INTERNATIONALJOURNALOFRESEARCH SCIENCE& MANAGEMENT

CYBER SECURITY AND THE CUSTOMS AGENCIES: CASE OF CAMEROON CUSTOMS ADMINISTRATION (CCA)

Dr. ALOUMEDJO ZAM Thierry Farrel
Senior customs officer
DOI: 10.5281/zenodo.10886327

Abstract
The aim of our study is to evaluate the impact of cyber customs on its performance after identifying how and why it should be put in place in the CCA. This research is important considering the fact that Cameroon Customs administrations is facing serious challenges and the bugetary assigned target to the said administration by Government is above 1 000 billions FCFA in 2024. The problem Statement is to question the shortcomings of the incumbent CCA, Why can cyber customs correct the observed gaps, How can we put in place an efficient cyber customs in the CCA and What could be the various recommendations that can be made. The objectives were to identify what is cyber customs and how it can be put in place in the CCA ; determine its strong holds and possible limits and formulate recommendations to guarantee its sound application. Our work present three main interests which are managerial, theoretical and methodological. Four theories guided our analysis i.e. rational choice theory, Institutional Anomie Theory, strain theory and routine activity theory. We came out with the main results that there is no specific customs unit specialized in fighting cyber crimes as it is the case of the Customs Enforcement (ICE) that have special divisions dedicated to combating cyber crime. As far as electronic crime is concerned, Customs administrations need to be properly equipped and further trained as far as the legal and technological aspects are concerned in order to deal with sophisticated offences committed in cyberspace and which pose a great many challenges. Therefore the novelty of our research is the need of creation of a specific customs unit specialized in fighting cyber crimes in the CCA. The vision Statement of cyber customs being to enhance the nation's security through innovation, intelligence, collaboration and trust in a context of the CCA becoming a member of the defense and security community alongside Police, army, gendarmerie, territorial administration, etc.

Keywords: Cyber security; customs services; intellectual property; counterfeiting; economic performance.

Introduction

Contextual background
Cameroon Customs administrations is facing serious challenges such as corruption, raising revenue collection and enhancing trade facilitation at this point it is worth underlining the fact that the bugetary objectives of the said administration is above 1 000 billions FCFA in 2023. In addition counterfeit goods, smuggling are other types of frauds are on the rise especially through internet. According to a study by Desmond (2023) the finding revealed that major challenges come as the results of clearance procedures in Cameroon being too long, surrounded with corruption environment due to multiple documentation requirements and the procedures are neither transparent enough. A report from the US International trade administration last published date on 2021-10-27, states in the exact words that « Cameroon routinely ranks near the bottom of the World Bank's Doing Business Report – 167th out of 190 countries in 2020 – and Transparency International's Corruption Perceptions Index – 149th out of 180 countries in 2020. It should be underlined that there is no specific customs unit specialized in fighting cyber crimes as it is the case of the Customs Enforcement (ICE) that have special divisions dedicated to combating cyber crime. As far as electronic crime is concerned, Customs administrations need to be properly equipped to deal with sophisticated offences committed in cyberspace and which pose a great many challenges

While significant economic opportunities exist, inefficiencies continue to be a drag on the growth needed to employ millions of young Cameroonians in the coming decade in a country where the median age is 18. Despite seemingly low salaries, Cameroon's civil service is one of the most expensive in sub-Saharan Africa after accounting for non-wage compensation. Delays in project completion and financially struggling state-owned enterprises add to the problem. Almost all business transactions require senior-level government approval, making for a cumbersome process susceptible to political influences and corruption. Poor infrastructure, a slow and burdensome, omnipresent civil service, and rapidly evolving tax and regulatory regimes that lack transparency pose challenges to small and medium-sized enterprises attempting to enter the market. Even minor

procurement decisions require Minister-level approval. Having a local partner is a must for companies hoping to do business in Cameroon».

Notwithstanding many reforms have been taken by the state and the customs administration to ameliorate the economic environment among which digital solution such as the customs clearing automatic system, performance contracts, geolocalisation of goods in transit, etc in clear many reforms are taken by the Cameroon government to facilitate businesses, trade and international transactions and the results are clearly visible.

Clarification of key concepts

Key concepts to clarify are cyber security, cyber criminality, counterfeiting, e-trade, customs services.

Cyber criminality

According to Smith (2023), computer-related crime is becoming more and more important globally. Cybercrime or any criminal activity that involves a computer, networked device or a network is followed up by the National Agency in charge of information technology (ANTIC) and in its glossary refers to it as an activity that consists in using systems, computer networks in general and the Internet in particular to perpetuate crimes prohibited by law. The term "cyber criminality" was invented in the late nineties when people saw the coming of the Internet in North America. These crimes include piracy, pornography, hatred telemarketing, economic and financial fraud such as counterfiting or smuggling or any fiscal fraud etc.

It has become more rampant because of the increasing development of Information and Communication Technologies. According to the European Commission, the term "cyber criminality" includes three categories of criminal activities such as traditional forms of crime including forgery, scams, fake payment cards, etc. ; broadcasting illegal content through electronic means and specific attacks on information systems, denial of service and hacking. All economic actors are the targets of these criminals. Public administrations and even citizens are no longer immune to these virtual practices that are prohibited by law.

The customs administration is also concerning especially in the case of online international trade since it is in charge of regulating and collecting taxes at the boundary, some goods are virtuals such as licenses, patents, software and some goods are ordered online and delivered without necessarily being physically appraised by the said administration that does not always have the technological, logistical and intellectual know-how therefore leading to considerable losses for the empty already state coffers. This have serious repercussions on the socio-economic development of the country.

Cyber security

According to Kapersky (2023), Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories. It aims to reduce the risk of cyber attacks and protect against the unauthorised exploitation of systems, networks, and technologies. Organizations that suffer cyber security breaches may face significant damages and losses. There are also non-financial costs to be considered, like reputational damage.

Cyber attacks are increasingly sophisticated. According to a study by McAfee and the CSIS, based on data collected by Vanson Bourne, the world economy loses more than $1 trillion each year due to Cybercrime. Political, ethical, and social incentives can also drive attackers. Every individuals and organizations connected to the Internet needs cyber security. This is because most cyber attacks are automated and aim to exploit common vulnerabilities rather than specific websites or organizations. There are Different Types of Cybersecurity as it is a wide field covering several disciplines. Cybersecurity therefore means the protection of internet-connected systems such as hardware, software and data from cyberthreats.

Cyber security's core function is to protect the devices we all use (Smart phones, laptops, tablets and computers), and the services we access online. It consists in measures or practices for preventing cyberattacks or mitigating their impact. Information security is all about protecting information and information systems.

INTERNATIONALJOURNALOFRESEARCH SCIENCE& MANAGEMENT

Digital customs services

Digital customs services are primarily meant to facilitate cross-border trade through a wide customs consultancy service and effective use of digital technology meant to optimize trade and customs management, improve trade performance, operational efficiency, risk management and customs duty control. The idea behind is to minimize customs hassle, reduce risk and save money to perform customs and border formalities remotely or online.

For instance in countries such as Malaysia, besides visiting Customs Offices, importers, exporters and the business community can access Customs services online. If you already manage your own Customs and Excise account, you can sign in. If you have not previously signed into the Customs and Excise online services. Customs declarations and excise documents and declarations are filled using several software applications. It is possible to make an appointment online with one of the customs offices of the Customs and Excise Agency. Customs and Excise payments can be made using online secured systems. Like in China, the possibility for "Intelligent Control" System Online combining «Internet + Customs" Platform to Facilitate Dalian Customs Services on verification and liquidation as well as fighting against fraud, controlling warehouses in order to be able to inspect goods instantaneously through video surveillance and geolocalisations, etc.

Intellectual property

Intellectual Property (IP) law relates to the establishment and protection of intellectual creations such as inventions, designs, brands, artwork and music. According to Menell (2023), it is organized around the two principal objectives of intellectual property law: promoting innovation and aesthetic creativity (focusing on patent, trade secret, and copyright protection) and protecting integrity of the commercial marketplace (trademark protection and unfair competition law). Bently (2013) believes that two (2) categories of IP industrial property includes inventions (patents), trademarks, industrial designs, and geographic indications of source; and copyright which includes literary and artistic works such as novels, poems and plays, films, musical works, artistic works such as drawings, paintings, photographs and sculptures, and architectural designs. Rights related to copyright include those of performing artists in their performances, producers of phonograms in their recordings, and those of broadcasters in their radio and television programs.

The law regulating intellectual property practice in Cameroon is the Bangui Accord of 02/03/1977 as amended on 24/02/1999. This law is essentially an agreement between 16 west and central African countries (Benin, Burkina Faso, Cameroon (headquarters), Central African Republic, Congo, Côte d'Ivoire, Equatorial Guinea, Gabon, Guinea Bissau, Guinea Conakry, Mali, Mauritania, Niger, Senegal, Chad and Togo). The African Intellectual Property Organization (AIPO) most commonly known and called by its French acronym, OAPI. The immediate fallout of this regional approach is that an IP registered in OAPI is covered and protected in all 16 member countries with a total population of more than 100 million. This law regulates the protection of Intellectual Property rights in patents of invention, utility models, trademarks and service marks, industrial models/designs, trade names, geographical indications and appellations of origin, literary and artistic property, protection against unfair competition, topographies of integrated circuits and protection of plant varieties. It also provides for the recordal of licenses, assignments, changes of name and changes of address in the special register. Yet the same law governs searches of anteriority, searches of identity, renewals of rights and extension of coverage to and from new adherents to the organization (Baaboh, 1998).

Counterfeiting

In simple terms, to counterfeit means to imitate something authentic, with the intent to steal, destroy, or replace the original, for use in illegal transactions, or otherwise to deceive individuals into believing that the fake is of equal or greater value than the real thing. Customs administrations are in the frontline to enforce intellectual property rights (IPR), Infringements of IPR are a widespread and worrying phenomenon. The reasons for the increase in rate of infringements are diverse, including the attractiveness of a 'look-alike product' at a cheap price, the ease of production of copies at minimal costs, the development of new forms of marketing such as e-commerce and social media and the growth of international trade. For the Customs administration to act there must be a suspicion of a property right violation. Such a right can only be violated in the course of trade. As the consumer demand for branded products increases, the number of counterfeit and pirated products is also increasing. Counterfeiting is a threat to legal economy, politics, security, health, and social development and need to be adressed by all possible legal means.

INTERNATIONALJOURNALOFRESEARCH SCIENCE& MANAGEMENT

Customs performance

The concept of organizational performance has been abundantly discussed in management literature. According to Cho and Dansereau (2010), it should be defined as the performance of a company as compared to its goals and objectives. In the same vein, Tomal and Jones (2015) define it as the actual results of an organization as measured against intended outputs.

It should be clarified here that the organization itself does not perform any work but its managers are performing their assigned works and it is the combination of these performed works that is called organizational performance. The organization gets some outcome such as effectiveness and efficiency.

According to Amitia (1964) being effective for an organization is all about whether or not an organization is achieving the outcomes intended to be produced. Organizational effectiveness measures how successful organizations are in reaching their goals. An effective organization runs smoothly and functions well. Organizational effectiveness is a concept that measures how thoroughly and efficiently an organization achieves its corporate and individual goals. An effective organization runs like a well-designed, well-oiled machine states Maloney (2014). Its moving parts function smoothly to produce the results the unit is set out to achieve.

Organisational efficiency refers to the relationship between inputs (resources) and outputs (goods or services provided) and in simple terms the more output we can achieve with a given amount of inputs or resources, the more efficient we are. Hence if being effective means doing the right thing, to be efficient implies doing right the said thing (Drucker, 1990).Organizational efficiency is also seen as the process of using fewer resources, as well as less time and less money, to achieve the same goal.

This implies good quality management of workforce, production, and communication. According to Schuler (2001), Organizational efficiency is operationalized by aspects of practicability such as the expenditure of the procedure, the required competence for its application, and its availability. Organizational efficiency is the organization's ability to implement its plans using the smallest possible expenditure of resources. It is an important factor in the firm organizational effectiveness, this being the ease and degree of success with which the unit is able to accomplish its objectives.

It should be reminded at this level that the organization is where resources come together. Organizations use different resources to accomplish goals. The major resources used by organizations are often as follow (1) human resources, (2) financial resources, (3) physical resources, (4) information resources, (5) time resources. In consequence managers are responsible for acquiring and managing efficiently all the resources available to accomplish organizational goals.

Osabiya (2015), Dobre (2013), Festré (2008), Muogbo (2013) and Uzonna (2013) are amongst the scholars who have studied the impact of employee motivation on organisational performance. Their findings show that high employee motivation has significant positive impact on organisational performance. These authors used survey design with correlation analysis. As concerns leadership styles and supervision, Malin (2013), Wang et al. (2010), Zehira et al. (2012) are among the numerous scholars who have found out that leadership and supervision driven by a positive outlook such as transformational leadership had significant positive impact on organisational performance. These studies mostly used correlational analysis in their methods of surveying data analysis.

Brief conceptual review

Customs and Border Protection missions

Customs is in charge of border protection let it be land, maritime or by air. Its priority mission is to prevent terrorists and terrorist weapons from entering the territory and ensuring the security of the nation at the level of borders and ports of entry. It must maintain this line of defense while allowing legitimate travel and trade that is vital to our economy and way of life. Customs is responsible for apprehending individuals attempting to enter the country illegally; stemming the flow of illegal drugs and other contraband; protecting our agricultural and economic interests from harmful pests and diseases; protecting national businesses from theft of their intellectual property; and regulating and facilitating international trade, collecting import duties, and enforcing national trade laws. In securing borders, Customs authorities protect the Homeland through the air, land and maritime environnements against illegal entry, illicit activity or other threats to uphold national sovereignty and promote national and economic security. This implies inspecting merchandise, agriculture, luggage, and people

coming into and out of the country, intercepting drugs, weapons, and other illegal goods before they get into the wrong hands and stopping people from trying to illegally enter the country. The vision Statement is to enhance the nation's security through innovation, intelligence, collaboration and trust.

Secured customs cyberspace network

Cyberspace is an interconnected digital environment. It is a type of virtual world popularized with the rise of the Internet. The Customs cyberspace network consists in an interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. The Customs cyberspace needs to be secured considering the fact that sensitive information are involved and risks of extorting money or interrupting business normal processes are at stake. Systems, networks, and programs from digital attacks therefore need to be protected. As much as people would like to believe in a global Internet community, Beijing believes cyberspace must still respect the culture, customs and personality' s private information (Burgman, Jr., 2016). Indeed, Network security is the armor that shields our digital world from the relentless onslaught of cyber threats. The Customs should therefore examines these Internet security vulnerabilities and offers a strategy for future research aimed at countering cyber criminality at borders and elsewhere to better secure the financial system.

Organizations effectiveness and the Nation's security

Organizational effectiveness refers to its ability to meet the set goals, it is identified most often through financial profits, efficiency, or growth. However, effectiveness can also be about staff retention, job experience, community impact, or market share, etc. An effective organization runs like a well-designed, well-oiled machine. Organizational effectiveness is made up of various factors such as clear vision and goals, strong leadership, strategic planning, efficient resource management, effective communication, talent management, performance measurement, adaptability, and stakeholder engagement. As far as Customs is concerned, effectiveness refers to improved operational efficiency, resource optimization and improved delivery of mandates requiring for that purpose transparency, harmonized procedures, facilitation and efficient fight against fraud. The effectiveness of the customs inspection of goods is therefore at stake. Three main functions of customs agencies are security and facilitation of international trade, fair and efficient collection of revenue and protection of public as well as the effectiveness of customs risk management selectivity. Times taken by customs officials and brokers to process files determine the effectiveness of customs services. Customs controls must be quick, effective and based on modern risk management techniques in order not to disrupt trade flows in a fast-moving economy.

Role of Customs in Cargo Security

Customs and regulations also play a critical role in maintaining the security of the transportation and logistics industry. They help prevent the movement of illegal goods, such as drugs, weapons, and counterfeit products, and reduce the risk of terrorism. This is particularly important in the sense that Customs has to deal with a massive number of containers arriving at ports. This massive flow of cargo provides an opportunity for organized action in the interest of countries (Pourakbar, 2018). Customs administrations in dealing with the security challenges faced by international transport and shipping service providers. According to Matityahu (2023), the way many customs administrations performed most of their preventive operations as goods arrived at seaports, airports, and land borders based upon an entry declaration made at the time of importation has changed nowadays with technology in order to improve security in the supply chain, requiring that this traditional method of operating must evolved and the solution adopted to new realities.

Maritime governance

Maritime governance means the coordination of various uses of the ocean and protection of the marine environment. It is also viewed as a complex set of rules over shipping regulations knowing that The maritime industry is responsible for transporting over 80% of global trade, and involves interrelations between international bodies, state parties, non-governmental organizations, shipping companies and other stakeholders which, in itself, brings about many intricacies.

The International Maritime Organization (IMO) is in charge of the regulation of this sector which involves a constant interaction among the different actors whereby the development of international regulationswithin the national jurisdictions of member States and the reporting of regulatory outcomes. It is also important to review in that perspective the relationship between the IMO, its Member States, and other key stakeholders within the context of maritime governance.

INTERNATIONALJOURNALOFRESEARCH SCIENCE& MANAGEMENT

Problem rationale

The followings are identified limits to customs administration efficiency (Glenday, 1997) :

- Unharmonised and unclear customs procedures.
- Lack of computerized and integrated customs managements systems.
- Inefficient manual customs processes.
- Inadequate staff compliment and skills which affect the speed at which services are rendered.
- Incorrect classification of goods imported, incorrect tariff classifications, false invoices and under invoicing.
- Long-time which is taken to complete and approve import documentation?
- Uncoordinated customs operating system.
- excessive documentation, physical inspections and controls which could be seen as anti-trade facilitation in that they lead to time wastages, inefficiency and inefficacies.
- Weak institutional structures with lack of capacity and delivery mechanisms to effectively address the challenges affecting the customs environment.
- Lack of transparency regarding customs procedures compounded by too many documents and language barriers.
- Corruption and underhand payments often facilitated by same actors administering customs procedures and operations.
- Certain actors seem to benefit from the existence of chaos at border posts and often manipulate manual procedures.
- Not every country clearly demonstrates political will and commitment to transforming the customs environment which weakens efforts to clean-up the environment of corruption and improve integrity.
- The above mentioned shortcomings observed in the customs administration question the relevance of e-customs in general and to a certain extent cyber customs whereby the following questions:

What are the shortcomings of the incumbent customs structuration?
Why can cyber customs correct the observed gaps?
How can we put in place an efficient cyber customs in the CCA?
What are the various recommendations that can be made?

Research rationale and objectives

The rationale of our analysis is aimed at evaluating the impact of cyber customs on its performance after identifying how and why it should be put in place in the CCA. The followings here under are our objectives :
Identify what is cyber customs and how it can be put in place in the CCA ;
Determine its strong holds and possible limits ;
Formulate recommendations to guarantee its sound application.

Research interests

Our work present three main interests which are managerial, theoretical and methodological.

- At the managerial level we intend to develop a framework adapted and able to be used as a guideline for the customs administration in terms of cyber system to efficiently tackle trade facilitation and fraud challenges.
- From the theoretical perspective, this study will permit us to peruse key concepts relating to cyber customs thus enabling us to develop a pertinent conceptual framework useful to leave from the abstract perception of our object to its materiality and therefore possible innovation and creativity.
- From the methodological point of view, it will be question to examine our choices and techniques through the « research onion » of Saunders (2019), this will permit to peruse a larger scope of our study.

Some guiding theories mobilized

In this study, we are guided by a number of theories among which ***rational choice theory*** which suggests that individuals engage in computer crime because they believe it is a profitable and low-risk activity. We also mobilized ***Institutional Anomie Theory*** according to which financial gain is the prominent and key driver of Cybercrime, with an estimated 90% of breaches motivated by money (Leukfeldt et al., 2017).***The strain theory*** according to Dearden et al., (2021 offers insights into the genesis and motivation of cybercrimes, online scams,

hacking, cyber harassment, piracy, as well as hate speech. To illustrate this cyberbullying is both a stressor and a stress-releasing strategy for the cybercriminels. As stated by the ***routine activity theory***, the perpetration and the subsequent increase of cybercrimes are primarily influenced by the convergence of the critical components that facilitate the execution of a crime. These factors include the potential offender, a suitable or attractive target, and the absence of a capable guardian (Adler et al., 2021; Governder et al., 2021).The social learning theory posits that people develop the desire and skills to commit crimes after associating with others who are active in the commission of illegal activities (Rokven et al., 2017).

8- Research methodology

As far as research methodology is concerned we are going to mobilize a comparative analysis implying that we are going to do a side-by-side comparison by systematically comparing two or more cyber customs systems in order to pin point their similarities and differences. The focus of the investigation will be both conceptual and practical with analysis on two different data sets. This will enable us to bring out the gaps and further recommendations.

9. Data collection and analysis

Here it will be question for us to present the population, the sample and the analysis method.

Population studied

Population	Male	Female	Total
Total	**2631**	**1264**	**3895**

Sample selected

Interviews	frequency	Percentage
planned	50	100%
treated	45	90%
Not validated	5	10%

Methods of analyses employed

- Content analysis (Krippendorff, 2003)
- BERELSON (1952), the founder of content analysis defined it as a research technique used for the objective, systematic and quantitative description of the content of a text
- The various stages of the data analyses include retranscription, coding and analysis of the data collected.

Research results and possible innovation

- Research results

The following results appear from our work namely :

- It should be underlined that there is no specific customs unit specialized in fighting cyber crimes as it is the case of the Customs Enforcement (ICE) that have special divisions dedicated to combating cyber crime.
- As far as electronic crime is concerned, Customs administrations need to be properly equipped to deal with sophisticated offences committed in cyberspace and which pose a great many challenges.
- Despite seemingly low salaries, Cameroon's civil service is one of the most expensive for users in Sub-Saharan Africa after accounting for non-wage compensation.
- Poor infrastructure, a slow and burdensome, omnipresent civil service, and rapidly evolving tax and regulatory regimes that lack transparency pose challenges to small and medium-sized enterprises attempting to enter the market.
- Competences of customs professionals are lacking in the use of systems, computer networks in general and the Internet in particular to better tackle cyber criminality and ensure enforcement of the laws.
- Cyber crimes consist in unauthorised exploitation of systems, networks, and technologies. Organizations that suffer cyber security breaches may face significant damages and losses. There are also non-financial costs to be considered, like reputational damage. This was the case of the Cameroon Customs administration, for instance in September 2023 the Customs operations system stopped

INTERNATIONALJOURNALOFRESEARCH SCIENCE& MANAGEMENT

functioning completely for almost 02 whole days. Though this phenomenon is scarce, it happens regularly that we notice interruptions.

- Cyber attacks are increasingly sophisticated. According to a study by McAfee and the CSIS, based on data collected by Vanson Bourne, the world economy loses more than $1 trillion each year due to Cybercrime.
- The idea behind digital customs services as a tool against cyber criminality is to minimize customs hassle, reduce risk and save money to perform customs and border formalities remotely or online.
- The reasons for the increase in rate of infringements are diverse, including the attractiveness of a 'look-alike product' at a cheap price, the ease of production of copies at minimal costs, the development of new forms of marketing such as e-commerce and social media and the growth of international trade.
- Osabiya (2015), Dobre (2013), Festré (2008), Muogbo (2013) and Uzonna (2013) are amongst the scholars who have studied the impact of employee motivation on organizational performance found that high employee motivation has significant positive impact on organizational performance.
- Malin (2013), Wang et al. (2010), Zehira et al. (2012) are among the numerous scholars who have found out that leadership and supervision driven by a positive outlook such as transformational leadership had significant positive impact on organizational performance.
- The vision Statement of cyber customs is to enhance the nation's security through innovation, intelligence, collaboration and trust.
- The Customs cyberspace needs to be secured considering the fact that sensitive information are involved and risks of extorting money or interrupting business normal processes are at stake.
- Beijing believes cyberspace must still respect the culture, customs and personality' s private information (Burgman, Jr., 2016).
- As far as Customs is concerned, effectiveness refers to improved operational efficiency, resource optimization and improved delivery of mandates requiring for that purpose transparency, harmonized procedures, facilitation and efficient fight against fraud.

Possible innovation

Creation of a specific customs unit specialized in fighting cyber crimes in the CCA. The vision Statement of cyber customs being to enhance the nation's security through innovation, intelligence, collaboration and trust in a context of the CCA becoming a member of the defense and security community alongside Police, army, gendarmerie, territorial administration, etc.

Organizational diagnostic (strategy)

In terms of organizational diagnoses, several possibilities are available to the manager including the PESTEL method, the analysis of Porter's 5 forces, the strategy by area of activity (DAS), the VIP model and the SWOT approach.

The PESTEL method makes it possible to study the organizational environment through its political, economic, sociological, ecological and legal components. The analysis of Porter's 05 forces is to evaluate the intensity of said forces and to prioritize the pressures exerted by each of them, in particular competitive intensity, customers, suppliers, substitute products as well as new entrants. Strategy by area of activity (DAS) refers to the division of an organization into strategic areas or strategic segmentation which consists of grouping together homogeneous activities having the same key success factors. The VIP model is designed to answer the 3 questions relating to Value, Imitation and Scope.

The SWOT approach (Strength, Weaknesses, Opportunities and Threats) is one of the main bases of the diagnostic procedures. This involves taking a look at the internal and external environment of the organization in order to draw up a picture of the strengths and weaknesses on the one hand and the opportunities as well as the threats on the other hand.

TYPES OF STRATEGIES	STRONGHOLDS	WEAKNESSES
Deduced strategy (External environment)	**Opportunities** Development of ICT External partners such as OMD, OMC, major schools, training centers, external expertise	**Threat** Budget requirements Economic crises International and national security conflicts

INTERNATIONALJOURNALOFRESEARCH SCIENCE& MANAGEMENT

	Notable support for government policies	Incomplete international legal framework
Built strategy (Internal environment)	**Strengths** Modern IT architecture Existence of a modern training center • Qualified staff Consistent regulations Strong organizational culture	**Weaknesses** Approximate skills management Insufficient monitoring and evaluation of professional training Ineffective skills development plan Absence of a real knowledge management policy GPEC non-existent Systematic overlapping of administrative skills and attributions Career plan to put in place Inadequate HRM, etc.

Conclusion and perspectives

In a nutshell our study which aimed at evaluating the impact of cyber customs on its performance after identifying how and why it should be put in place in the CCA. This research is important considering the fact that Cameroon Customs administrations is facing serious challenges and the bugetary assigned target to the said administration by Government is above 1 000 billions FCFA in 2024. To carry out efficiently our work, firstly we clarified some key notions such as cyber security, cyber criminality, counterfeiting, e-trade, customs services. Secondly we reviewed the following concepts i.e. Customs and Border Protection missions, secured customs cyberspace network, organizations effectiveness and the Nation's security, role of Customs in Cargo Security and maritime governance.

The problem Statement led us to identify areas of questioning concerning the shortcomings of the incumbent customs structuration, why can cyber customs correct the observed gaps, How can we put in place an efficient cyber customs in the CCA and What could be the various recommendations that can be made. The objectives were to identify what is cyber customs and how it can be put in place in the CCA ; Determine its strong holds and possible limits and Formulate recommendations to guarantee its sound application. Our work presented three main interests which are managerial, theoretical and methodological. Four theories guided our analysis i.e. rational choice theory, Institutional Anomie Theory, strain theory and routine activity theory.

As far as research methodology is concerned we mobilized a comparative analysis, Methods of analyses employed chosen was Content analysis (Krippendorff, 2003). We came out with the main results that there is no specific customs unit specialized in fighting cyber crimes as it is the case of the Customs Enforcement (ICE) that have special divisions dedicated to combating cyber crime. As far as electronic crime is concerned, Customs administrations need to be properly equipped and further trained as far as the legal and technological aspects are concerned in order to deal with sophisticated offences committed in cyberspace and which pose a great many challenges.

Therefore the novelty of our research is that the Creation of a specific customs unit specialized in fighting cyber crimes in the CCA. The vision Statement of cyber customs being to enhance the nation's security through innovation, intelligence, collaboration and trust in a context of the CCA becoming a member of the defense and security community alongside Police, army, gendarmerie, territorial administration, etc.

The study also showed that the CCA needs to tackle some external and internal challenges such as budgetary constraints, economic crises, international and national security conflicts, incomplete international legal framework, Approximate skills management, Insufficient monitoring and evaluation of professional training, ineffective skills development plan, absence of a real knowledge management policy, inexistent GPEC, systematic overlapping of administrative skills and attributions and lack of career plan and necessity to put in place adequate HRM, etc.

However the future is bright and the CCA is up to the task regarding its various opportunities and strengths which are development of ICT, external partners such as WTO, WCO , major schools, training centers, external

expertise, notable support for government policies, modern it architecture, existence of a modern training center, qualified staff, consistent regulations and strong organizational culture. Cyber security is a must for the CCA considering the fact that it was recently integrated in the national community of defense and security as a full member.

References

1. Ahmad et al., (2012) Ahmad, R., Yunos, Z., and Sahib, S. (2012). Understanding cyber terrorism: The grounded theory method applied. In Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on, pages 323–328. IEEE.
2. Ayres, N. and Maglaras, L. A. (2016). Cyberterrorism targeting the general public through social media. Security and Communication Networks, 9(15):2864–2875.
3. Aubret, J., & Gilbert, P. (2003). L'évaluation des competences. Editions Mardaga.
4. Cantens, T., Raballand, G., Strychacz, N., &Tchouawou, T. (2011). Réforme des douanes africaines: Les résultats des contrats de performance au Cameroun. Africa—Trade Policy Note, 13.
5. Dietrich, A., Gilbert, P., Pigeyre, F., &Aubret, J. (2010). Management des compétences: enjeux, modèles et perspectives. Dunod.
6. Green, J. (2002). The myth of cyberterrorism. Washington Monthly, 34(11):8–13.
7. Krippendorff, K. (2003) Content Analysis: An Introduction to Its Methodology. 2nd ed. Sage Publications Inc, Thousand Oaks, California.
8. Lewis, G. (2009). The impact of ICT on customs. World customs journal, 3(1), 3-11.
9. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186.
10. Newsome, Y. D. (2003). Border patrol: The US customs service and the racial profiling of African American women. Journal of African American Studies, 31-57.
11. Nguyen, H. T., Grant, D. B., Bovis, C., Nguyen, T. T. L., & Mac, Y. T. H. (2021). Factors affecting efficiency of electronic customs and firm performance in Vietnam. Journal of Asian Finance, Economics and Business.
12. Prince, C. E. (1989). The US Customs Service: A Bicentennial History. Department of the Treasury, US Customs Service.
13. Raus, M., Flügge, B., & Boutellier, R. (2009). Electronic customs innovation: An improvement of governmental infrastructures. Government Information Quarterly, 26(2), 246-256.
14. Urciuoli, L., Hintsa, J., & Ahokas, J. (2013). Drivers and barriers affecting usage of e-Customs—A global survey with customs administrations using multivariate analysis techniques. Government Information Quarterly, 30(4), 473-485.
15. Shirsavar, H. A., & Shirinpour, M. (2016). The effect of electronic customs administration on facilitating the export activities of export companies based in Gilan, Iran. Intellectual economics, 10(2), 114-121.