Global Scientific JOURNALS

GSJ: Volume 5, Issue 6, June 2017, Online: ISSN 2320-9186
www.globalscientificjournal.com

CYBER SECURITY INSTITUTIONAL FRAMEWORK IN TANZANIA: A POLICY ANALYSIS

SEMBOJA, Haji H. [1], SILLA, Beatus S.[2] and MUSUGURI, Joseph N.[3]

1Department of Economics, the University of Dar Es Salaam-Senior Lecturer
Email: haji@semboja.com
2Tanzania Police Force – Policy and Budget Analyst
Email: sillabeatus@yahoo.com
3Department of Sociology and Anthropology, the University of Dodoma – Assistant Lecturer
Corresponding Email: jmusuguri@gmail.com

ABSTRACT

Cyber security threats propagating through the globally interconnected cyberspace are difficult to manage with conventional national state instruments. Like other countries, Tanzania is struggling to comprehend its interests in the cyber domain. According to the Global Cyber security Index Tanzania is ranked 22nd out of 29 positions with 0.206 unsatisfactory level of preparedness in cyber security considering legal, technical, institution, capacity and international cooperation measures. The paper analyzed the cyber security institutional framework in Tanzania. Both qualitative and quantitative data and information were analyzed to assess the performance of the institutions relative to Global Cyber security Index (GCI 2015) designed from the ITU Global Cyber security Agenda (GCA). The paper found that Tanzania is less prepared in terms of strategies for prevention, detection, response and crisis management of cyber attacks. Tanzania has complex primary problems, constraints and challenges affecting performances of cyber security systems. These include lack of explicit national cyber security policy; many legally independent institutions with different laws, regulations and interests, top leadership system is not well defined, lack of formal institutional linkage; inadequate resources in each institution; lack of institutional dynamism. The study recommends that there is a need of national cyber security policy, laws and institution framework. To support the desired system immediately the government has to formulate implementation strategy of the policy as well as the institutions and regulations to smooth performance and interaction among the current cyber security systems.

Keywords: *Institutional Framework, Cyber security, Tanzania, Systems, policy, Laws*

1.0 Introduction

1.1 Background

Cyber security threats propagating through the transnational, globally interconnected cyberspace are difficult to manage with conventional national state instruments. While national states are struggling to comprehend their interests in the cyber domain, policy makers are viewing this situation to attain optimal systems of cyber security to focus on cybercrimes and ungoverned cyberspace. Cyber security has quickly evolved from a technical discipline to a strategic concept; globalization and internet give nations and individuals incredible new power, based on constantly developing networking technology. From that point of view cyber security is all about protecting computer systems, networks, and information from disruption or unauthorized access, use, disclosure, modification or destruction, (Gallaher, Link and Rowe, 2008). Nations in the world have undertaken different independent initiatives to maintain highest possible level of security required in their countries, these include national cyber security policies, strategies and laws to ensure smooth implementations of the policy.

Despite efforts through cyber security policies, strategies and laws still the problems of cyber security, cyberspace and cybercrimes cannot be avoided. Virtual nature of the cyber ungoverned space provides difficulties to prevent the problems. Absence of national boundaries on cyber components advantages the issues to be a global topic. Some of the developed countries such USA came up with International Cyberspace Strategy 2011 which demonstrates, the USA cyber security position in the world. In a case of developing countries still few have managed to come up with the cyber security policy, example of these countries include Rwanda whose policy was formulated in 2015. Implementation of the policy requires a focus and strong support from the laws and institutions as a complete set of system. Each component of the system; policy, laws and institutions have increased the performance of the country in cyber security. Countries with all three components ranked at high level compared to those with incomplete set.

According to Global Cyber security Index 2015 USA ranked the 1st with 0.824 satisfactory level of preparedness in cyber security considering legal, technical, institution, capacity and international cooperation measures; implying that USA has an adequate set of cyber security system required at international bases, while Tanzania ranked 22nd out of 29 positions with 0.206 unsatisfactory level of preparedness in cyber security considering legal, technical, institution, capacity and international cooperation measures (GCI, 2015). Tanzania has inadequate set of cyber security system, evidence by absence of cyber security policy and inefficient institutional framework.

1.2. Objectives of the Paper

The objective of this paper is to analyze the institutional framework of the cyber security systems in Tanzania. The paper will examine establishment, current status and performance of these participating institutions, their functioning, effects and linkages.

Furthermore, this paper shall identify primary problems, constraints and challenges faced by cyber security institutions in performing their functional. Lastly, the paper will conclude and provide policy recommendations on cyber security systems in Tanzania and a way forward on desired systems.

1.3 Methodology and Approaches

Preparation of this paper used different research interdependent methods and approaches. These included literature review, data collection, analysis, consultations and report writing. We managed to collect secondary data and information from International Telecommunication Union (ITU) reports, Crime Statistics Reports of Tanzania, USA International Cyberspace Strategy and other cyber related matters documents.

Both qualitative and quantitative data and information were analyzed to assess the performance of the institutions relative to Global Cyber security Index (GCI, 2015) designed from the ITU Global Cyber security Agenda (GCA). The Global Militarization Index (GMI) depicts the relative weight and importance of the military apparatus of one state in relation to its society as a whole. Additional quantitative and qualitative data obtained from the Tanzania Crime Statistics Report 2014 describing the performance of cyber security institutions in Tanzania, and explanatory data analysis method used through illustrations and tables.

The paper uses the Global Cyber security Model as articulated in GCA to elaborate and determine the Institutional framework of cyber security in Tanzania and examining the current inter-linkages of the institutions at domestic and international levels.

1.4. Paper Coverage

The paper has three main sections. Section 1 is the introduction covering the background of the subject matter, objectives and the methodologies and approaches used in analyzing cyber security in Tanzania.

Section 2 presents in brief the current cyber security institutional framework in Tanzania. This will entail an exposition of the current organizational and institutional arrangements, determination of performance of the cyber security systems in Tanzania using the ITU Global Cyber security Index, identification of major primary problems, constraints and challenges affecting performances of cyber security systems in Tanzania and proposition of principle elements and characteristics of desired systems of cyber security in Tanzania.

Section 3 is a conclusion which covers key findings, policy recommendations and the way forward.

2.0 Cyber Security Institutional Framework in Tanzania

Section 2 presents in brief the current cyber security institutional framework in Tanzania.

2.1. The Current Organizational and Institutional Arrangements

The current national organizational and institutional arrangement is composed of internal institutional organizational structures and institutions. There are both public and private organizational structures and institutions. These are civilian or non-civilian organizational structures and institutions. The non-civilian institutions include public safety and security, intelligence and defense institutions.

2.1.1. Civilian Organizational and Institutional Arrangements

The main civilian public institutions include government ministries, departments and agencies and private sector firms and associations.

The public includes Ministry of Work, Transport and Communication, Ministry of Education, Science and Technology, Tanzania Communications Regulatory Authority (TCRA), Tanzania Commission for Science and Technology (COSTECH).

The private cyber security organizational structures and institutions are also sub-divided into civil and non-civilian institutions which include private security companies, Mobile Operators Association of Tanzania (MOAT) and Tanzania Internet Service Providers Association, (TISPA).

2.1.2. Public Safety and Security, Intelligence and Defense Institutions

The main public safety and security, intelligence and defense institutions include Tanzania Police Force, Tanzania People's Defence Force, and Tanzania Intelligence and Security Service.

2.1.2.1 Tanzania Police Force (TPF)

According to the Police Force and Auxiliary Services Act 1995 which is an act to provide for the organization, discipline, powers and duties of the Police Force, a Police Reserve and an Auxiliary Police Force and for related matters. The responsibilities of the Tanzania Police Force are given under Section 5 of the 2002 Act (amendment - Military Police Service Provider) Cap 322. These responsibilities include peace keeping, protecting civilian lives and their properties, detecting crime before being committed, arresting criminals and bringing them to court, and overseeing the implementation of laws and regulations of the country.

Relative to ICT the police force has four sections performing the following main functional objectives and activities in cyber security, cyberspace and cybercrimes; these sections include ICT section which deals with developing ICT technology for internal use and communications; fraud section which deals with internet fraud and money laundering; forensic section which deals with forensic examination of all crime scenes including fingerprint services, examine computers used to undertake crime and assess software and programmes used to conduct a crime; Intelligence section which deals with assessing security of people and property. All these mentioned sections use different approaches and equipments to detect, prevent, and investigate the crimes, these include CCTV cameras for surveillance in sensitive places such as financial and government institutions , fingerprint analysis, DNA profiling and number plate recognition.

The uses of ICT technology within the police forces in Tanzania have increased the performance of the police to solve and prevent crime. This improvement in performance is evidenced by the increase in number of cybercrime identified by police officers from 453 in 2013 to 2962 in 2014 (Crime Statistics Report, 2014); implying that the capacity of police officers to detect the cyber crimes has improved at satisfactory level compared to 2013.

Despite the satisfactory performance of the police force on cybercrime, cyber security and cyberspace still the sector experiences different problems, constraints and challenges which include; technology lag that is the criminals are step ahead technologically and skills compared

to the police officers, hence failure of police force to detect, respond and prevent. The police force also experiences regulatory lag; rate of number of cybercrimes identified and number of cyber crime cases handled is low. This is evidenced by low rate between 2962 which is number of cyber crimes identified in 2014 and 380 number of cyber crimes cases handled (Crime Statistics Report, 2014); implying that time for crime investigation, trial is too long, hence being unable to complete the ongoing cases. The capacity of police officers on ICT technology is not adequate compared to the criminals; entailing that there is low investment in ICT projects and programmes of capacity building in order to improve capacity of police officers in ICT, hence being able to detect, respond and prevent attacks from cyber criminals.

2.1.2.2 Tanzania People's Defence Force

The Tanzania People's Defence Force (TPDF) is the armed forces of Tanzania and was established under the National Defence Act, 1966 and the National Security Act, 1970 of the United Republic of Tanzania. The aim of TPDF is to defend Tanzania and every Tanzanian, especially people and their political ideology. Some of the defence functions of TPDF are to provide aid to the civil power in any case in which a riot or disturbance of the peace beyond the powers of the civil authorities occurs and to exercise in addition to their powers and duties all the powers and duties of Police officers, ensuring a national basis for decision-making through timely surveillance and intelligence gathering to uphold Tanzanian sovereignty, predicting and protecting people against attacks and ensuring national security by effectively using gathered information through various sources such as international security agencies, and national security services.

Cyber security is considered fundamental to the military and economic security of the nation and requires an approach rooted in traditional national security arguments on protection of homeland (Harknett & Stever, 2009; the White House, 2009). Cyber Space is now widely recognized by the military as the 5th operational domain besides land, sea, air and space this has led some county such Norway to have a cyber force which is military branch devoted to cyber warfare, cyber security and counter-cyber warfare that is Norwegian Cyber Defence Force which was established in 2012. In Tanzania People's Defense Forces' ICT is similar to that of Police force, but in TPDF's ICT technology is hooked to military operations through communication, commanding, defending and attacking. The specialized department is responsible for maintaining and stabilize Information and Communication systems of the Army and ensuring that the confidential information are well monitored and protected from hackers ,cyber criminals and any other threats. Improving the ICT means effectively boosting up the performance of the army and national security systems.

The performance of the army is determined at every point in time. From that point of view the army has to be updated than other institution in technology, skills and equipment. Considering the position of Tanzania in militarization level as articulated in Global Militarization Index (GMI 2013) is ranked 120th out of 151 countries; depicting that the country is less equipped and modernized in military apparatus, focusing on military communications using ICT, Tanzania has no military satellite (GMI, 2014), which would maximize payload performance of the army, support legacy ground equipments and minimize impact in incorporating ground infrastructures.

2.1.2.3 Tanzania Intelligence and Security Service

Tanzania Intelligence and Security Service, (TISS) was established by the Tanzania Intelligence and Security Service Act, 1996. The responsibilities of TISS as articulated in the act include; obtaining, correlating, and evaluating intelligence relevant to security. TISS is directed to study an intelligence issue such as what activities terrorist organizations, analysis and information collection on behaviors of individuals and problems associated with national security are done through the use of ICT technologies such as computers. After the information is collected, intelligence analysts pull together the relevant information from all available sources and assess what is happening, why it is happening, what might occur next, and what it means for Tanzania interests.

Given the sensitivity of national security and intelligence information the performance of this institution depends on the use of ICT at efficient levels. Data and information analysis may be correctly undertaken through the use of cyber equipment; hence it is important to protect national cyber security systems in order not to endanger the national security.

With Tanzania experiencing a rising number of militant Islamist attacks that have targeted local police stations, public gatherings, churches, mosques, religious leaders and foreign tourists, as well as popular bars and restaurants, which began in 2012, suggests the need for global, regional and national security strategies. Evidence show that Tanzania's Islamists are increasingly interconnected with similar movements in Somalia and Kenya, particularly al Shabab and its Kenyan offshoot al Hijra, with four acid attacks that have taken place since November 2012 coincide with an increased number of arson attacks and the use of grenades or homemade explosives against similar targets (LeSage, 2014).

These incidences should serve as a wake-up call for Tanzanian security agencies to preempt the emergence of a more significant threat to national security. There are suggestions that Tanzania has proactive and efficient systems compared with other countries in the region. However, these incidences may suggest that our public and national safety and security systems are week and this may be due to weak cyber security systems. The systems are poorly funded, coordinated in obtaining, correlating, analysis and evaluating intelligence information on behaviors of individuals and problems associated with national security which are done through the use of ICT technologies such as computers to ensure the security of the country.

This is because of lack of modern and digitalized ICT related equipment for data and information collection and analysis, showing that there is high probability of TISS to fail to grasp information in prior hence risking the national security. Introduction of cyber as ICT concept on intelligence services requires undertaking capacity building initiatives to equip the intelligence officers in intelligent digitalized world.

2.1.3. Non-state Actors

The Non-State Actors, (NSA) are formal and informal institutes playing an important role in cyber issues related to ICT. These entities participate or act in international relations. They are organizations with sufficient power to influence and cause a change even though they do not belong to any established institution of a state. These actors include Non-governmental

organizations (NGOs), Multinational corporations (MNCs), The International Media, and Transnational Diaspora communities. Examples of these actors include; Mobile Operators Association of Tanzania (MoAT) and Tanzania Internet Service Providers Association (TISPA).

2.1.4. Foreign Institutional Arrangement

The foreign institutional arrangement and institutions include regional and international government ministries, departments, agencies and regulators. At the regional level, Tanzania cooperates with the Communications Regulators' Association for Southern Africa (CRASA), the East African Communications Organizations (EACO), the African Communications Regulatory Network (ACRAN), the Pan African Postal Union (PAPU), the Southern Africa Postal Operators' Association (SAPOA), the Southern Africa Telecommunications Operators' Association (SATA), the Southern Africa Broadcasters' Association (SABA), The African Advanced Level Telecommunications Institute (AFRALTI) and the African Telecommunications Union (ATU).

At the international level, Tanzania cooperates with the International Telecommunication Union (ITU), the Commonwealth Telecommunications Organization (CTO), the Universal Postal Union (UPU) and Conference of Commonwealth Postal Administrations (CCPA), Commonwealth Broadcasting Association (CBA) and Forum for Incident Response and Security Teams (FIRST).

2.2 Performances of the Cyber security Systems in Tanzania

Section 2.2 examines current performance of the cyber security systems in Tanzania using the ITU Global Cyber security Index, (GCI), (GCI, 2015). The GCI is an index which measure the level of readiness in cyber security considering five performance variables or pillars which include; legal, technical, organization, capacity building and cooperation. Considering that Tanzania is an active member of ITU thus can be assessed using these performance criteria.

Table 1: Global Comparison of Tanzania Position in Cyber security in the World

Country	Legal	Technical	Organizational	Capacity Building	Cooperation	Index	Regional Rank	Global Rank
Tanzania	0.5000	0.3333	0.0000	0.1250	0.2500	0.2059	11/18	22/29
Kenya	1.0000	0.3333	0.2500	0.2500	0.5000	0.4118	5/18	15/29
Uganda	0.7500	0.5000	0.8750	0.2500	0.5000	0.5588	2/18	10/29
Rwanda	1.0000	0.5000	0.5000	0.3750	0.5000	0.5294	3/18	11/29
Burundi	0.2500	0.0000	0.1250	0.1250	0.1250	0.1176	14/18	25/29
S. Africa	0.2500	0.5000	0.6250	0.2500	0.2500	0.3824	6/18	16/29
USA	1.0000	0.8333	0.8750	1.0000	0.5000	0.8235	1/18	1/29

Source: Global Cyber Security Index, 2015

2.2.1 Legal Measure

Legal measure includes on how criminal activities committed over ICTs could be dealt with through legislation in an internationally compatible manner. Tanzania is 50% prepared in terms

of legal measures to deal with cyber security matters, it is satisfactory level. This is due to two enacted laws which include Cybercrime Act of the 2015 and Electronic transaction Act of the 2015; implying that Tanzania is prepared though still much effort is quickly needed to complete once compared to Kenya, Rwanda and USA which have all three laws of cybercrime, electronic transaction and data protection score of 100% due to complete set of legal measures required; meaning that their position on legal measure in cyber security is at perfect level. In Tanzania this level is projected to increase above 70% once the data protection law will be completed; which will be at satisfactory state.

Recent reports detail a breathtaking and unrelenting rise in cyber breaches, with five malware events occurring every second, and 60% of successful attackers able to compromise an organization within minutes. But the law has not kept pace with technological innovation. There is no single uniform law protecting individual privacy, nor one that governs all of a company's obligations or liabilities regarding data security and privacy. (The Cyber security Law Report, 2015).Tanzania does not have specific legislations dealing with cyber security (ITU Cyber Security Country Report-Tanzania). Currently the laws which are in place are; Cybercrime Act, Electronic transaction Act enacted in 2015 and Data protection Act still in progress. The role of the cyber security law is to smooth the implementation of cyber security policy, mutual combination of the cybercrime, electronic transaction, and data protection Acts as well as cyber security laws will nourish the performance of ICT sector.

2.2.2 Technical and Procedural Structure

The technical and procedural structure focuses on key measures for addressing vulnerabilities in software products, including accreditation schemes, protocols and standards. Under this pillar Tanzania has 33% level of readiness in cyber security which is influenced by the establishment of CERT (not sure of what it means, more elaboration is needed here). This is not satisfactory hence more effort is required. While the absence of national (and sector specific) cyber security frameworks for the certification and accreditation of national agencies and public sector professionals thus lag behind compared to Uganda, Rwanda and South Africa which are 50% prepared, which is at satisfactory state once compared with other countries in Africa. Tanzanian score is expected to rise if the government will formulate cyber security frameworks for the certification and accreditation of national agencies and public sector professionals.

2.2.3 Organization Measures

The organization measure includes generic frameworks and response strategies for the prevention, detection, response to and crisis management of cyber attacks, including the protection of countries 'critical information infrastructure systems. Tanzania has about 0% suggesting that the country is less prepared in terms of strategies for prevention, detection, response and crisis management of cyber attacks. This implies that less effort has been employed in establishment of required organizations as well as policy formulation and implementation strategies.

2.2.4 Capacity Building Measure

Capacity building elaborates strategies for capacity-building mechanisms to raise awareness, transfer know-how and boost cyber security on the national policy agenda. It includes standardization development, manpower development, professional certification and agency

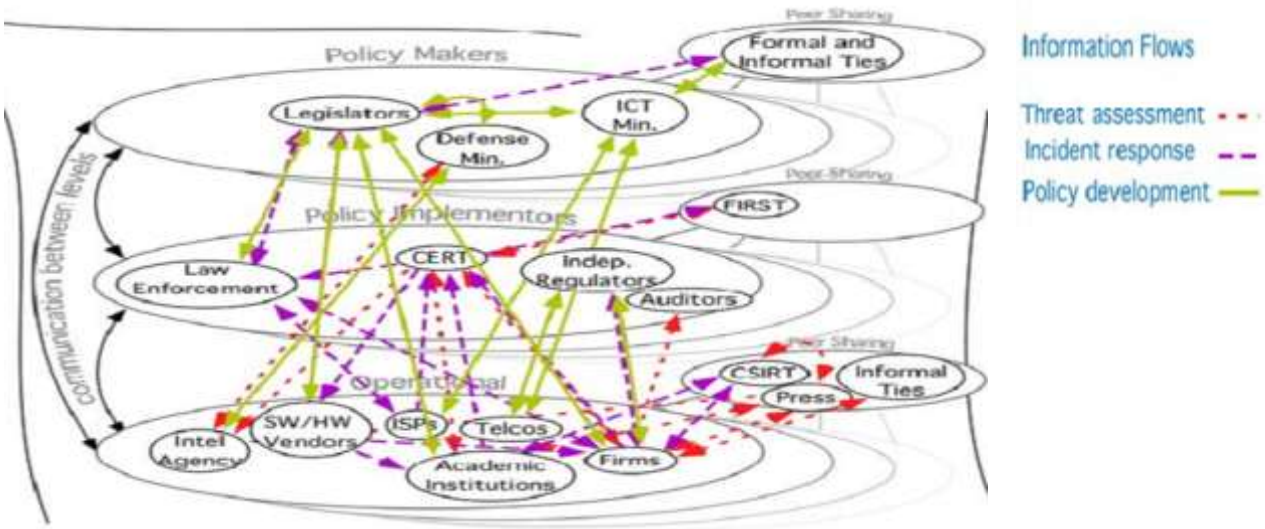
certification. Tanzania is 12.5% in undertaking different initiatives of capacity building related to cyber security. This rate is not satisfactory. This entails that the human resources employed in cyber security institutions are less skilled and thus less investment initiatives have been undertaken to raise the skills and knowledge of these individuals on cyber security, cybercrime and cyberspace.

Table 1 suggests that capacity building readiness in East African countries is unsatisfactory with only Rwanda having 37% level of preparedness meaning that they have less employed resources in terms of investment, research and development (R&D) and capacity building initiatives. To raise the percentage requires different R&D programs/projects, and recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cyber security courses in higher education and promoting certification of professionals in either the public or the private sectors.

2.2.5 Cooperation Measure

Cooperation pillar is sub-divide into two components which include (a) intra-state cooperation; facilitating sharing of cyber security assets across borders or with other nation states and (b) Intra-agency cooperation sharing information between agencies with other countries. Compared with Uganda, Kenya and Rwanda which are 50% collaborative; this score is satisfactory while Tanzania is only 25%, which is less significant and unsatisfactory; implying that despite the country being friendly with other countries still high commitment is required to have security collaborative relationship with other countries instead of political relationship only. Problems facing cyber security in Tanzania according to the GCI table can be categorized in two main parts; Secondary problems which is digital divide and the primary problems.

Figure 1: Global Cyber security Institutional Framework Model



Source: ITU (2007)

2.3. Major Constraints, Problems and Challenges of Cyber security

Section 2.3 identifies major primary problems, constraints and challenges affecting performances of cyber security systems in Tanzania.

2.3.1. Lack of Explicit National Cyber Security Policy

Tanzania does have an explicit national cyber security policy and strategy. The National Cyber Security Policy will provide framework for protecting the public and private infrastructure from cyber-attacks. It intends to safeguard information, such as personal information (of web users), financial and banking information and sovereign data. The cyber security policy translates what is understood about the risks and their impact into security measures for implementation. It facilitates both prevention and remedial action in response to security problems, and helps to reduce the risks and their impact (ITU, 2007). The effective cyber security policy is characterized by the following attributes; the resources, structure, procedures, and plans for defence and mitigation to ensure that operational, technological and information risks can be controlled *(ibid).* Absence of the cyber security policy risks the public and private infrastructure through cyber-attacks; hence Tanzania requires effective policy to ensure the public and private infrastructures' safety.

2.3.2. Many legally independent institutions with different laws, regulations and interests

Figure 1 suggests that there are many independent institutions. The multiplicity of these many institutions include; government ministries, departments, agencies, private firms and associations, civil society organizations. Each of these agents has their own established acts and operates as independent institutes. Public institutions are focused with public interests which are to maximize public social, political and economic welfare interests while private institutions are focused with profit maximization, in many times with conflicting of interests causing complexities of the cyber security matters. This may results to high probability of inefficiency due to absence of common goals and lack of legal relationships among the institutions.

2.3.3. Top Leadership system is not well defined

Figure 1 shows many and multiple leadership structures. There are many bosses and no formal top leadership system. Each institution has its internal leadership system in terms of decision-making on cyber security matters. There is absence of legal power for one top leader to question others on cyber security matters. There is no formal accountability system between and among these institutions.

This may lead to institutional ineffectiveness in execution of cyber security actions. The leadership in each institution has no clear national vision of what they need to do to attain an active defence in the long run and for the interest of the nation. The current status of the leadership focuses more on the internal organization reputation instead of national interest and this has direct risk and thus cost of cyber threat to the nation.

2.3.4. Lack of Formal Institutional Linkage

There are no laws and or policies which clearly formalize the relationship between and among these cyber security institutions. There are ad-hoc and informal relations which are based on practices, experience, leadership and friendships among these institutions. The absence of formal rules of engagement causes failures to identify who is responsible, at what time and what is next. This results to losses of time, wasteful resources, inefficiencies and delays on crucial matters of cyber security. For example, there is no common understanding on how to undertake the legal

investigations and procedures from the whole process of detection, responding and prevention. Absence of formal institutional linkage arises from differences on establishment laws of institutions which articulate the functional objectives of these institutions while ignoring the integrated cyber security systems.

2.3.5. Inadequate Resources in Each Institution

The concept of resources includes human capital, modern equipments and financial resources. Many of the human resources in cyber security system in Tanzania have no adequate skills from both theoretical and practical dimensions. These institutions are unable to catch-up with the technological pace. Moreover, the absence of capacity building initiatives has increased the incapability to handle cyber matters. Thus high investment is required to improve the capacity of these individuals on cyber security processes. Technology is facilitated with modern equipment which facilitates the whole processes in security matters. While developed countries are characterized with new modern technology, Tanzania has old technology communication vintage and has analogy systems to handle cyber security matters. The country has no potential information system for data recording and micro assessment and tracking. The country has limited financial resources for cyberspace investments. Small budgets for R&D, S&T and ICT uses, undermines the institutional capacities of these institution.

2.3.5. Lack of Institutional Dynamism

The absence of ability to transmit once a variation has occurred in the world, creating the ungoverned space, this reduces ability to raise creativity within cyber security systems. In Tanzania policy, laws and institutions fail to identify how to rectify equilibrium once changes have occurred causing imbalances in the performance. Considering that each institution experiences different constraints, thus absence of system dynamism causes failure to predict and project the revolutionary changes in different aspects. For example Police force still operates with analogy system while TCRA has shifted to digital system; this shift causes ineffectiveness within a system due to the fact that Police force will lag behind while TCRA is quickly catching up with a pace. Today's threats are not the same as tomorrow's threat, hence it is potential to adopt dynamism behavior so that to withhold with changes in the world. In peace time is optimal to prepare for attacks, develop and testing technologies and observe the perfection by comparing them to obtain the best to maximize possibility for security and defence.

2.3.6. Digital Divide

Section 2.3 suggests that there is a big gap of knowledge economy termed as 'digital divide' between Tanzania (the developing nation) and the USA (developed world). The digital divide is found to be evident in the national defence, security, safety and intelligence systems. This is characterized by poor data and information management; lack of timely and accurate information; delays in receiving and processing vital data; delays in receiving, processing and dispatching files. There are physical constraints of place and storage to maintain manual records (backup); and, lack of an integrated national defence, security, safety and intelligence management system.

Understanding this fact of the digital divide is very important due to the fact that it provides the relationship of technology accessibility and population, since cyber threats occur through the

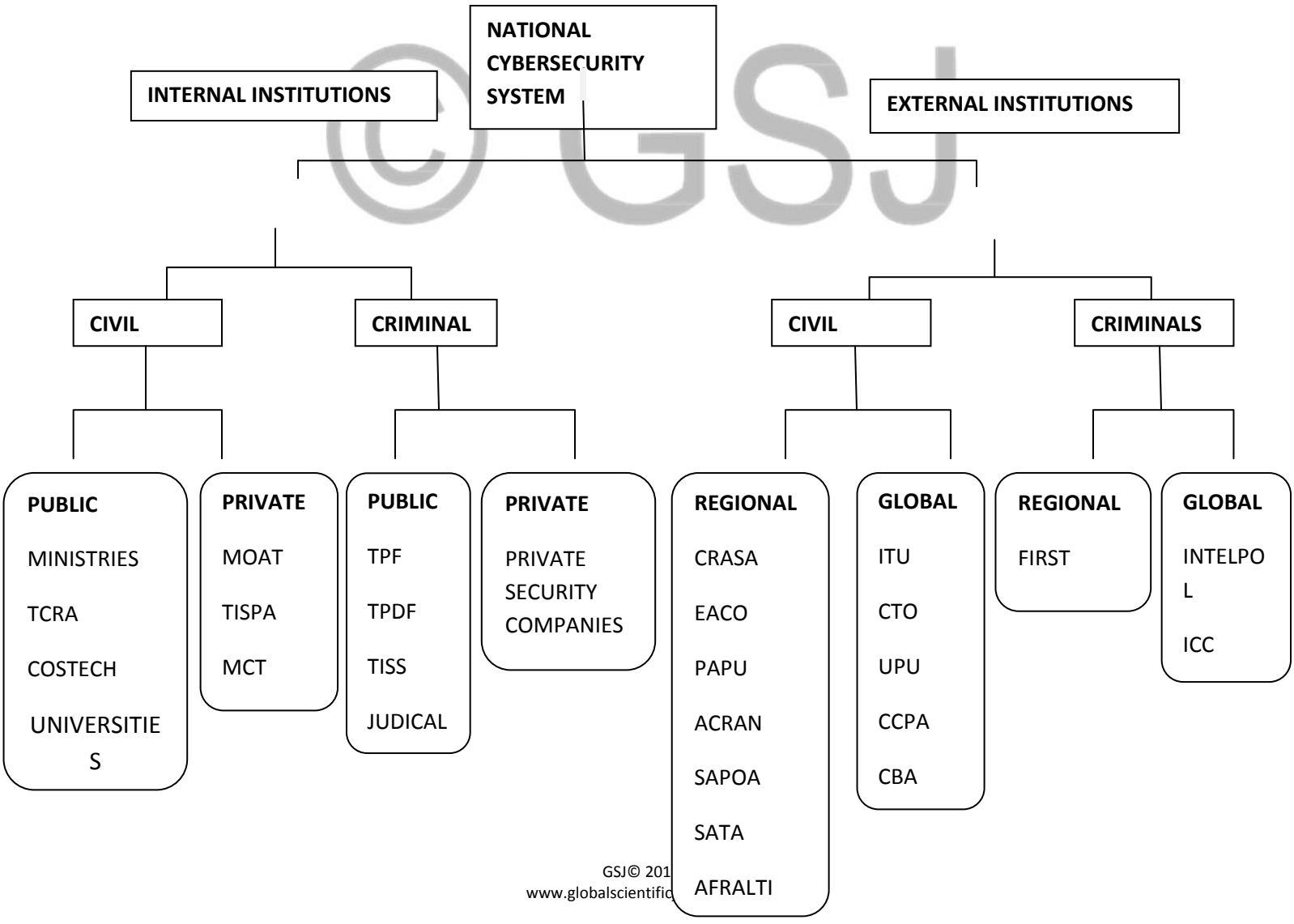
internet and other communication facilities. Thus it is necessary to identify the magnitude of effects in terms of number of people affected and technology used.

Section 2.3 suggests clearly on where and how far Tanzania is. Tanzania requires huge step-up in ICT accessibility and advancement. The dangers posed by the digital divide, and the risk of being excluded further from the knowledge economy and social development, is now propelling the government to put in place a cyber security policy framework through which coordinating mechanisms and harmonized strategies might be nurtured.

2.4 Desired System of Cyber security In Tanzania

Section 2.4 proposes principle elements and characteristics of desired systems of cyber security in Tanzania. The desired system has to be composed of policy, legal and institutional frameworks for effective cyber security system. The institutional system has to be based on legal and regulatory framework with clear vision and mission stipulated in a cyber security policy. The system has to identify top leaders and division of activities and specialization on carrying out different roles and duties.

Figure 2 Desired Cyber Security Systems in Tanzania



This paper proposes a desired model for cyber security systems in Tanzania, showing the participation of both private and public institutions, from the ministerial level to civilian level as a participatory approach in implementing the cyber security policy in Tanzania. The desired system is characterized by open, top-down and bottom-up multi-institutional, Coordination character as well as, dynamic behaviour which provide a strong assurance on handling the cyber security problems.

2.4.1 Effective Top-Down and Bottom-Up Multi-Institutional Framework

New ways of providing the nation in a top-down and bottom-up multi-institutional framework have to attach importance to greater participation, transparency, accountability, good governance and the rule of law. The cyber security system has to have enhanced shared functional objectives, responsibilities and co-ordination of multi-institutional framework.

2.4.2 Effective Institutional Linkage, Coordination and Relationships

It is acknowledged that an effective and well-coordinated organizational institutional framework is one of the important factors that determine the mode of operation of all stakeholders that will be involved in the cyber security system. There are several national, regional and international stakeholders, who are important in enhancing and maintaining institutional linkages, close collaboration, relationships and therefore promoting the growth of sustainable cyber security services. The government has to intensify the established formal institutional relationships with other regional and global authorities, public and private companies in order to mobilize human, financial, capital and information technology resources.

2.4.3 Dynamic Institutional Framework

A smooth implementation of the cyber security policy requires new ways of doing things, innovative and far reaching dynamic adjustments to institutional and administrative set-up, regulations and procedures of the government. The government, the President's Office shall foster secured system-wide policy coherence and reinforcing the co-ordination and direction functions of the Ministry of Science, Technology and Communication and put up a well elaborative, flexible, modern and an innovative dynamic institutional framework.

2.4.4 Implement various crosscutting and sector specific policy reforms and processes;

The government in collaboration with other stakeholders will implement various crosscutting and sector specific policy reforms and processes, in order to improve performance and optimal cyberspace and cyber security delivery. The country shall [1] ensure that cyber security policy implementation processes and institutional settings are appropriately harmonized, integrated, sequenced and properly timed in order to provide adequate linkages and synergies with other social economic and political systems; [2] design and provide an institutional framework on how cyber security strategy should be delivered to ensure that they do not undermine government machinery and systems, they are mainstreamed, consistent, sustainable and efficient; [3] have a well centralized, efficient and accountable institutional framework for effective management and coordination.

3.0 Conclusion

3.1 Main Findings

Cyber security threats propagating through the transnational, globally interconnected cyberspace are difficult to manage with conventional state instruments. While states are still struggling to understand and define their interests in the cyber domain, policy makers are modeling this situation to attain optimal systems of cyber security to focus on crimes and ungoverned space. Cyber security has quickly evolved from a technical discipline to a strategic concept; globalization and internet give nations and individuals incredible new power, based on constantly developing networking technology.

The cyber security institutional framework system from the GCA model lacks a well-defined leadership system, formal institutional linkage, resources and institutional dynamism. This resulted to decrease in efficiency and performance in cyber security systems Tanzania in terms of legal measures, technical and procedural structure, organization measures, capacity building and cooperation.

From the GCI of ITU the score on each pillar is not satisfactory though not at worse state, but once averaging to obtain the average percentage Tanzania has 20.59% degree of preparedness in cyber security; implying that the whole system is at worse state once compared with other countries such as Uganda which is 55.9% degree of preparedness in cyber security; meaning that the whole system is ready for cyber threat and cybercrime by 55.9% which is satisfactory. From that point of view it's clear that cyber security system preparedness does not depend on the level economic growth, though developed countries are at high position on preparedness in cyber security matters compared to developing countries. For example USA has a score of 82.4% while Tanzania has 20.59%, implying that there is a gap between the developed countries and developing countries in terms of accessing to modern ICT. This concept is what is referred as Digital Divide.

Problems facing the cyber security institutions in Tanzania are many and simple to handle if the country would have a desired cyber security system, modern technology and equipped human resources, while problems facing the developed countries are complex such espionage, the complexity arises not because of system or modern technology instead of the complexity nature of cyberspace. Cyber security systems in developing countries are at pre-mature stage hence being unable to pace with changes in technology, for example Tanzania has no cyber security policy, cyber security laws while having unsatisfactory institutional framework, comparing with developed countries which are characterized by professional stage of cyber security system accompanied modern and advanced technology.

3.2 Policy Recommendations

Specialization is highly required by dividing the institutions into identifying, protecting, detecting, responding and recovering units. These divisions will increase efficiency of the system

and support Top-Down and Bottom-Up Multi-Institutional Framework, and dynamism of the cyber security systems in Tanzania.

Participatory approach through formal linkage among institutions is of crucial concern towards efficient running of cyber security system. There should be a formal linkage between institutions due to the fact that the cyber insecurity effects hurt individual to national levels at large extent. Cyber security policy and laws are highly recommended in order to raise the effective performance of the system by providing guidance and implementation strategies and regulation on how to achieve the desired cyber security system hence raising the position in regional and international standards.

Capacity building initiatives are highly demanded in order to improve the skills and ability of the human resource in their specialized cyber security processes. R&D in universities and colleges are highly motivated as a strategy to explore the cyberspace and thus to identify the gaps facing the ICT sector. Raising the usefulness of research results there should be a collaborative behaviour between the research institutions, policy makers, implementers and operational.

3.3 The Way forward

Notwithstanding the magnitude of the limitations, constraints and challenge, however, we urge that given the current situation of cyber security in Tanzania there is an immediate need of formulation of national cyber security policy, (NCP), cyber security laws and cyber security institutional framework. To support the desired system immediately the government has to formulate implementation strategy of the NCP policy as well as the institutions and regulations to smooth performance and interaction among the current cyber security systems.

Nevertheless, for the nation to have an effective policy and implementation strategy there is a need of conducting an intensive policy study and research on cyber security, to review and provide analysis of the institutional framework both at national and international levels, in order to understand all the dimensions of the attacks in depth.

Cyber security with its complexities has proven difficult due to its nature. Extending awareness to Tanzanian community is a critical step towards creating a trustworthy environment for people and the nation at large.

References

[1] Bruce Schneier (2003) Beyond Fear, Thinking Sensibly About Security in an Uncertain World, Copernicus Books, ISBN 0-387-02620-7

[2] Bruce Schneier (2000) Secrets and Lies: Digital Security in a Networked World, Wiley, ISBN 0-471-25311-1

[3] Ellefsen, I., and Von Solms, S. (2010). *Critical information infrastructure protection in developing world*

[4] Gallaher, M.P., Link, A.N., & Rowe, B. (2008) Cyber Security: Economic Strategies and Public Policy Alternatives. *Cheltenham, UK, Northampton, MA: Edward Elgar Publishing*

[5] Ghulam Muhammad Kundi and Allah Nawaz (2014) Digital Revolution, Cyber-Crimes and Cyber Legislation: A Challenge to Governments in Developing Countries; *Journal of Information Engineering and Applications Vol.4, No.4,*

[6] Global Militarization Indices, 2013 & 2014

[7] Halder and Jaishankar (2011) *Cybercrime and the Victimization of Women: Laws, Rights, and Regulations.* Hershey, PA, USA

[8] Hammond and Allen (2001) The 2001 council of European convention on cybercrime, In an E_cient Tool to Fight Crimes in Cyber-Space? June, 2001

[9] ISSEU (2014) *Cyber capacity building as a development issue: What role for regional organizations?*

[10] ITU, (2007) *Cyber security guide for developing countries*

[11] ITU, (2015) *Global Cyber security Index and Cyber wellness Profile*

[12] Joseph S. Nye, Jr., (2014) "The Regime Complex for Managing Global Cyber Activities," in Paper Series (London: Global Commission on Internet Governance (CIGI) and Chatham House, p. 12

[13] Keith Krause and Jennifer Milliken, (2009) "Introduction: The Challenge of Non-State Armed Groups," Contemporary Security Policy, Vol. 30, No. 2, p. 202.

[14] Paulson LD. Spam hits instant messaging. Computer and Internet Security, 37 no 4:18, 2004

[15] Pawlak, P. (ed.) (2014) *Riding the digital wave: The impact of cyber capacity building on human development, ISSUE, report number 21*

[16] Van J Garcia F, Hoepman J and Nieuwenhuizen J. (2004) Proceedings of 19th International Information Security Conference, wcc2004-sec, Toulouse, France. In Spam analysis, Kluwer Academic Publishers

[17] Wolfgang Röhrig and Rob Smeaton (2014) EU Cyber Security Review Summer Cyber Security and Cyber Defence in The European Union Opportunities, Synergies and Challenges