ISSN: 0974-5823 Vol. 6 (Special Issue, Nov.-Dec. 2021)

International Journal of Mechanical Engineering

Cyber Security in African Union and Ethiopia and Its anticipation

Dr. Bhoomeshwar Bala[1], Dr. Bharat Kumar G J[2], Dr. Swapna Gangone[3] and Dr. Bhupendra Kumar[4]

[1] Associate Professor, Department of Information Technology, Debre Tabor University, Ethiopia

[2] Professor, Department of Computer Science, Mettu University, Ethiopia

[3] Associate Professor, Department of Computer Science, Mettu University, Ethiopia

[4] Professor, Department of Accounting and Finance, Debre Tabor University, Ethiopia

Abstract. In recent years the term "cyber" has been used to describe almost anything that has to do with networks and computers, especially in the security field. Another emerging field of study is looking at conflicts in cyberspace, including state-on-state cyber warfare, cyber terrorism, cyber militias etc. Unfortunately, however, there is no consensus on what "cyberspace" is, let alone what are the implications of conflicts in cyberspace. cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems. In this paper we review the implications on the potential for rapid deployments of offensive and defensive actions in cyberspace, the feasibility of mapping cyberspace, and the need for constant patrolling and reconnaissance. This paper also describes the occurrences of cyber security and cybercrime with a particular focus on cyber security as international aspect of cyber security threats, African context and Ethiopian context**.**

Keywords: Cyberspace, cyber conflicts, cyberattacks.

1 INTRODUCTION

The phrase "cyberspace" itself was created 1982 by William Gibson, the citizen of Canadian science fiction writer, in his novelette "Burning Chrome" as cited in (Fenz, 2005). Currently the term is simply used to reference the network which is known by most people as the internet. By definition the cyber-space is more than the internet, because every transaction or event which is not happening in "real" world is occurring in the cyberspace. An example would be the calculation in a single chip or the communication between certain chips which are not connected to the internet. The current paper will focus on the internet as a cyberspace "subdivision" (Fenz, 2005). The cyberspace is many from them next both definitions are describing the term "cyberspace" as a metaphor which is describing an abstract/non-existing terrain which is representing the real world with virtual objects and virtual communication which is happening between their users via e-mail or instant messaging.

"Cyberspace, a metaphoric abstraction used in philosophy and computing, is a (virtual) reality which represents the World both "inside" computers and "on" computer networks" (U.S. Department of Homeland Security, 2005). "A metaphor for describing the non-physical terrain created by computer systems. Online systems, for example, create a cyberspace within which people can communicate with one another (via e-mail), do research, or simply window shop" (Fenz, 2005). Business is way per-formed, government activities operate, and country security defence conducted and reformed. These operated activities now rely on an interdependent network of information technology infrastructures named by cyberspace. The Countrywide Approach to Secure Cyberspace provides a framework for protecting this infrastructure that is essential to economy, security and system of life managing through network integration. According to American journal that published (2003) shows in the past few years, intimidations in cyberspace have risen highly. The policy of the United States" is to protect against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States". Using cyberspace and security to reduce security annoying to these threats before they can be oppressed to damage the cyber systems supporting our Nation-state's critical infrastructures and ensure that such disruptions of cyberspace are irregular, of minimal duration, manageable, and because they are very dangerous (House & Washington, 2003).

1.1 OVER VIEW OF CYBER SECURITY THREATS

Cyber security is a national imperative and a government priority. Increased cyber security will help to protect consumers and businesses, ensure the availability of critical infrastructures on which our economy depends, and strengthen national security. However, cyber security efforts must be carefully tai-lored in order to preserve privacy, liberty, innovation, and the open nature of the Internet (Cong, 2009). To design an effective and balanced cyber security strategy, each part of the country's critical infrastructure must be careful separately. Solutions that may be appropriate for the power network or financial networks may not be suitable for securing the public portions of the internet that constitute the very architecture for free communication essential to our democracy. Policy toward government systems can be much more prescriptive than policy toward private systems.

The characteristics that have made the Internet such a success its openness, its decentralized and user-controlled nature, and its support for innovation and free expression may be put at risk if heavy-handed policies are enacted that apply uniformly to any and all infrastructure that may be considered “critical.” Some cyber security proposals take a “one size fits all” approach that ignores these nuances. This article analyses those proposed cyber security measures from a civil liberties perspective. It sug-gests alternative approaches that would protect the privacy and liberty of Internet users and promote rather than stifle innovation (Nojeim, 2009).

As African countries increase access to broadband Internet, issues relating to cyber security and cybercrime are initialed and there is a need to ensure that people, governments, on government and busi-ness are protected. African countries need to immediately potential efforts to struggle cybercrimes through multi stake holders approach involving governments, industry and civil society organizations in an integrated and comprehensive manner. African governments are at diverse level of forming policy instruments and legislative framework and given the international dimension of Cyber security it’s important to reinforce international cooperation including confidence building measures. Mostly African low level of security provisions sufficient to prevent and control technological and informational risks. Lack of know-how in terms of cyber security and inability to monitor and defend national networks, making African countries attacked to incidences of cyber radicalism and cyber spying.

Ethiopian, according to Reba, (2005) Information security mean the protection of information which is valuable, used for business, nationality information and critical elements that serve government and society. Including the systems and hardware help to store and transmit that information. Information security contains the wide-ranging areas of cyber security management, computer and data security management, computer and data security processing and network infrastructure security. Using Cyber security to protect information and its related systems, tools such as policy, mindfulness, training and education, and technologies are of energetic importance. Security is the quality or state of being secure, to be free from danger and terrorism. Mean that, security can be defined as building protection against vernal ability. The security of information and its systems entails securing all components and protecting them from potential misuse by illegal software and users in network communication (Reba, 2005).

1.2 African Union and Ethiopia convention on Cyber Security threats and personal data

The African Union (AU) Convention on Cyber Security and Personal Data improved greatly as the result of positive civil society input into the drafting process. However, the Convention has not yet entered into force and a number of countries have promulgated harmful new cybersecurity legislation after the text was finalized in June 2014 (Ephraim Percy Kenyanito, 2016).Ratification requires the executive or the legislature to deposit instruments of ratification with the AU secretariat in Addis Aba-ba, Ethiopia. As of July, 2016, eight African nations had signed the convention, including: Benin, Chad, Congo, Guinea Bissau, Mauritania, Sierra Leone, Sao Tome & Principe, and Zambia.3? Senegal ratified the convention in the July-November period, and remains the first and only country to have done so (Dr. Papa Assange Touré, 2016).

However, the lack of ratification has not stopped several countries from racing ahead with rushed, and potentially harmful, legislation. After surveying fourth five (45) Sub-Saharan African countries, a total of thirteen (13) countries have attempted domestic reforms of ICT laws in the period between June 2014 and September 2016, twelve(12) countries these are: Benin, Botswana, Chad, Ethiopia, Kenya, Madagascar, Namibia, Nigeria, South Africa, Tanzania, Uganda, and Zimbabwe. Several of the domestic reform bills fail to provide basic protections for user data (OAfrica, 2012).Worse, other bills enable the government to violate the rights of privacy, expression, and assembly. In this view, some of these errors stem from overbroad interpretation of the ITU Harmonization of the Telecommunication and ICT Policies and Regulation in Africa (HIPSSA) project, which was carried out prior to 2014 without public consultation. Unlike the ITU model regulations, this Convention was adopted after multi stakeholder input, with the African Charter on Human and People’s Rights as a reference.

For this reason, governments should not pass the suggested ITU regulations into law, but should fol-low the AU Convention instead. But before countries further codify harmful laws, Access Now urges them to first ratify the AU Convention. Once they have done so, they should carefully implement the Convention’s framework with legislation that respects human rights. These domestic reform efforts should be carried out in open, consultative, multi stakeholder processes with input from civil society organizations and subject-matter experts (Kenyanito et al., 2016).

1.3 POSITIVE PROTECTIONS FOR AU (AFRICAN UNION)

The current Computer and Cyber Crimes Bill 2016 contains clauses which allow for the protection for digital security investigators if they find and demonstrate the existence and extent of systems vulnerabilities.

1.4 PROTECTIONS AGAINST INTERMEDIARY LIABILITY

As rule across Kenya, Ethiopia, South Africa and Zimbabwe draft laws shows, there are clear provisions protecting intermediaries from liability for hosting third party content article 10. This type of legal protection enabled the growth of the internet and allows the smooth functioning of the global web at scale, so these provisions must be retained.

1.5 RESTRICTIONS ON WHISTLEBLOWERS AND DIGITALSECURITY RESEARCHERS

Ethiopia, Zimbabwe, and Kenya’s draft laws contain sections on “computer fraud” and “illegal ac-cess.” These provisions are vague and could be interpreted to criminalize the work of journalists, whistle-blowers, and digital security researchers.

1.6 ETHIOPIA ARTICLE 10 OF ITS 2016 COMPUTER CRIME PROCLAMATION

Focuses on computer-related fraud and can be harmful to journalists because the clause does not define the meaning of "distributing misleading computer data, misrepresenting his status, concealing facts which he had a duty to reveal." The vague language leaves open the possibility of potentially misuse of Article 10. In the course of prosecution or for state authorities to use the article to pressure journalists to reveal journalistic sources or to prosecute anonymous or pseudonymous activity online.

1.7 SOUTH AFRICA SECTION 4 OF THE CYBERCRIMES AND CYBERSECURITY BILL 2015

Makes it an offense for a person to gain "unlawful and intentional access to the whole or any part of" data, a computer device, a computer network, a database, a critical database, an electronic communications network, or a National Critical Information Infrastructure. For the section, "access" includes, to "make use of," "view," or communicate with," among other actions. A person's actions are unlawful to the extent that they exceed lawful authority to access article. This circular definition fails to offer guidance as to when access to such systems exceeds an individual's lawful authority.

1.8 VAGUE PROVISIONS AND CRIMINAL DEFAMATION PROVISIONS WHICH ARE OPEN TO ABUSE

Across all four jurisdictions, the found vague sections which added additional fines and jail time when offenses are stacked 12. The most dangerous clause is in the Ethiopian text, which aims to punish whoever causes "conflict among people." This provides no clear evidentiary standard to provide notice as to what behaviour is proscribed a requirement for any law to meet international human rights standards.

1.9 CRIMINALIZATION OF COMPUTER USE

Across Kenya, Ethiopia, South Africa, and Zimbabwe draft laws founded shows sections adding penalties and imprisonment terms for any person who commits an offense under any other law, through the use of a computer system in article 14. Author, recommend that these sections be removed as the offenses listed are already covered in existing laws in the respective countries. Redundant provisions adding penalties for using a computer do not achieve legitimate public policy goals, and can slow the adoption of new technologies.

1.10 ILLEGALLY OBTAINED EVIDENCE AND GOVERNMENT HACKING

In Ethiopia, Zimbabwe, and Kenya, in article18, Author, found provisions which can be interpreted to allow government hacking. Particularly, Author, found that the drafts were vague and lacked judicial and legislative oversight, and that the current language does not compel law enforcement to return devices upon completion of investigations. The practice of "government hacking" significantly interferes with human rights, such as the right to privacy, as well as threatening personal property rights and global cybersecurity. Author, recommend that amendments are made to prohibit the use of movement hacking operations to access data stored remotely. Particularly the laws should conform to Ac-cess Now policy brief, "A Human Rights Response to Government Hacking," requiring that: "Government hacking must be provided for by law, which is both clearly written and publicly available and which specifies the narrow circumstances in which it could be authorized. Government hacking must never occur with either a discriminatory purpose or effect in article 19"

1.11 LACK OF COMPETENT JUDICIAL AUTHORITY AND DUE PROCESS

In Kenya, Zimbabwe and Ethiopia, founded shows provisions which would bypass the judiciary be-cause police officers are not required to apply for a court warrant while investigating cybercrimes in article 20. According to Kenyanito et al.,(2016) article recommend that these sections be amended as they contravene the principle of "competent judicial authority" in the International Principles on the Application of Human Rights to Communications Surveillance in article 21. The amendments should require that cybercrime be investigated under the supervision of competent judicial authorities (Kenyanito et al., 2016).

1.12 CYBER SECURITY THREATS IN ETHIOPIA

The formation of information security program begins with the creation and review of the organization's information security policies, standards and practices. Policies shall be considered as the basis for all information security planning, design, and deployment. Policies do not specify the proper operation of equipment or software. This information should be placed in the standards, procedures and practices of users' manuals and systems documentation. A procedure is a plan or sequence of action used by an organization to convey instructions from its senior- most management to those who make decisions, take actions, and perform other duties on behalf of the organization. Polices are organizational laws in that they dictate acceptable and unacceptable behaviour within the context of the organization's culture. Like laws, policies must define what is right, and what is wrong, what the penalties are for violating policy, and what the appeal process is. Standards, on the other hand, are more de-tailed statements of what must be done to comply with policy. The information technology and Communication revolution has changed the way business is transacted, government operates, and national defence is conducted. These three functions now depend on an interdependent network of critical information infrastructures that we refer to as "cyberspace" to secure this cyberspace a nation-al policy shall be defined in such a way that to prevent or minimize disruptions to critical information infrastructures and thereby protect the people, the economy, the essential human and government services and the national security. Disruptions that do occur should be infrequent, of minimal duration and manageable and cause the least damage possible. Consistent to the policy in force, the national strategy to secure cyberspace shall have the following objectives:

- Prevent cyber-attacks against critical infrastructures, Reduce national vulnerabilities to
- Cyber-attack and, Minimize the damage and recovery time from cyber-attacks that do occur.

Despite the facts mentioned above there is no functional cyberspace security policy in Ethiopia. Currently, the Ethiopian ICT Development Authority is preparing national information security standards. However, information security policy should have been developed earlier to guide the preparation of standards. Due to lack of national cyberspace security policy and associated standards, ICT development programs have very little focus on security components. Similarly, the national network infra-structure and telecommunications service provider, the Ethiopian Telecommunications Corporation, also performs its duties without clearly defined national strategic procedures and guidelines in place. Instead, the Corporation is relying on security elements proposed by vendors and system installers.

1.13 STATUS OF CYBERSPACE SECURITY IN ETHIOPIA

In 2001, a national taskforce coordinated by the National Computer and Information Centre of the Ethiopian Science and Technology Commission initiated Data Disaster Prevention and Recovery Management (DDPRM) program which mainly sought to address data integrity and physical security. The objective of this project was to formulate a policy, which facilitates enabling environment and paves the way for designing of a secure institutional data centre. The overall intention was to protect data stored, processed and transmitted through computer system. In addition to this, the project was also supposed to develop guidelines and procedures that support corporate enterprises to put in place their own organizational data security in house policy.

As compared to data and information security is a broader system which deals with all critical elements and components of an information system namely: Software (sophisticated), Hardware (high quality platform taker), Data (huge: Data warehouse), People (professional), Procedures (rule) and Networks (.infrastructure) With regard to this, the Data Disaster Prevention and Recovery Management guideline developed by a taskforce organized by Ethiopian Science and Technology Commission is a good move towards adopting strategies to determine the level of protection required for applications, systems, facilities in ICT development and recover from any disaster without serious business discontinuity and major damages and loss to the system and data. However, escalation of the specific data security issue to more general information security systems was found to be mandatory.

In 2004, not long after the restructuring of IT sectors, the Ethiopian Telecommunications Agency took the initiative to invite the Ethiopian Information and Communication Technology Development Authority (EICTDA) and the Ethiopian Telecommunications Corporation (ETC) to discuss on issues of cyberspace security and encryption policy. On this initiative, the three institutions agreed on importance of cyberspace security policy and formed a joint technical committee, which follows up the process of formulating information security policy and standards. The institutions have also reached at a common understanding that EICTDA has broader legal framework and resources to lead the initiative. On the basis of this, EICTDA has employed a consultant to conduct a general assessment on how to go forward to develop a national information security strategy and action plan. Currently, the Ethiopian ICT Development Authority is working on preparation of information security standards. The final document is expected to be finalized and endorsed by the government for implementation as of September 2005. As part of the capacity building process for the ongoing information security pro-grams, the EICTDA has organized training on Information Security Principles to selected government employees working on ICT and related sectors.

1.14 EXISTING SECURITY TECHNOLOGY IN ETHIOPIA

According to Reba (2005) Ethiopia has not yet formulated information security policy and standards. However, currently the ISP is utilizing firewalls, network Intrusion Prevention Systems (IPS), Dial-up protection and packet filtering mechanisms to protect the internet infrastructure, corporate VPNs and Leased lines. Latest spam guards to get rid of viruses or malicious software (malware) are also in place to protect the system. The existing ISP security systems are based on technical proposal submitted by network installers and vendors. Therefore, it cannot be referred to as a system developed fulfilling all-rounded national information security policy and standards. In addition to this, when the existing ISP security systems are based on technical proposal submitted by network installers and vendors. There-fore, it cannot be referred to as a system developed fulfilling all-rounded national information security policy and standards. In addition to this, when implementing information security in an organization, there are many human resource issues that must be addressed. The organization should thoroughly examine the options possible for staffing information security function. In this regard, in Ethiopia there is a shortage of information security professionals. Hence, organizations are forced to draw on the current pool of information security practitioners (Reba, 2005).

2 Conclusion

This paper identifies quantify the impact of attacks on communications, and information flows on the operability of the component systems, and to evaluate and compare different architectures with respect to their reliability and robustness under attack. According to African Union Cyber Security and Personal Data improved greatly as the result of positive civil society input into the drafting process. However, the Convention has not yet entered into force and a number of countries have promulgated harmful new cybersecurity legislation important to keep security Communication through networked system in Africa.

REFERENCES

1. Ahmad, A. (2000). Type of Security Threats and It ' s Prevention. Int.J.Computer Technology & Applications, 3(2), 750–752.

2. Amoroso, E., Butterworth-Heinemann, (2010). Cyber Attacks, Protecting National Infrastructure.

3. Cert-UK. (2015). Common Cyber Attacks : Reducing The Impact. Common Cyber Attacks : Reducing The Impact.

4. Cong. (2009), Preventing Terrorist Attacks and Protecting Cyberspace.

5. Dr. Papa Assange Touré, (2016) .A decisive step by Senegal towards accession to and Ratification of the Budapest and Malabo Conventions.

6. Ephraim Percy Kenyanito, 2016 .Emerging threats in cybersecurity and data protection legislation In African Union countries.

7. EU. (2016). Committed to Europe. Cybersecurity and Telecommunications in the EU, (March).

8. Fischer, E. A. (2016). Cybersecurity Issues and Challenges : In Brief. Cybersecurity Issues and Challenges, (August).

9. Fujiwara, B. (2006). Cyber Security " Threats and Countermeasures ." Cyber Security " Threats and Countermeasures ," 1–8.

10. Guariniello, C., & Delaurentis, D. (2014). Communications , information , and cyber security in Systems-of- Systems : Assessing the impact of attacks through interdependency analysis. Procedia - Procedia Computer Science, 28(Cser), 720–727.

11. Hughes, B. B., Bohl, D., Irfan, M., & Margolese-malin, E. (2015). Quantitatively 12.Understanding and Forecasting the Balance Extended Project Report from the Frederick S . Pardee Center for International Futures Josef Korbel School of International Studies University of Denver In project collaboration with Cyber Benefits and Risks : and the, (September).

12. ISTR. (2016). Internet Security Threat Report. Internet Security Threat, 21(April).

13. ITU. (2012). RIMCYBERCRIME UNDERSTANDING CYBERCE : Understanding Cybercrime: Phenomena, Challenges and Legal Response.

14. Kenyanito, E. P., Analyst, S. A. P., Now, A., Jit, R., Chima, S., Now, A., … Cybercrimes, A. (2016). Room for improvement : Implementing the African Cyber Security and Data Protection Convention in Sub-Saharan Africa. Implementing the African Cyber Security and Data Protection Convention, (December).

15. MP, T. R. H. P. H., & Exchequer, C. of the. (2016). National cyber security strategy 2016-2021. National Cyber Security Strategy.

16. Nojeim, G. T. (2009). Cybersecurity and Freedom on the Internet. NATIONAL SECURITY LAW & POLICY, 4, 119.

17. Powell, S., (2010). Methodology for Cyber Effects Prediction, Black Hat Technical Security Conference, Arlington, Virginia

18. Reba, B. (2005). ETIOPIAN TELECOMMUNICATIONS AGENCY STATE OF CYBER SECURITY IN ETHIOPIA. TELECOMMUNICATIONS AGENCY STATE OF CYBER SECURITY IN ETHIOPIA, (June).

19. Report, (2009). Department of Homeland Security, Roadmap for Cybersecurity Research.

20. Report, (2009).Executive Office of the President of the U.S., Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure.

21. Report, (2011).White House Office of Science and Technology Policy, Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program

22. U.S. Department of Homeland Security, 2005. (2005a). Cyberspace Security : A definition and a description of remaining problems. Cyberspace Security, 1–10.