Arts and Social Sciences Journal
ISSN: 2151-6200

Asongwe, Arts Social Sci J 2019, 10:2
DOI: 10.4172/2151-6200.1000440

Review Article Open Access

Government Leadership and the Protection of Critical Information Infrastructures: Social Security a Critical Analysis of Cameroon's Cyber Code

Asongwe P*

Faculty of Laws and Political Sciences, University of Yaounde, 11 Soa, Cameroon

Abstract

The Protection of critical information infrastructures from cyber-attacks is becoming an acute problem for Cameroon. Cyber security has turned into a national policy priority while National cyber security strategies seek to drive economic and social prosperity and protect cyberspace-reliant societies against cyber-threats. This is why, in order to cope with this policy problem, the government must lead. Empirical findings and expert consultation/observation reveal that Government leadership is inhibited by the constant evolving and cross-border nature of cyber-attacks. Against this backdrops, this paper recommends a flexible, multifaceted and holistic leadership approach that ensures information sharing, collaboration amongst stakeholders and international cooperation.

Keywords: Cameroon; Cyber attacks; Critical information infrastructure protection; Leadership; Cyber code

Introduction

Since the security [1] of digital data, computers, digital communication technologies and information networks now have an overwhelming influence on almost all aspects of life and society, their security is an important aspect in Cameroons digital economy. By developing an effective leadership skills, an environment can be created where persons and businesses can continue to operate in the long term. Accordingly, implementing and sustaining effective and efficient leadership can contribute significantly to the achievement of secured and resilient critical information infrastructure [2].

It should however be noted that a legal framework on network security in the Sub-Saharan region was not a primary concern in the early days of networking protocol design, as leading computer scientists were more focused on developing the underlying building blocks than they were on developing inherent security controls [3]. This explains why earlier ICTs-related legislation in most countries of the sub-region including Cameroon had no provisions on network security [4]. Decades later, Cameroon's cyberspace is plagued with a growing list of vulnerabilities [5] that can be, and often are, easily exploited by cyber criminals, Malicious cyber activity is a security challenge for all Cameroonians. Cameroonians organisations across the public and private sectors have been compromised by state-sponsored or non state actors. Overseas, large multinational companies and government organisations have been targeted, losing substantial amounts of sensitive commercial and personal information or incurring major damage to their business and reputation. These abuses in the country's cyber space has become an undisputable threat to citizens' lives and businesses calls for leading to a need to redefined traditional notions of prevention [6].

In order to ensure that the country continues to enjoy the benefits that ICTs bring, vulnerabilities and risks have to be managed, to some extent or other, through the cyber security efforts of the stakeholders that own, develop, operate and use networks [7]. These stakeholders include government, business, private sector organisations and individual users. Such strategy should include the protection of critical information infrastructure as a permanent part of the government's structures and programmes, and ensure that clear responsibilities and goals exist within the government and the private sector in Cyber threats [8] and data breaches like skimming, insider threats, corruption of sensitive data, and critical infrastructure disruptions are ranked as the top threats to business continuity for companies [9]. Ever-increasing sophistication of threats, combined with expanded responsibilities for cyber professionals, mean there is the need to innovate rapidly to stay ahead of the curve. Being a cyber security [10] leader now means coping with a growing role, facing new demands of visibility into our operations, new expectations for information and privacy protection. The Government has a duty to protect the nation from cyber attacks and to ensure that all interests are defended [11]. Accordingly the paper appraises state leadership in the protection of Critical Information Infrastructures CIIP [12] under Cameroon Cyber Code [13].

The Concept of Leadership in CIIP under Cameroonian Law

Leadership relates to the art of, pursuing and motivating a group of people to act towards achieving a common goal, and comprises the principle, rule, or law designed to control or govern conduct. The provision emphasises the need for the government to ensure a permanent place for cybercrime prevention exclusively and through representation by government institutions in its structures and programmes. Thus Leadership in the protection of Cameroon's cyber space is exercised either exclusively by the state or by state institutions that represent the state.

The Cyber code does not expressly use the word Leadership. However Section 6 provides that laws and regulations on electronic communications; and the management of national frequency spectrum and orbital locations shall be under the exclusive domain of the State

***Corresponding author:** Asongwe P, Lecturer, Faculty of Laws and Political Sciences, University of Yaounde, 11 Soa, Cameroon, Tel: +237242322132; E-mail: kehbuma@gmail.com

Received March 06, 2019; **Accepted** March 15, 2019; **Published** March 22, 2019

Citation: Asongwe P (2019) Government Leadership and the Protection of Critical Information Infrastructures: Social Security a Critical Analysis of Cameroon's Cyber Code. Arts Social Sci J 10: 440. doi: 10.4172/2151-6200.1000440

and shall not be subject to concession [14]. The section further provides that activities such as the construction and operation, nationwide, of submarine cable landing points; the construction and operation of teleports to one or more satellite networks and the establishment and operation of multiplex and broadcast networks shall be within the exclusive domain of the State and may be the subject of concession to one or more corporate bodies governed by public or private law under the conditions set forth in Section 9 below [15].

Categories of Leadership under Cameroon's Cyber Code

The law provides for a permanent central authority, a cyber security plan with clear priorities and targets, Coordination and partnership between government agencies and private sector The rest of the of the article examines the leadership [16].

State's exclusive domain (Direct leadership) in protection of information and network infrastructure

This deals with acts that are under the exclusive domain of the state.

To a large extent, only national governments are in a position to lead national cyber security efforts that involve all national stakeholders.

Section 6 new (1) of the Cyber code empowers the state to enact laws and regulations on electronic communications and manage the national frequency spectrum and orbital locations.

Accordingly, only when the government establishes common objectives, define ways to achieve them and clarify the roles and responsibilities of stakeholders can cybercrime prevention be comprehensively addressed.

In addition to putting in place substantive measures to counter cyber security threats, the government has the central task of establishing, among all stakeholders, a common awareness and understanding of cyber security as well as a common recognition of each stakeholder's roles and responsibilities The purpose of this provision is to establish an exclusive leadership and to create and maintain an institutional framework for CIIP. It is the responsibility of the government to create, maintain and promote a context within which relevant governmental institutions and all segments of civil society, including the corporate sector, can better play their part in the protection of information and critical infrastructures. Hence the Presidency of the Republic plays a determinant role since it defines and lays down guidelines for the national ICT policy.

The Prime Ministers' Office is responsible for monitoring, that is, ensuring that the national ICT policy is effectively implemented [17]. The ideas that underpin this Strategy were drawn from a classified Cyber Security Review led by the Department of the Prime Minister and Cabinet. The Department, through the new position of a Special Adviser on Cyber Security, will lead implementation of this Strategy for the Government, in its central responsibility for cyber security policy. Assembly also plays a vital role in national policy implementation. Its role is mainly legislative, since it is responsible for voting ICT related laws.

Representative leadership

Importance of representative leadership: The institutional organisation and coordination of government institutions in CIIP is a vital element of a successful cyber security effort. In the context of the role and responsibility of government, representative leadership typically involves the organisation and coordination of cyber security roles and responsibilities among appropriate government institutions in order to carry out the actions that are required to meet cyber security objectives. In this light representative leadership plays a large role not only in the implementation of cyber security safeguards but also in policy-making and coordination.

Government institution are well placed to address the wide-ranging causes of cyber threats and to draw upon the skills, expertise, resources and responsibilities necessary to address those causes; the practical application of research and evaluation findings in the development and implementation of measures to reduce crime, targeted to areas of the greatest need and adapted to suit local conditions; a focus on outcomes and a commitment to demonstrating measurable results through evaluation and performance measurement, with clear lines of accountability; building and maintaining the capacity to implement effective crime prevention policies and interventions; promoting an active and engaged community, and being responsive to the diversity and changing nature of communities; long-term commitment to achieving sustainable reductions in crime and savings to the criminal justice system and the community; and coordination across sectors.

Ensuring that the state has the appropriate resourcing for the roles and responsibilities it intends to carry out in the field of cyber security is another key prerequisite [18].

Thus section 34 new (4) provides that the resources of the Special Telecommunications fund shall be collected by the Board referred to in section 36 below and deposited in an account opened for that, purpose in the financial institution approved by COBAC.

(8) A decree of the President of the Republic shall determine the conditions of management of the Special Telecommunications Fund.

Because of the cross-sector nature of cyber security, it necessarily means that various key elements of an overall cyber security policy will be implemented in practice through a very diverse set of institutional arrangements at different stages of development will have differing perspectives on the overall vulnerability of their own critical information infrastructure. They are likely to be at different stages of institutional development.

Government institutions and CIIP in Cameroon: Although institutions like the Ministries of Post and Telecommunication, Justice, Trade and Commerce, Communication and Finance are involved or will be involved in the development, deployment and exploitation of ICTs at various levels and will have to work in collaboration with institutions having the technical knowhow to introduce an enabling mechanism and environment for e-administration, government institutions like the National Agency For Communication Technologies (NAICT) [19] and the Telecommunication Regulatory Board (TRB) [20] will play a decisive role in the coordination and implementation in the protection of information and critical networks from cyber-attacks and are dedicated institutions in the protection of Cameroon's cyber space.

***National agency for information and communication technologies (NAICT)*:** Decree No. 2002/92 of 8 April 2002 set up the Agency in 2002. Its duty is to promote and monitor government action in the area of information and communication technologies. In this respect, as part of its guidance and regulation missions, NAICT is responsible for:

- Formulating and monitoring the implementation of the ICT national development strategy;

- Ensuring the harmonisation of technical standards, proposing technical references in order to facilitate interoperability among information systems and regulating the sector;

- Providing expertise to government services for the design and development of their technical projects;

- Coordinating the establishment and monitoring of Internet, Intranet and Extranet sites for the State and public bodies;

- Contributing to the technical training of trainers for universities, high schools, colleges, teacher training colleges and primary schools;

- Participating in the training of State personnel in ICTs by making recommendations on the content of technical training courses and on the programmes of professional and competitive examinations.

Accordingly, NAICT is mainly responsible for guidance, regulation, monitoring and coordination of activities in the ICT sector.

More specifically, NAICT will be responsible for:

- Formulating and monitoring the implementation of the national ICT development strategy;

- Ensuring the harmonisation of technical standards, proposing technical references in order to facilitate interoperability among information systems and regulating the sector

- Providing expertise to government services for the design and development of their technical projects;

- Coordinating the establishment and monitoring of Internet sites for the State and public institutions;

- Contributing to the technical training of trainers of State personnel in the ICT domain by making recommendations on the content of technical training courses and on the programmes of professional and competitive examinations [21].

Telecommunications regulatory board: The Telecommunications Regulatory Board (TRB) is instituted by the Law of 2010/013 of 21 December 2010 regulating electronic communications in Cameroon. It is a public administrative institution with a legal personality and financial autonomy, whose organisation and functioning are defined by the provisions of Decree No2012/203 of 20 April 2012 defining the organisation and the functioning of the Telecommunications Regulatory Board (TRB). It ensures on account of the State, the regulation, control and follow-up of the activities of operators in the sector of Telecommunications and Communications Information Technologies. It equally ensures the respect of the principle of equal treatment of users in all electronic communications companies. The TRB is placed under the technical supervision of the Ministry of Telecommunications and under financial supervision of the Ministry of Finances. The Telecommunications Regulatory Board, (hereinafter referred to as "the Board"), regulates, controls and monitors the activities of electronic communications operators and service providers [22].

Accordingly, the Board:

- Ensures the application of laws and regulations regarding electronic communications and information and communication technologies;

- Ensures access to networks to the public is provided under objective, transparent and non-discriminatory conditions.

- Guarantees healthy and fair competition in the telecommunications and information and communication technologies sector;

- Sanctions the breach of obligation and anti-competitive practices by operators;

- Defines the principles governing the pricing of services provided;

- Examines applications for licenses and prepare the decision relating thereto;

- Formally issue declaration receipts;

- Defines the conditions and obligations for interconnection and sharing of infrastructure;

- Gives an opinion an all draft legislature or regulatory in treatment on electronic communications;

- Ensures the assignment and control of the frequency spectrum;

- Prepares tender documents for concessions and licences:

- Draws up and manage the numbering plan;

- Submits to Government any proposal and recommendation aimed at developing and modernizing the telecommunication and information and communication technology sector.

- Allocates addressing resources; -

- Examines files for the approval of terminal equipment and prepare decisions relating thereto;

- Issues authorizations;

- Ensures consumer protection;

- Carries out any other general interest mission that may be assigned to it by the Government in the telecommunication ad information and communication technology sector;

(3) The organization and functioning of the Board shall be laid down by a decree of the President of the Republic. The Board shall, under objective, transparent and non-discriminatory conditions, allocate addresses, prefixes and numbers to users who apply for them against a fee to be determined by joint order of the minister in charge of telecommunications and the minister in charge of finance [23].

The conditions for renting, or using the prefixes, numbers or groups of numbers shall be laid down in the management rules adopted by the Agency and, where necessary, in the specifications of operators [24].

Accordingly, government institutions play a large role not only in the implementation of cyber security safeguards but also in policy-making and coordination.

Objectives and Components Leadership in CIIP under the Cyber Code

General objective

The general objective of state's leadership in the protection of the country's cyber space is "To take all necessary measures to ensure the protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or distraction through coherent coordination, synergy and raising information security awareness among all stakeholders." Specifically the Cyber Code provides for the regulatory and institutional framework to;

- Provide strategic leadership and coherence to respond to cyber security threats against the identified critical information infrastructure.
- Coordinate, share, monitor, collect, analyse and forecast, national level threat to CII for policy guidance, expertise

sharing and situational awareness for early warning or alerts. The basic responsibility for protecting CII system shall lie with the agency running that CII.

- Assisting in the development of appropriate plans, adoption of standards, sharing of best practices and refinement of procurement processes in respect of protection of Critical Information Infrastructure.
- Undertaking research and development and allied activities, providing funding (including grants-in-aid) for creating, collaborating and development of innovative future technology for developing and enabling the growth of skills, working closely with wider public sector industries, academia et al and with international partners for protection of Critical Information Infrastructure.
- Developing or organising training and awareness programs as also nurturing and development of audit and certification agencies for protection of Critical Information Infrastructure.
- Developing and executing national and international cooperation strategies for protection of Critical Information Infrastructure.
- Issuing guidelines, advisories and vulnerability or audit notes etc. relating to protection of critical information infrastructure and practices, procedures, prevention and response in consultation with the stake holders, in close coordination with Indian Computer Emergency Response Team and other organisations working in the field or related fields.
- Exchanging cyber incidents and other information relating to attacks and vulnerabilities with Computer Emergency Response Team and other concerned organisations in the field.

All this can be achieved through regulation, monitoring and certification.

Components of leadership

Regulation under the cyber code: Regulation is a rule of order having the force of law, prescribed by a superior or competent authority, relating to the actions of those under the authority's control, and are issued by government departments and agencies to carry out the intent of legislation [25].

Regulation can be in the form of statute; rules and administrative codes issued by governmental agencies at all levels, municipal, county, state. Although they are not laws, regulations have the force of law, since they are adopted under authority granted by statutes, and often include penalties for violations. This mechanism is further complemented by soft law instruments that include recommendations relevant to the telecoms sector and which are indispensable for the security of network infrastructure. These measures are the subject of a specific communication strategy targeting the various categories of institutional and non-institutional stakeholders, including by means of public consultations [26].

By virtue of this law, the following activities are regulated;

- The setting up and exploitation of infrastructure to issue preserve and deliver qualified electronic certificates;-the provision of public keys to all public users;

-The provision of security auditing, security programmes editing, and other authorised security services to the public.

- The setting up and exploitation of infrastructure to issue, preserve and deliver qualified electronic certificate.

Firstly the provisions on electronic communications networks and services contains provisions on security and integrity, in particular to strengthen operators' obligations to ensure that appropriate measures are taken to meet identified risks, guarantee the continuity of supply of services and notify security breaches. The objective here is: to allow efficient and innovative network operators and service providers to benefit from relevant economies of scale; to enable all citizens and businesses to be connected and effectively protected; to ensure a level playing field for all market players and consistent application of the rules; to incentivise investment in high-speed broadband networks for all; to achieve an effective regulatory institutional framework.

Thus regulation will help to define the main problems and key issues to be addressed in the law. Regulation also functions to ensure uniform application of the law. The judicial and legislative functions of administrative agencies are not exactly like those of the courts or the legislature, but they are similar. Because regulations are not the work of the legislature, they do not have the effect of law in theory; but in practice, regulations can have an important effect in determining the outcome of cases involving regulatory activity. Much of the power vested in NAICT the TRB comes from the fact that parliament can only go so far in enacting legislation or establishing guidelines for government institutions to follow. Language that is intrinsically vague and cannot speak for every factual situation to which it is applied, as well as political factors, dictate that the Agency has much to interpret and decide in implementing legislation.

Regulation will directly affect the sector providing electronic communications networks and communications services (for example telecom operators, online service providers) and consequently users of those services (users' associations and end-users). It will involve national governments, national regulatory authorities. It may also affect other parties, such as employee.

Part II of the Cyber Code lays down the principles, means of co-ordination and control for Cameroon's information security and the activities necessary for the protection of the information infrastructure. Regulation is the first step towards establishing common standards for both state agencies and the private sector in order to protect the country's critical and information infrastructure and to ensure the country's information security. Therefore the law provides primary and secondary regulation that individuates specific competency areas. This is intended to reduce threats and security breaches, and therefore prevent online crimes. To some extent, the early role of the regulation has a crosscutting competencies and prerequisites. These include institutional maturity, engagement of the private sector, technical and industry expertise.

Thus regulation covers issues related to cyber security cannot be taken for granted, given the rapid developments in the field of cyber security.

As such, in many cases there is a lack of clear jurisdictional boundaries that delineate the areas of responsibilities between the different government institutions dealing with cyber security issues. In such a situation, the exact scope of responsibility of a regulator with regard to cyber security may not be marked out clearly, leaving regulators little guidance as to their role in that field. Such a situation presents both challenges and opportunities.

To encourage public-private sector efforts to develop cyber security

standards, procedures, and codes of conduct, developing or enforcing mandatory cyber security regulations and mandating or encouraging the adoption of international cyber security standards are required In a similar fashion, regulation can play a critical role in providing a first line of defence against a range of new threats arising from the use of poorly protected PCs that are connected to the Internet (for example denial of service attacks using zombie PCs by encouraging or mandating service providers to include, as part of their service offering, access to cyber security protection for individual users. Regulation has the mandate to require the adoption of standards or procedures in the interest of consumer protection or even general ICT development.

Regulation provides a milestone in defining roles and responsibilities in the protection of information and networks infrastructure and safeguarding cyber security, while taking into account the technological and regulatory evolution of the different aspects of the telecommunications sector, with particular attention to security.

Regulation also has the effect of evaluating emergencies and planning the measures to be taken in the event of crisis. Also the law considers other hypotheses of risk, not directly related to malicious acts, which can lead to situations of crisis for the continuity of government as well as damage to the population and, in general, the security of the country.

Also, regulation improves standards because it expands the number of firms required to maintain an acceptable standard of cyber security.

Specifically, regulation is important in the following aspects:

- Promoting competition (including tariffs);

- Interconnecting networks and facilities;

- Implementing universal service/access mechanisms;

- Managing the radio spectrum; and

- Minimising the burden and costs of regulation.

However, it is notable that, for the most part regulation reflects the characterisation of cybercrime primarily as a law enforcement and criminal justice challenge, rather than a "communications and technological" challenge.

Importantly, such regulations would not only enable users to continue to use strong encryption technology but enable investigators to gain access to the relevant data by forcing the user to submit the key to a special authority which holds the key and provides it to investigators if necessary.

However, opponents of such a solution fear that people could obtain access to the submitted keys and with them decrypt secret information. In addition, offenders could relatively easily circumvent the regulation by developing their own encryption software that does not require the submission of the key to the authority. In this respect, the following measures are recommended.

Also, firms are just as concerned about regulation reducing profits as they are about regulation limiting their flexibility to solve the cyber security problem efficiently. Thus many private-sector executives oppose regulation because it is costly. Excessive regulation on security can on the other hand stifle entrepreneurial potential.

Furthermore, regulation in cyberspace is usually difficult because of the pervasive nature of networks. Hence a mechanism, which consists of policies and procedures which deals with formally defined for the physical environment is not appropriate.

Finally, finding an acceptable balance between liberty and the protection of network infrastructures is difficult. Over emphasising security can severely restrict one's freedom of choice, as how do individuals gain access to cyberspace? with whom do they interact?; and how do they behave? Conversely, liberty without cyber security leadership presents rising unacceptable threats. In liberal constitutional democracies, we expect the freedom to access, use, and conduct legal inquiry and business online as part of our inalienable individual freedoms to be closely guarded by regulation.

Certification and standardisation: Certification is a formal procedure by which an accredited or authorised person or agency assesses and verifies (and attests in writing by issuing a certificate) the attributes, characteristics, quality, qualification, or status of individuals or organizations, goods or services, procedures or processes, or events or situations, in accordance with established requirements or standards. Accordingly, by virtue of section 9 (new) (1) the establishment and operation of national electronic communication networks open to the public may wholly or partially be subject to a concession to one or more public or private law corporate bodies under agreements setting out in particular the rights and obligations of the holder of such concession. The section further states that concession shall be granted to any corporate body that undertakes to comply with the provisions of the law, the clauses of specifications, as well as the general conditions relating to:

- Type, characteristics and service area;

- Service continuity, quality anti availability;

- Confidentiality and neutrality of service in relation to messages transmitted

- Network and service norms and standards;

- Use of allocated frequencies;

- Regulatory requirements for natural defence, public security, health and environmental protection and town planning purposes;

- The operator's contribution to research, training and standardization regarding electronic communications;

- Conditions of interconnection and, where applicable payment of charges for access to electronic communications networks open to the public:

- Conditions for infrastructure sharing;

- Contribution to the general missions of the State and, in particular, to universal service missions anti costs and regional development;

- Free routing of emergency electronic communications;

- Commercial operation necessary to ensure fair, objective, transparent anti non-discriminatory competition at affordable cost, without flawing or impeding free competition, by ensuring equal treatment of all users;

- Duration, revocation and renewal;

- Calculation and revision of contributions due as financial investments for electronic communications development nationwide.

Subject to the penalties provided for by the regulations in force, electronic communications operators shall ensure, before broadcasting

audio-visual content, that aggregators and publishers have an appropriate operating licence obtained in accordance with the laws and regulations in force. Thus, responsibility for CIIP is based on fulfilling the conditions provided by section 9.

The licence shall be issued to any natural person or corporate body to establish and operate in particular and may provide to the public value added services related to its licence, under conditions defined by law.

According to section 14, electronic communications equipment and infrastructure installer; electronic communications equipment testing and measuring laboratories and the sale of electronic communications equipment shall be subject to obtaining an approval;

In order to avoid institutional gaps in the national cyber security effort as well as to avoid overlaps in responsibilities, which can prove just as damaging, the law provides for a mechanism aim at organising and coordinating the work of multiple authorities and government departments, who have different mandates and perspectives on cyber security. In this light, the Cyber code provides that qualified electronic certificates should be valid only for the objects for which they were issued and that the devices used to design and verify qualified certificates should, from the technological standpoint, be neutral, standardised, certified and interoperable. Such Certification Authorities must justify adequate financial guarantee, allocated particularly for the payment of sums they may owe people who relied logically on the qualified certificates they issue, or an insurance that guarantees the pecuniary consequences of their civil professional responsibility. Further the law specifies that qualified electronic certificates shall be valid only for the objects for which they were issued and also standards for devices used for verified certificates. The law equally states that Certification Authorities are responsible for prejudice caused to people who relied on the certificates they presented as qualified in the case where the information contained in the certificate on the date of its issuance was inaccurate.

The Cyber Code protects users of electronic certifications by stating in section 16 (1) that Certification Authorities are responsible for prejudice caused to people who relied on the certificates they presented. However, there is a defence to such responsibility if the prejudice caused by the use of the qualified certificate exceeds the limits fixed for its use or the value of transactions for which it can be used, provided that such limits appear in the qualified certificate and are accessible to users.

As per section 17 of the Cyber Code, the legal value of an electronic certificate is the same as that of a handwritten signature. To guarantee the effectiveness of the standards the following conditions must be met: the data related to signature creation shall be exclusively linked to the signatory and be under his exclusive control; each modification shall be easily detectable; it shall be created using a protected device whose technical characteristics shall be defined by an instrument of the Minister in charge of telecommunications; the certificate used to generate signatures shall be a qualified certificate. An instrument of the Ministry in charge of telecommunications shall determine the criteria of the qualification of certificates.

The law provides that advanced electronic signature shall have the same legal value as that handwritten signature and produce the same effects as the latter. However the conditions for such electronic signature are as follows; the data related to signature creation shall be exclusively linked to the signatory and be under his exclusive control, each modification should be easily detectable; electronic signatures shall be created using a protected device whose technical characteristics shall be defined by an instrument of the Minister in charge of telecommunications, the certificate used to generate signatures shall be a qualified certificate. Finally, the Cyber Code provides that an instrument of the Ministry in charge of telecommunications shall determine the criteria of the qualification of certificates.

The protection of Electronic signature is spelt out in section 22 which stipulates that any person using an electronic signature device must fulfil the following; take minimum precautions fixed by the law, to avoid any illegal use of the encoding elements or personal equipment related to its signature; inform the Certification Authority about any illegitimate use of his signature; ensure the authenticity of all the data he declared to the electronic certification service and provider, and to any person he requested to trust his signature. Section 23 provides that a holder of the signature is responsible for the injury caused to others.

The provision on certification and standardisation portrays not only the control of public institutions, but also a shared responsibility between the public sector and certification authorities in the protection in the use of information networks. Thus certification and standardisation is an indication of the existence of a government-approved (or endorsed) framework (or frameworks) for agencies and public sector professionals. This has as a consequence the insurance of integrity, availability and confidentiality. Accordingly, an effective and sustainable cyberspace can only be achieved if it is open and secured. As in other domains of political and commercial activity, there is a trade-off. As government intervention increases, there is a promise of greater security, but that security comes with economic costs and potential limits on liberty and privacy. This trade-off, it seems, is inescapable, but requires continuing management. There is therefore a seesaw between the two; we do not want all security and no liberty nor all liberty and no security. In this light standardisation can be seen as both an advantage and a disadvantage. Standards are necessary for the interoperability and are important factors for international cooperation.

Furthermore, with increased interconnection and unified standards, comes increased vulnerability, both to external and internal threats. The use of identical security processes on every computer network does not seem to be an optimal solution at least not without weighing the competing costs. The negative effect of interoperability is greater potential vulnerability of the entire system, which is easily accessible once a part of it is compromised. This includes the spread of viruses and other malware, as well as hacking. The defence for such systems should be absolutely impenetrable to outweigh the risks, which in itself is a rather remote possibility, if a possibility at all.

The adoption of electronic signatures as a legally valid mode of executing signatures under the Cyber Code introduces technological neutrality. The law also includes digital signatures as one of the modes of signatures which is far broader in ambit covering biometrics and other new forms of creating electronic signatures not confining the recognition to digital signature process alone. Electronic signatures as stipulated in the law is not a digitised signature or a scanned signature. In fact, in electronic signature (or digital signature) there is no real signature by the person, in the conventional sense of the term. Electronic signature is not the process of storing ones signature or scanning ones signature and sending it in an electronic communication like email. It is a process of authentication of message using the procedure laid down in the law. However, the duties of electronic signature certificate issuing authorities for bio-metrically based authentication mechanisms have to be secured and the necessary parameters have to be formulated to make it user-friendly and at the same time without compromising

security. The importance of electronic signature can be seen in its role to provide information integrity. Hence section 40 of the law provides for penalties of compensation and adjudication. This is a significant step in the direction of combating data theft, claiming compensation, introduction of security practices and preventing abuses on ICTs.

Monitoring and evaluation under the cyber code: Security Monitoring is the collection, analysis, and escalation of indications and warnings to detect and respond to intrusions.

This strategy involves ensuring coherence among activities programmed, ensuring coherence of sectorial programmes with ministerial policies, initiating or participating in all sectorial framework studies, establishing and managing databases relating to monitoring and evaluation and collecting, updating and analysing all information on the sectors concerned

Thus, monitoring and evaluation is intended to partially guard computer and network, and notify the network administrator (via email, SMS or other alarms) in case of outrages. It is part of network management. This can be done by conducting real-time surveillance on, make threat-based decisions on, and provide an intrusion prevention system for any activity taking place in certain computer networks. In performing these functions, the state shares information and cooperates with the Agency. The government closely coordinates among departments, personally identifiable information from shared security data, and operates on a real-time response basis. This mechanism enables the Agency to perform activities like collection, analysis and dissemination of information on cyber incidents, forecasts and alerts of cyber security incidents, emergency measures for handling cyber security incidents etc. These security incidents include website intrusions, phishing, network probing, spread of malicious code like virus, worms and spam. Hence monitoring plays a very crucial role not just in giving out the alerts but in combating cyber crimes by intercepting and blocking the site, whenever so required and with due process of law.

Also monitoring helps in detecting and reporting failures of devices or connections. It normally measures the processor utilisation of hosts, the network bandwidth utilisation of links, and other aspects of operation. It will often send messages (sometimes called watchdog messages) over the network to each host to verify if it is responsive to requests. When failures unacceptably slow response, or other unexpected behaviour is detected, these systems send additional messages called alerts to designated locations (such as a management server, an email address, or a phone number) to notify system administrators.

Monitoring also allows organisations to baseline the network performance of their hardware and software infrastructure. With a baseline of nominal operations in hand, IT is positioned to recognise and respond to conditions that can negatively impact network performance and threaten the user community's productivity and quality of experience.

The ideal performance monitoring tools must be comprehensive, scalable and robust enough to accommodate an end-to-end perspective, must possess depth, with the capability to span all layers of the network stack. Without both dimensions, monitoring is severely restricted in its efforts to identify the location of the problem, and to pinpoint if the root cause of the problem.

More significantly, a comprehensive performance-monitoring tool promotes the resolution of more complex anomalies. Straightforward, linear degradations are often obvious, but intermittent issues are far more challenging to address. Likewise, while some problems may manifest themselves on the network, the source of the trouble may reside outside the enterprise's domain-with a service provider. These types of anomalies simply cannot be brought to closure quickly by point solutions.

Although monitoring is a key aspect of counter-attack and de-radicalisation, including operations aimed at preventing cyber crimes, individual liberty, and privacy in particular, can be compromised by the wrong use of data obtained by cyber surveillance the recent phenomenon of lone-wolf political violence. Gathering information on the bad actors may often mean that information on ordinary citizens is collected. In cyberspace there is currently an unfortunate trade-off where, at times, a certain degree of anonymity and privacy that certainly fall within the sphere of most conceptions of liberty is violated to enhance security. That sacrifice does not have to lead to harmful results if managed and supervised correctly. Thus the research recommends that surveillance should be open and largely unencumbered. Note that the nature of threats in cyberspace keeps changing. Therefore, curtailing the government's ability to gather data is too risky a measure. Instead, the key checks should be at the output level and not the input level.

Also, as the state monitors and observes new technological developments, hacker activity and related trends must be monitored in order to help identify future threats. Issues that should be analysed include legal stances, social or political threats, and emerging technologies. This includes the reading of secure mailing lists, secure websites, news and current newspaper articles on issues within science, technology, politics and government in order to extract information that is relevant to the security of the critical systems and infrastructure. As a result should be followed by announcements or recommendations on how intrusions can be prevented. Unfortunately, since cyber-threats are not territorially limited, monitoring is often soloed by geography, department, service, or network layer, which inhibits realising the objective. However, continuing to monitor cyber attacks helps to reduce their impact on the community.

An important feature of the Cyber Code is that it supports the development of different priorities and targeted responses. This ensures the development of appropriate mechanisms to: identify and prioritise local issues of concern based on evidence of need, develop practical responses to these issues and evaluate and measure the effectiveness of each response; consult and engage with the local community to help understand cyber attacks priorities, exchange information and to identify opportunities to engage the community in local problem solving; improve the quality and availability of information for stakeholders required to appropriately target interventions to address cyber threats; and integrate cyber rime crime prevention within other services and preventive strategies delivered at the national, regional and local government levels.

Conclusion and Recommendation

Cameroon's Cyber Code provides a wide range of roles available to the government in which it can lead by defining and facilitating security roles and innovations in CIIP. However, effective implementation of these roles is inhibited by the fact that they are to some extent overlapping and such government strategies would surely brand reputations and burden companies with high compliance costs Moreover, the ICTs was not designed to allow for easy monitoring of users' behaviour. The ease and anonymity with which people throughout the world can access information systems via the Internet,

coupled with the Internet's inherently flawed design, is consistent with the growing recognition among corporate leaders that cyber and physical security are interdependent and must be the core aspects of their risk management strategies. Statistics from the Cameroon's National Agency for Information and Communication Technologies (NAICT) reveals that some FCFA 4 billion has been lost due to cyber scamming and phishing. NAICT further reveals that since 2011, some FCFA 3.5 billion has been lost in skimming with cases of 137 Facebook profiles suffering from spoofing and cyber blackmail in the country. Many institutions have incurred losses due to inadequate protection of their information systems Particularly, there are several services, the continuous accessibility to, and availability of which are critical to the smooth functioning of the society. For example, services such as telecommunications, banking and finance, transportation, oil supply, electricity, water supply, emergency services (fire, health, police), government operations and other utilities are now being controlled by computers. In Cameroon particularly, the Cameroon Railway Corporation, (CAMRAIL) Cameroon Energy Company (ENEO),Cameroon Water Company (Societe National des eaux de Cameroun (SNEC), Cameroon Telecommunications (CAMTEL) and Cameroon Airlines Corporation (CAMAIRCO) highly depends on computer networks and data for better service delivery. The importance of information networks can equally be seen in the functioning of the stock exchange market which uses telephone and the Internet to provide facilities for stockbrokers and traders to trade stocks and other securities For example, in the Douala Stock Exchange, network of computers enables billions of shares to be traded each day. It is important that government leadership and commitment ensures clear policy objectives and setting up of government agencies with responsibility and authority to implement them. Also, since Cameroon now classifies cyberspace as a new domain of battle, as significant as air, land, or sea, cyber security Leadership should provide a coordinated national action relating to the prevention, preparation, response, and recovery from an incident on the part of government authorities at the national, regional, divisional and village levels. This should set up a cyber security activities and desired outcomes, and ensure five simultaneous and continuous functions, that is, identify, protect, detect, respond, and recover. In line with Contreras et al, the cyber security policy should be based not only on reactive vulnerability mitigation, that is, on developing protection against cyber-threats, but also, and for the most part, on threat deterrence. Against this backdrop the paper recommends the following for an effective leadership in CIIP;

1. Adoption of a National risk management strategy

This includes a risk management process setting out the detailed organization, tools and monitoring mechanisms required to implement the risk management strategy at every level, and the creation of a computer security incident response team (CERT/CSIRT).

2. Effective collaboration in cyber security framework

A comprehensive national cyber security leadership requires the establishment of a framework that will ensure the coordination and ensure the collaboration of all cyber security stakeholders. In particular, such a framework would allow government's, collaboration with and between private sector, international organisations, private sector, civil society, the media, academia; and individual users to work together to develop and implement measures that incorporate technical (for example, standards), procedural (for example, guidelines, standards, or mandatory regulations) and personnel (for example, best practices) safeguards. Such measures must include, for example, promoting government and industry adoption of international standards related to cyber security (for example Information Security Management System) and the implementation of certification schemes (for example, Public Key Infrastructure). This strategy must be provide a 'prioritized, flexible, repeatable, performance-based, and cost-effective approach' to help technology service operators 'identify, assess, and manage' risks, and focusing on determining 'cross-sector security standards and guidelines applicable to critical infrastructure.' The Cyber security Framework should facilitate guidance about neutral technologies, enabling 'critical infrastructure sectors to benefit from a competitive market for products and services'.

3. Information sharing

It is considered a national priority to increase 'the volume, timeliness and quality of cyber threat information shared with authorized individuals and companies.' The main goal of that Order is to enable information sharing between the private sector and all levels of government. In order to achieve this goal, the Order mandates the production and dissemination of both unclassified and classified reports of cyber threats to targeted entities. Also, and perhaps more importantly, program to all critical infrastructure sectors, real-time sharing of information on cyber threats to critical infrastructure companies and state and local governments. This will mean that information sharing will be bidirectional (from Government towards private entities and from private entities towards Government) and that the Internet giants would be involved in the goal of achieving critical infrastructure protection. This would hugely help in the process of notifying major Network information systems.

4. Ensuring cooperation international arena

Leadership should effectively address the protection of critical information infrastructures across borders and promotes the engagement in bilateral and multilateral cooperation at regional and global levels with a view to sharing knowledge and experience, developing common understanding to facilitate collective action on vulnerabilities, and enabling robust information-sharing. This should include identifying threats to and reducing the vulnerability of such infrastructures to damage or attack, minimizing damage and recovery time in the event that damage or attack occurs, and identifying the cause of damage or the source of attack for analysis by experts and/or investigation by law enforcement.

References

1. Eric Akuta, Ong'oa M, Chanika RJ (2011) Combating Cyber Crime in Sub-Sahara Africa; A Discourse on Law, Policy and Practice. J Res Peace, Gender Development 1: 129-137.
2. Asongwe P (2012) e-Government and the Cameroon Cybersecurity Legislation 2010: Opportunities and Challenges. Afr J Information Communication.
3. Asongwe P (2017) Cybersecurity and Challenges of Cyber criminality: Response, Strengths and Weaknesses of Cameroonian Law, PhD unpublished Dissertation, University of Yaounde II, (Yaounde) at 356.
4. Tibad P (2013) Fighiting Cyber criminality To Foster Economic Development In CEMAC Sub-Region; The Case of Cameroon. A Dissertation Submitted In Partial Fulfillment of The Diplôme D'etude Approfondies (DEA) in Law. University of Yaounde II 33-43.
5. Yufeh NB (2016) Cyber Security: Government Takes Measures Cameroon Tribune.
6. Yanke A (2013) The Policy, Legal, and Regulatory Framework for Cyber security And Cyber criminality In Africa. Commonwealth International Cyber security Forum.
7. Melanie JT (2013) Fiddling on the Roof: Recent Developments in Cybersecurity. 2 American University Business Law Review.

8. Scott S, Craig A, Proia AA, Martell B (2015) Toward a Global Cyber security Standard of Care?: Exploring the Implications of the 2014 NIST Cyber security Framework on Shaping Reasonable National and International Cyber security Practices. Texas Int Law J 50: 305-340.
9. Thakar U (2010) Pattern Analysis and Signature Extradiction for Intrusion attacks On Web Service. Int J Networks Security & Applications 2: 190-195.
10. Shackelford S, Craig A (2014) Beyond the New Digital Divide: Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cyber security. Stanford J Int Law 50: 119.
11. Chiemeke SL (2006) The Design and Implementation of An E-Mail Encryptor for Combating Internet Spam. In Proceedings of the Ist International Conference of the International Institute of Mathematics and Computer Sciences.
12. Richardson M (2013) President Obama Shows No CISPA-like Invasion of Privacy Needed to Defend Critical Infrastructure. ACLU.
13. Goodman S (2007) Towards a Safer and More Secure Cyberspace. National academies press.
14. GAO (2010) Cyber security: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative.
15. Cameroon (2017) Digital Economy: Government Moves to Alleviate Cyber Insecurity Cameroon Tribune.
16. Demirg-Kunt A, Levine R (1996) Stock Markets, Corporate Finance, and Economic Growth: An Overview. World Bank Economic Review 10: 223-239.
17. Nykodym N, Taylor R (2004) The World's Current Legislative Efforts against Cyber Crime. Computer Law & Security Report 20: 390-395.
18. Contreras L (2013) Mapping Today's Cyber security Landscape. American University Law Review.
19. Kesan JP, Hayes CM (2014) Creating a Circle of Trust to Further Digital Privacy and Cyber security Goals. Michigan State Law Review 5: 1474-1537.
20. Fleming MH, Goldstein E, Roman J (2014) Evaluating the Impact of Cyber security Information Sharing on Cyber Incidents and Their Consequences.
21. Broggi JG (2014) Building on Executive Order 13,636 to Encourage Information Sharing for Cyber security Purposes. Harvard J Law & Public Policy 37: 658.
22. Serrano AS (2015) Cyber security: towards a global standard in the protection of critical information infrastructures. European J Law & Technology 6: 67-73.
23. Brumfield C (2014) Four Key Take-Aways from the Sixth NIST Cyber security Framework Workshop. Digital Crazy Town.
24. Fleming J (2013) EU, US go separate ways on cyber security. Euro Active.
25. Gyenes R (2014) A Voluntary Cyber security Framework Is Unworkable-Government Must Crack the Whip. Pittsburgh J Technology Law & Policy.
26. Palmer RK (2014) Critical Infrastructure: Legislative Factors for Preventing a Cyber-Pearl Harbour. Virginia J Law & Technology.