North American Policing in the Digital Age

Maria R. Haberfeld
John Jay College of Criminal Justice, New York, N.Y.

Abstract
This article addresses the varying levels of training preparedness and legal challenges facing the American local law enforcement agencies in the Digital Age. From the example of the New York City Police Departments' multiple units like: the SMART Unit (Social Media and Research Team), Real Crime Unit, Domain Awareness and Vehicle Recognition Unit to the overview of the majority of smaller police departments that have very limited, if any, type of preparedness. The majority of police departments in the United States are staffed with less than 50 sworn officers and the Digital Age policing challenges are numerous and addressed in a very uneven manner. However, the larger departments, like the N.Y.P.D., can provide a template for a more professional and effective response. Finally, in addition to the different modalities of numerous tactical responses embedded in the creation of the specialized units, there are challenges related to the legal aspects of these initiatives. Some of the legal challenges facing the specialized unit are discussed, focusing on the hurdles in obtaining legal subpoenas for the information posted on various social media platforms like the Instagram, Facebook and Snapchat. A template for proper proactive preparedness concludes this overview.

Keywords: Digital policing; North American policing; preparedness; digital interoperability; tactical response

Introduction

Policing in the 'Digital Age" is a somewhat obsolete concept in the year 2022. According to Goodwin (2016), the digital era, in all business like environments (which would include policing as well) commenced over a decade ago and right now we actually seem to be well immersed in the mid-digital environment. Goodwin further identifies three distinct stages of digital development:

- *Pre-digital age* – At first, the pre-digital age evolved slowly. Products became digitized. Photos became bits. Knowledge moved from encyclopedias to Wikipedia. The phone book became an online directory. Printed magazines became websites. This first age was all about physical products becoming digital. It led to creative destruction in retail, manufacturing and distribution, which is where we are now: the mid-digital age.
- *Mid-digital* – This is a period that straddles the age where digital is just becoming accepted into the mainstream, and the age where digital is fully immersed into our society.

- *Post-digital* – Like pre-digital, nobody will think of "digital" in this age. The concept of it will move into the background and, much like oxygen or electricity, we'll understand digital to be transformative yet irrelevant. There will be no more Chief Digital Officers in the same way that a Chief Electricity Officer doesn't exist today. In the post-digital age, digital technology will be a vast, quiet element forming the seamless backbone of life. The internet will be a background utility, noticeable only in its absence. Smart homes will work. Video will follow us around. Content will be paid for… all seamlessly and effortlessly (Goodwin, 2016).

Based on the fact that these developmental stages were identified by Goodwin over eight years ago, I would argue that we are past the mid-digital stage and well into post digital. Thus, looking at police organizations one needs to ponder if the departments themselves realize that they might be late into the game that started over a decade ago.

This article provides a brief insight into the level of preparedness of some of the 18,000 North American police departments, ranging from the largest, the New York City Police Department, to the smaller ones, with less than 50 sworn officers, while the latter truly represent the average size of a police department in the United States.

Research Questions

While looking at the concept of policing in the digital era, one needs to ponder what kind of research questions we need to answer to arrive at the conclusion regarding the level of preparedness of various law enforcement agencies. Lack of proper operationalization of complex phenomena goes back decades ago, when researchers started to look at cyber criminality and law enforcement ability to respond in a timely and proactive manner.

Going as far back as over four decades ago, Kupperman & Trent (1979) argued that the problem with technological terrorism has generally been ignored and that the United States government is woefully under-prepared to deal with a technological threat. Following their premonition into the year 2022, I posit that there are a number of vital research questions that need to be addressed, in order to arrive at a realistic picture of the level of proactive response of the American police forces.

These research questions are divided into two categories, one with a more general focus and the other centers on actual case studies. The case studies provide a perfect backdrop for understanding of the challenges facing American law enforcement.

- Digital age policing can be divided into crime challenges and, on the other end, preparedness and response - do these two align?
- Since January 2022 over 7000 shooting deaths with 197 mass shootings took place while at the same time 847,376 complaints of cyber-crime were recorded by American police forces, based on the latter, what are the local police departments' challenges/priorities?
- Case study 1: Hudson County, NJ: need versus response – do they align?
- Case study 2: New York State: size versus capabilities – do they align?

Understanding United States Law Enforcement Agencies

In 2016, there were about 100,000 full-time federal law enforcement officers in the United States and U.S. territories who primarily provided police protection. 701,000 full-time sworn officers served in general-purpose state and local law-enforcement agencies nationwide. However, in 2022, in the aftermath of over two years of some extremely negative coverage of the police profession (Haberfeld et al, 2022), less than 690,000 remained in state and local agencies, with some projections that these numbers will decline throughout the year, American law enforcement is struggling with recruitment of new officers while experiencing an unprecedented decline in the numbers of its sworn officers (Young & Sayers, 2022).

An insight into the Decentralized Nature of the American Police from NYPD to Chester, NJ from In-house to Outsourcing

A quick peak into the way digital crime is handled in American law enforcement. Depending on the jurisdiction and any of the 50 states, the following entities may be designated as the lead investigative agencies:

- Prosecutors Office
- FBI
- Attorney General
- Homeland Security

- Joint Terrorism Task Forces (JTTFs)
- Fusion Centers
- And so many more, including local police departments, the ones that have the capacity to investigate, which are primarily the larges agencies only, like the NYPD (LEMAS, 2016).

Increase in Digital/Cyber Crimes

- The majority of first response is still in hands of the municipal police departments – that outsource the investigations into state and federal agencies

YET

- As the number of cyber-crimes increase the federal and state agencies cannot handle the increase

According to the FBI's Internet Crime Report 2021, a record 847,376 complaints of cyber-crime were reported to the FBI by the public, a seven percent increase from 2020. The Federal Trade Commission's (FTC) Consumer Sentinel Network took in over 5.7 million reports in 2021 of which 49 percent were for fraud, and 25 percent for identity theft (Federal Bureau of Investigations, Internet Crime Complaint Center, 2022).

From Guttenberg Police Department to Jersey City Police Department: A Tale of Two Cities yet very similar approach

Guttenberg, New Jersey Police Department, is a local Police Department in the State of New Jersey, an independent entity, with 22 full time sworn officers, 8 full time civilians and 17 part time civilians (Guttenberg Police Department, 2022). In contrast to one of the largest police department in the State of New Jersey, Jersey City Police Department with its 975 uniformed officers 200 crossing guards, and 200+ civilian employees dedicated to the safety of Jersey City's residents and visitors (Jersey City Police Department, 2022). Despite clear difference in the size of the departments the way both handle digital crimes is identical – through outsourcing. Both departments reside in the New Jersey Hudson County, where the approach to digital crime is pretty much uniform through the outsourcing of the investigations to the Hudson's County Prosecutor's Office (Haberfeld, 2022).

I interviewed a detective from the Hudson County Prosecutor's Office to obtain a realistic insight into the way digital crimes are investigated in the field. The following bullet points summarize the information collected (Haberfeld, 2022).

- NJ county prosecutors oversee major crime investigations
- There are 22 Police Departments in Hudson County, New Jersey, serving a population of 679,756 people in an area of 47 square miles. There is one Police Department per 30,898 people, and one Police Department per two square miles (Police Departments in Hudson County, 2022).
- The Prosecutor's Office receives referrals from other police departments in the County. Following the information received detectives access, externally, suspects Instagram/Facebook accounts. The law enforcement officers open fake profile accounts, sometimes friend the suspect. Needless to say that these investigative tactics lead to legal challenges, when the cases end up being prepared for the prosecution.
- No warrants are needed to access the suspects account, similar to the American legal doctrine: 'in plain view' (Legal Information Institute, 2022).
- In the case of parallel investigations in a number of interrelated cases and when there is a probable cause to suspect a more intricate investigation, detectives petition the court for "communication data warrant " which allows them to extract all the information from suspect's profile like: chat messages, videos, photographs, etc., as well as all the data related to the IP addresses, where the illegal images come from. The challenges involved in obtaining these warrants are numerous (JD Supra, 2022).
- The next step involves the location of the alleged victims, providing that these actions reach a level of criminality, the challenges here are, primarily, related to the willingness of the alleged victims to cooperate to enable the detectives to apply for an arrest warrant.
- In case the alleged victims do not provide enough support to apply for an arrest warrant, the next step is to initiate a meeting with the suspect which, once again, can lead to legal challenges and accusations of entrapment (United States Department of Justice, 2022).
- An example of a complicated case included a pervasive distribution of sexual images, which according to the detective constitute a bulk of under reported crimes. These cases are investigated once or twice a month just in one unit. Subsequently, the victims are lured to unknown locations. One such case involved a 14 years old, who was developmentally challenged. The alleged perpetrator sent an Uber to bring him to his location, he befriended the victim through a contact on the Instagram. The family intercepted this communication, called the JCPD, which immediately referred the case to the Prosecutor's Office. According to the detective: "They (the Jersey

City Police Department) just don't have the tools. Assistant prosecutors have to handle it." (Haberfeld, 2022).

- Finally, the detective pointed out that in the last few years there is a huge learning curve facing the investigators, especially when it pertains to forensic crime training: "…they have to catch up on learning all about how to conduct the investigation and then the technical aspects... (Haberfeld, 2022).

From the NYPD to the Sodus Point Police Department

In the neighboring state, the New York State, the digital crime phenomena is handled slightly different depending, once again, on the size of the department. As unusual as it may sound, the Sodus Point Police Department, an independent and one of the almost 600 autonomous and independent police departments in New York State, is comprised of 1 full time police officer, 3 part time officers and a civilian (Sodus Point Police Department, 2022). On the other end of the spectrum, still within the same state of New York, the New York City Police Department (NYPD) is the largest and one of the oldest municipal police departments in the United States, with approximately 36,000 officers and 19,000 civilian employees (New York City Police Department, 2022).

The NYPD is divided into major bureaus for enforcement, investigations, and administration. It has 77 patrol precincts with patrol officers and detectives covering the entire city.

The department also has 12 transit districts to police the subway system and its nearly six-million daily riders, and nine police service areas (PSAs) to patrol the city's public housing developments, which are home to more than 400,000 residents.

Additionally, uniformed civilians serve as traffic safety agents on the city's busy streets and highways, and as school safety agents, protecting public schools and the over-a-million students who attend them (New York City Police Department, 2022).

Needless to mention that the Sodus Point Police Department does not handle its digital crime problems. However, the NYPD created a remarkable response to the ongoing and increasing rate of web related criminality.

The New York City Police Department in the Digital Age – a Template for Success

Real Time Crime Center and the S.M.A.R.T. UNIT

- Real Time Crime Center is a centralized, technology-driven support center which uses state-of-the-art technology, such as facial recognition and link-analysis software, to provide instant, vital information to detectives and other officers at the scene of a crime.
- T.A.R.U. – Tactical Response – technologically advanced support unit.
- The Social Media Analysis & Research Team (S.M.A.R.T.) analyzes social media for chatter, videos and relative information in regards to active investigations.
- The SMART unit also identifies patterns and trends on social media such as bullying, gang activity, and types of crimes and translates the information into useable intelligence for patrol officers in the field.
- SMART also collects and memorializes this information as evidence in police investigations. The unit also offers presentations to agencies and the public on the dangers and uses of social media (NYPD, 2022).

The S.M.A.R.T. Unit as a Tactical Template

Based on a thorough overview of the NYPD's tactical response to the digital crimes, it is recommended that other law enforcement departments adopt the S.M.A.R.T. units as their tactical template. The benefits of this approach are summarized below.

- Every shooting and/or gang related activity reported by detectives from each precinct is referred to S.M.A.R.T. This approach allows for a tactical alignment of, otherwise, dispersed criminal patterns.
- This approach allows for identification of digital footprints and the interrelated connections.
- In addition, this approach allows for alignment of information and proper connections between different investigative units.
- Further, it creates a mechanism of effective internal information dissemination to other units, that might otherwise be not informed.
- The above approaches lead to the elimination of the proverbial "linkage blindness" that plaques American law enforcement agencies, almost from their inception (Brown, 2018).

How is the knowledge disseminated?

One of the most critical issues that needs to be addressed in order to enhance law enforcement agencies' abilities to face, target, and effectively respond to digital crimes is directly related to the way knowledge about this phenomenon is disseminated to the smaller and less technology savvy and adapted agencies. A White Paper disseminated by Officer.com website, one of the American law enforcement publications (not peer reviewed but popular with law enforcement audience) identifies the following challenges facing policing in the era of digital criminality:

- Digital evidence has become an integral part of today's criminal investigations.
- As agencies struggle to adapt to growing volumes and complexity of digital data, a new paradigm for digital investigations is emerging – one that leverages a modernized approach to fuel greater collaboration at all levels. When agency teams are able to work together more effectively, the quality and speed of their investigations can be greatly improved.
- The digital evidence review process can be accelerated by empowering investigators and other stakeholders to collaborate on evidence review securely in real-time, regardless of their physical location, and with tools designed to help them easily find the evidence that matters across a variety of sources. (Officer.com, 2021.)

Police Chief Magazine 2022 – Awareness is there but not the Implementation

Police Chief Magazine, a widely disseminated official publication of the IACP (International Association of Chiefs of Police), is yet another example of awareness to the problem but, not necessarily a solution to the field implementation, as the membership in this association is voluntary and only a fraction of American police executives holds membership in this organization and is exposed to its recommendations (Haberfeld, 2018). Nonetheless, in its May 2022 issue the publication recommends the following steps to be taken by law enforcement agencies to better prepare them for the ongoing challenges of digital related crimes:

- Traditional Public Information Offices must evolve into aligned, strategic Communications Operations
- Agencies need to get in front of Facial Recognition
- Agencies need to make more use of remote Drone Dispatch
- Agencies need to address the opportunities and challenges of Intelligent Emergency Response (Police Chief Magazine, 2022).

Recommendation: In-house versus the Outsourcing Approach

Upon the review of the responses to digital policing challenges, I would recommend the following steps police practitioners and agencies should consider to enhance their proactive capabilities and capacities in the era of digital policing:

Interoperability – critical in the age of digital policing.

Interoperability became a buzz word in the aftermath of 9/11. Many practitioners and academics used in term to denote lack of proper cooperation between law enforcement agencies, especially in the field of technology. Prior to 9/11 law enforcement agencies in the US operated their radio communications, using different frequencies which, in turn, prevented them from communicating effectively during times of crises. The 9/11 Commission identified this problem as one of the failures of first responders (Falkenrath, 2004). Over twenty years later, the implementation of the 9/11 findings is still sporadic which, in turn, creates a larger challenge in the fight against web based crimes where speedy communication between agencies can make a real difference in the apprehension of criminal actors and disablement of their networks.

An in house unit – allows for proper sharing and connectivity

An in house digital crimes investigative unit, while part of the overall structure of any given department, can quickly and effectively share the information on the intranet of the organization and thus enable other internal units to make the connections between the investigated crime and other reported crimes that are currently not classified as internet related.

When you outsource you miss the connections to other serious crimes from Organized Crime to terrorism

Related to the above bullet point, the concept of outsourcing internet based crimes makes it much harder to identify the relevant connections to other serious crimes investigated by other units within the police organization like the Organized Crime and Counter Terrorism. These units are frequently stand- alone units

that suffer from what is referred to as organizational "linkage blindness" (Sheptycki, 2004).

An in house unit mandates better and ongoing training

As one of the detectives interviewed for this article mentioned, training for digital crime investigations is a huge curve and challenge for many police officers, especially the ones from the smaller police departments where in-service training is rare and usually related to some high profile organizational failure (Haberfeld, 2018). An in house unit would advance the concept of a more frequent and updated training, especially in the knowledge area that changes so frequently and rapidly.

The danger of leader technology illiteracy, and the importance of embracing new ideas in a more proactive rather than reactive manner

Related to the previous bullet, technological illiteracy, from the top of the organizational pyramid up to the specialized investigators, can only be addressed properly in an in house unit as the inability to effectively investigate serious crimes has a direct impact on the clearance rate of a given organization. In the era of laser focus on police effectiveness, the clearance rate becomes even more critical for police executives and the probability of approval of the more proactive and innovative ideas increases contemporaneously with the increase of internet based crimes.

Establish specialized units in larger police departments

Although the idea of having specialized units that are capable of effective investigations of digital crimes is a tempting one, in reality only the large police department can afford to establish them. However, "larger police department" term needs to be re-evaluated in terms of the actual staffing numbers. It is probably wise to recommend that each unit that exceeds 100 sworn officers should consider creating a specialized digital investigations bureau.

Digital crimes are no longer a domain to outsource

As the internet crimes increase in volume, in a manner that is highly disturbing, the idea of not been able to investigate these law violations within the police organization is no longer acceptable and appears to be obsolete. The times when internet related crimes were rare occurrences are long gone.

Need to adapt to crime patterns that are increasingly cyber related

Embracing the seriousness, intensity and scope of the new crime patterns is an obligation of any police executive who wants to be not just proactive in the response to crime patters but, first and foremost, up to speed with the daily reactive realities.

Change in recruitment and training need to be considered, it is possible that we need more technologically savvy officers than ones who can do a certain number of pushups in a minute.

While police training in the United States remains far behind many of its counterparts around the world, and while the calls for reduction of standards for recruitment, selection and training become more of an ongoing theme, the numerous police oversight bodies need to rethink the tactical and operational needs of the local police departments and their capabilities to respond effectively to the digital crimes phenomena.

Into the future

From the overview of the state of American Policing in the past few years, it appears as if police departments are focused more on Police Community relations rather than the digital age threats and challenges, this approach needs to change before it is too late.

It appears that moving into the proactive approach by tomorrow is a misguided approach that is probably already too late to be able to deliver any effective response. I would posit that, actually, even today might be too late! Although not all of the research questions posed at the beginning of this article were fully answered, the critically of a proper response has been established.

Borrowing from Goodwin's (2016) advice to businesses owners it appears that adapting his concept for law enforcement agencies is the savvy way to move into the future:

"*…as we move from the mid- to the post-digital era, the advice is simple. Prepare for eventualities. Ensure that your business is culturally prepared for what's to come. Consider extremities. Be aware of the bleeding edge. Leave nothing off the table ….*" (Goodwin, 2016.)

Figure 1. Introducing the P.E.C. approach to the era of Digital Policing

Time is of essence, this old adage cannot be more relevant than when it comes to the investigations of web related crimes. The legal challenges can be enormous, the need to *prepare* ahead of time cannot be overstates. A thorough familiarization with the local, state and federal laws and statues becomes a critical part of the preparedness. *Ensuring* the interoperability and law enforcement collaboration cannot be overstated. *Considering* and acting upon international cooperation and collaboration is the way forward.

References

- Brown, R. (2018) Understanding law enforcement information sharing for criminal intelligence purposes. *Trends and Issues in Crime and Criminal Justice [electronic resource]*, (566), 1-15.
- Falkenrath, R. A. (2004) The 9/11 Commission Report.
- Federal Bureau of Investigations (2022) Internet Crime Complaint Center.
  Retrieved on August 30, 2022 from https://www.fbi.gov/investigate/cyber
- Goodwin, T. (2016). The 3 Ages of Digital. Tech Crunch.com.
  Retrieved from: https://techcrunch.com/2016/06/23/the-three-ages-of-digital/ on June 1, 2022
- Guttenberg Police Department (2022)
  Retrieved from https://www.guttenbergnj.org/Departments/police-department
- Haberfeld, Maria R. *Critical issues in police training* (2018*)* NJ: Pearson Customs Publishing.
- Haberfeld, M.R. (2022) Field notes.
- Haberfeld, M.R., Cheloukhine, S., Herrmann & Schneider, J. (2022) Policing the Streets of New York City during the COVID Pandemic: with a Comparative Angle. Forthcoming (fall, 2022) *Journal of Policing*.
- J.D. Supra (2022). A Communication Data Warrant or Wiretap Order - Which is needed for Law Enforcement to Obtain ESI from Facebook.
  Retrieved from https://www.jdsupra.com/legalnews/a-communication-data-warrant-or-wiretap-6197099/
- Jersey City Police Department Official website (2022)
  Retrieved on August 30, 2022 from https://www.jerseycitynj.gov/cityhall/PublicSafety/Police
- Kupperman, R. H., & Trent, D. M. (1979) Terrorism: Threat, reality, response (pp. 48-74). Stanford, CA: Hoover Institution Press.

- Legal Information Institute (2022) Plain View Doctrine.
  Retrieved from https://www.law.cornell.edu/wex/plain_view_doctrine_0
- Law Enforcement Management and Administrative Statistics (LEMAS) 2016.
  Retrieved from https://bjs.ojp.gov/data-collection/law-enforcement-management-and-administrative-statistics-lemas
- New York City Police Department (2022) Official website
  Retrieved from https://www1.nyc.gov/site/nypd/index.page
- Officer.com (2021) White Paper on Digital Forensics.
  Retrieved from https://www.officer.com/whitepaper/whitepaper/21278776/magnet-forensics-digital-forensics-software-a-new-paradigm-in-digital-investigations
- Police Chief Magazine (2022) Policing in Digital Era.
  Retrieved from https://www.policechiefmagazine.org/
- Police Departments in Hudson County (2022)
  Retrieved from https://www.countyoffice.org/nj-hudson-county-police-department/
- Sheptycki, J. (2004). Organizational pathologies in police intelligence systems: Some contributions to the lexicon of intelligence-led policing. *European Journal of Criminology*, *1*(3), 307-332.
- Sodus Point Police Department (2022) Official website.
  Retrieved from https://www.villageofsodus.org/police-department
- United States Department of Justice (2022) Entrapment Defense.
  Retrieved from https://www.ojp.gov/ncjrs/virtual-library/abstracts/entrapment-defense
- Young R. & D. S. Sayers (2022). Why police forces are struggling to recruit and keep officers, CNN.
  Retrieved from https://www.cnn.com/2022/02/02/us/police-departments-struggle-recruit-retain-officers/index.html