Defense information system

Defense Information System (DIS) refers to a military global protected telecommunication network that simplifies the conveyance of information in a worldwide space. It is driven by transmission requirements, security demands, and geographical needs of the targeted end-user groups (Soomro 2016).

Centrally, it is designed and managed to provide a long-haul information transfer. Furthermore, it is configured to provide a more sophisticated point – to-point exchanged voice and data, teleconferencing video and image services. The DIS offers an integrated operational standard user services to satisfy the connectivity requirements. It is a digital-based defense strategy, that facilitates access to vital information across the globe through efficiently designed services such as information assurance, data services, multinational sharing of information and computer hosting.

Moreover, DIS forms a key spectrum of military force operations which include defensive tactics, humanitarian efforts, offensive tactics as well as counterterrorism (Stahl, 2008). The ultimate goal of Defense information system is to help in achieving information governance by providing an effective infrastructure that may be of an advantage to the user in a combat. On the other hand, ethics refers to the prescribed code of conduct which are morally justified to administer the defense information system.

Major ethical issues involved herein include privacy of information, Access to information, information accuracy and right to Intellectual property. Rapid growth in informationtechnologythrough its improved dimensions forcommunication, computation, surveillance, retrieval and storage has

sounded an alarm on privacy matters (Kizza, 2007). This is to say that, the unethical retrieval of data and access to information by unauthorized persons has greatly threatened the privacy of integrated security systems networks.

Therefore, principles of ethics agitates for protection of privacy policies in relation to access of every sensitive information. Information accuracy is another ethical issue of concern. Upholding to an inaccurate information is misleading hence, it is a soleresponsibilityof the defense information system to be vigilant in pursuing the accuracy of its information. Imperatively, they should be certain that their information are based on facts as opposed to fiction (Stahl, 2008).

The final ethical issue in defense information system is the right of intellectual property. This forms the most complex right faced by many in the contemporary society and the military is not an exemption. Substantial ethical concerns surrounding this stem from the information traits which makes it transferable. Any Defense Information system information is believed to be costly (Stahl, 2008). Furthermore, once produced, it is easier to copy and transfer to others.

This makes it difficult to safeguard such information due to its intangible nature. It is worth noting that several institutions such as copyrights and patents have come in to managed and protect the rights of intellectual properties. The worldwide process is narrowing the space steadily as a result of what Kant describes as the public use of reason. Information Technology has greatly improved the effectiveness of the Defense Information System.

It has enabled quick decision making through enabled rapid access to functionalities of creating, finding, using and sharing of the needed information. Quicker access to information by commanders from anywhere has also improved control and commanding. Additionally, it has also accelerated the speed of actions thus heightened the ability to coordinate all security issues across the globe.

Other expeditious contributions of information technology on DIS includes improved cyber security, improved information security postures, as well as the defense effectiveness. However, the state territory is privately constrained by certain interests which differ from the individual reflection concerning the general subjects in a public domain. The greater disparity therefore emanates from the free public use of internet and other media due to their enormous private control.

Since information is provided on demand in our cloud computing era, access to web-based tools by users via browsers has led to abstraction of customer details, which has raised questions of privacy and transparency. Ethics in relation to privacy of information for both individuals and organizations have been heavily affected negatively as a result of technology (Mingers, 2010).

On this aspect, cyberspace has posted more security threats to nation-states in a context of increased dependency of worldwide networks and computer based interactions. Cyber-attacks, scams, image manipulations, infringements to computer systems and copying particular unauthorized software demonstrates the unethical practices facing the defense information system unit. It is therefore imperative for stiff ethical measures

to be put in place to hasten security of the nation states with the advancements in technology.

Contemporarily, no state agency can apply control to privacy to prevent the exposure of one's close secrets to others (Zizek, 2013). Regarding to the larger size of data, computers have failed to interpret and register multi-millions of data therefore making it difficult to detect suspicious message making state communication of information more unsafe. However, the defense information system has not been much helpful due to increased illegal malpractices according to Snowden and other whistleblowers.

On this regard, denouncing of the public authorities and engaging in public use of information has greatly threatened the secrecy of individuals (Snowden, 2013). In conclusion, defense information system is a telecommunication network enabled system designed to simplify the transfer of information across the globe. It was majorly implemented by the military operational forces in United States which include defensive tactics, humanitarian efforts, offensive tactics as well as counterterrorism.

The ultimate goal was to achieve control of information by providing an effective infrastructure for users in a combat and to improve on the general security across the globe. However, ethical issues in defense information system include Privacy of information, accuracy of information, access to information and the Property right. Despite of the drawbacks, DIS has remained focused to work with the new technological innovations and achieve their set missions.