

FOSTERING INNOVATION FOR — FUTURE SECURITY CHALLENGES

VOLUME
07

TECHNOLOGY AGAINST CRIME, AFRICA



SMART POLICING CONCEPT

LAW ENFORCEMENT GUIDE

· GLOBAL PERSPECTIVES FROM EXPERTS ·



FOSTERING INNOVATION FOR FUTURE SECURITY CHALLENGES

PREVENT DETECT INVESTIGATE



Dr. Jerry I. Akubo
Chief Executive Officer,
Technology Against Crime, Africa

Dr. Jerry Akubo founded TAC Africa as a futurist oriented, Law Enforcement Centric NGO, borne out of an International Forum on Technologies – a high level meeting dedicated to Technologies for a Safer World, co-organized by INTERPOL and the Ministry of Interior in Lyon, France in 2013. The NGO was officially registered in Abuja, Nigeria in 2016. Prior to this, he worked over a decade and half as the National Technical Officer for INTERPOL NCB Abuja under the auspices of the Nigeria Police Force.

Dr. Akubo has been recognized by the INTERPOL Global Complex for Innovation and the Directorate of Innovation Center, Singapore for his exemplary service, partnership and contributions having actively attended and participated in over eight (8) INTERPOL General Assemblies and Eight (8) INTERPOL World Congress in a roll amongst other high level technical meetings and presentation he organized on extending INTERPOL Secured Communications Network to authorized Law Enforcement Agencies across the African Region.

He is a frequent speaker on Emerging Technologies and the maximal utilization of INTERPOL tools by Law Enforcement Agencies within the African Region while pushing a number of research and developmental projects to improve the technical know-how and easy accessibility of tools and technologies for Law Enforcement Agents especially the front line officers.

Dr. Akubo is an evangelist on the use of Innovative Aerial Surveillance, remote sensing and emerging technology to tackle most unique set of challenges the African region is facing including on the one side. Transnational Organized Cyber Crime and on the other, battling insurgents and terrorist group often domiciled in very remote & inaccessible locations.

LAW ENFORCEMENT INNOVATION

Innovation is not just about the latest gadget—it's about finding new ways to do things better.

Innovations can take the form of new concepts, new methods, or new tools. But innovation tends to work best when all these forms come together to enable police and law enforcement agencies to have greater insight and impact than ever before. The innovations that are shaping the future of law enforcement begin with emerging technologies that support new concepts of operations, enabling the interventions, and relationships that keep society safe.

Police and law enforcement agencies across the country are driving the change, pioneering creative ideas, adapting to changing contexts, and incorporating insights from officers and community partners. To understand how these innovative practices may transform the future, we must begin by understanding the journey an officer takes from evidence to insight. Officers need to be able to assess their environment rapidly, leverage technology as they pursue public safety, mine data for insights on what to do next, scale up their successes, and get deeply involved in their communities.



Table of Contents

04

Community Engagement and social media

08

Safe Cities/Analytics

10

PREDICTIVE POLICING

14

SITUATIONAL AWARENESS

19

AUTHENTICATION (BIOMETRICS)

Smart Policing Concept

Community Engagement and social media

In the Internet age of the 21st century, it would be simply naive for law enforcement agencies to depend solely on traditional means of community engagement. Though important, having a physical presence in the community is no longer sufficient to combat crime on its own. Instead, technology has made it vital for community policing efforts to take a step further by embracing social media and other technology enabled forms of communication.

This is compounded by the fact that cyber-enabled crimes have increasingly moved beyond regular cases of online fraud and sex exploitation toward facilitating terror attacks. By expanding their virtual presence online, law enforcement agencies can increase their community engagement. This then presents even more opportunities to improve policing in today's world in a myriad of ways such as to publicize initiatives, develop trust and maintain an ongoing relationship with the community.

As part of its efforts to reduce crime rates, the Panama Police Force uses social media to maintain a direct and ongoing relationship with its community both online and offline. The Unidad Preventiva Comunitaria is a task force charged with "maintaining a direct and an ongoing relationship with the community" in an effort to reduce crime rates. The Panama Police Force regularly updates its Facebook page to broadcast its ongoing campaigns, policies, and activities to the public.

This strategy offers "society's youngest and most vulnerable members, credible alternatives to the drug market, whether [in] job training or sports activities". This method of community engagement has been successful in reaching out to younger citizens who tend to be the most vulnerable and prone to drug addiction and drugrelated violence. Results have been positive with Panama's murder rate significantly falling to 18.0 (per 100,000 inhabitants), as well as a decrease in other crimes such as theft.

The importance of social media in the community engagement is once again underscored by how it has been used to bridge cultural divides between diverse populations. California's Alhambra Police Department, Arcadia Police Department and San Gabriel City Hall Police Departments are examples of law enforcement agencies that have adopted social media for this purpose.

As the demography of these local cities is predominantly Chinese, the police departments turned to Weibo, a popular Chinese social networking website similar to Twitter, to reach out to and engage with its large Chinese population. Weibo is used in multiple ways by the police departments to facilitate communication with the community, increase public safety awareness, encourage cooperation, and even mobilize immigrant civic engagement.

This is done by disseminating information, such as updates on crime trends, city policies and events, traffic alerts, and prevention tips not only in the right language but also in a context that Chinese users can understand. This is especially since many of its Chinese residents are migrants who only speak Mandarin or other Chinese dialects.

The success of using Weibo can be seen in how it was previously difficult to engage Chinese immigrant communities, and even Chinese citizens planning to tour the country. But now, they have started to get in touch with the Alhambra Police Department to make inquiries about law and order issues. Increased interaction with the community has improved public trust in the police as residents change their negative perceptions of the organization.

This has led to better cooperation between the department and the community, a greater willingness of the community to use police services, and a better understanding of existing laws and regulations. Although the police departments of these cities had traditionally used popular American social media channels such as Facebook and Twitter, these mediums were unable to effectively reach out to the Chinese community.

The following are the advantages embracing social media and other technology-enabled forms of communication in combating crime:

For example, the Weibo account of Alhambra Police Department garnered more than 40,009 followers over two years, as compared to its Twitter and Facebook accounts with 1,200 and 8,000 followers respectively, despite having been set up for a much longer period of time. The use of popular Chinese social networking sites by the aforementioned police departments highlights the value of having a social media presence to aid community policing efforts today.

This is largely because it not only prevented alienation by tapping on a platform that many Chinese residents were already using but also because the sites provided a means for the police to interact and engage the community. At the same time, it also highlights the need for police departments to adopt flexibility, adaptability, and innovation when reaching out to communities and tailoring efforts to their needs.

Provide credible information in real-time

The importance of physical presence in the community remains necessary and was clearly highlighted in the case of the New York Police Department (NYPD). While crime in New York City has fallen to its lowest in recent decades, tensions between police officers and the communities they work with persist. To deal with these tensions, the NYPD introduced a culture change in their agency, transforming their policing mindset from 'warrior' to 'guardian'. This was observable in its Neighborhood Coordination Officer (NCO) program, use of social media for public engagement, and relaxing of the existing 'command and control' culture.

Social media allows for law enforcement agencies to be the direct source of news to the public, particularly during times of emergency. This is perhaps most evident in the Boston Marathon bombings that took place in April 2013, which saw the Boston Police Department (BPD) bypassing traditional media outlets and immediately turning to social media to keep the public informed.

Twitter was used to keep the public updated on the situation as it unfolded, the status of the investigation, and the steps the police were taking to manage the crisis. By communicating directly with the public, the BPD minimized the spread of misinformation as it ensured that only accurate and complete information was disseminated to the public through social media.

Enabling Two Way Communication

In doing so, it also demonstrated transparency in public communication and kept the public calm. As a result, public trust in the BPD increased; an important outcome to combat misinformation and fake news. It must, however, be acknowledged that the BPD's success in using social media during its investigations was in large part possible due to previous trust-building efforts by the department, further highlighting that there is still a need to have a physical presence in the community.

The NCO program represented an NYPD initiative to reduce crime and repair frayed relationships between the police and communities, which had worsened in recent years. Under this program, 166 neighborhood summits (community meetings involving the NCOs, residents, workers, and visitors of the neighborhood) were held in the five boroughs of New York. They enabled the NYPD to meet residents, strengthen relationships and gain feedback on how crime and other problems could be better dealt with. At the same time, the NCO program also required officers to spend 20 percent of their time 'off the radio. This meant that NCOs were expected to move around their assigned neighborhoods, engage informally with the residents, and familiarize themselves with the community.

These initiatives were received favorably by the public and more importantly, helped to build trust. The program's success is reflected in the 2017 crime statistics of neighborhoods where the NCO program was implemented. Compared to the same period in previous years, it was reported that overall crime had decreased by 6.2 percent, shootings had fallen by 29.5 percent, and murders reduced by 8.5%. In addition, the NYPD also uses Twitter as a tool to engage citizens, shifting from its traditional command and control culture.

The idea behind this approach was to co-opt the public to assist the NYPD in their crimefighting efforts. However, while regarded positively, there continue to be challenges associated with the NYPD's online engagement strategy. One key example was the unintended backlash from a public engagement initiative on social media. The NYPD's Twitter campaign inviting New Yorkers to post photos with NYPD officers under the hashtag #myNYPD (which aimed to highlight the close relationship between the police and community), was ironically used by individuals to criticize the department.

Traditionally, law enforcement agencies rely on public p-offs and missing person bulletins to gather information for investigations. However, smartphones and social media have drastically altered the way people communicate today. In light of this, many law enforcement agencies increasingly turn to social media platforms (such as Instagram, YouTube, Facebook, Snapchat, Telegram and Twitter) to gather intelligence.

One such example is the Gyeongnam Provincial Police Agency in the Changwon City of South Korea. Over time, officers found that the conventional method of crowd-sourcing information via wanted-person advertisements was ineffective, and turned to social media as a result. Screen capture of the CCTV footage featuring the suspect was uploaded on the agency's Facebook page, along with a description of his offenses. Following this, the post went viral almost immediately, and the police received key information that resulted in an arrest within two days.

In Georgia, the police department of Johns Creek took a step further by developing a mobile application to increase citizen engagement and enhance two-way public communication. The application, JCPD4Me not only provides information on missing people, traffic news, and community events, but also links to social media platforms and other municipal services provided by the city.

Crowd-sourcing information

Most importantly, the app posts information on the city's most wanted criminals, which has greatly helped the police department in investigations. For instance, moments after the police department posted information of a wanted suspect on all social media platforms connected to JCPD4Me, the department received useful intelligence from residents that enabled them to arrest the individual within a day.

Crime Prevention

In recent years, social media has become a primary instrument for terrorist groups to recruit and spread extremist propaganda. Perhaps the most evident example is how violent extremist narratives are disseminated over popular social media websites such as Facebook, Ask FM, YouTube, Twitter, and online blogs.

This has contributed to the radicalization of many young individuals from all over the world, and in some cases, inspired them to perpetrate attacks that were falsely justified in the name of Islam.

In response to this phenomenon, the UK Metropolitan Police enlisted the help of social media-savvy young Muslims as part of its counter-terrorism strategy. The vast amount of extremist content online prompted many Muslim youths in London to come up with various ideas and suggestions to help law enforcement. This includes working together with the police alongside imams, parents and "disengaged" peers to combat Islamic extremism by helping to prevent online radicalization of the young.

By integrating the first-hand experience of young Muslims into its counterterrorism strategy, the Metropolitan Police attempted to improve their engagement with Muslim youths, and at the same time, crowd-source critical information to counter violent extremism. Apart from a 'shift in the mindset' of the Muslim community in London, this strategy has also resulted in more tips from individuals wanting to travel from London to Syria to join the terrorist group Islamic State of Iraq and Syria (ISIS), as seen in the 83 tips reportedly received in 2015.

The Metropolitan Police's success can be attributed in part to its use of the most suitable candidates to counter violent extremism on social media - savvy young people within the Muslim community. These various case studies show how social media has now become an important resource for community policing that law enforcement cannot ignore. Having an online presence removes barriers to communication and provides a framework for changing the way the community perceives law enforcement.

Nonetheless, it is important to understand that law enforcement must continue to have a strong physical presence within the community. This two-way approach of balancing a physical and virtual presence will then allow for community policing and engagement to be truly effective.

Safe Cities/Analytics

Modern cities have changed dramatically in recent decades; cities have grown more congested and crime has become more complex. In light of the shrinking municipal budgets and rising costs of manpower, the model of the friendly neighborhood now seems antiquated and quaint.

Safe Cities are becoming a necessity in the increasingly complex and threatening environment. In essence, 'safe cities' utilizes a network of IoT-enabled devices as tools to improve policing tasks ranging from crime fighting to dealing with emergencies and conducting surveillance.

Benefits to the law enforcement community and city governance departments include a proactive, 'smarter' approach to crime and disaster management, better allocation of resources, performance indicators, faster response time and better situational awareness. In recent years, many countries have started to implement safe city initiatives, as in the case of Singapore, China and Pakistan.

These are exemplified below.

Singapore Government

Singapore's Safe City Test Bed is perhaps one of the best examples that showcase how technological advancement can pave the way for largescale smart policing. The Safe City Test Bed is part of the country's wider initiative to develop a Smart Nation by using advanced analytics to complement its public safety solutions. Both approaches are envisaged to improve security and service delivery in the most efficient manner.

A single precinct of the Jurong Lake District was used as a test bed for a range of urban digital experiments. The trial involved the integration of data from diverse digital sources such as mobile and Wi-Fi, as well as government data and data from social networks. More than a thousand sensors were deployed to monitor every aspect of the precinct, and the live data obtained from surveillance cameras was then integrated and applied to various policing/public safety tasks.

Singapore's Safe City Test Bed is perhaps one of the best examples that showcase how technological advancement can pave the way for largescale smart policing. The Safe City Test Bed is part of the country's wider initiative to develop a Smart Nation by using advanced analytics to complement its public safety solutions. Both approaches are envisaged to improve security and service delivery in the most efficient manner.

A single precinct of the Jurong Lake District was used as a test bed for a range of urban digital experiments. The trial involved the integration of data from diverse digital sources such as mobile and Wi-Fi, as well as government data and data from social networks. More than a thousand sensors were deployed to monitor every aspect of the precinct, and the live data obtained from surveillance cameras was then integrated and applied to various policing/public safety tasks.

This included crowd control, emergency response, resource coordination, effective multiagency collaboration, sense-making, traffic and disaster management. In addition, the system also monitored anomalies online (e.g., sudden changes in behavioral communication patterns on social media) to improve the overall analysis. The onset of data analytics, combined with intelligent infrastructure enables public safety to be achieved without using much resources.

As advanced analytics allow for better situational awareness and sensemaking, senior decision makers can deploy resources in a more targeted and efficient manner. As a result, specialist police officers and accompanying support systems can be deployed for other purposes. Most importantly, by integrating real time inputs with advanced analytics that exploit big data, more meaningful insights can be produced in real time for law enforcement officers to respond quickly to threats, as opposed to relying on static standard operating procedures.

Nanjing, China

The city of Nanjing adopted LTE technology developed by Chinese company Huawei to improve public security and improve crime-fighting capabilities. Like the Singapore Safe City Test Bed, the Huawei solution enabled authorities to integrate a diverse range of information modules and communication methods across departments and regions.

Officers also had their smart devices connected to private broadband networks to access live feeds from a monitored location. Law enforcement was thus able to better coordinate responses and reduce vulnerability to cyber-attacks by using the Huawei solution. As Nanjing was the host city for the Asian Youth Games in 2013, the city government used Huawei's technology to provide better surveillance and protection of key areas.

For instance, Nanjing applied the technology by connecting drone-mounted cameras to ensure that law enforcement would not be hampered by blind spots in video networks or by low-quality imagery. By adopting the safe city concept, public safety and security during the large-scale event was ultimately strengthened.

Additionally, smart police cars with integrated cameras connected to a command and control center monitor difficult-to-cover areas. The combination of these different cameras enabled a faster and more accurate means of identifying suspicious and dangerous vehicles, which ultimately prevented the attack from taking place.

Islamabad's Safe City Project

In July 2016, Pakistan's Capital Police Force was reported to have thwarted a major terrorist attack similar to the multiple terror attacks in Mumbai in 2008. Security snap checking to identify suspicious vehicles via state-of-the-art security equipment was made possible under Islamabad's Safe City Project. Since June 2016, around 1,850 modern surveillance cameras around the capital monitor entry and exit points, roads, commercial centers and other important buildings.

PREDICTIVE POLICING

Predictive policing is an emerging technological approach in the domain of smart policing. It refers to the application of analytical and statistical models to help identify targets for police intervention to prevent or solve a crime. Tools for predictive policing have different uses.

They can range from the prediction of high-risk areas for crimes to the identities of perpetrators and victims of crimes. In recent years, many law enforcement agencies have started to experiment with predictive policing. Predictive policing represents one of the latest attempts at introducing smart policing in law enforcement.

It effectively leverages big data and automated data mining in many ways that the human brain is unable to replicate. There are several benefits associated with the adoption of such tools. It paves the way for more efficient and proactive policing (rather than reactive policing), and secondly, it provides law enforcement agencies with a more structured approach to resource allocation for better strategic planning and long-term sustainability.

PredPol

PredPol is a cloud-based crime prediction software that focuses primarily on identifying locations where crimes are most likely to occur within a specific timeframe. Initially capable of only predicting crimes like burglary and car theft, PredPol's core technology has expanded to also include predictions of drug-related crime, gang-related crime, anti-social behavior, and gun violence. It has been utilized by many law enforcement agencies, such as the Los Angeles Police Department, Seattle Police Department, Florida Police Department, Maryland Police Department, and Kent County Police Force.

PredPol adopts a specific geographical approach in predicting crime and does not take into account personal information or socioeconomic factors such as race and income levels. The technology customizes predictions to different areas based on a 500-by-500 foot framework, to ensure all areas are covered. The PredPol system works by analyzing data through a sophisticated algorithm that applies proven criminal theories to predict the top 10 to 20 spots where crime is most likely to occur in the next few hours. To do so, it leverages a variety of factors, such as historical and recent crime data, real-time activity, and weather forecasts.

Once these 'hot spots' are identified, patrol officers can then visit these locations multiple times during their shift, making their presence felt in the area, thereby preventing crime from taking place. This means that for PredPol to be more effective, community-based services and positive outreach programs must already be in place. As the model depends on the presence of police officers to prevent/solve a crime, PredPol enables officers to access its predictions on the go by linking its system to the computers onboard patrol vehicles.

Due to the comprehensive and usable framework developed by PredPol, law enforcement agencies using PredPol are of the view that the program represents a paradigm shift in how officers have conventionally done policing and is a valuable tool in helping to reduce crime. For example, in 2014, the Los Angeles Police Department's (LAPD) Foothill Division reported a 13% decrease in crime within a mere four months after adopting PredPol, a significant improvement compared to the 0.4% increase in the rest of the city where the program has yet to be implemented.

The LAPD Foothill Division also saw a 20% fall in predicted crimes over a year, and even experienced a day without crime in February 2014. Similarly in 2014, the Alhambra Police Department in California had reported a 32% fall in burglary cases, as well as a 20% reduction in vehicle theft since it started using PredPol. Moreover, the analysis provided by PredPol has helped improve community policing efforts. In using PredPol, the Alhambra Police Department was able to increase its visibility to the community as officers spend more time patrolling the high-risk crime areas.

This swift response was due to the 'smart mapping' provided by the GIS platform as well as the system's ability to detect anomalies in the social media space (many bystanders were tweeting the incident as it occurred.) The information helped officers to quickly collate and make sense of what was happening on the ground. This example highlights how advanced data analytics can play an important role in improving police capabilities in terms of responding to social disturbances and maintaining public safety.

Geographic Information Systems (GIS)

The GIS refers to a 'smart mapping' platform that enables predictive policing. Similar to the safe city concept, it allows information aggregation from various data sources. For instance, security surveillance and social media feeds can be plotted on a map to help law enforcement agencies shorten response times by quickly collating data and improving ground sensing. Additionally, GIS technology can also be used in the areas of cyber and supply-chain security.

Users of the GIS platform include Singapore government as part of its Safe City Test Bed. It has also been tested by other law enforcement agencies such as the Santa Clara Police Department, Boston Police Department, Los Angeles Police Department, US Department of Homeland Security as well as the Royal Malaysia Police. In the case of the Santa Clara Police Department, officers were able to respond to a public brawl, pinpoint the location of the victim, and identify the suspects within three minutes.

SITUATIONAL AWARENESS

To make better strategic and operational decisions, it is essential for law enforcement to improve their situational awareness. Apart from the implementation of intelligent infrastructure in smart cities, other technological innovations, such as those discussed below, can be very useful. Such innovations serve as important force multipliers while lowering operational costs.

More importantly, they can be used to support police missions in many fields, such as kidnapping, search and rescue operations, bomb investigations, drug interdictions, fugitive investigations, crowd control, collection of evidence, investigations on traffic accidents, tactical operations, police pursuits, emergency and disaster response, and CBRNE/HAZMAT management.

Unmanned Aerial Vehicles (UAVs)

UAVs, more commonly known as drones, are one new technology that can be used to increase situational awareness in operations. Many law enforcement agencies, such as the Federal Bureau of Investigation (FBI), San Jose Police Department, Santa Rosa Police Department, and the Dutch Police Force are using drones to conduct surveillance, gather intelligence, and assist police pursuits. In 2015, the London airport police adopted drones as part of its counterterrorism strategy.

Surveillance drones are used at the four London airports to monitor external security from the air. The surveillance provided is envisaged to allow counter-terrorism officials to carry out missions seven times faster, and reduce operational costs by at least £1.2 million. Such technological innovations are immensely beneficial as it enables more ground to be covered quickly without the need to deploy more police officers.

Hence, drones represent yet another aspect of the new digital movement that can help to counter current, new-age security threats more effectively and efficiently. Yet at the same time, concerns over the use of drones for malicious purposes have arisen despite it being an extremely useful tool for law enforcement.

This is exemplified by the 2016 incident where a small drone containing traces of radiation was found on the roof of the Japanese Prime Minister's office. As drone technology is constantly improving, the security risks associated with unauthorized drone use naturally increases.

The potential weaponization of drones for carrying out attacks is a case in point. Drones can be fitted with automatic weapons, IEDs, or large payloads and used offensively. Law enforcement agencies in many countries have therefore adopted several innovative measures to manage these risks.

For instance, it has become mandatory for drones in the US to be registered with the Federal Aviation Administration, as part of its approach to addressing safety/security concerns. Japan's Metropolitan Police Department possesses a special drone equipped with a camera and a large net to capture rogue drones.

Interestingly in the Netherlands, the Dutch Police Force has turned to a low-tech solution to counter this high-tech problem. It recently experimented with using eagles to capture or take-down unlicensed drones in mid-flight. Anti-drone technology has also been developed to mitigate the risks associated with drones.

One such example is the HP 47 Counter AV Jammer, which several law enforcement agencies have started using. The HP 47 Counter AV Jammer can block drones up to 1,000 feet from sending data (including video feeds) back to its operators. It can also disable operators' remote access to the drone and trap it within an invisible fence.

Once trapped, authorities can either capture the drone with a net or shoot it down with the help of snipers. This anti-drone technology was used by the Swiss authorities during the World Economic Forum, as well as the German police when the former US President Barack Obama visited the country, to prevent any UAVs from getting too close to their locations.

Unmanned Underwater Vehicles (UUVs)

UUVs refers to underwater drones that can operate without a human pilot. Compared to UAVs, which are increasingly sophisticated and used by many police agencies, UUVs are still in the early phases of development. Given the potential benefits, UUVs can bring to police work, this technology should be closely monitored by law enforcement agencies.

UUVs can be particularly useful for operations involving body recoveries and/or underwater evidence-retrieval. More importantly, it can serve to ensure the efficiency, effectiveness, and safety of law enforcement officers. In the near future, countries with vast coastal areas or significant in-land water surfaces will likely deploy UUVs for police operations in the same way they use drones today.

Interestingly in the Netherlands, the Dutch Police Force has turned to a low-tech solution to counter this high-tech problem. It recently experimented with using eagles to capture or take-down unlicensed drones in mid-flight. Anti-drone technology has also been developed to mitigate the risks associated with drones.

Persistent Surveillance Systems

Like drones, the Persistent Surveillance Systems is a surveillance technology that uses airborne cameras to monitor the city and record data in real-time. The system has been tested by the Los Angeles County Sheriff's Department to monitor the city of Compton, and even track fleeing suspects.

By using these airborne cameras, law enforcement agencies can monitor a wider area of the city more cost-effectively and efficiently, as compared to using police helicopters or land surveillance cameras.

AUTHENTICATION (BIOMETRICS)

Biometric innovations are not limited to border security usage but can be adapted for other law enforcement purposes. Technological advancements have given rise to many biometric devices that allow law enforcement to identify suspects and criminals more effectively and efficiently. Biometric innovations are not limited to border security usage but can be adapted for other law enforcement purposes.

Mobile Biometric Device

As its name suggests, the Mobile Biometric device is a handheld gadget that is used in the field to identify individuals by scanning fingerprints, irises, and other biometric information. The information is sent to a remote DNA database for processing, and the results are transmitted to the investigator within a short period. Evidence technicians can use the device to scan a latent fingerprint and electronically transmit the print to a fingerprint database, which will then provide potential matches.

The Mobile Biometric Device is used by the Stockton Police Department to process fingerprints at crime scenes. The use of such a device is expected to improve police investigations as it shortens the time taken to process fingerprints.

The Mobile Biometric devices can provide matches with an average response time of 10 minutes, thereby allowing investigators in the field to begin their work almost immediately. This is a stark contrast to traditional processing methods where investigators would often have to wait for days/weeks for the results. Additionally, the Stockton Police Department has reported that the device is particularly useful in identifying suspects in cases involving commercial crimes, residential crimes, and automobile theft.

Rather than replacing the traditional method of processing evidence, the Mobile Biometric Device should be used to complement existing methods. This is because crime investigations benefit when more information on a crime scene is available, and the device can potentially provide leads or identify persons of interest to approach when there are no witnesses.

RapidHIT DNA Testing Machine

The RapidHIT DNA Testing Machine is a portable device that can help investigators identify criminals and victims quickly. This is done by matching swabs taken from a crime scene against a national DNA database. The device can process DNA samples from sources such as teeth, sweatbands, cigarette butts, and even clothing, and does not require any specialist knowledge to operate.

The whole process takes about two hours, which is considerably shorter than using traditional DNA analysis methods. Many law enforcement agencies are currently using the RapidHIT DNA testing machine. They include the Arizona Police Department, Tucson Police Department, Pima County Sheriff's Department, Alameda County Sheriff's Department, Richland County Sheriff's Department, and Palm Bay Police Department, US Department of Justice, Department of Homeland Security as well as the crime lab in Orange County, California.

The RapidHIT machine has been used in investigations involving burglaries, violent crimes, immigration offenses, tracking suspects, and human trafficking. This technology gives law enforcement an edge by generating investigative leads, identifying potential suspects, and providing evidence quickly. For example, the current system for most California law enforcement agencies involves shipping DNA samples to a state lab where DNA analysis can take up to weeks or months. The lab is often overwhelmed and cannot process the samples expeditiously, thereby delaying overall investi-

Facial Recognition Software

Facial recognition software is an advanced forensics biometric technology that was first developed in the 1960s, but has only recently evolved to become accurate enough for widespread use. It generally works by extracting key facial identifiers from a still photo or video image of an individual and then comparing these identifiers to biometric profiles in a criminal database.

For instance, the software can determine if an individual is wanted within seconds simply by comparing his/her eye size or shape of the nose bridge against information from an INTERPOL database. An added advantage is that an officer can also access this information through a mobile device. Facial recognition software is commonly used by law enforcement agencies to identify individuals in crowded areas, it is also particularly useful for locating suspects on the run, border security, conducting missing person searches, and pre/post-attack surveillance.

The Leicestershire Police, for example, used NEC's facial recognition software 'NeoFace' to enhance public safety and security during 'Download' is a large-scale outdoor music festival that saw almost 100,000 attendees. The digital images (including low-resolution ones) captured by the software, were matched against a database of criminals in Europe who specifically targeted music festivals.

The San Diego Police Department's fugitive task force also relies on facial recognition software to search for wanted criminals in high-profile violent crime cases. In addition, the Honolulu Police Department uses the MorphoFace Investigate system developed by Morpho, to determine if a suspect is linked to a particular crime by analyzing his/her facial identifiers from an image.

Facial recognition software can be used in conjunction with spatial-temporal profiling technology to detect behavioral anomalies. The 14 international airports throughout Brazil has adopted technologies developed by NEC to enable officials to identify watch list individuals easily and alert authorities in real-time, thereby enhancing the effectiveness and the efficiency of customs procedures and border control.

Considering there can never be sufficient resources to deal with the widespread proliferation of crime, facial recognition software empowers law enforcement to carry out "upfront crime prevention" amid a complex and vulnerable security landscape. Other law enforcement agencies using the facial recognition software include the Seattle Police Department, Boston Police Department, Federal Bureau of Investigation, US Immigration and Customs Enforcement, and the US Border Patrol.

FORENSICS

Forensics is critical in any investigation, be it chemical or digital analysis. Technological advancements have paved the way for law enforcement to obtain forensic information quickly and convert it into actionable intelligence.

TruNarc Handheld Narcotics Analyzer

TruNarc Handheld Narcotics Analyzer is a mobile device that can identify more than 100 substances, cutting agents, and precursors within seconds. Using Raman spectroscopy, the device can quickly determine the composition of the stimulant, depressant, analgesic, or hallucinogen. Upon identifying the substance, the device will automatically capture the results, date, and time stamp the results and provide automated reports to law enforcement officials.

The device does not require samples to be taken by direct contact, and the number of different substances that TruNarc can identify is updated every three months to include new and emerging drugs in its database. Law enforcement agencies using TruNarc includes the South Australian police, Yarmouth police, Gadsden Police Department as well as the Franklin County Sheriff Department.

A mobile device capable of identifying substances in near-immediate time, TruNarc is yet another innovation of smart policing that will greatly benefit law enforcement in many ways. It brings immediacy to investigations involving drug dealing and trafficking; helps law enforcement stay ahead of the constantly evolving narcotics threat; increases officer safety when dealing with harmful substances, and eliminates the possibility of any contamination of evidence.

TruNarc Handheld Narcotics Analyzer is a mobile device that can identify more than 100 substances, cutting agents, and precursors within seconds. Using Raman spectroscopy, the device can quickly determine the composition of the stimulant, depressant, analgesic, or hallucinogen. Upon identifying the substance, the device will automatically capture the results, date, and time stamp the results and provide automated reports to law enforcement officials.

The device does not require samples to be taken by direct contact, and the number of different substances that TruNarc can identify is updated every three months to include new and emerging drugs in its database. Law enforcement agencies using TruNarc includes the South Australian police, Yarmouth police, Gadsden Police Department as well as the Franklin County Sheriff Department.

A mobile device capable of identifying substances in near-immediate time, TruNarc is yet another innovation of smart policing that will greatly benefit law enforcement in many ways. It brings immediacy to investigations involving drug dealing and trafficking; helps law enforcement stay ahead of the constantly evolving narcotics threat; increases officer safety when dealing with harmful substances, and eliminates the possibility of any contamination of evidence.

In helping to improve the efficiency and effectiveness of law enforcement in getting illegal drugs off the streets, TruNarc also contributes to improved public safety and security, as there is a high likelihood that crimes motivated by drug use and addiction, such as assaults and robberies, can be reduced.

Compared to existing methods of sending drug samples to a laboratory for analysis, TruNarc expedites this process. This, in turn, enables the police to formally charge the suspect in a shorter time. The Gadsden Police Department for instance, used TruNarc to analyze a small bag of meth within 30 minutes.

In 2013, the Gadsden Police Department took three days to conclude investigations that would have taken 18 months if the samples were sent to a laboratory, which subsequently resulted in the seizure of over 700 bags of synthetic marijuana. Similarly in 2014, the Franklin County Sheriff Department also used the device to speed up investigations, which led to the seizure of over 8.8 pounds of methamphetamine. Given the speed and accuracy with which TruNarc identifies substances, the device can benefit various law enforcement agencies such as police departments, customs, and border patrol officers.

Synthetic DNA Spray

Although the introduction of synthetic DNA increases the possibility of criminals manipulating it to perpetuate crime, it also offers law enforcement additional solutions for crime-fighting.

Using synthetic DNA put together by mathematical algorithms, unique lines of DNA code can be created for every individual building or home. Invisible to the naked eye, odorless, and virtually impossible to be washed off, the synthetic DNA glows in a bright shade of blue under ultraviolet light. When sprayed onto a person who enters or exits a building or shop, the chemical traces left on him/her provide investigators with hard evidence to identify as well as connect the individual to a crime at a specific location.

Furthermore, the synthetic DNA solution stays on the skin for almost two months and clings to clothes, it provides investigators with the necessary forensic evidence to support ongoing investigations even after days or weeks have passed.

The main advantage of using synthetic DNA spray is deterring crime. By placing a sign in the store/establishment warning patrons that the system is in use, potential shop-lifters maybe deterred as the risk of getting caught is higher. Businesses and homeowners who have used the system have reportedly experienced a decline in break-ins and theft.

Companies producing this technology are DNA Security Solutions and Selecta DNA. The technology is currently in use in more than 30 countries, including Australia, New Zealand, The United States and the Netherlands.

Cellebrite Universal Forensic Extraction Device (UFED) Software

Given that computers, smartphones and tablets have become part and parcel of daily life today, gaining lawful access to the content in these devices can significantly impact the outcome of investigations. The Cellebrite UFED Link analysis is an example of a digital forensics software with the ability to distill a wealth of mobile data into meaningful formats for law enforcement, removing the need for officers to engage in tedious manual analysis.

To retrieve data from mobile devices, investigators simply plug the device into a computer installed with Cellebrite software. The software enables investigators to access the data on mobile devices. It would then only take two to three minutes for the software to search through the device for call records, GPS locations, and application data. The software can even recover deleted data. The software also has a timeline feature, which displays the interactions between the user and his/her acquaintances in a single diagram. This data is particularly helpful in speeding up investigations by revealing motives and establishing relevant connections between suspects and victims.

Digital forensics is primarily used to obtain critical evidence needed to convict criminals such as sexual predators, murderers, and terrorists. For instance, the Boulder Police Department used the Cellebrite software to access data on the mobile phones of drug overdose victims to uncover the identities of drug dealers. The Connecticut Police Department used Cellebrite technology to recover a series of incriminating text messages that were deleted from the mobile phones of murder victims, which subsequently resulted in the arrest of the murderer.

Wynyard Digital Evidence Investigator

With the prevalence of digital evidence today law enforcement now have to analyze vast amounts of complex data. The Wynyard Group's Digital Evidence Investigator, a criminal analytics technology that processes, locates, and analyzes the electronic evidence contained within confiscated digital devices, is designed to help law enforcement meet this challenge. The technology, developed in association with the New Zealand Police, can benefit police agencies, customs, border control, fusion centers, and homeland security.

To retrieve data from mobile devices, investigators simply plug the device into a computer installed with Cellebrite software. The software enables investigators to access the data on mobile devices. It would then only take two to three minutes for the software to search through the device for call records, GPS locations, and application data. The software can even recover deleted data. The software also has a timeline feature, which displays the interactions between the user and his/her acquaintances in a single diagram. This data is particularly helpful in speeding up investigations by revealing motives and establishing relevant connections between suspects and victims.

Project Spotlight by Thorn

The Internet has, unfortunately, become an enabler of human trafficking, and in particular, child trafficking. In the US alone, the number of human trafficking cases has increased exponentially over the years. Unfortunately, the sheer amount of data, combined with the use of the Dark Web by criminals to mask their activities, makes it very difficult for law enforcement to deal with such cases expeditiously.

Spotlight is a web-based application developed by Thorn to address this challenge, but also transform the massive amounts of data into an asset for law enforcement. Thorn is a company that focuses on defending children against child sex trafficking, dark web child abuse, and exploitation, as well as operating as a social platform for cyber safety.

Spotlight leverages digital footprints to better analyze and track data, which can ultimately lead to the discovery of the traffickers and their victims. It is a neural net that gets more intelligent and efficient each time the software is used. More than 4,000 officers from 780 law enforcement agencies all across the US have adopted Spotlight in their work.

The Federal Police of Honolulu for instance, regards Spotlight as "a force multiplier at every stage of the operation" and "allows us to conduct faster, more precise investigations that will remove criminals from the street and most importantly, recover victims". In 2016, 6,325 victims, 1,980 children and 2,186 traffickers were identified through Spotlight.

By reducing investigation time by at least 60%, Spotlight enables law enforcement officers to better manage their caseload. Spotlight makes tracking down traffickers and their victims much faster and easier for the law enforcement, and shows how the Internet can become a disabler of human trafficking.

CONCLUSION

The future of policing should encompass new technological innovations. This document has laid out several key examples of innovative policing solutions and tools already available to law enforcement agencies. Technological advancements today present invaluable opportunities for law enforcement to improve policing in a world with diverse criminal challenges, largely in terms of increasing the efficiency and effectiveness in fighting crime.

Relying on traditional means will no longer suffice and will only result in law enforcement constantly lagging behind criminals. Instead, it is now time for law enforcement to start embracing and incorporating the concept of smart policing to improve public safety and security for its citizens



WWW.TACAFRICA.ORG