The Changing Nature of Crime and Criminal Investigations

Kevin Morison, Chief Operations Officer
Police Executive Research Forum

Madeline Sloan, Research Associate
Police Executive Research Forum

November 28, 2018

BJA NTTAC
National Training and Technical Assistance Center

WEBINAR AGENDA

Time	Agenda Item
2:00 p.m. – 2:05 p.m.	Welcome and Introduction
2:05 p.m. – 2:40 p.m.	Presentation: The Changing Nature of Crime and Criminal Investigations
2:40 p.m. – 3:00 p.m.	Question and Answer Session

ABOUT THE POLICE EXECUTIVE RESEARCH FORUM (PERF)

Who we are:

- National membership organization founded in 1976
- Approx. 3,000 police chiefs, sheriffs, other law enforcement leaders, academics, and government officials
- Board of Directors elected by members
- Full-time staff of approximately 30 professionals

What we do:

- Research
- Policy Development
- Management Services
- Executive Search
- Senior Management Institute for Police

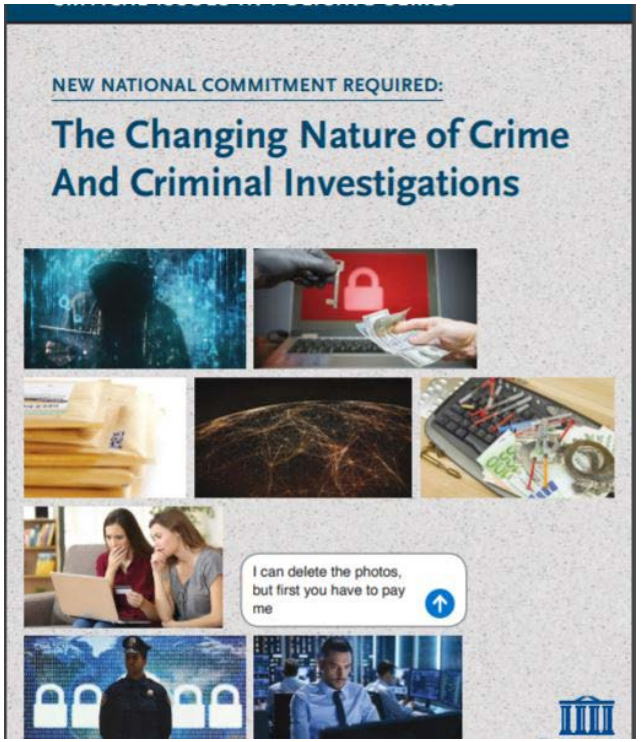
POLICE EXECUTIVE RESEARCH FORUM

ABOUT THE PROJECT

PERF assessed the **impact of computers and other technologies** on the nature of crime itself, and on how technology is changing criminal investigations.

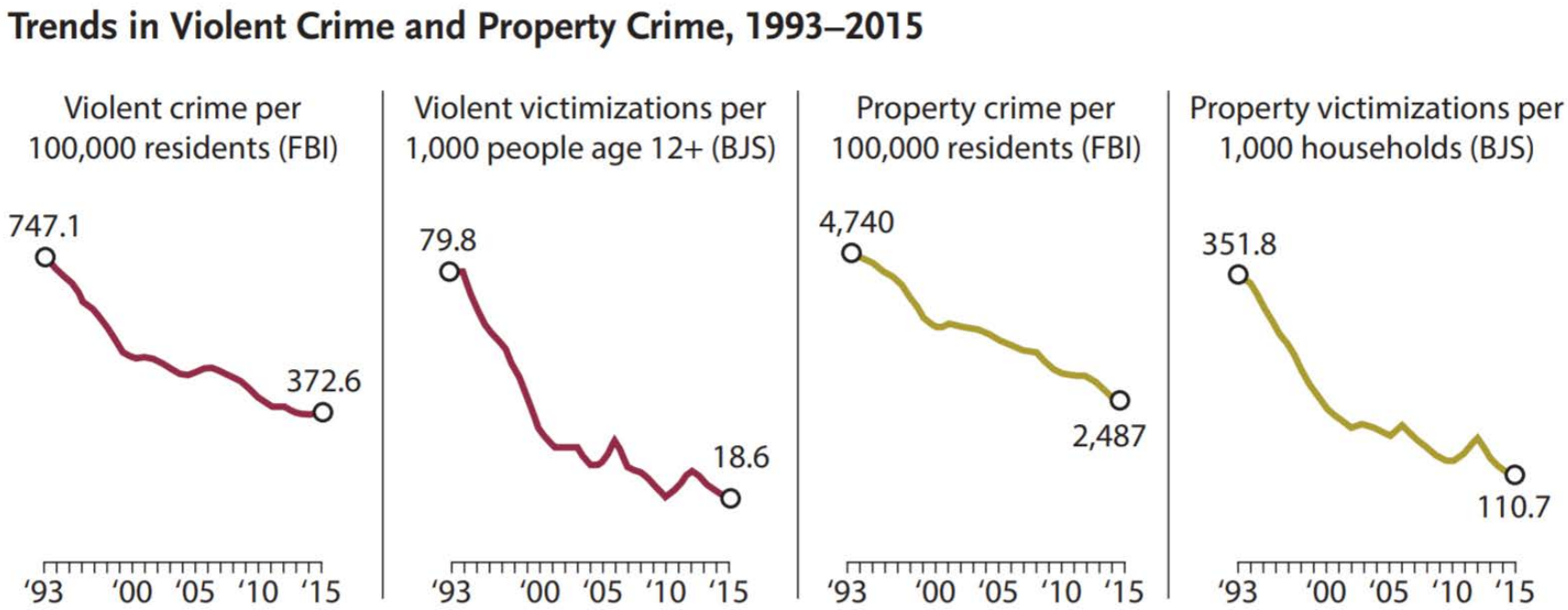
PERF assembled nearly 200 experts in criminal investigations, technology, and police operations and management to explore these issues during a **day-long conference in Washington, D.C.**

The findings are documented in PERF's **January 2018 report**, *New National Commitment Required: The Changing Nature of Crime and Criminal Investigations.*



CRIME TRENDS IN THE UNITED STATES

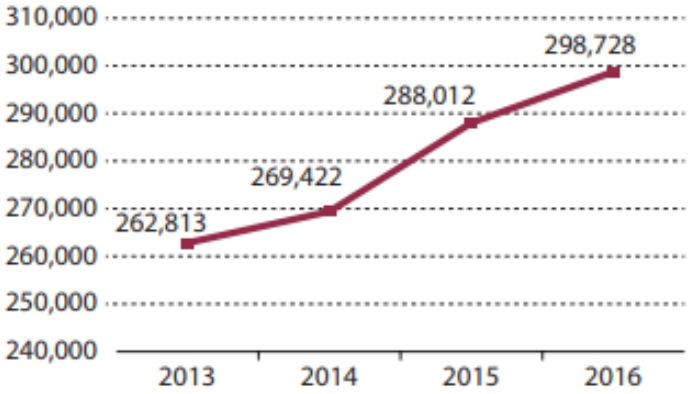
As measured by traditional reporting systems, crime in the United States has declined sharply in recent decades.



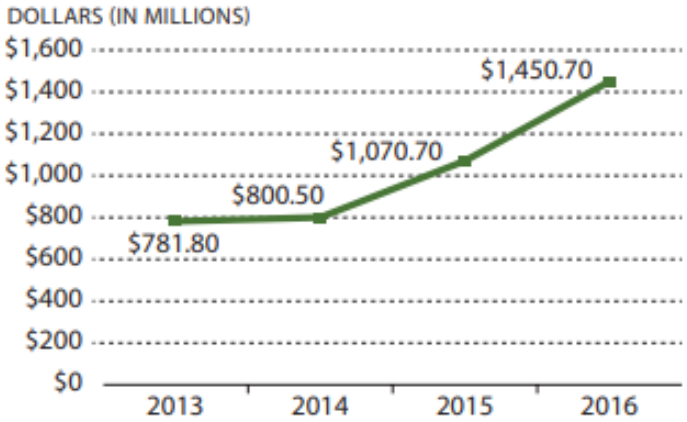
CRIME TRENDS IN THE UNITED STATES

But even as rates of homicide, robbery, burglary, and other crimes have fallen since the 1990s, new types of crimes – many of them enabled by computer technology – have begun to proliferate.

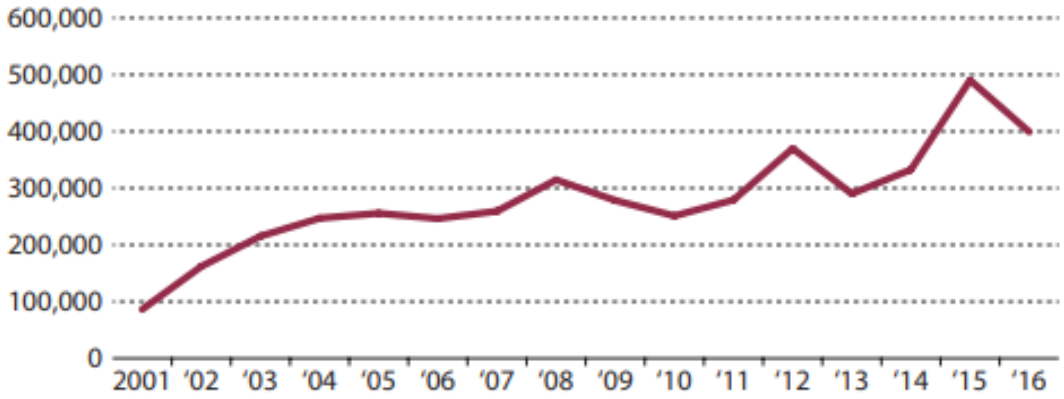
Total Internet Crime Complaints



Total Monetary Losses



Identity Theft Complaints



BJA NTTAC National Training and Technical Assistance Center

LIMITATIONS OF CURRENT CRIME MEASURES

The Uniform Crime Report (UCR) and the National Crime Victimization Survey do not adequately measure new and evolving types of crime. As such, they do not provide a complete and accurate picture of crime in the United States.

Limitations of current crime measures:

- New crimes (e.g., identity theft) do not fit easily into the UCR framework
- Technology-driven crimes are often complex and multijurisdictional
- Many of these crimes are underreported

> *"Without a more comprehensive set of crime statistics, we cannot know whether the large-scale declines in the 1990s in traditional and well-measured violent and property crimes reflect broader declines in crime, or whether these recorded changes were offset by notable increases in alternative and newly-emerging forms of crime that are not captured in current data systems."*
>
> — Janet Lauritsen and Daniel Cork, Panel on Modernizing the Nation's Crime Statistics

HOW CRIME HAS CHANGED

Criminals are using technology to invent new types of crime:

- **Ransomware:** A type of online attack that blocks a user's access to his or her computer system until a ransom is paid
  - *Law enforcement agencies are falling victim, too*
- **Sextortion:** A type of online sexual exploitation in which offenders coerce or blackmail victims into providing sexually explicit images or videos of themselves. These demands often come from the offender's threat to publicly post sexual images or to send them to the victim's friends and family
- **Synthetic identity theft:** Involves taking pieces of information from multiple people to create an entirely new, fictional identity that can often be exploited for long periods of time
  - *Children are especially vulnerable*

HOW CRIME HAS CHANGED

Criminals are developing new methods to commit traditional crimes:

- Drug transactions moving from street corners to web-based dark markets and digital currency
- Gang activity shifting from violent crime to elaborate fraud schemes
  - *Van Dyke Money Gang case*
- Credit card skimmers
- Auto thefts
  - *Use of jamming devices*
  - *Thieves targeting personal documents (e.g., registration, insurance documents)*

NEW INVESTIGATORY CHALLENGES

Digital Evidence

- Broad in scope
- Difficult to obtain
- Large volume of data
- Creates demand for new skill sets among investigators

Encryption/Going Dark

- Hindered access to evidence
- Lack of cooperation from tech companies
  - Delays
  - Suspect notification

Courtroom Actors

- Judges do not fully understand technology
- “CSI” effect among juries

NEW INVESTIGATIVE TOOLS

Social Media

Twitter, Facebook, Instagram, and other social media platforms can be used to collect evidence, locate suspects, and identify criminal networks.

Internet of Things (IoT) Devices

As IoT devices (e.g., Fitbits, Amazon Echos, home security systems) become integrated with everyday life, police should be looking to extract data to support their investigations.

Mobile Apps

As people use more mobile applications on their smartphones (e.g., navigation, shopping, banking), police are increasingly turning to suspects' use of mobile apps to trace their location and activities.

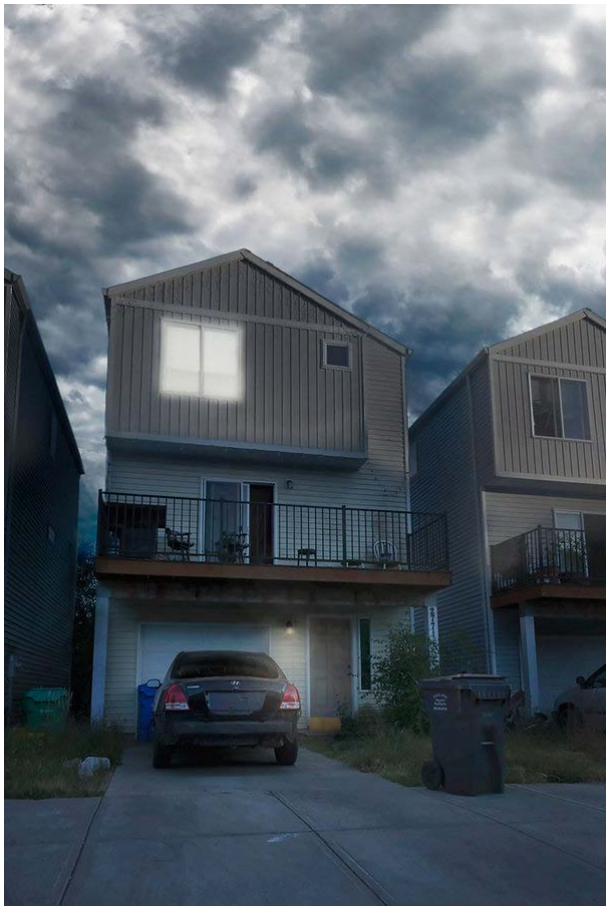
Other Innovations

- Bluetooth in cars
- Tracking Wi-Fi connections
- K-9s to detect digital media

CASE STUDY: PETER THE GREAT

On February 16, 2017, 18-year-old Aisha Zughbieh-Collins was found dead in her southeast Portland, Oregon apartment from an overdose of a synthetic opioid called U-47700 (or simply U4).

CASE STUDY: PETER THE GREAT



At the scene, detectives uncovered important physical evidence indicating that the **drugs had likely been shipped through the mail.**

- Pregnancy test kit (sold only at Dollar Tree stores)
- Mailing envelope with fictitious return address
    - *Purchased in Greenville, South Carolina*

Detectives also discovered a notepad **containing an alphanumeric code.**

- Pretty Good Privacy (PGP) key

CASE STUDY: PETER THE GREAT

With assistance from **Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI),** detectives determine that Aisha's PGP key was used to purchase drugs on AlphaBay. The online seller's username was "Peter the Great," which was linked to nearly 10,000 transactions on the site.

Detectives purchased U4 from Peter the Great. The drugs arrived wrapped in the same pregnancy kits and containing the same type of shipping labels found in Aisha's apartment.

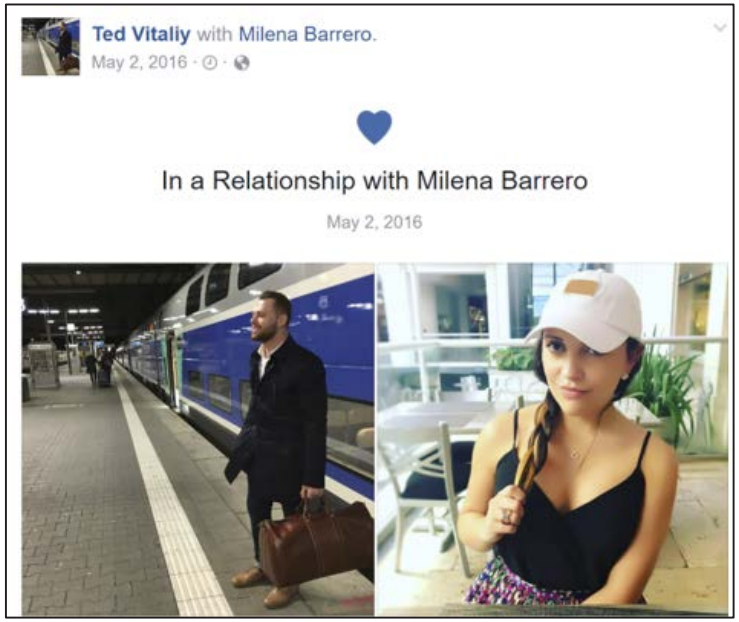
Postal inspectors further determined that the shipping labels used on the packaging originated from an **online company that accepts only Bitcoin digital currency.**

CASE STUDY: PETER THE GREAT

Further investigation revealed that the online shipping label purchases were tied to **two secure email addresses.** Investigators filed a subpoena for any records connected to those email addresses.

That led them to **Theodore Khleborod,** a person of interest living in Greenville, South Carolina. Detectives determined that Khleborod had received numerous international packages from China, where a great deal of U4 is made.

Through social media postings, they also found out that Khleborod was in a relationship with a woman named Ana Barrero.



CASE STUDY: PETER THE GREAT

Next, investigators collected sales information showing a spike in pregnancy kit purchases at a particular Dollar Tree store in Greenville. They also **retrieved store video** showing Barrero purchasing numerous pregnancy kits at that store.

CASE STUDY: PETER THE GREAT

Portland officials traveled to Greenville and, with the assistance of the Greenville, South Carolina Police Department and ICE/HSI agents in South Carolina, **began surveillance of both Khleborod and Barrero.**

They witnessed Barrero mailing large numbers of parcels that matched other packages in the investigation, including the one from Aisha's apartment.

CASE STUDY: PETER THE GREAT

In April 2017, officers **arrested Khleborod and Barrero.** They faced federal drug distribution charges in both South Carolina and Oregon, where officials considered additional "Len Bias charges." Investigators believed "Peter the Great" may be connected to **more than a dozen other overdose deaths** across the country.

9 STEPS POLICE AGENCIES CAN TAKE

1

Evolve, quickly: As crime continues to change, law enforcement agencies must change as well.

That means **rethinking organizational models** that reflect traditional "silos" such as organized crime, gangs, and narcotics. Instead, agencies should look at ways to integrate computer-focused criminal investigations, digital forensic science, and leading-edge technologies such as artificial intelligence and real-time crime analysis throughout their organizations.

9 STEPS POLICE AGENCIES CAN TAKE

2 **Personnel**: Law enforcement agencies need to attract and retain personnel with the skills needed to operate effectively in this new environment.

In trying to keep up with changing patterns of crime and new investigative strategies, law enforcement agencies need to find officers, detectives, and analysts who have the skill sets and capacity to understand and operate effectively in this new environment. In many cases, that will involve recruiting – and then working to retain – employees with **specialized skills in technology, information retrieval, and data analytics.**

9 STEPS POLICE AGENCIES CAN TAKE

3 **Continuous training**: Agencies need to continuously train and retrain their employees on issues related to computer-enabled crime.

Because almost every type of crime today can have a digital footprint, it is especially important that agencies **train all of their personnel – patrol officers, crime scene technicians, and detectives** – in how to recognize, handle, process, and manage digital evidence. And because criminals' strategies and tactics are constantly changing, law enforcement training must be a continuous process as well. Agencies should take advantage of the **training offered by federal and state agencies,** as well as other organizations such as the **National White Collar Crime Center.**

9 STEPS POLICE AGENCIES CAN TAKE

4

The "dark web": As crimes like drug trafficking move from street corners to the internet, police agencies need to develop a working knowledge of the dark web, the use of crypto-currencies such as Bitcoin, and other online enablers of crime.

As agencies begin to undertake dark web investigations, they need to thoroughly train their personnel in how to **operate safely in the dark web**, protecting their identities and avoiding potentially dangerous "blue-on-blue" encounters with other law enforcement agencies conducting similar investigations.

9 STEPS POLICE AGENCIES CAN TAKE

5 **Partnerships**: To strengthen their investigations of computer-enabled crime, local law enforcement agencies should form partnerships with federal, state, and other local agencies.

Partnerships with agencies such as the Federal Bureau of Investigations, the U.S. Secret Service, and ICE/HSI are especially important in dark web investigations and those involving data encryption. Local police agencies should form **close working relationships with the U.S. Postal Inspection Service (USPIS)**, as many criminal enterprises that operate on the dark web use the U.S. mail to transport illegal drugs, firearms, and stolen goods. USPIS has trained inspectors who can help local agencies conduct investigations that involve the mail.

9 STEPS POLICE AGENCIES CAN TAKE

6

Small and mid-size agencies: Regional efforts to combat computer-enabled crime should include small and mid-sized agencies.

Smaller jurisdictions are being disproportionately impacted by problems such as opioid addiction, which is increasingly connected with the dark web. Yet many of the police departments and sheriffs' offices in these communities lack the resources to initiate their own dark web investigations. These agencies should look to **form compacts with larger departments and state agencies** that can pool the resources and expertise needed to investigate a range of computer-enabled crimes.

9 STEPS POLICE AGENCIES CAN TAKE

7

Legal and privacy issues: Investigations in which law enforcement agencies seek information from technology companies can raise legal, privacy, and technical issues.

Technology companies often are unwilling (or, in some cases, claim to be unable) to unlock criminal suspects' smartphones, computers, or other devices. Unfortunately, this situation will only get worse **until law enforcement agencies can find a new working relationship with the private sector.** At the moment, there are more problems than solutions for law enforcement agencies on this issue.

9 STEPS POLICE AGENCIES CAN TAKE

8

Police must educate others: Law enforcement leaders should educate the public and, when necessary, other criminal justice officials about the digital aspects of crime and criminal investigations.

Judges, prosecutors, and juries don't always seem to understand the basic elements of digital evidence, and how and why it is important to so many of today's criminal investigations. This problem can be acute among members of the public, whose understanding of digital evidence is **influenced by the entertainment media and the so-called "CSI effect."** Law enforcement leaders should work with subject matters experts and practitioners to educate the public and justice system personnel about computer-enabled crime, and about the **advantages as well as the limitations of digital technology** and evidence in their criminal investigations.

9 STEPS POLICE AGENCIES CAN TAKE

9 Integration of new and old investigative techniques: To be successful, law enforcement agencies need to integrate new technology-driven approaches to criminal investigations with traditional investigative techniques.

Very few crimes can be solved solely through technology-led investigations and digital evidence. Even the most complex of dark web investigations will likely **require some measure of traditional investigative work.** Police and sheriffs' departments need to develop investigative strategies that take advantage of, and coordinate, both types of approaches.

RESOURCES

Free or low-cost training programs:

- National White Collar Crime Center
- U.S. Secret Service National Computer Forensics Institute
- Federal Law Enforcement Training Center

Other helpful resources:

- SEARCH (The National Consortium for Justice Information and Statistics)
  - *Internet Service Provider list*
- National Domestic Communications Assistance Center
  - *Search warrant templates*
- U.S. Department of Justice's Computer Crime and Intellectual Property Section
  - *24/7 service line for oversees data preservation*

The **Law Enforcement Cyber Center (LECC)**, managed by the Bureau of Justice Assistance, has compiled a web page of searchable training opportunities for executives, officers, and prosecutors.

Visit LECC at:

www.iacpcybercenter.org

QUESTIONS?

Kevin Morison
Chief Operations Officer
kmorison@policeforum.org

Madeline Sloan
Research Associate
msloan@policeforum.org

The Changing Nature of Crime and Criminal Investigations report is available online at:

https://www.policeforum.org/assets/ChangingNatureofCrime.pdf