to agree a robust and realistic approach to addressing the digital skills gap in policing. Policing has to be moved away from large volumes of face-to-face or online learning and towards a ‘just in time’ approach. Reference materials in the hands of users, which are kept current and correct, and can be referred to when there is a need would be preferable (rather than frontloading with an acceptance that training will be out of date within days). More streamlined and tailored face-to-face training would also be appropriate. Fast paced, immersive training can be delivered to large numbers to reduce abstraction.

**5. Detecting crimes before it happens:**

The idea of forecasting and detecting of crime dates back at least to the 1990s, when the U.S. Department of Justice launched projects aimed at developing statistical models of where crime might occur [6]. The maps produced were crude and because of limitations in computing power at the time, they were unable to handle large amounts of input data at the same time.

Some science-fiction media and literature are starting to become realities now; an artificial intelligence (AI) that can predict and detect crime is now in the works [7]. Despite the crime rate in Sudan being relatively low compared to other countries, Sudanese military and police are still intent on developing such a technology. For the crime detection to happen and be accurate though, police organizations will have a lot of things to keep in check, such as unusual transactions in banking systems, potential crime spots, and even an Individuals and communities economic situation. Afterward, it will rely on artificial intelligence algorithms in order to decide when and where crime will happen to send alerts. For now, AI applications are still not ready and are still undergoing tests, but progress may soon be made.

**6. The role of technology in managing crimes:**

The rational perspective suggests that organizations behave rationally by identifying official goals, designing strategies to accomplish those goals, and then implementing technology that supports and facilitates the strategies that they have designed [8]. Technological advances in recent years have changed the nature of policing so significantly that many methods and tools from just a decade ago have become antiquated and incompatible with current technology. Some of these advances include location-monitoring devices for the tracking of high-rate offenders, predictive analytics and crime mapping software for the deployment of officers into locations that cause or are likely to cause crime, crime scene technology that enhances the collection and processing of evidence, and interoperable Web-based and other communication devices that facilitate connections between police and the communities they serve.

**6.1 Predicting crimes:**

Predictive policing is the application of analytical techniques particularly quantitative techniques to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions. Several predictive policing methods are currently in use in law enforcement agencies across the world, and much has been written about their effectiveness [9]. Financial institutions are sharing information together to predict crimes, Anna Tims wrote " Last September Mohammad Rahman won a four-year battle for compensation for disabilities caused by clinical negligence. A court awarded him £500,000, which was paid into the current and savings accounts he held with Barclays. The victory was short-lived: when he withdrew £60,000 of the payout, Barclays froze both accounts"[10], so criminals attempting to commit crimes and launder funds should rightly be worried as all banks and regulators will detect, disrupt and prevent their activity. Predictive methods allow police to work more proactively with limited resources. The objective of these methods is to develop effective strategies that will prevent crime or make investigation efforts more effective.

Predictive policing” has received a substantial amount of attention in the media and the research literature. However, some myths about these techniques have also propagated. This is partly a problem of unrealistic expectations. There is an underlying, erroneous assumption that advanced mathematical and computational power is both necessary and sufficient to reduce crime. Here, we dispel four of the most common myths about predictive policing [11]:

Myth 1: The computer actually knows the future. Some descriptions of predictive policing make it sound as if the computer can foretell the future. These computer algorithms predict the risk of future events, not the events themselves. The computer, as a tool, can dramatically simplify the search for patterns, but all these techniques are extrapolations from the past in one way or another. In addition, predictions are only as good as the underlying data used to make them.

Myth 2: The computer will do everything for you. Although it is common to promote software packages as end-to-end solutions for predictive policing, humans remain by far the most important elements in the predictive policing process. Even with the most complete software suites, humans must find and collect relevant data, preprocess the data so they are suitable for analysis, design and conduct analyses in response to ever-changing crime conditions, review and interpret the results of these analyses and exclude erroneous findings, analyze the integrated findings and make recommendations about how to act on them, and take action to exploit the findings and assess the impact of those actions.

Myth 3: You need a high-powered (and expensive) model. Most police departments do not need the most expensive software packages or computers to launch a predictive policing program. Functionalities built into standard workplace software (e.g., Microsoft Office) and geographic information systems (e.g., ArcGIS) can support many predictive methods.

Myth 4: Accurate predictions automatically lead to major crime reductions. Predictive policing analysis is frequently marketed as the path to the end of crime. The focus on the analyses and software can obscure the fact that predictions, on their own, are just that—predictions. Actual decreases in crime require taking action based on those predictions. Thus, we emphasize again that predictive policing is not about making predictions but about the end-to-end process.

Depending on computer applications, CrimeRadar [12] is designed, specifically to empower citizens in so many cities round the world to better understand the crime risks they face and plan their routines accordingly. CrimeRadar is known also as crime mapping [13], crime mapping as a technology to combine geographic data with police report data, in order to display the information on a map to analyze where, how and why crime occurs, it shows users on computer of Smartphone application how crime is (unevenly) distributed in any geographical area any geographical area, as we can see in Rio de Janeiro (figure1). CrimeRadar also highlights the highly variable timing and seasonality of criminal incidents.

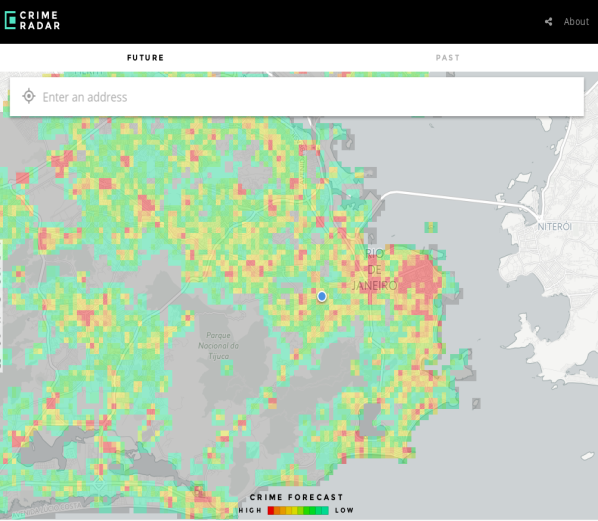


Figure 1. CrimeRadar for crime prediction

**6.2 Preventing crimes:**

Crime prevention is a pattern of attitudes and behaviors directed at reducing the threat of crime and enhancing the sense of safety and security, to positively influence the quality of life in our society, and to develop environments where crime cannot flourish [14], so the Metropolitan Act of 1829 says “The primary object of an efficient police is the prevention of crime: The next is that of detection and punishment of offenders if a crime is committed”. Preventing crime is an everyone’s business, it is more than security, also it is a responsibility of all levels and agencies of government, it is must be linked with solving social problems, and it is defiantly Cost-effective. One of the most useful methods of crime prevention is social Media, though it is a social trend as much as it is a technological breakthrough, social media use nonetheless furnishes law enforcement advantages for agencies that use the technology effectively. For example, criminals leave trails using social media platforms, so justice agencies turn to Facebook, Twitter and other channels for vital clues and insight into criminal behavior. The technology also enables officers to distribute information directly to concerned citizens, informing them of unfolding crimes and dangerous developments. Social media links law enforcement directly to the public at large, so it is a great tool for spreading descriptions, videos and other information about criminals. Communicating in real-time closes the crucial gap between the point at which crimes occur and when investigations begin, enabling citizens to respond with timely information.

The other method of crime prevention is web reporting, through which so many more peoples can access a computer to submit anonymous tips or photos using flying cameras (figure.2) to police departments. It’s one way to empower a disenfranchised community to move from being a “victim community” to a proactive part of the solution [15].



Figure 2. Flying camera

**6.3 Combating crimes:**

The word combating means to take action to reduce, destroy, or prevent (something undesirable) [16]. Combating crimes is the series of measures and actions taken by police authorities to reduce, destroy, or prevent crimes. There are five Common-Sense Ideas to Combat Crime:

a. Use and expand drug courts: Drug courts, which combine judicial supervision with substance abuse treatment, are rapidly gaining popularity as a tool to combat crime and drug use.

b. Make use of DNA evidence: By vastly improving the ability to identify and arrest suspects, DNA evidence has the potential to be a powerful crime-fighting resource, also DNA testing can provide evidence to support the exoneration of many convicted sex offenders.

c. Help ex-offenders find secure living-wage employment: Securing a well-paying job can help returning prisoners remain crime-free once they go back to their communities.

d. Monitor public surveillance cameras: public cameras can play crucial role in investigations of high-profile criminal acts. Cameras can also be a cost-effective means of preventing crime [figure 3].

e. Providing stable housing to returning prisoners: Access to stable housing can dramatically reduce crime committed by former prisoners.

The above five ideas will lead directly to these objectives for reducing the motivation to commit crime, which are:

a. Target urgent and coordinated initiatives towards young people judged to be at risk of falling into crime.

b. Provide sufficient support for people wishing to leave a life of crime.

c. Reduce the risk of those who have committed a crime reoffending after serving their sentence.

d. Develop effective preventive methods for dealing with violent offenders.



Figure 3. Public surveillance camera

**7. Findings and Discussion:**

**References:**

[1] Paul W. Tappan, “American Sociological Review”, Vol. 12, No. 1 (Feb., 1947), pp. 96-102.

[2] Harris, C. “Police and soft technology: How information technology contributes to police decision making”. In J. Byrne & D. Rebovich (Eds.), the new technology of rime, law, and social control (pp. 153–183). Monsey, NY: Criminal Justice Press, 2007.

[3] Darin Swan, “Physical and Cyber crime: A brief comparative analysis”, University of Maryland.

[4] <https://www.hg.org/legal-articles/how-computers-are-used-to-help-commit-crimes-40716>, “ How Computers Are Used to Help Commit Crimes”, *Provided by HG.org.*

[5] <https://www.gov.uk/government/>

uploads/system/uploads/attachment\_data/file/456623/Fire\_Statistics\_Monitor\_April\_2014\_to\_March\_2015\_Updated260815.pdf

[6] Captain Elizabeth Morales, “Using predictive policing zone maps with the Los Angeles Police Department in the LAPD Foothill Division”, October 24, 2016. https://www.nbcnews.com/mach/science/how-science-helping-stop-crime-it-occurs-ncna805176.

[7] <https://socialnewsdaily.com/75527/> artificial-intelligence-that-can-detect-crime-before-it-happens-now-in-development/

[8] Cyert, R. M., & March, J. G. “ A behavioral theory of the firm” , Malden, MA: Blackwell,1963.

[9] Walter L. Perry, Brian McInnis,” The Role of Crime Forecasting in Law Enforcement Operations”, Library of Congress, ISBN: 978-0-8330-8148-3

[10] The Guardian, International Edition, sun 22 Jan 2017, https://www.theguardian.com/money/2017/jan/22/barclays-took-my-440000-customers-caught-up-banks-de-risking-money-laundering-laws

[11] James Bridle, “New Dark Age: Technology and the End of the Future”, CPI group UK, Croydon 2018.

[12] https://igarape.org.br/en/what-happens-when-we-can-predict-crimes-before-they-happen/

[13] Jia, Ma,“How the use of computerized crime mapping was affected by characteristics of law enforcement agencies in 2007”, Graduate Theses and dissertations. 13616, https://lib.dr.iastate.edu/etd/13616

[14] [Ann M. Harkins](https://www.google.com/search?q=Ann+M.+Harkins&stick=H4sIAAAAAAAAAOPgE-LUz9U3MClOT8lV4gIxi0wry5IrtRSzk63084vSE_MyqxJLMvPzUDhWyan5APk1Jr88AAAA&sa=X&ved=2ahUKEwjF_Y6VwNbfAhUDWywKHexIDxoQmxMoATAhegQIBhAS&biw=1440&bih=764), National Crime Prevention Council, <https://ncpc.org.sg/>, 2007.

[15] Thaddeus A. Hoffmeister, “ Social Media in the Courtroom: A new era for criminal justice”, Library of Congress, ISBN:978-1-4408-3005-1, 2014.

[16] <https://www.collinsdictionary.com>.