National Database as Core Field of National Security.

Ogechikanma Linda Ihekweaba[1*]; Chukwugoziem Ihekweaba[1]; and Prof. H.C. Inyiama[2]

[1]Computer Engineering Department, Michael Okpara University of Agriculture, Umudike, Abia State, Nigeria.
[2]Department of Computer Electronics, Nnamadi Azikiwe University, Awka, Nigeria

E-mail: gozihekwaba@yahoo.com*

ABSTRACT

This paper presents a solution to the present tensions in our national security in view of the strong need to develop a mechanism for the support of a national intelligent fusion cell. This paper advocates a structure for the design and use of a National Database that is encompassing and built after understanding the pattern of activities associated with terror attacks and crime incidence in the country. The approach used leverages some data mining techniques appropriate for the study of crime and terrorist patterns. It is proactive in that it is developed to serve as a defeat framework against criminals and terrorists within our national boundaries. The paper advocates the establishment of National Database and setting up of National Cryptographic Unit and Forensic Unit. Also included are ways to achieve sustainability for this critical E– governance project and so safeguard our national critical data from digital terror and fraud. This paper initiates concepts relating to the establishment of an effective framework for data management of digital evidence. It also suggests ways to upgrade our law enforcement and judiciary stakeholders in order to focus on the new and emerging species of digital criminals.

Decisions that have to be made towards the establishment of a database were outlined together with the attendant benefits. Intelligent agents are presented as the most optimal response tool to use to tackle the issue of complexity and overload.

(Keywords: national database, attacks criminals, terrorists, law enforcement, security, digital evidence information overload, intelligent agents)

INTRODUCTION

It is obvious that our national security apparatus is driven by a reactive focus on the crime or terror incidents. However, the crime incidents or terror attacks are merely the end products of a complex set of criminal or terror activities. It is understood from [1] that a terror attack is the result of a planned tactical operation with several key elements that work in coordinated and synchronized manner to attain a desired effect.

Consequently, a successful criminal/ terror defeat operation should begin with a thorough understanding of the adversary; the pattern of activities associated with a terror attack or criminal incident. This entails extensive use of intelligence. Our national intelligence infrastructure has to be redesigned or expanded. We need a security intelligence framework based on the global information and communication revolution. We need to develop a security intelligence architecture requiring the systematic collection, storage and analytics of huge amount of data in order to generate information of national security value. This core element of national security requires extensive use of database technology.

We have a collection of security data in Nigeria that cannot be called a national security database; a national system that supports data storage is not necessarily a database system that supports data analytics that yield intelligence, and also noting that not all the information provided by computer systems is produced from databases. However, the few less optimal database systems currently spread across our national security agencies are mainly oriented towards data storage and retrieval, rather than the extensive data analytics and data mining required to harvest the intelligence for proactively

defeating crime and terror in Nigeria. Hence, the kind of national database required as a core element of national security is one mainly designed not merely for data storage and retrieval but to support high speed optimized data processing and analysis. The properties of this system include interests to gain valid intelligence into the possibilities of security breaches, national security vulnerabilities, and pattern of criminal and terror attacks.

There has to be a strong proposal to coordinate an enhanced National Security Database solution for the current and emerging dimensions of crime and terror threatening our national survival. The construction of a capable National Security Database should form part of a national security strategy to defeat criminality and terrorism in Nigeria. As part of the broader goal of the strategic and tactical use of the database, it must predict, detect and prevent attacks against Nigerians. This should form part of our security campaign plan.

THE ATTRIBUTES OF A NATIONAL DATABASE SYSTEM

The National Database serves as an important resource in investigation and intelligence gathering. Searching for security data through paper security records and then abstracting data from them is tedious, costly, ineffective and at best not feasible in this fast century [2]. When a National Database is available, the collection effort will be minimized as a feedback from the database will aid planning and execution. Responses to security incidence would have verified the correctness of the data retrieval of security data from a well-organized database is currently an easy task thus making such a system a useful national resource.

The fact that the National Database supports information sharing among all our security agencies promotes consistency of information for decision – making and reduces duplicate data collection. Also, a key benefit of the database is not only due to the application of the information to the management of national security services and the allocation of resources needed for those services, but communication through the shared information among security agencies (the State Security Service SSS, police, military, Civil Defense, etc.), departments and security contractors, and the validation of security incidence hypothesis from the data mining of these data are also significant.

Considering the need to coordinate national security resources (information, effort, materials, personnel and equipment) found within the different security agencies across the country, the National Security Database becomes an enabling mechanism for matching the needs of a national security situation to the available specialties, training, personnel, and equipment within the Nigerian security organization thus facilitating the achievement of comprehensive response.

The database could help compare the characteristics of a security incidence with those that have previously occurred with reference to implemented responses. The comparison would help generate a prognosis of planned response effectiveness within the new scenario [3].

The National Security Database surveillance would not be limited to tracking state adversaries, but can also be employed to track the behavior of security personnel or the performance of our security agencies. Security quality assurance surveillance (based on the use of the database) can, for instance, determine if notorious criminal gangs are monitored and that potential security breaches or highly analyzed and detected state adversaries are appropriately handled. Such security surveillance will improve data recording as well as security incidence response.

The effect that security incidence analysis obtained through use of the National Security Database has on national security could be difficult to measure. However, there is little doubt that if reasonable models of crime and terror cause and effects are used, such analysis increases our understanding of many criminal and terror processes. Such security evaluations will improve national security response quality and reduce cost. If understanding of terrorists attack pattern using the technology of data mining leads to reliable prediction of locations likely to be attacked, then security provision would have been improved. For example, if the bomb was found in an unexpected location in the country, the security organization would have to develop a hypothesis for how it got there. To arrive at conclusions about the incidence, they need to develop and test hypothesis about the events that it was an effect of and, when

applicable, to determine what events it could have been a cause of.

NATIONAL DATABASE STRUCTURE DEVELOPMENT AND SUSTAINABILITY

The potentials of a National Database present great opportunities and challenges for the restructuring of our national security infrastructure. A key challenge is the area of development and sustainability.

Due to the complexity of ICT and the growing dimension of criminality and terrorism [1], the establishment of a National Security Database Integrated Capability Development Team (probably a specialized security agency) to develop and integrate strategy becomes necessary. The Nigerian government has to assign this agency to conduct technical and operational analysis and determine resources requirement for the development and sustainability of the National Database.

The agency/ team will interface with the national security agencies (police, military, SSS, and other paramilitary agencies) to provide and assign the appropriate priority through the development process as necessary. This agency will also identify and resolve any capability gaps in the current form of our security forces and should develop writings, and publications of manual on the use of the National Database to defeat criminality and terror within our national borders.

The database among others contains descriptors of persons and groups, equipment and material movement of interest, descriptors of financial transactions, phone cells details records call logs, movements and activities of foreign nationals, criminal records and other security related data, data on cross border trade, data on movement of arms and ammunition, data on religious, ethnic sentiments, etc.

In order to support the operation of country's intelligence fusion cell, the National Database should be structured to grant varying level of access to all our security agencies in order to facilitate the sharing of security data and information enabling the fusion of intelligence. However procedures, guidelines, authorization and access control has to be specified in order to grant varying level of access to different security organization, knowing that all security agencies should do not have similar levels of authorization within the National Database. Consequently the formulation of facts classification and handling policy has to be integrated into the National Database project development. Information classification is required to determine the relative sensitivity and criticality of information assets, which should provide the basis of protection and access control (different security organs having varying level of authorization in the National Database).

The development of the database has to incorporate the database technology standard and practices. Considering the fact that the infrastructure would become target for digital terrorists for hackers, spies, and infiltrating foreign agents, the development of the facility includes specifications and development of standards and procedures for encryption, for the establishments of database forensic unit and cryptographic analysis unit.

The development of strong encryption standard to ensure sensitive data is protected from disclosure has to be form part of the terms of reference for the development of the national database.

The development of capacity for cryptographic analysis should be part of the integrated strategy for the development of the national database. This unit is to be setup and trained to provide crypto-analytic support for the effectiveness and sustainability of the national database. It is a matter of national security that data cannot be read by unauthorized people and that it cannot be forged. The cryptographic unit is assigned the task of developing algorithms for the encryption of data in storage and in transits.

The cryptographic unit and database forensic unit should form part of specification of information security plan for the establishment of the structure and operation of the national security database infrastructure.

In order to ensure the security and confidentiality of sensitive information and to protect against any anticipated threats or hazards to the security of data within this national critical infrastructure, the national interests assigned the development of this infrastructure has to put in place all reasonable technological means and internal control based on the conduct of effective risk analysis. The national security agency has to

define appropriate controls which has to be equal or greater than security requirements and controls prescribed by standard bodies (e.g., ISO). That is the design of the National Database Project includes a comprehensive risk assessment. In this case risk assessment is the process which determines what information resources would exists in the national database that require protection, and to understand and document potential risk from IT security failures that may cause loss of information confidentiality, integrity, or availability [4][5]. The purpose is to help our security agency create appropriate strategies and controls for safeguarding information.

The incorporation of a database forensic unit is one of such risk mitigating strategies. Due to the critical positioning of such a National Database, there exists the risk of its exposure to digital terror and fraud. Hence the forensic examination may focus on identifying transactions within the National Database that indicate evidence of wrongdoing, such as fraud-data forgery, mutilation, deletion, etc. Database forensics is a branch of digital forensic science relating to the forensic study of database and their related metadata [6].

Critical issues of national security involving data integrity, data loss, deletion or mutilation might occur, leaving national security relying mainly on database forensics to reconstruct the digital events (including retracing user DML and DDL operations, identifying data pre and post transaction, helping to improve/ disprove data security breach, determining scope of the database intrusion). Hence, the establishment of a database forensic unit with the required capability should form part of the requirement for the development of the National Security Database infrastructure.

THE NATIONAL DATABASE SUSTAINABILITY

Critical failure factors have to be taken into consideration and planned for and addressed in the plan for the development of the National Database infrastructure. A failure factor that has to be taken into consideration is institutional weakness and shortage of qualified personal and training.

No advance can be made unless there is a cadre of knowledgeable personnel. Traditionally, there has been lack of competent personnel within our security force who could integrate security and computing knowledge. Plans have to be put in place to increase the number of computing-oriented security personnel with the insight needed to provide the technical support for the use of database systems in combating crime and terror.

Even when all the right decisions towards the establishment of the database have been made and the infrastructure exists, there has to be an ongoing concern with reliability, adaptation to changing operation environment and institutional needs, planning for growth and technical updating of the infrastructure.

Political support is a critical success factor. The non-technical challenges for sustainability of the National Security Database program can best be addressed by strong political leadership who can help spur bureaucratic action and implement strategies that promote the sustainability of the project. Almost invariably, successful IT projects have been championed by strong, committed leaders whose vision and ability to build support within government, secure the necessary funding required for managing the project sustainability.

ENCODING SYSTEMS, DATA MINING AND EPISTEMIC PREDICTIVE SYSTEMS

Considering the fact that the National Security Database has to be distributed supporting data and information sharing across all government agency and contractors concerned with security; standardized encoding systems become necessary. To this effect requirement for the development of the National Security Database is the design and implementation of enabling protocols to ensure consistent encoding systems across agencies.

Collecting and sharing security related data from multiple security agencies and national institutions require a major effort to standardize data collections. In particular, the consistent encoding of investigation records, already difficult within one agency becomes a major problem when the data are collected from multiple agencies.

A comprehensive database schema can provide a common definition for the data elements that are to be shared. The procedures to encode data within the database schema maybe made

particular to each participating security agency if they have differing conventions for their source data collection.

The solution provided through a schema, as described above, cannot overcome all problems of inter–agency data comparability. Because different security agency/ institution will have differences in security handling and reporting protocols. Hence the standardization of encoding systems becomes very necessary.

Data mining, which is reported in the literature [7][8][9] to be a field at the intersection of computer science and statistics, is the process that attempts to discover patterns in large data sets. It utilizes methods at the intersection of artificial intelligence, machine learning, statistics, and database systems [7]. The overall goal of the data mining process is extract information from a data set and transforms it into an understandable structure for future use [7]. Aside from the raw analysis step, it involves database and data management aspect, data processing, model and inference considerations, interestingness metrics, and complexity considerations, post processing of discovered structure, visualization and on line updating [7]. Using data mining, our law enforcement interest might be able to generate new security knowledge using the data within the National Database. The predictive capability of determining might enable our security agency to answer the following questions:

- What can go wrong?
- How likely is to let go wrong?
- What are the consequences of going wrong?

A holistic approach to understand the requirement for a particular criminal or terror incident could entail the use of data mining on the national Database to assist law enforcement and other security personnel's in identifying vulnerabilities. The vulnerabilities (obtained by running the data in the National Database) can be exploited to break the operational chain of events of the criminals or terrorists.

Criminals and terrorists need to communicate with others nationally and internationally including not just their criminal or terrorist confederates but also legitimate organizations such as banks. The National Database is structured to allow phone calls log surveillance. The database containing call details records (CDR) for all phone calls made domestic and international. The call data records might not be useful on its own as a tool of national security; the national security interest could use it as an element of broader national security analytical efforts. Data mining techniques might be used to organize and view linkage that are demonstrated through such information as telephone calls and final records, crime records, etc. which might be linked or imported from other data sources in the country.

Neural network techniques can be used to detect patterns, classify and cluster data to forecast future events. Using relational mathematics it is possible to find out for example if someone changes their telephone number by analyzing and comparing call patterns. Using data mining on the National Database could reveal pattern that can be used for example and defeat criminal or terrorist leaders, suppliers, trainers, enablers and executors responsible for terrorism or crime while protecting the citizenry from criminal or terror attacks.

The data mining of data security data (e.g., related to police operations) could enable the discovery of systemic inefficiency in connection to security response, crime incidence analysis and prevention efforts. Data mining could help provide explanation of crime and terror cell clustering (geographic), changing society pattern, economic factors, and political pattern, etc.

Our national security interest can leverage data mining techniques to develop a defeat framework for criminals and terrorists. With the national database and data mining, our security agency can plan and take proactive measures to seek out and defeat criminal and terror events before they occur. With these techniques the government security team can identify and understand criminal or terrorist leaders, equipment, infrastructure, support mechanism, or other actions to forecast specific criminal or terrorist operations directed against Nigeria interest.

The data mining predict assist in:

- Identifying patterns of criminal or terrorist behavior.
- Identifying emerging criminal or terror threats.
- Predicting future criminal or terrorist actions.
- Prioritizing intelligence.
- Exploiting criminal/ terror threat vulnerabilities.

- Targeting terrorist attack nodes (such as funding and supplies)
- Disseminating alert information rapidly to specific people that might be affected.

Consider that the operational environment for law enforcement and security in this country is complex, dynamic, multidimensional, and comprises a collection of interrelated and sometimes overlaps. Data mining techniques can be used to understand the nature of these variables, enabling our national security interest to predict, detect, prevent, avoid and neutralize the threat.

Data mining might be used to find patterns in the economic situations within our operational environment. This can be carefully analyzed to determine what is currently available to the terrorists or criminals, their ability to acquire materials, the level of sophistication and their ability to sustain their operations.

Several things have to happen to prosecute coordinated terror or criminal execution [1]. Acknowledging the difficulty of successfully predicting outcomes in our complex environment and the multitude of constantly occurring complex interactions, we need to use data mining to develop possibilities or hypothesis about the systems and operations of criminals and terrorists.

DIGITAL EVIDENCE AND ITS ROLE IN CRIME DETECTION

First we define basic and fundamental concepts. Digital data are data represented in the numeric form. With modern computers, it is common for the data to be internally represented in a binary encoding, but this is not a requirement. A digital object is a discrete collection of digital data, such as a file, a hard disk sector, a network packet, a memory page, or a process [10].

In addition to its numerical representation, digital data has a physical representation. For example, the bits in a hard disk are magnetic impulses or patterns that can be read with analog sensors. Network wired contain electric signals that represent network packets and keyboard cables contain electric signals that represent when keys were pressed, the computer coverts the electric signals to digital representations. Digital photography and video are a digital representation of the light associated with physical object.

Digital objects have characteristics, or unique features, based on their creator and function. For example, the characteristics of a hard disk sector will be different when it is used to store the contents of an ASCII text document versus a JPEG image. We can use the characteristics to identify the data. The state of an object is the value of its characteristics. If a letter were changed in an ASCII text document, then the object corresponding to the file would have a new state. Similarly, the state of a running computer process changes and that is every time data is written to its memory.

A digital event is an occurrence that changes the state of one or more digital objects [11]. If the state of an object changes as a result of an event it is an effect of the event. Some types of objects have the ability to cause events and they are called causes. Note that because digital objects are stored in a physical form, then their state can be changed by both physical and digital events. An object is evidence of an event if the event changed the object's state [10]. This means that the object can be examined for information about the event that record.

An incident is an event or sequence of events that violates a policy and more specifically, a crime is an event or sequence of events that violate a law. In particular, a digital incident is one or more digital events that violate a policy. In response to an incident or crime, an investigation may begin. The only proof that a digital event may have occurred is if the digital evidence of the event exists [10] [12].

A little more definition of evidence which do not focus on the cause and effect relationship can be deduced from relevant literature [6] which is physical evidence of an incident is any physical object that contains reliable information that supports or refutes a hypothesis about the incident and digital evidence of an incident is any digital data that contains reliable information that supports or refutes a hypothesis about the incident. It is understood that an object has information about the incident because it was a cause or effect in an event related to the incident.

Note that because digital data has a physical form, then physical evidence can contain digital evidence. Using this definition, a hard disk is physical evidence and the sectors and files that contain information about the incident are digital

evidence. The electronic crime scene investigation guide [8] describes the recognition and collection of a hard disk or other storage device as the collection of electronic or digital evidence. It is important to note that the difference between physical and digital evidence is in their format and has nothing to do with the type of incident. Therefore, we can have digital evidence for a physical incident or crime [10]. For example, a digital video camera will create a digital representation of a physical event and the resulting file will be digital evidence of the event. We can also have physical evidence for a digital crime.

It is interesting to note that the Central Bank of Nigeria, CBN, has strongly been pushing for E-payments and cashless policy (note, the E-project heavily relies on ICT, with great opportunity for computer crime). Cases of fraudulent ATM transactions, SIM card cloning, unauthorized access to digital data, computer data mutilation, malicious data destruction and forgery have been reported.

Our judiciary and law enforcement interests require a new kind of ability, tool and framework to engage this new generation of criminals. The country's law enforcement personnel's have to be able to present concise digital evidence in our courts to secure convictions for these new and emerging computer crimes.

Considering the national imperative for the development and use of E-government infrastructure, especially as relates to the implementation of the national security database with the great opportunity for fraud, manipulations, data distortion, suspicious computer operations which might be perpetrated both at the central National Database house and at the data entry and access nodes at the various participating security agencies (considering our country's severe corruption problem), it becomes very crucial to develop an effective and reliable national framework for the management of digital evidence.

A digital investigation process model is required. This includes the development of procedures for investigating digital crime scene. An electronic crime scene investigation guide has to be constructed. This might probably be based on the "Electronic Scene Investigation Guide" [13].
When a victim or another party detects a computer crime incident, for example, a network intrusion could be detected by an intrusion detection system and, concerning the operations of the National Database; a contraband digital incident could be detected using the database logs or the transactions or communication pattern of the suspect using data mining technology, procedures for notification and the legal procedures for confirmation and authorization where investigators receive authorization to conduct the investigation has to be clearly outlined and documented.

Furthermore, after theories have been developed (by security officials) and tested about the events related to the digital incident, the specifications and procedures by which the results may be presented to the court of law has to be properly outlined and documented. Our court systems have to develop requirements for entering digital evidence into court proceedings. Furthermore, appropriate guidelines have to be developed that would be followed by our law courts to determine the reliability of digital evidence.

NATIONAL DATABASE INFRASTRUCTURE: MANAGING COMPLEXITY AND INFORMATION OVERLOADING USING INTELLIGENT AGENTS.

With the extensive use of ICT and the attendant explosion of data available to users, complexity and information overload becomes a problem [14]. Consequently information access and management become an area of great activity.
Considering the huge amount of data that must be managed (stored, searched, filtered, processed, analyzed, communicated, etc.) in the National Database, this paper advocates the use of intelligent agents to help Nigerian security personal to manage complexities and the information overload problem by helping locate information which is truly relevant, and by providing a way to relate that information in a prioritized way, based upon the preference of different security agency.

In the literature many different definitions of intelligent agents have been reported. However intelligent agents can be described as software entities that carry out some set of operations on behalf of a user or another program with some degree of independence or autonomy, and in so doing employ some knowledge or representation of the user's goals and desires [14][15]. An agent is expected to have the following properties:

autonomy, communication, cooperation, responsiveness, pro activeness and learning.

Autonomy means that the agent has control over its actions and over its own state, decides by itself what action to do under which circumstances and is able to accept abstract high– level missions and to ensure their achievement [14].

Communication means that the agent can communicate with other agents and with its user. Collaboration means that a set of agents carry out tasks cooperatively, possibly using delegation or coordination mechanisms. Responsiveness requires that the agent reacts in a timely fashion to possible changes in its environment in a way to ensure the achievement of its duties. Pro–activeness is even a stronger property and means that the agent is able to anticipate changes in the world to perform preventive actions or to take the opportunity to achieve more quickly or more efficiently some goals. Learning means basically the ability to improve its behavior in time and to induce new knowledge of its environment during its operation. The agents reasoning and learned behavior enables it to accept the user's statement of goals and carry out the task delegated to it.

Concerning the effective operation of the National Database, the use of intelligent agents would provide a level of automation that can vastly reduce complexity, save labor, and reduce expense. In this way intelligent agents can provide help to both experienced and inexperienced users of the National Database.

Intelligent agents can be deployed to operate in the background to perform tacks automatically for the National Database users, such as filtering data in the database, sending alerts, looking for particular pattern in the data, or automatically achieving older data.

The incorporation of the use of intelligent agents with the implementation of the National Database infrastructure should help in intelligent information retrieval and management. The agents could weave together all forms of data, connecting knowledge into meaningful patterns, which can aide security personnel in concentrating on relevant information. Intelligent agents can automate the identification of patterns in the database that can help security personnel in understanding useful patterns relating to the activities of criminals and terrorists.

Data returned to each security agency by querying the National Database can be automatically prioritized by intelligent agents based on the preferences the agents learned from the particular security.

The integration of the intelligent agents with the operational use of the National Database infrastructure would ease the information overload problem by helping locate information, which is truly relevant, and by providing a way to relate that information to existing information in a prioritized way, based upon the preferences of the particular user or security agency: intelligent agents can be deployed to help users of the National Database not only with search filtering, but also with categorization attentional prioritization, selective dissemination, annotation, and collaborative sharing for inter security agency collaboration.

There is need for security for sharing personnel on the field to gain access to the National Database from their remote locations using mobile wireless technologies. They would need such as access despite bandwidth limitations of mobile computing technologies (e.g, the field wireless communication), and despite network volatility. Intelligent agents, which reside in the national network rather than on the remote field personnel's personal computer can address this need by persistently carrying out the user request despite network disturbances or intermittent connections. In addition intelligent agents can process data at the National Database servers and ship only compressed answers to the field security personnel, rather than overwhelming the network with large amount of unprocessed data.

SUMMARY

This paper considered criminal or terror attack as the result of a planned tactical operation with several key elements that work in coordinated and synchronized manner to attain a desired effect. Hence in order to build an effective security strategy, a National Database is required to build a thorough understanding of the adversary, the pattern of activities associated with terror attack or crime incidence in the country.

As part of the development and sustainability plan for the National Database, the paper proposes the establishment of a National

Security Database integrated capability development team (probably a specialized agency) to develop an integrated strategy for its actualization. The team has to be empanelled to conduct technical and operational analysis and determine resources requirement for the development and sustainability to the National database. As part of strategies and controls for the safeguard of the national critical data from unauthorized access and to effectively manage digital terrorism, the term of reference for this project should also include the establishment of cryptographic analysis unit and database forensic unit.

It is advanced in this paper that our national security interests can leverage data mining techniques to develop a defeat framework for criminals and terrorists. A holistic approach to understand the requirements for a particular criminal or terror incident should entail the use of data mining on the National Database to assist law enforcement and other security personnel in identifying vulnerabilities. The vulnerabilities could be exploited to break the operational chain of event of the criminal or terrorists. Using data mining on the National Database could reveal pattern that can be used for example to defeat criminal or terrorists leaders, suppliers, trainers, enablers and executors responsible for terrorism or crime.

Considering the national imperative for the development and use of E–government infrastructure, especially as it relates to the implementation of the National Security Database with the great opportunity for fraud, manipulations, data distortion, suspicious computer operations which might be perpetrated both at the central National Database house and at the data entry and access nodes at the various participating security agencies, it becomes crucial to develop.

Finally, considering bandwidth limitations of mobile computing technologies (needed by field personnel to access the National Database) and huge amount of data that must be managed (stored, searched, filtered, processed, analyzed, communicated, etc.) in the National Database, this paper advocates the use of intelligent agents to help Nigeria's security personnel to manage complexities and the information overload problem by helping locate information which is truly relevant, and by providing a way relate that information in a prioritized way, based upon the preferences of different security agency. Intelligent agents can be deployed to help users of the National Database not only with search filtering, but also with data mining analytics, categorization, attentional prioritization; selective dissemination, data annotation, and information collaborative sharing for inter security agency collaboration.

REFERENCES

1. Castro, RR. (Major General). 2007. U.S Army. "Army Knowledge Online". www.us.army.mil.

2. Boyd, D.G. 2001. "A Guide for Applying Information Technology in Law Enforcement". Law Enforcement and Correction Technology Advisory Council, USA. March 2001, NCJ 185934.

3. Chong Ho Yu. 2009. "Data Mining as an Extension of EDA and Resampling".

4. Michigan Technology University. 2011. "Information Security Plan". 3-10/3/2011.

5. Duncan, W.R. 1996. *A Guide to the project Management Body of Knowledge*". Project Management Institute: Newtown Square, PA.

6. Oliver, M.S. 2009. "On Metadata Context in Database Forensics" http:// www sciencedirect.com/ science/ article/ B7CW4 - 4TSD9G6-1/2/a5031117d753034d92f2abfa 332 eadf.

7. ACM SIGKDD. 2011. "Data Mining Curriculum" (http://www.sijkdd.org/ curriculum.php).

8. Clifton Christopher 2010. "Encyclopedia Britannica: Definition of Data Mining". http://www.britannica.com/ EB checked/ topic/ 1056150/ data mining

9. Hastic, T., R. Tibshirani, and J. Fhedrian. 2009. "The Elements of Statistical Learning: Data Mining, Inference, and Prediction". http// www. state.standard. edu/tubs/elemstart learn/.

10. Carrier, B.D. and E.H. Spafford. 2005. "An Event – Based Digital Forensic Investigation Framework". Center for Education and Research in Information Assurance and Security – CERIAS. Purdhe University West: Latayette, IN.

11. Carrier, B.D. and E.H. Spafford. 2004. "Defining Event Reconstruction of a Digital Crime Scene". *Journal of Forensic Sciences*. 2004.

12. Ryneanson, J. 2002. “Evidence and Crime Scene Reconstruction”. *National Crime Investigation and Training, 6th edition*.

13. Technical Working Group for Electronic Crime Scene Investigation. 2001. *Electronic Scene Investigation. A Guide for First Responders*.

14. Cheikhrouhou, M., P. Conti, J. Labetoulle, and K. Marcus. 2004. “Intelligent Agents for Network Management: Fault Detection Experiment”. BP IG3 – 06904 Sophia – Hatipolis: Cedex, France.

15. Nwana, H.S. 1996. “Software Agents: An Overview”. *Knowledge Engineering Review* II(2):205 – 244.

SUGGESTED CITATION

Ihekweaba, O.L., C. Ihekweaba, and H.C. Inyiama. 2014. “National Database as Core Field of National Security”. *Pacific Journal of Science and Technology*. 15(2):145-154.