GSJ: Volume 11, Issue 10, October 2023, Online: ISSN 2320-9186

www.globalscientificjournal.com

Strategies for Obtaining Intelligence Function in Infrastructure Security::

Zems Mathias, SP. Retd, Ph.D.
Africa Regional Representative
Professor of Intelligence & Security Studies
The University of America, Temecula, California, USA.

This article aimed to address intelligence-gathering techniques for infrastructure security in Nigeria in general and the Niger Delta in particular. The objectives of the study were to: comprehend some of the intricate issues that were different. This article aimed to address intelligence-gathering techniques for infrastructure security in Nigeria in general and the Niger Delta in particular. The study set out to understand some of the complex issues that different economic sector operators deal with on a daily basis; to network, strategize, and discuss key issues affecting job creation, economic development and regeneration, and business start-ups; and to facilitate direct access to policymakers and stakeholders in the defense and security sectors in order to develop and strengthen existing and new opportunities and ensure that the study's objectives were realized. The research project investigated intelligence activities in Nigeria using a case study. It covered a wide range of themes, including the public's perception of infrastructure security, the sources and functions of intelligence, their utilization, classifications, and the intelligence management cycle. It was proposed that managers of all security intelligence agencies should have access to the intelligence function and that it be effectively consolidated and coordinated. Additionally, the government ought to put in place a strong security framework that includes the police, military, paramilitary, and epistemic intelligence organizations. The intelligence community should also be equipped with the means to perform its duties, unhindered by political favor, retaliation, or other forms of interference. It is everyone's obligation to address the infrastructure security concerns facing Nigeria.

1. Introduction

Intelligence, like warfare, is an art rather than a science. It is not an exact science if it can even be called that. To name a few basic requirements, it is a mental task that requires education, experience, common sense, teamwork, technical knowledge, and the ability to explain the product to the consumers and decision-makers, Zems, (2013:46). It takes intellectual bravery to provide the user with the results of intelligence assessments without the tendency to be evasive to justify inaccurate intelligence predictions in the future. It is still a human endeavor that is prone to error, Lerner, (2010: 1).

There are many misconceptions about intelligence. Too much focus is put on clandestine operations, counterintelligence, and secrecy, which are areas of action that are informed by intelligence but are not integral to it. Intelligence focuses on threats while ignoring chances to gain an advantage. Intelligence is often secretive for one or both of two reasons, even though it is not required, Wilson. (2008), Zems, (2013:18).

One requirement is to protect the method(s) or source(s) through which intelligence is gathered or produced from information gathered. The other is the need to keep information from getting out too soon about a decision that was made or helped by intelligence.

To put it lightly, prostitution is the second-oldest profession in human history behind espionage, which is the gathering of intelligence. More than 8,000 years ago, information collection began in Mesopotamia, the first modern nation in South-West Asia. This was accomplished by establishing organizations and assigning individuals the responsibility of gathering information on any dangers to the security of the government system, whether those threats came from the government or from other individuals or groups (Andrew, 2004).

Even though there has always been a need for intelligence, there have been big changes in what information is available, how it is communicated, how it is gathered, how much it costs, and how accurate the final intelligence is for making decisions.

(Security has always been and will always be a major concern in civilizations. As a result, infrastructure security needs an intelligence management role to fight infrastructure asset insecurity, Zems, (2011).

The perception of security is also influenced by how state institutions and organizations offer it. Even while there are many indications that life is safer and more tranquil than before, some people nevertheless feel quite uncomfortable, Aradu, (2010).

Therefore, the interpretation frameworks that are used to understand security are crucial. In Nigeria, institutions and organizations produce data on their operations and environment and create frameworks for interpretation that assess their dependability, functionality, and suitability for critical conceptual inquiry.

To put it bluntly, critical infrastructures (CIs) are the foundation of society's daily operations, safety, and security (Bernet, 2018; Zabokilicka, 2020). According to Hellstrom, (2007), critical infrastructure is critical not because it is important in general but because it is strategically linked in such a way that it focuses on society's total vulnerability to a few specific points in the system. In this sense, critical infrastructure assets, (CIs) have the potential to cause adverse effects that go deep into society’s functional ability, Graham, (2010).

2. **Core principles of infrastructure security**.

The increased sophistication and complexity of Nigeria's organized crime, which is a cause for concern, highlights the necessity of a potent criminal intelligence function to manage infrastructure security.

The study of criminal intelligence is also yet in its infancy. Numerous intelligence operations in Nigeria were reportedly abandoned since they didn't work out as planned, according to sources, Ibegbu, (2014).

The criticism is based on the observation that intelligence is frequently no more than a collection of unimportant information that is merely slightly beneficial. According to Sommers (1986), these flaws result from misunderstandings about how intelligence analysis works and the advantages it offers security managers, Zems, (2011 & 2013).

Nevertheless, the role of intelligence functions is increasingly being acknowledged as a crucial one in the fight against the insecurity of critical infrastructure assets. Infrastructure security is

the protection offered to safeguard infrastructure assets and organizations, particularly critical infrastructures (CIs), such as electricity grids, dams, power plants, seaports, hospitals, bridges, transportation hubs, and water **systems.** Infrastructure security is to reduce the vulnerability of these systems and structures to terrorism, sabotage, and pollution. Andrews, (1990).

Information technology is naturally used by critical infrastructure as this capability is becoming more and more accessible. They have consequently grown to be very dependent and interrelated; handling interdependencies is crucial. To put it mildly, intrusions and interruptions to one infrastructure asset may result in unforeseen failure and destruction of another, John, (1990).

A nation's basic infrastructure (CIs) is important to its proper operation. Destruction, whether by accident or on purpose, will have a big effect on the economy of the country and the services it provides to the local community and society as a whole.

Critical infrastructure assets need to be carefully watched, protected, and guarded against several bad things that people or groups of people could do. These include:

Terrorism: Targeting vital infrastructure for political advantage by an individual or group of individuals constitutes terrorism.

Illegal Oil Bunkering: The act of stealing crude oil and its by-products through a variety of channels is known as illegal oil bunkering. For the economy, society, environment, and security, this has tremendously negative repercussions.

Oil and GAS infrastructure Sabotage: Oil and GAS infrastructure as referred to therein, concerns the illegal or unauthorized act of destroying or puncturing pipelines. And cannibalizing the national grid, transformers, and/or telecommunication towers is an example of economic sabotage.

Information warfare and cyberterrorism are when individuals break into computer systems for their gain or when nations undertake attacks to seize information or harm a nation's information infrastructure.

Oil terrorism: Unlike oil bunkering and pipeline vandalism, oil terrorism is a new term coined by security analysts and scholars to describe deliberate pipeline system attacks carried out by militias, freedom fighters, and insurgents in Iraq and around the world. However, Oil terrorism in Nigeria includes using explosives to blow up oil pipelines, installations, and platforms, as well as seizing oil barges, oil wells, flow stations, support vessels, and other oil facilities to stop the use or distribution of crude oil or its refined products (Onuoha, 2012:107).

3. Conceptual framework/Elements

3.1. Intelligence conceptual clarification

At the state level, intelligence function management contributes to lifesaving and protection of propriety; at the international level, it may serve as or be used as a justification for war, which would result in the loss of lives and proprieties (Gill & Phythian, 2006, p. 172). It is undeniable that much intelligence work must be done in secret if it is to be useful, and historically, intelligence has been subject to a specific set of insiders.

First, it will clarify the contentious idea of intelligence by setting it apart from mere "information" and false spy tales. Second, people will question both the need for intelligence agencies today and the existence of "national intelligence" in that case.

In his textbook on intelligence and policy, Mark Lowenthal (2002) proposes three distinct approaches to interpreting the term "intelligence." The process of obtaining, processing, and providing information to "consumers" like decision-makers or operational commanders is just the beginning.

The term "intelligence cycle" is frequently used, but its fundamentals are currently hotly debated (Hulnick, 2006). It is a product that was once supplied as paper but is now made available through multilevel secure electronic databases.

Finally, we can discuss the institutions that make up the intelligence agencies and intelligence community. As their name implies, they frequently provide the government with a variety of "services," and this increasingly includes working actively to change the world rather than just reporting on it (Lowenthal, 2002, p. 8). It is now clear that it is difficult to define "intelligence" and its significance.

Knowing that **information is power** leads to the conclusion that intellect is likewise a form of power. Information can facilitate the use of other types of power, such as coercive or material. Intelligence provides the basis for policy or decisions-people, organizations, and states, if they are to act "rationally," will do so after thoroughly weighing all of the options, including the costs and advantages, that are available to them" (Gill & Phythian, 2006, p. 33).

As a result, there may be conflicts between intelligence findings and the demands of politicians for specific solutions. While intelligence is created by analyzing **"dry" data**, the '**policy'** is typically created based on concepts or ideologies. When they compete, the odds are stacked against intelligence: "But when information runs up against power, information is the casualty," Zems, (2013: 26)

Evidence is disregarded when perception, or more precisely, conception, contradicts information (Fry & Hochstein, 1994, p. 20). This restores the relationship between knowledge and power so that intelligence information is judged by how well it supports a plan of action that was already made before the search for information.

Secrecy is a further factor at the heart of security intelligence since "intelligence is not possible without secrets" (Warner, 2009, p. 9). Secrecy is crucial in many areas of the process itself, not merely as a safeguard against observation. Arrests are an example of an action that makes no sense unless it has some element of surprise (Herman, 2001, p. 5). Secrecy also brings up important questions of accountability, morality, and the law.

Additionally, intelligence plays a key role in educating and carrying out acts that are not generally recognized and may even violate local or international law. It is not just a foundation for official policies. The CIA's use of "covert action," or "special political activity," is heavily contested.

In addition to the largely inactive function of gathering intelligence on international affairs, intelligence organizations also make covert attempts to intervene to affect events. Covert action is viewed differently by different authors; some perceive it as a distinct activity from the core functions of intelligence (Russel, 2007, p. 281).

"Intelligence" is information gathering and information collection; it does not directly harm someone. Even though some agencies do secret operations, which makes the moral questions harder to see, this is a separate and supplementary job (Herman, 2004, p. 180).

There isn't one definition of intelligence that is accepted everywhere. According to our view, someone who is clever can make rational, reasonable decisions; assess circumstances quickly and accurately; have read widely; have good ideas, and be an authority on a given topic.

For the sake of this study, intelligence is defined as the capacity of an organization to predict change in real-time and respond to it. Finding changes that are coming, whether they are positive and present possibilities or negative and pose a threat to the national economy, takes foresight and understanding.

The result of gathering, compiling, assessing, analyzing, integrating, and interpreting gathered raw data and information is intelligence. It is a specific kind of information product that gives a state or an enemy the knowledge they need to further their own national goals. The elimination of ambiguity in the observation of external actions is one of the intelligence's most crucial roles, (1989, Bruce Deta).

Additionally, the term "criminal intelligence" refers to the systematic collection, assessment, and synthesis of unprocessed data on specific actions or actions that are known or believed to be unlawful in character (National Advisory Committee on Criminal Justice Standards and Goals, 1976).

4. Intelligence and human perspective of infrastructural security

According to Bowers (1984:168), intelligence has been collected since the dawn of time. A primitive man sought answers to survival and comfort questions. Thus, the desire to know is as deeply ingrained in the biological and social makeup of humans as the desire to reproduce.

Humans require information about their surroundings, such as threats and food supplies, to survive. As a result, gathering information on these basic needs is critical to survival. As one of humanity's basic survival instincts, intelligence is as old as humanity itself (Hughes-Wilson, 2005:15).

Naturally, humans and their institutions have their secrets, which are things that are kept hidden from one human being to the next, from one institution to the next, and from one nation or state to the next. Fear, weakness, greed, or shame all contribute to the desire to keep things hidden from one another.

Humans, on the other hand, have the inherited trait of curiosity. This is also an instinct of wanting to know and explore the secrets of the other side. Curiosity and secrecy are opposing forces. This resulted in competition between enemies, friends, and allies (Huges-Wilson, 2005: 15-15**).** The existence of these two mutually opposing forces, namely curiosity, and secrecy, led to natural competition amongst enemies and sometimes amongst friends and allies (Huges-Wilson, 2005: 15–17).

5. Theoretical framework of the intelligence function

In the current state of international events, security is a top priority for all states, and it extends to critical infrastructure assets. Every state collects intelligence to aid in security-related research; some simply invest more resources in the effort than others.

Since ancient times, intelligence has been valued highly. In one of the earliest instances in which spies were used for information gathering and to determine whether or not the Israelites might settle in the promised land, **Moses** sent twelve spies into each of the twelve tribes to spy on the possibility of getting to the promised land.

Also, **Joshua** was in charge of the second act. He was supposed to spy on Jericho (Wall) before launching a military attack on the city.

Roman soldiers established the biggest empire in antiquity, requiring the administration of the biggest infrastructure, military, and bureaucracy, where **Julius Caesar** devised the first real-time "national" intelligence network system. The information was generally helpful but not necessarily essential to the success of the conflict. This was due to a breakdown in intelligence (that even caused the death of **Julius Caesar** on March 15, 44 BC).

Finally, the Chinese **General Sunzi-Tzu Ping-fa** (a 500), a warrior-philosopher, devoted the final chapter of his still widely read work ***The Art of War to the function of spies.*** So, SUN-TZU, like most of the early people who used intelligence, looked for information about military strength and plans for possibly eliminating enemies.

''You don't have to fear a hundred fights if you know your opponent and yourself. If you understood yourself better than the opposition, every success would be followed by a setback. However, you will be ambushed if you don't know either yourself or your adversary''

6. Functions of Intelligence Analysis

The prominent functions of intelligence analysis are mostly related to sorting relevant data with a perspective of providing strategic intelligence, meticulously selecting and framing the pieces of information, building analytic methods, and providing insight for intelligence questions (McDowell 2008, 216).

Strategic intelligence, in its integrative perspective, requires a strong analytic effort. As the analytic culture has been born and grown up because of the failures in history, analysis has a function to assist with other intelligence activities such as the collection and processing of the collected information.

Certainly, the analytic process has its methodology or set of methodologies. Exploiting these methods facilitates the understanding of complex inputs and finding the connections among different pieces of data and information.

Intelligence analysis should make a distinction between facts and opinions and should work on testing the hypotheses, as well. As Borek states, intelligence analysis transforms information that conflicts in itself into an appropriate understanding, in brief (2019, 816).

7. Why Intelligence Analysis Matters in terms of Preventing Surprises

There is a critical question for the researcher who studies intelligence analysis: why is intelligence analysis crucial not only for intelligence agencies but also for the security of a state? In this section, we present two arguments to explain intelligence analysis's "reason for being."

The first one is on a literal vital point of reason, which is to prevent strategic, operational, and tactical surprises. As intelligence failure happens when a surprise attack or development occurs, the primary responsibility of the intelligence analysis is to avoid these surprises by presenting a timely and effective insight that facilitates prediction (Wirtz 2017, 128).

8. Typology of Functional Intelligence

- **Basic Intelligence**: it is Knowledge that is a starting point for planning and a building block for processing further information. It is kept in databases that are regularly updated and consists of background information on any pertinent issue. It might include information on the capabilities, deployments, leadership, background, and training of the adversary. The main purposes of basic intelligence are to provide context at the commencement of operations and to explain relatively static information, such as the geography and climate of the fighting field.
- **Current intelligence**: It is a piece of information that tries to explain what is happening right now and what is likely to happen next. It's a crucial component of situational awareness (SA).
- **Estimative intelligence:** intelligence that offers prognostication and forward-looking assessment. It makes an effort to predict potential future adversary actions and their effects.
- **Target Intelligence:** Target intelligence is intelligence that offers data for the targeting process.
- **Warning Intelligence:** It locates and identifies the parts of a target or target complex, highlighting their relative importance and degree of vulnerability. (Cox, 2009).

9. Use of intelligence functions to safeguard infrastructure assets.

We must come to grips with the definitions of information and intelligence before we can discuss and conduct theoretical and applied studies on these topics. Information is nonetheless recognized **as a process, a piece of knowledge, and a thing.**

Information-as-process: Information as a process refers to the act of informing and being informed.

Information-as-knowledge: The information being communicated is intangible knowledge or information as knowledge. An individual is made aware of specific facts or data through communication, and knowledge can occasionally eliminate uncertainties. Buckland (1991). (1991).

Information-as-thing: The tangible objects of information, including data and documents, are considered to be informed as a thing. Due to their instructive character, these objects are mentioned. Since it cannot be quantified explicitly, this information is regarded as abstract.

After the data has been obtained or collected, it will be "evaluated" in terms of the validity and relevance of its content as well as the dependability of its source before being "collated," or organized and ready for use. After taking the information in its whole context into account, the analysis will figure out what it means and make reports, briefings, and other documents that reflect that meaning, Godfrey and Harry, (1971).

The people who need to know will then be "disseminated" the outcomes or products of this process. To operate with sensitive information and intelligence, one must adhere to the "need to know" principle.

It means that information should not be disclosed to a person, even if they have the necessary degree of security clearance unless there is a clear professional need to do so. The fewer people who are aware of it, the simpler it is to keep information private.

The vast majority of people believe that intelligence and information are interchangeable. According to Shulsky (2002), what distinguishes intelligence from other types of information is the fact that intelligence activities are conducted in secret. Intelligence, on the other hand, is based on a cycle that gathers and evaluates information all the time.

Intelligence can be defined as the act of giving meaning to information through interpretation. It has also been used to describe a department or group that collects or manages such data, as well as the result of such an activity or department. Intelligence can be defined as simply processed information. "Intelligence" could be defined as data that law enforcement agencies collect, use, and safeguard to make decisions about infrastructure security and support it.

The intelligence function also includes obtaining, analyzing, and disseminating pertinent information for decision-making. It may also involve formulating predictions based on this information and planning for any unforeseen events. There is a very subtle connection between the two intelligence aims. Intelligence works within the limits of approved goals, but it is the job of good intelligence to evaluate these goals in light of what is known.

For intelligence analysis to be accurate, there must be a process that ensures the data produced is valid. The majority of intelligence analysis is successfully collected through an intellectual process, which is usually five steps. The steps in the intelligence functions process include:

10. **Intelligence Management Cycle**

Source: Zems, (2013)

1. Requirements: Requirements involve defining questions that identify what data or information is expected to be gathered, and it can also mean a detailed assembly of certain types of intelligence.

2. Collection: When the requirements are established, the process of collecting a variety of information takes place. Some requirements are specific and involve several different forms of data, which are determined by how each requirement should be met.

3. Processing and Exploitation: After the collection step is completed, the information must go through processing and exploitation before it can be considered intelligence information. Conversion is an important part of this step and can include translations, decryption, and interpretation.

4. Analysis and Production: Analysis and production are crucial steps in the intelligence analysis process. This step includes the evaluation, integration, and analysis of all the intelligence data, which can consist of detailed reports as well as single-source and all-source studies. All-source intelligence analysis is solely performed by the DFI, NIA, DIA, and DSS of the intelligence and research unit

5. Dissemination and Consumption: Dissemination is the last stage of the intelligence cycle. Dissemination is the transfer of knowledge to the consumer in a form that can be used. A variety of media, including oral reports, written reports, visual products, and intelligence databases, can be used to deliver intelligence to the consumer. For dissemination, you can use both physical data exchanges and a networked data and communications system.

6. Feedback: Feedback is the dialog that takes place between the intelligence producers and consumers, which starts and continues after the information is received. An intelligence analyst should have an idea of how his or her intelligence requirements are met and be ready to make any adjustments based on feedback. The intelligence cycle components give the security management plan the data it needs, and the cycle model can restart the process thanks to the feedback component.

The cycle-like aspect of the process, however, ensures that it is only as successful as the methodology's weakest link or the extent to which each mode in the cycle is completed. So, until the necessary levels of intelligence have been reached, the intelligence cycle is repeated. In reality, though, the steps don't happen in order. Instead, they all happen at once.

11. Broad Categories of Intelligence

Importantly, there are three main duties that intelligence functions can fulfill within the intelligence network system:

1. **Tactical Intelligence**: Gaining or creating knowledge on the dangers to infrastructure security is a component of tactical intelligence (preventive measures), which can then be used to identify offenders, fortify targets, or implement tactics that would neutralize or minimize the dangerous threats. To combat crime and take preventative measures,

tactical intelligence offers real-time information about the present competitive landscape and operational performance. With the help of strategic intelligence, they can reach their goals, stay on track, and stick to the strategies and plans they made.

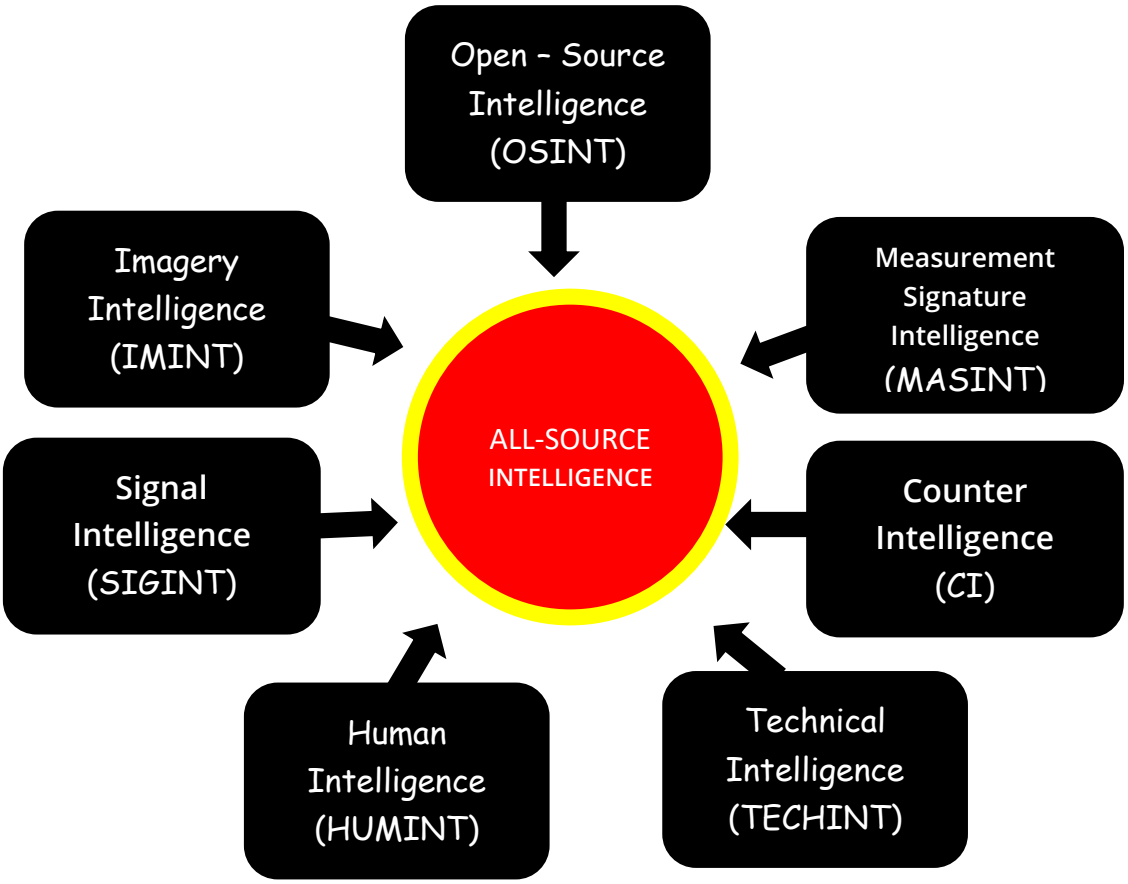
2. **Strategic intelligence** is the process of collection, processing, analysis, and dissemination of intelligence that is crucial in policy-making (Kuosa, 2011). The perspective of what an organization wants to know about its operational environment so that it can gain insight into its current process and anticipate and manage future changes. This is achieved through designing appropriate strategies for intelligence functions that are aligned with the organization's vision and mission.

   The creation of synergy in an organization's intelligence and knowledge management to facilitate the acquisition of useful information in an organizational decision-making process is known as strategic intelligence, which combines various types of intelligence, such as criminal and security intelligence. Additionally, strategic intelligence is crucial for firms that want to successfully address opportunities and problems related to anticipated future infrastructure security threats. Kuosa, (2011). (2011).

3. **Intelligence led-policing:** Policing that is "intelligence-led" Advanced data analytics, community engagement, and cooperation with other law enforcement agencies and organizations **are key components of this** policing strategy. By sharing information and making direct observations, the police can be proactive instead of reactive when assessing threats, and criminal activities to critical infrastructure assets. This is an effective way to eliminate and fight infrastructure insecurity. It also has roots in several other crime-fighting theories, such as problem-oriented policing (POP), community-oriented policing (COP), and cultural intelligence (CQ).

12. All-source of information

Information obtained through HUMINT, SIGINT, IMINT, MAS1NT, and OSINT is included in all source intelligence. The goal of this kind of work is to create supporting evidence and use a variety of sources to verify important facts. The advantage of an all-source strategy is that each intelligence field excels in gathering a particular kind of data. This gives the intelligence agency a chance to look at every part of an intelligence target and learn more about how it functions.



Source: Zems, (2013:4. 25)

1. The term "**open-source intelligence**" (OSINT) refers to the collection of all publicly available data and information from sources like books, grey literature, studies, official reports, Internet searches and conversations, the deep web, as well as information from people in the business world, academic institutions, think tanks, travelers, etc.

2. Human intelligence (HUMINT) is data gathered by humans from sources like spies, agents, insiders, or informers; defectors, turncoats, or walk-ins; diplomats, businesspeople, travelers, or academics; as well as from debriefings, interrogations, conversations with foreign personnel; or counterintelligence operations, etc.

3. Signal intelligence (SIGINT) is data and information gathered by overt or covert ground sites, ships, submarines, aircraft, UAVs, or satellites through intercepts, monitoring, and localization of radio, microwave, radar, and other electromagnetic emissions, including laser, visible light, and electro-optics. These devices all typically record and report what has occurred. SIGINT can offer information about threats' objectives, plans, activities, or events as well as the properties of materials and weaponry. SIGINT's collection disciplines are divided into five groups: Communications intelligence (COMINT

4. Intelligence in imagery (IMINT) is data and information collected by satellites, aircraft, unmanned aerial vehicles (UAVs), and ships using photography (PHOTINT), film, video, high-definition TV, or radar. It is imagery and satellite signals, which are data streams that are captured and reconstructed as images from the reflections of several bands, including infrared, ultraviolet, and other image-capturing technologies97, that are increasingly recording and informing us about what may happen. IMINT is now used more and more in cartography and mapping.

5. **measurements and signs** (MASINT) - Using data from spectral analysis of light reflections across the spectrum, physical or magnetic properties, emitted and reflected energy of radio frequencies, lasers, shockwaves, the acoustics of mechanical sound, vibration, or motion, as well as materials sampling of soil, water, it enables one to perform both IMINT and SIGINT. These methods include using visible light, infrared light, ultraviolet light, multi- (2-100 bands), hyper-(100-1,000 bands), and ultra-spectral imaging.

13. The Nigeria Situation

In order to fulfill its primary duty of protecting its citizens from both internal and foreign attacks, a state creates its security services. In Nigeria, criminal activity and criminal enterprises present a serious threat that puts this function to the test.

However, disjointed intelligence efforts daily contribute to the insecurity that could have been prevented. Despite the claims of national security organizations that they will lessen and eradicate these criminal activities and the continuous violence threats, this still happens or the standard catchphrase of the security service, "**We are on top of the matter**"

Every government's main goal is to provide appropriate protection for its people through efficient and effective intelligence operations. This includes but is not limited to, protecting their lives, property, and critical infrastructure assets from any internal or external threat that non-state actors might pose to them.

14. Summary and Conclusion

Although there has always been a need for and desire for intelligence activities, foreknowledge is required to attain outcomes that are beyond the capabilities of regular individuals. It is important to stress that foresight cannot be drawn from the spirit and cannot be inferred solely from experience or by deductive reasoning. Intelligence disciplines could be used to figure out how to protect infrastructure and all assets ahead of time.

Security is, nevertheless, a fundamental objective of all governments, particularly of a corporate organization of this size, in all of its manifestations in modern international politics. Because of this, the value of intelligence operations has been known for a long time, and they have been used from the beginning to fight organized crime, technical crime, and crime against infrastructure security.

To put it mildly, intelligence operations have always been and always will be a crucial weapon for winning both war and peace, as well as battling insecurity in Nigeria's important infrastructure assets.

Lastly, it's hard to say enough about how important it is to find ways to get intelligence collection activities and disciplines that can help fight, stop, and get rid of threats of violence against key infrastructure assets and organizations.

15. CONCLUSION

Every Nigerian has a duty to solve the nation's security concerns with regard to its infrastructure. Regardless of the political, religious, or ethnic affiliations of the participants, a cohesive stance must be founded on a shared national interest.

All security intelligence agency administrators should have access to the intelligence function, according to a suggestion. The coordination and harmonization of intelligence operations would be made simpler as a result.

We contend that Nigeria's national security framework ought to make it considerably simpler for the nation to put an end to the recent spike in violent crime.

The government must establish a reliable and efficient security intelligence system in order to do this. A wide spectrum of security and intelligence organizations, including the military, police, paramilitary, and epistemic intelligence community, should be part of this framework.

Profile summary
Professor Zems Mathias, SP. retd. Ph.D.
PhD. USA, MSC. Italy, MSC. Uk, MSC.
PGD, Ghana, BSC, HND, USA, NIG.

He is an author, publisher, facilitator, instructor, advisor, and criminologist. A criminal intelligence profiler, cybersecurity expert, and digital forensics expert. He held several positions, which included: case officer, intelligence coordinator, field officer, security intelligence analyst, and criminal intelligence analyst. His investigations cover bank fraud, wire

fraud, cybercrime, militancy, kidnapping, homicide, cultism, terrorism, narco-terrorism, robberies, and forensics investigations, among others.

Academic Competence: Crime and criminology; cyber-criminology; police and forensic sciences; security; community policing; crime science management; criminal & corporate investigations; espionage; undercover & surveillance investigations; intelligence; terrorism; counterterrorism; and deradicalization, Forensic intelligence, forensic accounting, and fraud examination, cybersecurity and digital forensics

Professional Honors and Scholastic Awards: An Honour for Excellent Scholarship and Research by California Legislature Assembly, United States, (2018). Certification of Recognition for Excellent Scholarship and Leadership by County of Riverside, California, United States, (2018). An award for Achieving Academic Excellence and Support Services by The Council of the City of Murrieta, California, United States, (2016). An award for Excellence in Intelligence and Crime Investigation by Be-Great Security and Intelligence Academy, Ghana. (2014).

Professional Affiliation and Membership: International Association for Counter-Terrorism & Security Professionals, USA. International Association for the Study of Organized Crime (IASOC), USA. International Association for Law Enforcement Intelligence Analysis (IALEA) USA. Global Organization for Security and Intelligence, (IOSI) Canada. British Society of Criminology, (BSC) UK. International Criminologists Association, (ICA), Italy. America Society of Criminology, ASC, USA. ASIS International Council Member: Crime & Loss Prevention Council, USA. Institute of Safety Professionals of Nigeria. Nigeria Institute of Management, NIM. Fellow: Institute of Criminology and Penology, ICPN, Nigeria.

References

Abdullah, A.H. (2012), The Effect of Strategic Intelligence on the Productivity of Human Resources in the National Petrochemical Company (Case Study: Head Office in Iran, Tehran). (Unpublished Master's Thesis). Business Management. Iran, Mazandaran: Payame Noor University

Acros, R. (2015). Review Public relations strategic intelligence: Intelligence analysis, communication and influence. Public Relations Review. http://dx.doi.org /10.1016 /j.pubrev.2015.08.003

Andrew, C. (2004). Intelligence, International Relations and 'Under-theorisation'. *Intelligence and National Security* , 19 (2), 170-184.

Abrahams, M. and Gottfried, M.S. (2014) 'Does terrorism pay? An empirical analysis', Terrorism and Political Violence, 28, pp. 72–89. doi: 10.1080/09546553.2013.879057.

Blanding, M (2012) "Strategic Intelligence: Adapt or Die" Harvard Business School Working Knowledge, August 6.

Coward, M. (2009) 'Network-centric violence, critical infrastructure and the urbanization of security', Security Dialogue, 40, pp. 399–418. doi: 10.1177/0967010609342879.

Critical Five. (2014) Forging a common understanding for critical infrastructure. Shared narrative. Available at: https://www.cisa.gov/publicati... (Accessed: 10 June 2022).

Dahl, E. J. (2005). Warning of Terror: Explaining the Failure of Intelligence against Terrorism. *Journal of Strategic Studies* , 28 (1), 31-55.

Hong, S. L., Ouyang, M., Zhang, J. and Chen, X. (2013) 'Vulnerability analysis of interdependent infrastructure systems under edge attack strategies', Safety Science, 51, pp. 328–337. doi: 10.1016/j.ssci.2012.07.003.

Fleisher, C. & Bensoussan, B. (2007). Business and Competitive Analysis: effective application. Upper Saddle River: FT Press.

Wiśniewski, M. (2016) 'Concept of situational management of safety critical infrastructure of state', Foundations of Management, 8, pp. 297–310. doi: 10.1515/fman-2016-0023.

Żaboklicka, E. (2020) 'Critical infrastructure in the shaping of national security', Security and Defence Quarterly, 28(1), pp. 70–81. doi: 10.35467/sdq/118585

Dupont, A. (2003). Intelligence for the Twenty-First Century. *Intelligence and National Security* , 18 (4), 15-39.

Fry, M. G., & Hochstein, M. (1994). Epistemic communities: Intelligence Studies and International Relations. In W. K. Wark (Ed.), Espionage: Past, Present, Future? (pp. 14-29). lford: Frank Cass & Co.

Gottfredson, L. S. (2001). Book Review: Practical Intelligence in Everyday Life. Intelligence, 29, 363-365.

Herrnstein, R. J., & Murray, C. (1994). The bell curve: Intelligence and class structure in American life. New York: Free Press.

Jensen, A. R. (1993). Test validity: g versus "tacit knowledge". Current Directions in Psychological Science, 2(1), 9-10.

Ree, M. J., & Earles, J. A. (1993). g is to psychology what carbon is to chemistry: A reply to Sternberg and Wagner, McClelland, and Calfee. Current Directions in Psychological Science, 2(1), 11-12.

Schmidt, F. L., & Hunter, J. E. (1993). Tacit knowledge, practical intelligence, general mental ability and job knowledge. Current Directions in Psychological Science, 2(1), 8

Sternberg, R. J. (1998). Abilities are forms of developing expertise. Educational Researcher, 27(3), 11-20.

Coward, M(2009) Daase, C. and Kessler, O. (2007) 'Knowns and unknowns in the "war on terror": uncertainty and the political construction of danger', Security Dialogue, 38, pp. 411–434. doi: 10.1177/0967010607084994.

Godefroidt, A. and Langer, A. (2018) 'How fear drives us apart: explaining the relationship between terrorism and social trust', Terrorism and Political Violence, 32, pp. 1482–1505. doi: 10.1080/09546553.2018.1482829

Hellström, T. (2007) 'Critical infrastructure and systemic vulnerability: towards a planning framework', Safety Science, 45, pp. 415–430. doi: 10.1016/j.ssci.2006.07.007.

Reniers, G.L.L. and Audenaert, A. (2014) 'Preparing for major terrorist attacks against chemical clusters: intelligently planning protection measures w.r.t. domino effects', Process Safety and Environmental Protection, 92, pp. 583–589. doi: 10.1016/j.psep.2013.04.002.

Sternberg, R. J., Forsythe, G. B., Hedlund, J., Horvath, J. A., Wagner, R. K., Williams, W. M., et al. (2000). Practical intelligence in everyday life. Cambridge: Cambridge University Press.

Sternberg, R. J., & Grigorenko, E. L. (2000). Teaching for successful intelligence: To increase student learning and achievement. Arlington Heights, IL: Skylight Professional Development.

Taub, G. E., Hayes, B. G., Cunningham, W. R., & Sivo, S. A. (2001). Relative roles of cognitive ability and practical intelligence in the prediction of success. Psychological Reports, 88, 931-942.

Torff, B., & Sternberg, R. J. (1998). Changing mind, changing world: practical intelligence and tacit knowledge in adult learning. In M. C. Smith & T. Pourchot (Eds.), Adult learning and development: Perspectives from educational psychology. Mahwah, NJ: Lawrence Erlbaum Associates.

Wagner, R. K., & Sternberg, R. J. (1986). Tacit knowledge and intelligence in the everyday world. In R. J. Sternberg & R. K. Wagner (Eds.), Practical intelligence: Nature and origins of competence in the everyday world (pp. 51-83). Cambridge: Cambridge University Press.

Interagency OPSEC Support Staff, Compendium of OPSEC Terms, Greenbelt, MD: IOSS, April 1991.

- Bruce D. Berkowitz and Allan E. Goodman, Strategic Intelligence for American National Security, Princeton, NJ: Princeton University Press, 1989.

3The Joint Staff, Doctrine for Intelligence Support to Joint Operations, Washington, DC: Office of the Joint Chiefs of Staff. June 30. 1991.

Interagency OPSEC Support Staff, Compendium of OPSEC Terms, Greenbelt, MD: IOSS, April 1991.

Air Force Pamphlet 200-18, Target Intelligence Handbook: Unclassif ed Targeting Principles, Washington, DC: Department of the Air Force, October 1, 1990.

Suzanne Wood, Katherine L. Herbig, and Peter A. W. Lewis, (1990) (American Espionage, 1945-1989, Monterey, CA: Defense Personnel Security Research and Education Center, 1990.

Defense Science Board, Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield, Washington, DC: Office of the Under Secretary of Defense for Acquisition and Technology, **October 1994.**

Jeffrey Richelson, American Espionage and the Soviet Target, New York: William Morrow, 1987.

Intelligence Community Staff, Glossary of Intelligence Terms and Definitions, Washington, DC: ICS, June 1989.

Sternberg RJ, Salter W1982 Handbook of intelligence Cambridge University Press Uk

Zems, M (2011) Crime is Normal 1st edition Corpus Publisher Printers and Partners Ltd Port-Harcourt, Nigeria.

Zems M (2013) Understanding Crime: Analysis for Intelligence, Investigation and Security Vicious virus! help fight it' Guangzhou Quick Printing Coy. 68 Hengzhigang Hengfu Road Guangzhou, China.

Zems, M. (2013) Crime is Normal 2st edition Guangzhou Quick Printing Company ltd. 68. Hengzhigang Henngfu Road Guangzhou China.