International Journal of Developments in Big Data and Analytics
Volume 1 No. 1, 2014, pp. 70—84

Leveraging Big Data in Enhancing National Security in Nigeria

MATHEW E. NWANGA, ELIZABETH N. ONWUKA,
ABIODUN M. AIBINU & OSICHINAKA C. UBADIKE
Federal University of Technology Minna, Nigeria

ABSTRACT The spate of terrorist attacks in Nigeria has been on the increase in the last few years. The recent successes recorded by terrorist elements in Nigeria have been attributed to lack of actionable intelligence that would enable preventive action against terrorists. To successfully defeat terrorism in Nigeria, there is a need for actionable intelligence gathering for effective repositioning of the country's security system. This paper explores how big data can be used to generate investigative lead and electronically gather intelligence for combating terrorism in Nigeria through analysis of the dark web portal. It discusses how big data analytics can be leveraged to improve situational awareness by transcending from reactive approach of security challenges and terrorism to proactive approach aimed at nipping the act in the bud. The paper also presents a notional information flow as an approach for understudying how big data technologies can underpin the improvement of national security. The paper concludes with a framework for getting started with Big Data in Nigeria.

Keywords: Insecurity, Big Data, Notional Information Flow, Dark WebPortal, Terrorist Network

Introduction

The recent security challenges in Nigeria have negatively affected the growth and development of the country. In recent times, the sounds of guns and bomb blasts have enveloped the many parts of the world (Akinode et al). There are many security problems that are currently confronting Nigeria such as socio-economic agitations, ethno-religious crises, ethnic militias, boundary disputes, cultism, kidnapping, criminality and most recently terrorism—notably the *Boko Haram* insurgency—and [more recently], the outbreak of Ebola virus. The frequent bomb blast occurrences in the Northern part of Nigeria and kidnapping in the Eastern part are indicatives of insecurity problems in Nigeria. This lack of security for life and property has assumed a crisis dimension in the country. It has negatively affected the socio-political and economic landscape of the country. The broader human security is important for the attainment of individual and national security and overall peace and development, as social unrests arising from the absence of such basic human security can indeed lead to security problems and conflicts (Abubarkar, 2004). It is, therefore, about time the nation seeks new techniques to tracking and curbing crimes.

The deregulation of the mobile phone market in Nigeria over a decade ago has led to the introduction of Global System for Mobile communications (GSM) network providers operating on the 900/1800MHz spectrum. These operators are MTN Nigeria, Airtel, Globacom and Etisalat—all stiffly competing for survival. Nigeria has the largest mobile market on the African continent with over 90 percent of individuals and corporate organisations relying completely on the mobile industry for their day-to-day transactions (Nwanga et al, 2015). This has impacted positively on the country's GDP. The statistics from National Communication Commission (NCC), the Nigerian telecommunication regulator put the *teledensity* in Nigeria at 94.4 percent in August, 2014 and active lines at 133 million subscribers in a country of about 160 million population NCC, 2014). This shows a rapid growth in the country's connectivity.

A direct result of this growth is the generation of quintillion bytes of user and network-related data in the country. This huge datasets contains the footprints of users, which includes the criminals, it can therefore be put to good use. In this age of big data, as this data is generated by people in real time, it can be analyzed in real time by high performance computing networks, thus creating a potential for improved decision making and insight (Bansal and Rana (2014). Big data analytics could be used to detect and defeat or prevent terrorist threats or attacks. In many places across the globe, information technology has been adopted to combat the problem of terrorism, insecurity and uproar (Akinode et al 2013). Big data has great potential to predict crime, crime hot spots and criminals (DHS, 2012).Like everyone else, terrorists, leave digital traces with much of what they do, whether using e-mail, cell phones or credit cards. This data can be mined and used to fighting them (DHS, 2012).

Big Data

What is big Data?

Big data refers to large datasets. Data volumes are growing exponentially. There are many reasons for this growth, including the creation of most data in digital form, proliferation of data sensors and new data sources such as high-resolution image and video (Fahey, 2010). The amount of data and frequency at which they are produced are so vast that they are currently referred to as "Big Data" (Linch, 2008). With the increasing development of internet and database technologies, the data that can be obtained is increasingly voluminous and bigger (Lavalle, 2011; Zikopolos and Eaton, 2011).The term "big data" has a variety of definitions and has been used in a variety of contexts. It is a term that is used to describe data that is high volume, high velocity, and/or high variety; requires new technologies and techniques to capture, store and analyze and is used to enhance decision making, provide insight, discovery, support, and optimize processes (Miller et al., 2012; Sicula, 2013). The term is used to reflect that a quantitative shift of this magnitude is in fact a qualitative shift demanding new ways of thinking, and new kinds of human and technical infrastructure. The key is converting this "new oil" into a public good by fostering new kinds of literacies and ethics, and combining commercial services with open data and services (Anderson and Rainie, 2012). The size of digital data in 2011 is roughly 1.8 Zettabytes (1.8 trillion gigabytes). That is, supporting network infrastructure has to manage 50 times more information by year 2020 (Bakshi, 2012). Data is predicted to double every two years, reaching about 8 Zettabytes of data by 2015 (Intel, 2012). These data are generated from Online transactions, e-mails, videos, audios, images, click streams, logs, posts, search queries, health records, social networking interactions, science data, sensors and mobile phones and their applications (Eaton et al (2012); Schneider, 2012).

Big Data Differentiators

Big data is relevant to this nation due to their vast amount, variety, complexity and variability of data produced (NAS, 2012). Nigeria may be described as an enormous data generation engine. Big data has six characteristics that actually differentiate it from ordinary or simple data. These differentiators are: Volume, Velocity, Variety, Validity, Veracity and Volatility. In fact, they are referred to as 6 Vs of Big Data (Tan, 2013).

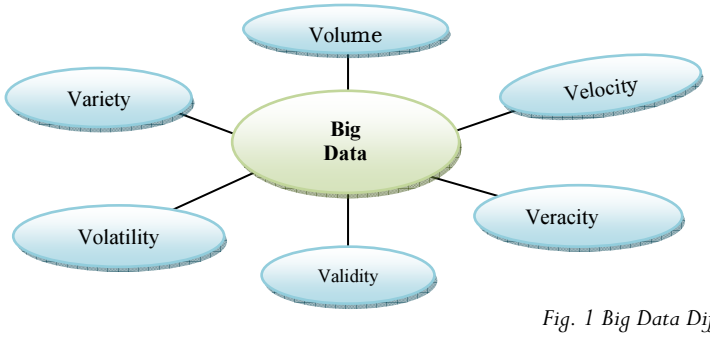

Fig. 1 Big Data Differentiators

The 3 fundamental differentiators are the Top Vs:

Volume- the vast amount of data generated every second that are larger than what the conventional relational database infrastructures can cope with.
Velocity –the frequency at which new data is generated, captured and shared
Variety – the increasingly different types of data that no longer fits into neat, easy to consume structures.

The 3 Bottom Vs are the additional characteristics:
Validity – The correctness and accuracy of the data for the intended usage
Veracity – How meaningful is the results for the given problem space
Volatility – How long do you need to look/store the data

Big Data is all about tapping into diverse data sets, discovering and co-relating unknown relationship within data and data driven insights for faster and accurate business decisions [2]. Since the activities of terrorist in Nigeria are in an unstructured form then, the application of Big Data and analytics would help to deepen proper understanding of these data for better decision making.

Big Data Analytics

Analytics is driving new capability for competitiveness and effectiveness (NAS, 2012). The act of applying software tools to process, analyze and make sense of data is called Analytics. The idea is to allow the data to speak for itself, bringing out not just the obvious correlations and connections, but the unexpected ones as well. In other words, it is a systematic way of identifying and gathering footprints or traces of activities of an object of interest from a huge mound of data. The tracking of terrorist group can be achieved through analyzing the data generated from their activities, which left traces via phone calls, e-mails, videos, images, click-streams, logs from various said networks and telecommunication lines and facilities.Identifying and understanding the full portfolio of issues facing the nation with the view of enhancing national security is possible through Big Data Analytics. Not all data must be of the highest quality. The quality of the data will depend on:

- the purpose of its use,
- the magnitude of related outcomes and potential resource investment to achieve these outcomes,
- the time –to-effect or time –to-impact of an issue, and
- the level of reliance and criticality to national strategy and operation.

The use of big data analytics to improve national security places will enable the nation achieve the following:

- transform the mode of operation of the Nigerian Security Agencies,
- lead the country to solve today's data problems,
- augment the national existing information fabric

- finally, build competitive advantage for the country to fight terrorism.

In fact, the drive for analytics creates the seeming frenzy for big data. Recent surveys conducted by MIT and IBM (2010 and 2011) with the objective of gaining perspectives on the burgeoning demand for analytics revealed the following:
(i) a 50% increase in the number of respondents to the 2011 survey, and
(ii) a 57% jump in the number of respondents that believe analytics provide "substantial" or "significant" contribution to effectiveness.

These findings can be translated to competitive advantage for Nigeria as well effective operational advantage in addressing the challenges of insecurity. The Nigeria needs experienced engineers and scientists in analytics to expand its capabilities in analytics. In essence, analytics is permeating the enterprise and impacting more and more decisions (NAS, 2012). One ultimate goal of analytics in Nigeria is to enhance the decision-making process in intelligence requisite for combating terrorism—a capability with higher Return on Investment (ROI) than that of the traditional Business Intelligence (BI) as illustrate in figure 2 below.

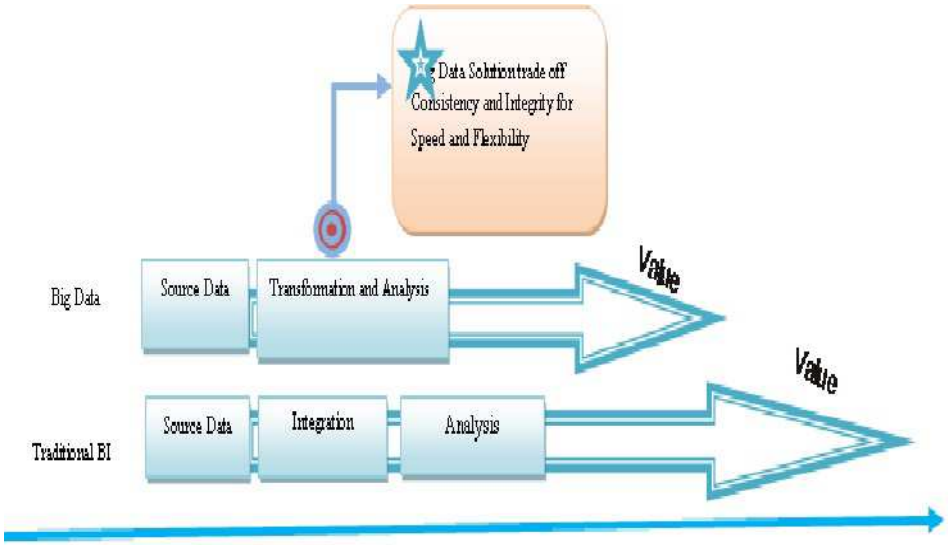

Fig. 2 ROI Benefits of Big Data Analytics— Hopkins and Evelson (2011)

The Road Map for Getting Started with Big Data for Nigerian Security Agencies

The world currently generates a huge volume of data. The capacity to store, broadcast and compute this information continues to grow exponentially, with one estimate suggesting that the installed capacity to store information would reach 2.5 Zettabytes in 2012 (Couch and Robins, 2013). International Data Corporation research suggests that the world's digital information is doubling every two years and will increase by fifty

times between 2011 and 2020, according to Hopkins and Evelson (2011).

In recent years, with the growing reliance on big data-informed intelligence operations, governments in the developed economies—the US and the UK in particular—are increasing the resource allocations to improve their ability to collect intelligence. For intelligence experts, however, automated analysis technology is a top intelligence, surveillance and reconnaissance (ISR) priority. According to William (2012), the UK 'has reached an inflection point in data deluge… [and is] now in danger of data asphyxiation and decision paralysis.' This latter comments supports the need for algorithms for discovering useful intelligence essential in fighting the menace of terrorism in Nigeria.

There are five steps to successful startup of the Big Data project—which, essentially, are cyclic approach to Big Data opportunity. These five steps are: Define, Assess, Plan, Execute and Review as illustrated in Figure 3 below.

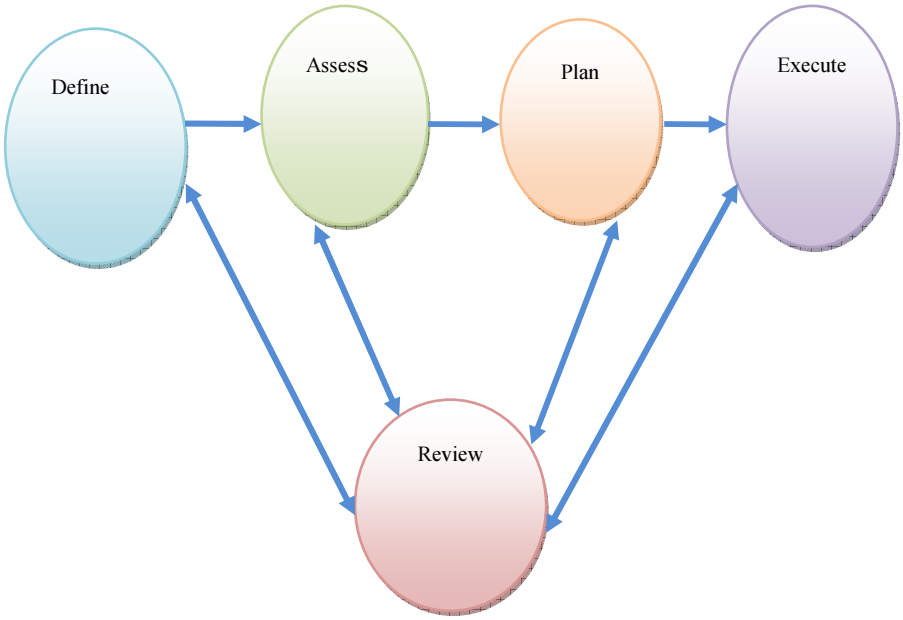

Fig. 3: Road Map for getting started with big data—Miller et al., (2012)

Figure 3 shows that review is a continual process that cuts across the remainder of the roadmap steps. The security agencies in Nigeria consist of military and paramilitary. An active collaboration between them and the federal government would lead to an improvement in the current state of national security and, specifically, the Nigerian government should consider this road map as it would enable the country to:

1. Build capacity and expand the talent pool by creating a formal career truck for line of business and IT managers and establish a leadership academy to provide big data and related training and certification.
2. Leverage data science talent by establishing and expanding "college-to government service".

3. Establish a broader and more long-lasting coalition between industry, academic centers and professional societies to articulate and maintain professional and competency standards for field of big data.
4. Expand the ministry of information and communication technology to include a center for big data and analytics. These would encourage further research into new techniques and tools and explore the application of those tools to important problems across varied research domains.
5. Provide further guidance and greater collaboration with industry and stake holders such as the Ministry of Defence, the Ministry of Interior and the Ministry of Information and Communication Technology.

It is important that the Nigerian government take the lead on Big Data Analytics initiatives. The country needs to start adopting smarter approaches to national security and start looking for indicators and any unusual events as these are the best source of intelligence. In this changed [Nigerian] landscape, Big Data Analytics could be an important terrorist-bursting tool for the Nigerian government.

Big Data Notional Information Flow

The notional information flow (NIF) is also called information supply chain (ISC). This is a five-step underlying flow, representing the data processing design to bring the analytics visualization and specific insights of the given data (program). These five steps are:

1. Understanding source and data applications: this represents the first stage of deciding what data needs to be acquired and where it is going to be acquired from.
2. Data preparation: this is a stage of data filtering, cleansing and validation.
3. Data transformation and metadata repository: this is a critical step to preparing data for analysis by aggregating different data types and applying a structural format. This is where relevance is given to different data sets, even if they are seemingly unrelated data sets.
4. Business intelligence and decision support: this is the actual analytics stage, where statistics, algorithms, simulations and fuzzy are employed.
5. Analysts and visualization: at the end of this process, there is usually a human, the analyst, who needs to make sense of insights surfaced by the analytic engine that has run against the entirety of available data (Murrow, 2006).

Advanced analytics solution requires several interacting design steps (Murrow, 2006) These underlying steps are reflected in the notional information flow. The further analytics considerations are shown in Figure 4 and it is called Cross Industry Standard Process for Data Mining (CRISP-DM) process. The CRISP-DM is a process model that breakdown the life cycle of data mining into six phases to achieve better insight and decision. This helps users to develop tool and application process for conducting analytics.

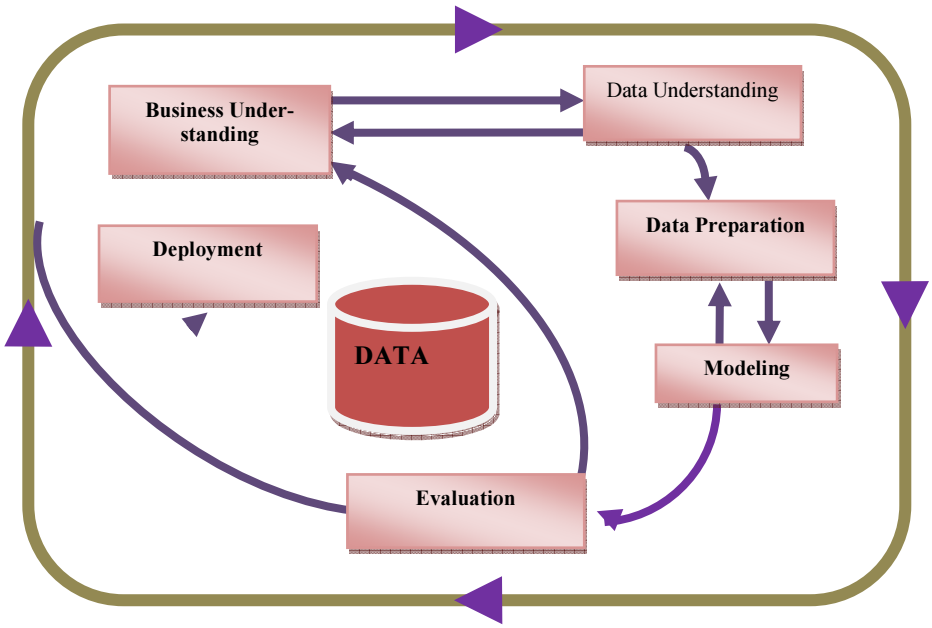

Fig. 4: CRISP-DM Process—Murrow (2013)

Terrorism

The resulting battle against terrorist activities of the Bokoharam group in Nigeria has become a national focus and the us of Big Data could go a long way in addressing the problem. According to Poop and Paindexter (2006), advanced and emerging information technologies are key assets in confronting the secretive, asymmetric and networked cells of terrorists. Terrorists are typically indistinguishable from the local civilian population. They are not part of an organized, conventional military force—rather, they form highly adaptive organizational webs based on tribal or religious affinities. They conduct quasi–military operations using instruments of legitimate activity found in any open or modern society, making extensive use of the internet, cell phones, the press, schools, houses of worship, prisons, hospitals, commercial vehicles and financial systems. Terrorists deliberately attack civilian populations with the objective to kill as many people as possible and create chaos and destruction. They see weapons of mass destruction not as an option of last resort but as a weapon of choice (Poop and Paindexter, 2006). Terrorist cells are linked to each other through complex networks of direct or mediated exchanges (Sageman, 2004).Terrorism are carried out through many data-oriented activities, which means that terrorist footprints can be captured by big data. There is a need to design the right algorithm that would extract these footprints from big data, nit them together and bring out the identity of the terrorist.

Web Portal Analysis

Terrorist across different jurisdictions heavily utilize modern transportation and communication systems for relocation, propaganda, recruitment and communication purposes (Chen et al., 2004).The basic premise is that terrorist networks can be evaluated using transaction-based models. This type of model does not rely solely on the content of the information gathered, but more on the significant links between data (people, places and objects) that appear to be suspicious (Allanach et al., 2004). How to trace the dynamic evolution, communication and movement of terrorist groups across different jurisdiction in Nigeria and how to analyze and predict terrorists activities, associations, and threats becomes an urgent and challenging issue (Chen, et al., 2004). Many terror-related groups use the web as a convenient, anonymous communication infrastructure. This infrastructure enables an exchange of information and propagation of ideas to active and potential terrorists. The part of the web used for such illegitimate and malicious purposes is referred to as Dark web.

The data analysis methods, before now, are primarily limited to manual approaches (Reid, 1983; Silke, 2001). A more modern technique is needed to analyze the Dark web to enable a better understanding and analysis of terrorist activities (Chen, et al., 2004). The presence of information overload is a problem that overwhelm the counter terrorism experts. Most of the activities of *Bokoharm* in Nigeria are hosted on the web; analyzing these digital traces through Big Data technologies can yield insightful terrorist tracking leads.

Language barrier is also a problem in Dark Web analysis, but Dark web portal integrates terrorist-generated multilingual datasets which can be used as a basis for predictive analytics models, terrorist network analysis and visualization of terrorists' activities, linkages and relationships (Chen, et al., 2004).

The dark web portal analysis consists of three major components:

(i) Dark Web Test – bed building
(ii) Dark Web link analysis and social network analysis (SNA), and
(iii) Dark Web portal building.

Detecting Terrorism Network

Terrorist groups consist of actors linked to each other through complex network of direct or mediated exchanges (Sageman, 2004). Identifying how relationship between groups are formed and dissolved in the terrorist group network would help in deciphering the social milieu and communication channels among terrorist groups across different jurisdictions (Chen et al., 2004). It means that the efficient detection of terrorist network has also to do with analyzing Nigerian transportation system. For example, the use of big data algorithms would enable the examination of passenger or freight manifests as cross-checked against databases of known and suspected risks to identify threats as early as possible. Nigeria has various points of entry and exit, such as airports, seaports, and land ports. Using big data to overhaul these ports would not only help in solving crime but also yield a huge revenue to the country. The boarders need to be

tightened through surveillance. Boarders represent massive flows of goods and people and are no longer viewed as the first line of homeland defense, but rather as the last (DNS, 2013). These massive flows of people and goods generate data that can be used to enhance security, enabling analysts to differentiate among the risks presented by a particular person or cargo.

The major terrorist group in Nigeria is the *BokoHaram* group. Various other terrorist groups exist around the globe such as Al-Gama'a, al-Islamiyya (Islamic group, IG), Hezbollah (party of god), Al-Jihad (Egyptian Islamic Jihad, Palestinian Islamic Jihad PIJ) and their supporters (Chen et al., 2004).

An example of a terrorist operational network is illustrated in Figure 5 below. The use of big data provides significant value-added services to identify the terrorist groups. The use of big data will help to identify patterns in terrorist-group relationships and, therefore, relationship between any two terrorist groups can be easily tracked. Big data analytics can provide insights as to the relations between terrorist organizations.

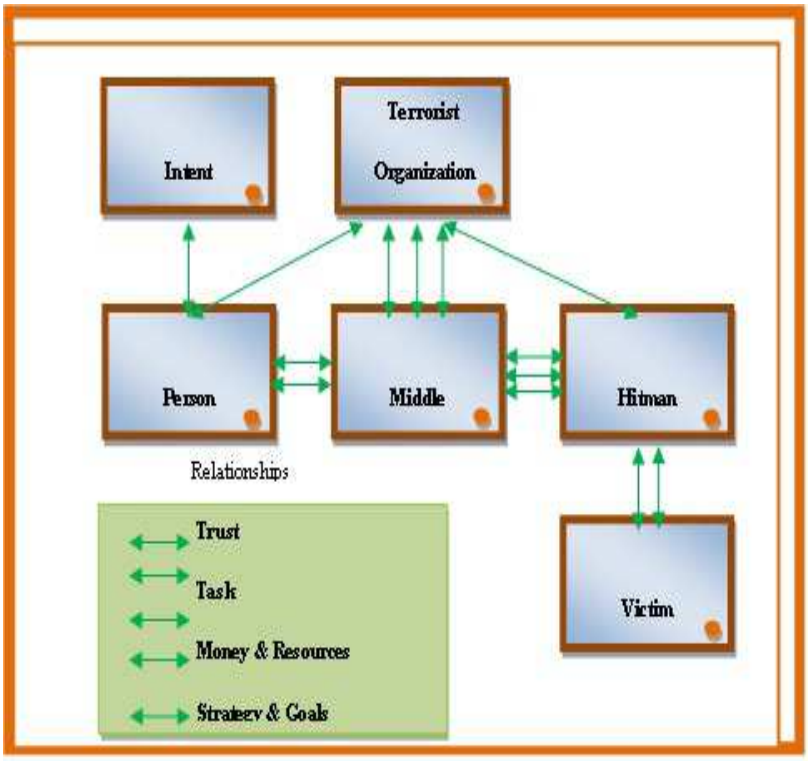

Fig. 5: Terrorist network—Allanach et al. (2004)

In the above diagram, the node labeled "person" represents someone who has the intent to kill another person. The basic premise behind this network is that the person will live a terrorist organization to murder someone else so that they will be dissociated with the victim. The "middle man" is a person who forms a task relationship between the "person" and the "Hitman". Through Big Data and Analytics the link of communica-

tion among them can be established, since the main task of the "middle man" is to communicate information between the "person" and the "Hitman" such that two of them remain anonymous (Allanach et al., 2004).

Big Data Active Security Framework

We proposed a Big Data Active Security Collaboration Framework as shown in Figure 6 below.

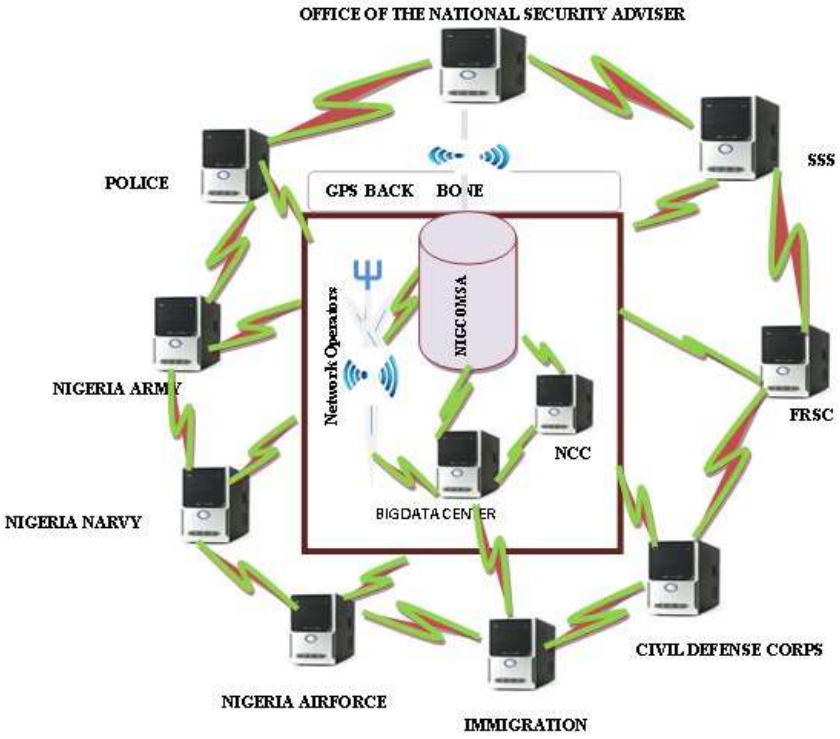

Fig. 6: Proposed Big Data Active Security Collaboration Framework

Discussion

This model advocates for a collaborative information gathering, analyzing and sharing system among the security agencies in Nigeria through Big Data Center. The framework consists of Military Agencies from Ministry of Defense, Paramilitary Agencies from Ministry of Interior, Big Data Center, National Communications Commission, Nigerian Communication Satellite Limited (NIGCOMSAT) and Network Operators from Ministry of Information and Communication Technology. The system is connected to the GPS backbone via NIGCOMSAT to link the office of the National Security Adviser to ensure effective real time information gathering and sharing among the

security agencies for underpinning the terrorists in Nigeria. In fact, through the use of the GPS, the results generated from Big Data Center can be shared across the security networks to forestall any threat or form of terrorism in the country.

In operational terms, the Ministry of Defense (office of National Security Advisor) would ensure that information generated on any act of insecurity is effectively disseminated across the security networks. In this regards, the military and paramilitary would utilize the data generated to track the terrorists on the move. The Nigerian Communication Commission regulates the network provider for providing call data or records etc for proper analysis by the Big Data Center. The NIGCOMSAT hosts the GPS that ensures surveillances and efficient transmission in real time of the information generated through actionable intelligence of Big Data Center. The officer of the national security advisor coordinates the military agencies and paramilitary agencies for actionable intelligence while the ministry of Information and Communication Technology ensures complete synergy among the Network operators, NIGCOMSAT, Big Data Center and NCC for delivery the needed data for security utilizations.

For effective implementation and deployment of this framework certain challenges need to be overcome, such as:

a. Administrative issues that have to do with speed of internet and availability of constant power supply.
b. The current level of understanding of this framework is low, since it does not exist before.
c. Lack of complete synergy among the stakeholders as experience has shown to be a problem in the past.

However, the country can overcome these limitations with consented effort among the stakeholders.

Conclusion

The Security Agencies in Nigeria are playing a significant role part of as a national effort to fight terrorism, and to secure the life and property of the citizenry. Big Data technology will greatly enhance this effort. This paper discussed how big data analytics can be leveraged to fight terrorism. It defined big data and analytics and cited examples of how big data technology can be leveraged to fight crime. It also presented the road map of getting started with Big Data and the notional information flow. Finally, it advocated for the creation of Big Data Center as an active security collaboration framework to fight terrorism in Nigeria.

Correspondence

Mathew E. Nwanga, PhD
Telecommunications Engineering Department
Federal University of Technology, Minna
Nigeria
Email: enwanga@yahoo.com

References

Abubarkar, A. (2004) "The challenge of security in Nigeria", Excerpts of Lecture at NIPSS Kuru, Jos, Nigeria.

Akinode, J.I., Alawode A.J. and Ojuawo, O.O. (2013) "Improving national Security GPS Tracking System Technology" proceedings of the 1st International Technology, Education and Environment Conference, African Society for Scientific Research (ASSR) pp. 634-644.

Allanach, J., Tu, Singh, H. S., Willett, S. P. and Pattipati, K. (2004) "Detecting, Tracking and Counteracting Terrorist Networks via Hidden Markov Models" *IEEE Aerospace Conference*, Big Sky MT, March, 2004. [Online] http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1368130&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1368130.

Anderson, J. A. and L. Rainie, L. (2012) "The Future of Big Data Pew Research Center's Internet & American life Project". http://www.pewinternet.org/Reports/2012/future of big – data.aspx.

ANS [Nascio Analytic Series] (2012) "Is Big Data a Big Deal for State Government? The Big Data Revolution-Impacts for State Government Timing is Everything". [Online] Http:/ www.nascio .org/publications.

Bakshi, K. (2012) "Considerations for Big Data: Architecture and Approach". Aerospace Conference, IEEE, [Online] http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6187357.

Bansal, S. and Rana, A. (2014) "Transitional from Relational Databases to Big Data", Int. *Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, Issue1, pp.626–627.

Chen, H., Wang, F. and Zeng, D. (2004) "Intelligence and SecurityInformatics for Homeland Security: Information, Communication and Transportation", *IEEE Transactions on Intelligent Transportation Systems*, Vol. 5. No 4, pp. 333-336.

Couch, N. and Robins, B. (2013) "Big Data for Defence And Security" Royal United Services Institute, pp. 8-10.[Online] https://www.rusi.org/downloads/assets/RUSI_BIGDATA_Report_2013.pdf.

DHS [Department of Homeland Security] (2012) "Big Data: The next big deal in Anti-Terrorism, new data – mining tools give officials sweeping view" November 7. [Online] http: www.newhaven.edu/467016.pdf.

DHS [Department of Homeland Security] (2013) "A Policy Forum on the use of Big Data in Homeland Security" Bipartisan Policy Center. pp. 2-3; available: http://bipartisanpolicy.org/library/policy-forum-use-big-data-homeland-security/.

Drewitz , D. (2013) "Revisiting the Network as a Big Data Problem" Riverbed. [Online] http://www.riverbed.com/blogs/revisiting-the-network-as-a-big-data-problem.html.

Eaton, C., Deroos, D., Dentsch, T., Lapis, G. and Zikopouhos, P. C. (2012) "Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data", McGraw-Hill Compa nies.

Fahey, S. (2010) "Big Data and Analytics for National Security" The John Hopkins University Applied Physics laboratory. [Online] http://web.stanford.edu/group/mmds/slides2012/s-fahey.pdf.

FuturICT, (2012) "The FuturICT Flagship Report" FuturICT flagship consortium, [Online] http://www.futurict.edu.

Hopkins, B. and Evelson, B. (2011) "Promotional Webinar: Expand your Digital Horizon with Big Data" Forrester, [Online] http://solutions.forrester.com/Global/FileLib/webinars/Big_Data_Webinar.pdf.

Intel (2012) "Planning Guide: Getting Started with Hadoop, [Online] http://www.intel.co.uk/content/dam/www/public/us/en/documents/guides/getting-started-with-hadoop-planning-guide.pdf.

Lavalle, S. (2011) "Big Data, Analytics and the path from insights to value", MIT Sloan Management Review, vol. 52, no.2, pp. 21-31.

Lynch, C. (2011) "Big Data: How do your data grow" *Nature 455*, pp. 28–29, 2008.

Miller, S., Lucas, S., Irakliotis, L., Ruppa, M., Carlson, T. and Perlowitz, B. (2012). "Demystifying Big Data: A practical Guide to Transforming the Business of Government", Washington: Tech America Foundation.

Murrow, B. D. (2013) "What Big Data means to you?" IBM Corporation. [Online] http://murrow.net/Portals/0/Publications/Brian%20Murrow%20-%20What%20Big%20Data%20Means%20To%20You.pdf.

NCC Monthly subscriber statistics Report, August 2014. http://www.ncc.gov.ng; accessed 8th November, 2014.

Nwanga, M. E., Onwuka, E. N., Aibinu, A. M. and Ubadike, O. C. (2015) "Impact of Big Data Analytics to Nigerian mobile Phone Industries". Paper accepted for publication in the proceeding of the 2015 Intl' conference on *Industrial Engineering and Operations Management* (IEOM), March, 2015.

Oblinger, D. G. (2012) "Insights into Analytics" *Educause Review*, pp. 98–99. [Online] http://www.educause.edu/ero/article/lets-talk-analytics.

Popp, R. and Paindexter, J. (2006) "Countering Terrorism through Information and Privacy Protection Technologies", *IEEE Computer society*, pp. 18-20.

Reid, E. (1983) "An Analysis of Terrorism Literature: A Bibliometric and Content Analysis Study" *Working Papers*, School of Library and Information Management University Southern California, Los Angels.

Sageman, M. (2004) "Understanding Terror Networks", Philadelphia, PA: University of Pennsylvania Press.

Schneider, R. D. (2012) "Hadoop for Dummies Special Edition", John Wiley & Sons: Canada.

Sicular, S. (2013) "Gartner's Big Data Definition consist of Three parts not to be confused with Three's", [Online] http://www.forbes.com/sites/gartnergroup.

Silke, A. (2001) "Devil You Know: Continuing Problems with Researchon Terrorism," *Terrorism Political Violence*, Vol. 13, no. 4, pp.1-14.

Tan, A. H. (2013) "Big Data Analytics: Challenges and What Computational Intelligence Technique May Offer". pp. 9-10, [Online] http://www.ntu.edu.sq/home/asahtan.

Zikopolos, P. and Eaton, C. (2011) "understanding big data: Analytics for enterprise class Hadoop and streaming data", McGraw-Hill Osborne Media.

William, M. (2012) "Data surge and Automated Analysis: The latest ISR Challenge; Industry Insights", Government Business Council, p.3. [Online] http://www.emc.com/collateral/analyst-reports/the-latest-isr-challenge-insights-gbc.pdf.