Research

Roles of ICTs in assisting Internal Security and Community Policing: A Window into Nigeria

Victor Chuks Nwokedi Ph.D., CLN, FIASR

University of Jos, Faculty of Education, Department of Social Science Education, Library and Information Science Unit. E-mail: victorchuksnwokedi@yahoo.com

Accepted 19 June 2020

This paper discussed the Roles of ICTs in Strengthening Internal Security and Community Policing in Nigeria using Information and Communication Technologies (ICTs). The need to embrace ICT-enhanced policing in Nigeria becomes imperative because insecurity, robbery, kidnapping, terrorism and insurgency have taken a new dimension and have gone sophisticated as criminal elements have deployed high-tech approach such as mobile technology, internet technology for exploiting and unleashing criminal activities on the society. To reduce this incessant and unpleasant proliferation of modern crime, calls for the fortification of existing policing approach in Nigeria using Information and Communication Technologies. This study is an attempt at strengthening the existing policing approach to be able to meet the insecurity challenges currently being faced and facing the Nigerian society. The study revealed that the incidences of insecurity, terrorism and insurgency can effectively be rendered impotent in Nigeria through the use of ICT. Notably among the proposal for an ICT-enhanced policing is the concept of virtual community policing which explore the availability of mobile devices for easy and effective crime reporting and crime control in Nigeria.

Keywords: ICT, Security, Policing, Community, Nigeria.


INTRODUCTION

ICT is a broad term referring to multitude of means which can serve for storage, dissemination, replication of all types of knowledge and information (Nwokedi & Nwokedi, 2018). Generally, it stands for Information and Communication Technologies that are broadly perceived as economic development tools, allowing countries and societies to benefit all knowledge and information that can be acquired by their usage (Nwokedi & Nwokedi, 2018); ICT can be seen as an acronym for Information and Communications Technologies. It is an umbrella term that includes all technologies for the manipulation and communication of information. The term is sometimes used in preference to information technology (IT), particularly in two communities, education and government. ICTs are being used increasingly by global industry, international media, and academics to reflect the convergence of computer and communication technologies. Thus, ICTs can be viewed as a set of activities and technologies that fall into the union of IT and telecommunications; ICT is a general term that describes any technology that helps to produce, manipulate, store, communicate, or disseminate information (Nwokedi, Nwokedi, Chollom & Adah, 2017). Information and communications technologies can be described as computers and digital technologies that are used to prepare and share information;
ICTs are also seen as Electronic devices such as Internet, Web sites, e-mail, mobile telephones, fax, telephone, and radio; ICT is a Broad term referring to multitude of means which can serve for storage, dissemination, replication all types of knowledge and information. Generally it stands for Information and Communication Technologies that are broadly perceived as economic development tools, allowing countries and societies to benefit all knowledge and information that can be acquired by their usage (Cox, 2007).

For the purpose of this paper, the abbreviation ICTs stands for computers and digital technologies that are used to prepare and share information.

Community policing is a philosophy that promotes organizational strategies that support the systematic use of partnerships and problem-solving techniques to proactively address the immediate conditions that give rise to public safety issues such as crime, social disorder, and fear of crime.

Community policing comprises three key components:

1. **Community Partnerships**
   Collaborative partnerships between the law enforcement agency and the individuals and organizations they serve to develop solutions to problems and increase trust in police

2. **Organizational Transformation**
   The alignment of organizational management, structure, personnel, and information systems to support community partnerships and proactive problem solving

3. **Problem Solving**
   The process of engaging in the proactive and systematic examination of identified problems to develop and evaluate effective responses.

Internal Security refers to upholding national law and maintenance of peace, law and order within a country's territory. Internal security, or IS, is the act of keeping peace within the borders of a sovereign state or other self-governing territories. Generally by upholding the national law and defending against internal security threats. Responsibility for internal security may range from police to paramilitary forces, and in exceptional circumstances, the military itself.

Having examined the major concepts in the paper, we can now discuss the roles of ICTs in strengthening internal security and community policing in Nigeria.

**Nigeria Security Issues**

The high rate of crime in both urban and rural communities of Nigeria call for evaluation of the existing approaches to crimes fighting and its prevention. Some of the frequently reported crimes are kidnapping, robbery, murder, insurgency, tribal feud to mention but a few (Ratcliffe, 2007). Another dangerous dimension to insecurity in Nigeria that has overwhelm the present policy system is the endemic conflicts between ‘indigenes’ (farmers) and ‘settlers’ (herders) leading to killings in Benue, Plateau and other parts of Northern Nigeria (Institute for Peace and Conflict Resolution, 2016)

Had the policing system in the country been fortified and strengthened by ICT backbones, so of these avoidable communal crises would have nipped in the bud.

Internal Security refers to upholding national law and maintaining peace, law and order within a country's territory. Internal security, or IS, is the act of keeping peace within the borders of a sovereign state or other self-governing territories. Generally by upholding the national law and defending against internal security threats. Responsibility for internal security may range from police to paramilitary forces, and in exceptional circumstances, the military itself. Having examined the major concepts in the paper, we can now discuss the roles of ICTs in strengthening internal security and community policing in Nigeria.
policing in Nigeria can never be over-emphasized. This will help the relationship between both the police and technologies go a long way in the determination of the achievement and sustainability of their ultimate goals, and the success and well-being of the nation at large (Ratcliffe, 2007). New technology has huge implications for policing. The advent of Technologies such telecommunication devices, computers, GPS tracking, smartphones, CCTV and biometrics etc., backed by access to large amounts of public and police-specific data. This means that the technologies will be a potential tool for officers to be better informed, improve intelligence and investigative capabilities, better access to criminal records and prevention of crime in the law enforcement community. The role of technology in police institutions and police practices has long been recognized as relevant and ambivalent (Ogunbameru, 2008).

Technological advances are particularly relevant for policing because they are seen to influence the organization and practices of police in the ways that intimately connect to the police function of crime control. This will bring new and more efficient means of crime detection and control, communication among police, and police transportation, all these influence the police job of fighting crimes and affect the level of legitimacy information police receive from the public and relevant bodies of governments (Simon, 2004). ICT in policing make possible the collection, storage and rapid dissemination of information, it enhances public safety and reduces crime.

**Community Policing Activities**

According to the literature (Ogunbameru, 2008), COP efforts usually comprise, but are not limited to, the following activities to improve public safety and establish trust between police and community.

1. **Regular Patrols.**

Regular patrols have in some contexts been shown to have significant effect on police-community relations as well as reducing crime rate and fear of crime in communities. This contrasts with a traditional policing model where the police are available at the police stations and people are to required visit police station to report the crime. In COP models, police officials often perform regular patrols, on foot or vehicle, to meet and interact with the community. Moreover, it is believed that continuous and regular presence of police in neighborhoods has been found to have a positive impact on police-community relationship because people feel more comfortable to approach and share their concerns with a person that they are familiar with. Similarly, presence of police in the neighborhood may also act as a deterring factor to reduce crime (Adewole, 2007).

2. **Mobile Police Services.**

These help in providing essential police and administrative services to remote communities that otherwise may have to travel long distances to reach police stations. This is particularly beneficial for the people living in remote villages and hilly areas with sparse transport access and road connectivity. Since it can be difficult to provide such services on a daily basis, the mobile police services are often provided on designated days on weekly, fortnightly, or monthly basis depending on the requirements and available resources.

3. **Community Forums.**

These provide a common platform for various stakeholders of COP, such as government, police, and community. The primary objective of these forums is to highlight and address the persistent community concerns before these escalate to bigger problems. Keeping in view the available resources, key community concerns are discussed and solutions are provided at the community forum meetings held regularly. The advantage of these forums is that many smaller issues can be resolved on the spot that otherwise might require more formal police or government intervention. They can also uncover competing interests and concerns within communities (Ogunbameru, 2008).

4. **Community Awareness-Raising.**

These activities are meant to provide community members with necessary information required to stay safe and avoid common dangers. Community awareness is conducted in many ways, including:

(a) door-to-door visits,
(b) trainings,
(c) television ads,
(d) local announcements,
(e) school visits
(f) mobile alerts, and
(g) use of social media.

5. **Complaint Management.**

These are systems where any member of community can raise their concerns related to the safety of their neighborhood or about the behavior of police officials. There is usually a platform for submitting individual and community complaints and providing feedback. The community members can also provide their feedback related to various problems highlighted in the forums.
Information Technology and National Security

Information technology (IT), as defined by the Information Technology Association of America (ITAA), is "the study, design, development, implementation, support or management of computer based information systems, particularly software applications and computer hardware." (eNotes.com, 2011). IT deals with the use of electronic computers and computer software to convert, store, protect process, transmit, and securely retrieve information. Today, the term information has ballooned to encompass many aspects of computing and technology, and the term has become very recognizable.

IT professionals perform a variety of duties that range from installing applications to designing complex computer networks and information databases. A few of the duties that IT professionals perform may include data management, networking, engineering computer hardware, database and software design, as well as the management and administration of entire systems.

Information technology (IT) will play a critical role in strengthening Nigeria's National security against potential future attacks. Specifically, IT will help enable the nation to identify potential threats, share information more readily, provide mechanisms to protect the Nation, and develop response capabilities.

Tjin-A-Tsoi chief executive officer of the Netherlands Forensic Institute (NFI) one of the leading forensic service providers in the world is convinced that a true breakthrough in the near future will be that security measures are transparently implemented within software. According to him "Users need not to be aware of these security measures anymore. IT offers great possibilities for the welfare and health and safety of people. In order to use all the benefits of this great technology, special care should be taken of a number of challenges such as mobile security and secure identification. New technological innovations and their implementation need the involvement of politicians, the public and private sector and other stakeholders".

The Nigeria security services to be able to address Security issues adequately there is need to focus on three research areas, these are Security, (these includes authentication, availability, containment, detection and identification, privacy, recovery, and new security models); Information fusion (Information fusion includes research in data and text mining, data integration, language technologies, image and video processing, and evidence combination), and critical infrastructure-based as recommended by a National Research Council Committee on Science and Technology for Countering Terrorism in the USA.

That committee also called for research in information and network security, new information technology for emergency response, and new information technology for the detection, remediation, and attribution of attacks (information fusion). Information technology for emergency response includes a variety of problems-most notably problems for critical infrastructure. As a result of the April 16, 2007, shootings at Virginia Tech, campus leaders in safety, security, emergency management, and information technology met in Washington, D.C. August 2008, to put emergency management firmly at the top of the agenda during an EDUCAUSE summit on “The Role of IT in Campus Security and Emergency Management.” In the closing session, the group put together an Action Agenda "rooted in a common desire to increase information sharing between one another and to put emergency management and campus security at the forefront of campus conversations and at the top of the research agenda, even after the national spotlight has dimmed". Emergency Management according to The International Association of Emergency Managers (IAEM) is “the managerial function charged with creating the framework within which communities reduce vulnerability to hazards and cope with disasters.” Most campuses in the conference accept a four-phased approach to emergency management: These include:

- Preparedness: Mobilizing and preparing the campus response to emergencies, from the development of emergency response plans and the procurement of supplies to educating the campus community about procedures for disaster response

- Mitigation and prevention: Taking steps to reduce or prevent the possibility of disaster on campus, from identifying and assessing risk to putting preventative measures in place to reduce the risk occurrence

- Response: The way that a campus reacts to disaster, including crisis communication and the treatment and protection of key assets, from university students and personnel to critical information systems and university property

- Recovery: The timely resumption of standard operating procedures on campus, moving from “disaster” mode to “normal” mode through treatment, rebuilding, reorganization, and recovery.

All the above measures must be employed in addressing security issues in most public places. All emergency management, as defined by IAEM, must be
applied by the Nigerian security authorities:

- **Comprehensive**: Taking into account the full range of hazards and societies vulnerabilities while preparing a response that encompasses all assets (cyber, human, and physical) and members of the society / community.

- **Progressive**: Anticipating new and emerging threats and securing the society and community against them.

- **Risk-driven**: Rooted in sound principles of risk and impact assessment and identification.

- **Integrated**: Considering all members society and surrounding communities, from federal response agencies and local law enforcement to society police and IT.

- **Collaborative**: Cultivating a sense of trust, respect, and responsibility among all parties.

- **Coordinated**: Providing a safe, efficient, and well-maneuvered response to disaster and recovery.

- **Flexible**: Allowing for creativity and innovation when established responses may fail or fall short of needs and expectations.

- **Professional**: Relying on a knowledge-based approach to research and planning.

Summit participants, noted that the hallmarks of Effective Emergency Management are:

- Relevant players understand their roles in advance and execute accordingly.
- Crisis communications are clear, consistent, and well received.
- Life and property are preserved to the greatest extent possible.
- Response plans are easily accessible, appropriate, and updated.
- Critical technologies work without delay or interruption.
- Society transitions from “crisis” to “normal” in a timely fashion.
- The Country image is maintained in the eyes of internal and external communities.

**Emerging Opportunities for Security Management**

The integration of information technology and emergency management presents significant opportunities for innovation in the way to assess, manage, and respond to security challenges. Most technologies today are increasingly mobile, highly integrated, and inherently flexible. From social networking sites to geospatial imaging, the society today can take advantage of emerging tools to address critical security needs. (An EDUCAUSE White Paper, 2008)

**Emergency Communication Systems**

Emergency notification systems are Vendor applications that offer a plethora of opt-in services that can push emergency messages to cell phones via text messages, e-mail accounts, instant message accounts, or college or university voicemail systems. This system can help the Nigeria Security system respond to distress call from citizens. The most frequently cited technological answers to emergency notification system according to (Young, 2008), are Sirens, digital signage in common spaces and classroom buildings, notification systems that include both emails and text messages, and automatic messaging to classroom projectors and alarm systems.

**GPS Technology**

GPS-enabled devices can also help citizens signal for help when emergency situations arise. For example cell phones with Rave Guardian software, can activate a timer on their device when they would like surveillance from the police. On a University campus for example “student stepping outside the library at night, might activate the system while crossing campus. If the timer is not deactivated within a given time frame, authorities can use GPS technology to track the student’s location. Students can also press a panic button, alerting officials that they may be in trouble and broadcasting the specific coordinates of their position” (An EDUCAUSE White Paper; 2008).

**Social Networking Tools**

To reach members of the society who are constantly connected to the Web and actively creating and sharing content in their own time, security agencies should be turning to familiar social networking tools to share news and strategies for community security. Social networking sites like Facebook and MySpace will usually allow communities to create pages that store information about security plans, emergency procedures, and community events. The widespread popularity of networks like YouTube and iTunes can create opportunities for security agencies to educate through quick, entertaining videos and podcasts, these can easily be shared and stored.

Members of the society are encouraged to become “friends” with security agents on Facebook and MySpace,
this can create an alternate pathway for pushing information to the wider community. Facebook and MySpace allow members of the community to add their own commentary through “on the scene” reporting, sharing messages with security agents.

**Virtual Emergency Operations Centers**

Physical emergency-operation centers (EOCs) can be used as a hub of community response in times of emergency. Communities can consider supplementing physical locations with virtual EOCs, these can coordinate response teams across geographic areas. It is noted that a virtual EOC dashboard can store and integrate unit response plans, incident reports, and operational reports from a variety of community agencies. A single user can access the virtual EOC to send communications through various channels to relevant players. In cases when the physical communities are unreachable or unsafe, the virtual EOC provides a safe and accessible alternative to coordinate groups across the wider community (An EDUCAUSE White Paper; 2008).

**Intelligent Monitoring**

Important buildings and business areas in Nigeria must turn to new advances in intelligent monitoring, from biometrics and speech-recognition software to intelligent video and swipe-card access to such buildings. These must be done by striking a balance between security and openness, personal freedoms and reasonable expectations of privacy must be maintained.

**Data Mining and Database Tracking**

Weeks after the shootings at Virginia Tech, It is noted that “campus administrators were criticized for failing to heed potential warning signs during Seung-Hui Cho’s time at the university, particularly a history of mental illness and a faculty member’s request that Cho seek counseling.” One of the issues that came up after the shootings is whether predictive modeling, aided through data mining software and other actuarial tools, offers some promise for preventing campus violence or suicide in colleges and universities. Many believe that the ability to predict violence is a nebulous process. Being able to turn to databases to share information between institutions will also be very helpful. The report by EDUCAUSE White Paper (2008), also indicated that “After two separate incidents in 2004 at the University of North Carolina Wilmington in which students were murdered by other students, officials at the UNC system’s 16 campuses began feeding suspension and expulsion data into a shared database, allowing schools to check to see if a potential applicant had a violent history at another university. The 2004 murders were not connected, but both assailants concealed past offenses from school officials.” (Cox, 2007)

**Information Sharing**

ICTs can facilitate police-community interaction through improved communication opportunities. The basic philosophy of COP encourages the development of bi-directional communication and constant dialog between police and community. ICTs can help to achieve these goals through online interactive applications, such as web portals, email and mobile alerts, micro-blogs, and social networks. For instance, after the explosion of bombs at the Boston Marathon, Boston police department used Twitter (a micro-blogging service) to inform the public about investigations, request assistance, correct wrong information propagated through press, and calm the nerves and stay restraint (Simon, 2004). After- wards, state and federal investigation agencies decided to crowd source and ask the public for help to forward any media (e.g., videos and photos) or leads related to bomb attacks. Within few hours, thousands of photos, videos, and textual data was received that led to successful identification and arrest of the two lead suspects (Adewole, 2007).

**INHIBITING FACTORS TO THE SUCCESSFUL COMMUNITY POLICING IN NIGERIA**

Despite several efforts by various security agencies administrations to curtail the level of crime in Nigeria, criminal activities and social disorder still persist in the country. Some believed that the insecurity challenges currently facing Nigerians was inability of the Nigeria police to ensure maximum security in the country, lack of equipment and sour relationship between police and public (Dawn Newspaper, 2011). Other variant factors that influence criminal activities and behaviors in the society are poverty, unemployment, bad governance, institutional constraints, lack the skills and weaknesses in law enforcement or crime-control bodies. Others (secondary) are corruption, social inequality, moral decadence, urbanization, greed and disintegration of family ties (Ajaegbu, 2012). The following factors constituted impediments to the successful implementation of community policing in Nigeria.

i. Corruption has become pervasive norms in Nigeria police force and driving abuses against ordinary citizens and led to undermining the rule of law

ii. Unfriendly relationship between police and public

iii. Institutional Constraints: perversion of justice and delay in the administration of justice.

iv. Poor incentives and inadequate manpower of
the average policeman to perform effectively and
efficiently.
v. Lack of political will to address police bribery,
extortion, and wholesale embezzlement
threatens the basic rights of all Nigerians.
vi. Inadequate funding, inadequate logistic support
and infrastructure, lack of serviceable information
and technological equipment.
vii. Unemployment is a plague that bedeviling
Nigeria and has steadily interlinked with urban
crimes.
viii. Poverty has a serious socio-economic problem
of Nigeria as a nation and had synonymously
induced criminal behaviors that influence crimes.

THE STRATEGY FOR VIRTUAL COMMUNITY
POLICING

A community policing entails community partnership in
creating safe and secure environment for all where the
people take active part in their own affairs (Ajaegbu,
2012). A virtual community is an aggregation of
individuals or business partners who interact around a
shared interest, where the interaction is supported by
information communication technology and its protocols
or norms. The unfriendly nature of the relationship
between the police and members of the public has made
the development of the concept of fortified virtual
community paramount.

Virtual community policing provides an online forum for
the police to interact with the community, other
government agencies, and other stakeholders with the
primary objective of addressing crime and disorder
problems and provide quality services to the public. The
operation of the police in a society that can be classified
into three which are:

1. Crime reporting,
2. Crime investigation and

Each of these operations can be enhanced using ICT.
The principal services rendered by a virtual community
portal are:

i. providing information to the community,
ii. soliciting information from the community,
iii. providing online services,
iv. engaging the community and
v. problem solving

Information shared with members of the public by the
police via the virtual community portal may include
information on wanted persons, crime prevention tips,
traffic conditions, and new initiatives. These information
goes a long way in promoting the peace of the
community and safety of the individual. The police also
get information from the public. This information from the
public assists the police in the area of crime reporting,
crime prevention and investigation.

The police can officially enroll some community
informant that gives them information on the incident of
crime in their area. Informant can assist the police in
fishing out wanted offenders through information. The
police can through the virtual community portal render
administrative services to the people such as applying for
permits, submitting a report of crime, recruiting police
officers. The virtual community portal can as well be used
as a forum to educate the populace on vital issues of
security interest. Users include Community Members,
Police officer, assigned Mass Media, Government
Agencies, NGOs:

a. Providing useful information to the police
b. Providing information to the public
c. Providing online services
d. Engaging members of the public

CONCLUSION

The research therefore, concludes that for effective
policing of Nigeria, all hands must be on deck. The
government must fund and empower its Police force
adequately. The masses must cooperate with the police
by giving the police force adequate information. Modern
intelligence gathering devices must be acquired and
deployed by security services, like the police, the SSS,
the Army, the Navy, the Air Force and other Para-
military. Surveillance system that can monitor most
sensitive equipment and public places must be put in
place. Real time communication systems that will enable
information sharing must be installed. Adequate scanning
of imported goods using modern scanners that can detect
weapons and other materials used in making bombs and
explosives must be put in place. There is need for
adequate border patrol and use of GIS and surveillance
equipment to monitor people and weapon proliferations.
There is need to ensure the loyalty of security agents
because lack of loyalty can cause the leak of security
information to agents of destabilization in the Country.

REFERENCES

Adewale (2007). “Overview of Policing in Nigeria:
problems and suggestions in crime and policing in
Nigeria, challenges and options” Pp. 3, Ahmadu Bello
University, Zaria.


