Concordia University College of Alberta

Master of Information Systems Security Management (MISSM) Program

7128 Ada Boulevard, Edmonton, AB

Canada T5B 4E4

Modeling Information Security Governance in the ECOWAS Zone: The Maturity Model Revisited

by

FIOGBE, Jose

A research paper submitted in partial fulfillment of the requirements for the degree of

Master of Information Systems Security Management

Date: February 2008

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Andy Igonor, Associate Professor, MISSM

Modeling Information Security Governance in the ECOWAS Zone: The Maturity Model Revisited

by

FIOGBE, Jose

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Andy Igonor, Associate Professor, MISSM

Reviews Committee:

Andy Igonor, Assistant Professor, MISSM
Dale Lindskog, Assistant Professor, MISSM
Ron Ruhl, Assistant Professor, MISSM
Pavol Zavarsky, Associate Professor, MISSM

Date: February 2008

The author acknowledges the significant contributions to the work by Academic Advisors and Review Committee Members and gives the right to Concordia Univeristy College to reproduce the work for the Concordia Library, Concordia Websites and Concordia MISSM classes.

Concordia University College of Alberta
Faculty of Professional Education
7128 Ada Blvd, Edmonton, AB, Canada

Modeling Information Security Governance in the ECOWAS Zone: The Maturity Model Revisited

by

Jose Fiogbe

jfiogbe@yahoo.com

Supervisor: Dr. Pavol Zavarsky – Associate Professor and Director of Research

Advisor: Dr. Andy Igonor – Assistant Professor

A research paper submitted in partial fulfillments of the degree of

Master in Information Systems Security Management

February 2008

"Today, we all recognize that ICT is not a matter of choice: it is a necessity. ICT is an indispensable tool for enhancing innovation, competitiveness, modernization, and ushering in other opportunities in the achievement of our collective developmental objectives" –
H. E. John Kufuor, President Of the Republic of Ghana, West Africa

Table of Content

ABSTRACT…….4

1. INTRODUCTION ……..4

2. INFORMATION SECURITY GOVERNANCE AND MATURITY MODEL…….6

2.1 Information Security Governance……..6

2.2 Information Security Governance Maturity Model……...7

3. DIGITAL OPPORTUNITY INDEX (DOI), E-GOVERNMENT RATINGS, AND RESEARCH METHODOLOGY…….9

3.1 Digital Opportunity Index ……..……...9

3.2 E-Government Ratings by Country, 2006……...12

3.3 Research Methodology ...…….……...12

4. ANALYSIS OF INFORMATION SECURITY GOVERNANCE PRACTICES IN THE ECOWAS ZONE…….14

4.1 Virtues and Limitations of the Digital Opportunity Index …….14

4.2 Quantitative Methodology……...18

4.3 Towards a New Maturity Paradigm ……19

5. MODELING INFORMATION SECURITY GOVERNANCE PRACTICES IN ECOWAS.…….....….... .20

5.1 Maturity Assumptions……..……21

5.2 Modeling of Country Information Security Governance Maturity……..……21

5.3 Analyzing the Results…….. ……..…….24

6. Future Work…….....26

7. Conclusion……....28

8. Reference……..28

9. Appendix One: Digital Opportunity Index 2006 Ranking – Africa……..30

10. Appendix Two: Overview of Past, Ongoing and Planned Information and Communications Technology (ICT) Initiatives in ECOWAS……..32

11. Appendix Three: Overview of Past, Ongoing, and Planned Information and Communications Technology (ICT) Initiatives in Nigeria……...35

ABSTRACT

Governance directly impacts information security, focusing in protecting business-critical assets, providing confidentiality, integrity, and availability. Good security practices give assurance of information security to other governments and businesses. In particular, the request for better security governance stems from the necessity to deal with past and emerging risks, threats, and vulnerabilities.

This paper examines information security governance in the Economic Community of West African States (Ecowas). It uses the digital opportunity index 2006 (DOI) computed by the International Telecommunication Union (ITU) and the e-government ratings as in West (2006) to compute a country security governance index. The author then uses that index to rank countries by their current maturity level of information security governance. It proceeds to offer a causal analysis and pinpoint factors that could improve that maturity.

In the paper, we extend the initial maturity model. Our innovation is to do what nobody have done before us, that is to evaluate information security governance in underprivileged West African countries, using an extension to the information security governance maturity model. Although not perfect, this work should be seen as a trailblazer. Our pioneering research helps to open up a new line of research in the promising field of information security governance. It was a difficult and challenging task.

1. INTRODUCTION

What is the maturity level of information security governance in West African countries and how does it compare with Canada and South Africa? Our research aims at answering those two fundamental questions. Our research focuses on the information security governance within an exceptional group of fifteen West African nations called ECOWAS. This group is exceptional because despite having different historical and economic backgrounds, these nations join force for economic growth, sustainable development, to overcome prejudice in many sectors including that of information communication technology (ICT). The “Economic Community of West African States

(ECOWAS) is a regional organization of fifteen West African nations formed in 1975. There used to be sixteen nations in the group until recently when Mauritania withdrew its membership from ECOWAS. The main objective of forming ECOWAS was to achieve economic integration and shared development so as to form an economic community in West Africa. Later on, the scope was increased to include socio-political interactions and mutual development in related spheres"[1].

.Figure 1: Economic Community of West African States (ECOWAS)

Source: http://www.ecowas.info/. Retrieved on January 9, 2008

Figure 1 above lays out the geographical topology of each West African States that has the Ecowas membership, whereas Figure 2 below indicates their respective domain name.

Figure 2: The Fifteen West African Countries and their Top-Level Domain Names

Benin (.bj)	Mali (.ml)
Burkina Faso (.bf)	Niger (.ne)
Cape Verde (.cv)	Nigeria (.ng)
Cote d'Ivoire (.ci)	Senegal (.sn)
Ghana (.gh)	Sierra Leone (.sl)
Guinea (.gn)	The Gambia (.gm)
Guinea-Bissau (.gw)	Togo (.tg)
Liberia (.lr)	

[1] Source: http://www.ecowas.info/. Retrieved on January 9, 2008

First, we present information security governance and the maturity model. Second, we present the digital opportunity index (DOI), secondary data from the International Telecommunication Union (ITU) and our research methodology. Third, the main outcome of our work, we innovate to suggest an extension to the maturity model, to account for regional, inter-country, and intra-country disparities. The next section offers an insight into security governance and the maturity model.

2. THE INFORMATION SECURITY GOVERNANCE AND THE MATURITY MODEL

The present section deals with information security governance and the maturity model.

2.1 Information Security Governance

For the IT Governance Institute, "Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly"[2]. Information security governance concerns the leadership, organization, and processes that protect information assets. It must have a desired outcome, capture knowledge and provide protection of critical assets, earn benefits, and lead to a process integration.

First, strategic alignment, risk management, resource management, performance measurement, and value delivery are all desired outcomes. Second, knowledge, which is a fruitful set of information, is progressively outweighing capital and labor inputs to be the unique productivity factor in the globalized digital economy. In the latter, information is analogous and akin to significance, pertinence, and aim. An effective and sustainable organization's mission requires that security be understood at the highest level of leadership.

Besides, Information security governance can also be defined as the management's capability and skills or ability to manage or guide by advice, helpful information, instruction, and control the organization's IT tasks in harmony with organizational strategic goals. The main challenge is to meet stakeholder expectations when many

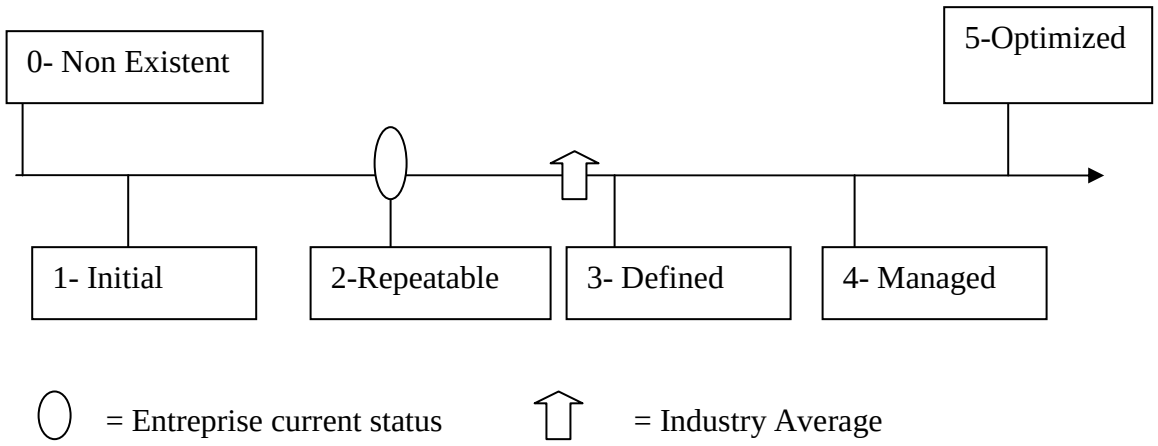
[2] IT Governance Institute. 2003. Board Briefing on IT Governance, 2nd Edition, USA.

business departments have ownership and usage of the same collection of services and where individual business sections that manage the budget for requirement analysis, design, development, maintenance, training, and support possess most applications

2.2 Information Security Governance Maturity Model

We would like to introduce the original information security governance maturity model (ISGM model), in this section. We favor the maturity level paradigm because it follows the guideline of the IT Governance Institute.

Figure 3: Maturity Model Dashboard



Source: IT Governance Institute. Information security Governance. Guidance for Boards of Directors and Executive Management, 2nd Edition. Page 36

The ISGM model has six stages of ripeness, which are non-existent, initial, repeatable, defined, managed, and optimized, from the least to the most mature level.

Non-existent Level

This maturity level comes first. The non-existent level is mainly characterized by the lack of integration of risk assessment during the decision-making processes. Managers ignore security risk, threats, and vulnerabilities.

Initial Level

After the non-existent level comes the initial level. The second phase is the initial level of maturity. No formal security policies, procedures are followed. Moreover, are forgone such concepts as liability, answerability, responsibility, enforcement, blameworthiness and other expressions linked with an expectation of account-giving. Information security is mainly reactive. Though, individual leaders might have some awareness of security.

Repeatable but Intuitive Level

In the repeatable but intuitive level, the third phase, the organization leaders start mastering and paying more attention to IT risks, in an immature and emerging manner. The information systems security is in place but fledging.

Defined Process Level

The fourth maturity level has a defined process in place, implementing documented risk assessment process, formalized security awareness, defined security policies, and consistently applied accountability. Besides, at this level, the process is IT focused instead of business-focused. Though, managers know about the requirements for continuous service.

Managed and Measurable Level

The fifth maturity level is managed and measurable, using standard procedures, enhanced accountability, risk management, and mandatory security awareness. Proactive information security is applied. Senior executives and managers are involved in setting up the risk benchmarks, assigning formalized, standardized, strong security objectives to information security co-coordinators. A consistent procedure is applied.

Optimized Level

Eventually, in the sixth maturity level, when the process is optimized, then security is of the highest concern to senior business and technology leaders in the whole organization. IT Security governance becomes an active and strong part of the corporate governance and strategy. There are verified security plans, end-user accountability, formalized incident response procedures, frequent security assessments, and intrusion testing. At this level, we also have proactive identification of risk to provide the best protection to critical assets.

In the next section, we write about the secondary data and our methodology.

3. DIGITAL OPPORTUNITY INDEX (DOI), E-GOVERNMENT RATINGS, AND RESEARCH METHODOLOGY

This section gives successively information about the secondary data and the methodology. Our analysis is based on data from the International Telecommunication Union, from West (2006), and each country's ICT policy documents. Our purpose is to model the information security governance in the Ecowas zone. We assign a security governance maturity level to each country. Bearing in mind the major classification done by the composite digital opportunity indices (DOI), we update our analysis using e-government ratings, and each country's official ICT policy documents to come up with amore realistic ranking. The latter is used to peg each nation at a given maturity level. The policy documents are those published by the United-Nation Economic Commission for Africa (UNECA) and the West African governments. We ultimately rely on the Worldbank document entitled "Information Communication for Development: Global Trend and Policies, 2006" to get a deeper mastery of the issue.

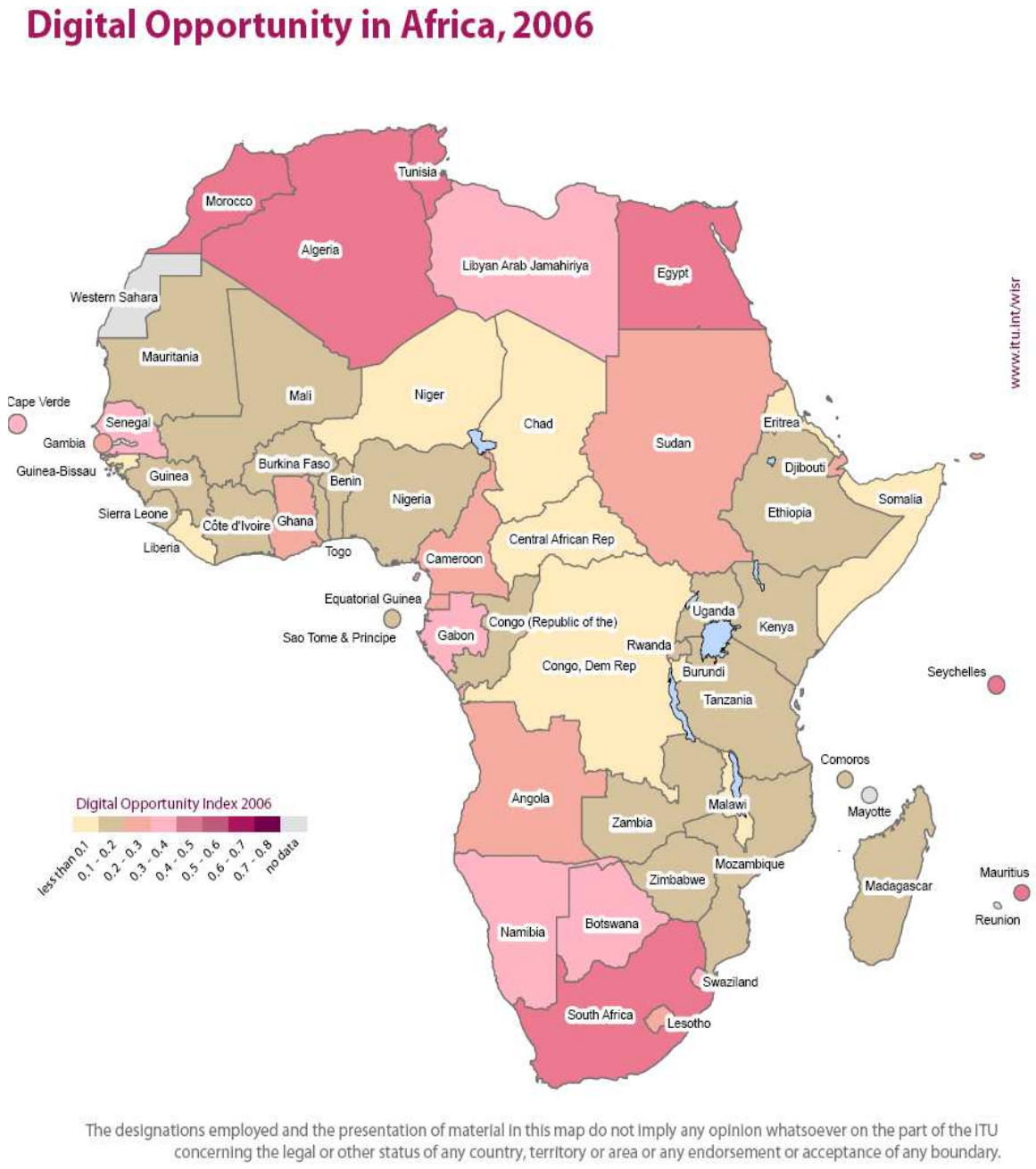
3.1 Digital Opportunity Index (DOI)

The International Telecommunication Union (ITU) elaborated the DOI as a composite index. The DOI rank all countries according to their ICT level based on the three criteria of opportunity, infrastructure, and utilization. The Digital Opportunity Index (DOI) is a composite index that has been generated from a group of eleven internationally-agreed core ICT indicators (recommended by the Partnership on Measurement of the Information Society). It gives a measure of access to telecommunications and digital opportunity in 180 countries worldwide and pays heed to the policy implications for the future evolution of the Information Society. The DOI, along with the ICT-Opportunity index (ICT-OI), constitutes one of the two indices endorsed in the World Summit on the Information Society (WSIS) Tunis Agenda. We choose the DOI over the ICT-OI because it is computed as a mathematical average within a definite range of 0 to 1.

Again, the DOI rank all countries according to their ICT level based on the three criteria of opportunity, infrastructure, and utilization. The DOI is standard, yet very flexible indicator and a tool for benchmarking. The DOI can assist governments, policy-makers,

researchers, and academics in evaluating policies and their effects. It can also be used to monitor growth of technological advances, to promote a rich and inclusive information society worldwide, in conformity with the WSIS targets.

Table 4: DOI from International Telecommunication Union (ITU).



Created by the ITU, the digital opportunity index (where 1=full ICT access) ranks countries on ICT policy, access to computers and phones, as well as cost and quality of

infrastructure. The digital opportunity index (DOI) is a good instrument to evaluate information technology performance, and hence information security governance, amongst West African countries and measures their e-readiness, by an internationally agreed standard. According to the International Telecommunication Union (ITU), "*The Digital Opportunity Index is an e-index based on internationally-agreed ICT indicators. This makes it a valuable tool for benchmarking the most important indicators for measuring the Information Society. The DOI is a standard tool that governments, operators, development agencies, researchers and others can use to measure the digital divide and compare ICT performance within and across countries. The Digital Opportunity Index (DOI) is based on 11 ICT indicators, grouped in 3 clusters: opportunity, infrastructure and utilization. The DOI has been compiled for 181 economies for a period of three years from 2004-2006. An even longer time series for 62 leading economies for the period 2000-2006 is also available"*[3].

Eventually, the digital opportunity Index is a composite index that can be used to facilitate the comparability of data for the Ecowas countries. Most importantly, the index has been elaborated following a modular methodology, in order to allow future extensions easily and an adaptation for national use, or used alongside other indices, such as the UNDP's Human Development Index. As a proof-of-concept, we will extend the DOI to describe the information security governance.

In this paper, we rely partially on the digital opportunity index. The DOI indicator ranks countries by level of technology development. The DOI rank all countries according to their ICT level based on the three criteria of opportunity, infrastructure, and utilization.

We use the Digital Opportunity Index, along with information from West (2006), National Information Communication Infrastructure (NICI)[4] Policies - published for each African nation by the Economic Commission for Africa -, and the Worldbank. Those country documents contain useful information about each African country level implementation. For Nigeria, for example, we add information from the Nigerian Information Technology Development Agency (NITDA). The document we explore is

[3] International Telecommunication Union; http://www.itu.int/ITU-D/ict/doi/index.html. Retrieved on 28/01/2008

[4] http://www.uneca.org/AISI/nici/documents.htm

the Nigerian National Policy for Information Technology (IT) 'use it', National Information Technology Policy.

The Ecowas data are the author's computation based on secondary data from the International Telecommunication Agency (ITU), and West (2006).

3.2 E-Government Ratings by Country, 2006

We follow West (2006)[5] to collect more secondary data. In his report, West (2006) presents the sixth annual update on global e-government. Using an analysis of 1,782 government websites in 198 different nations undertaken during summer 2006, he investigates electronic government. The author explores e-government issues by choosing representative websites for each country: the government official websites themselves. He focuses on many criteria like privacy policies. West (2006) finds huge variations among countries in their overall e-government performance based on his analysis.

In a country, at the macroeconomic policy level, we believe that the overall importance attributed to information security governance by a government is reflected on its own website. Therefore, data from West (2006) report can be a good candidate to the evaluation of IT security governance, along with the digital opportunity index (DOI) for the year 2006.

3.3 Research Methodology

Created by the ITU, the digital opportunity index (where 1=full ICT access) ranks countries on opportunity, infrastructure, utilization, i.e. ICT policy, access to computers and phones, as well as cost and quality of infrastructure, for example. The digital opportunity index (DOI) is a good instrument to evaluate information technology performance, and hence information security governance, amongst West African countries and measures their e-readiness, by an internationally agreed standard

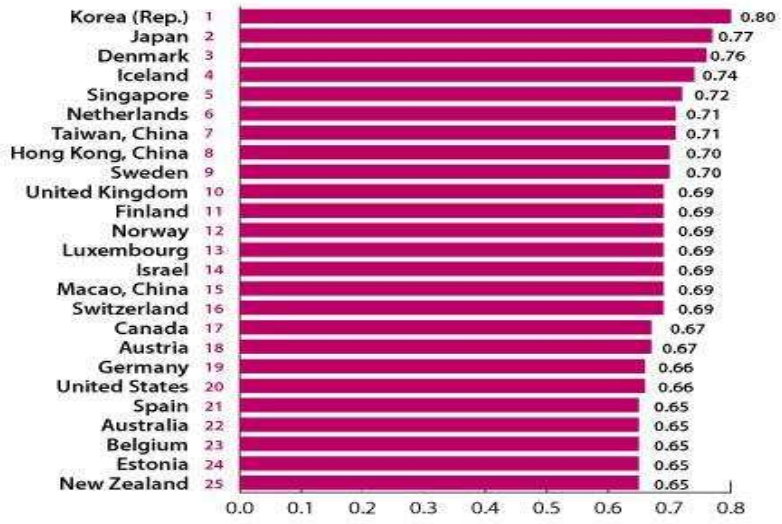
We concur within the International Telecommunication Union (ITU) to write that, as a composite index, the DOI permits the tracking and comparison of states in various

[5] West D.;2006; Global E-Government, Center for Public Policy, Brown University, Providence, Rhode Island 02912-1977 United States, Darrell_West@brown.edu, (401) 863-1163, www.InsidePolitics.org

aspects of the information society. It assesses countries' ICT capabilities in quality, affordability, infrastructure, access path and device, and coverage.

In a nutshell, we follow the ITU to conclude that "the Digital Opportunity Index (DOI) measures these aspects, including price and affordability of ICTs (Internet and mobile, relative to average income. The Digital Opportunity Index measures the ICT penetration of households and individuals relative to 100% ownership, to measure growth in the ICT development of each economy over time. This enables cross-country comparisons, as well as comparisons of growth in digital opportunity over time"[6]. In our study we give a weight of 80 percent to the digital opportunity index and a weight of 20 percent to the secondary data from the West (2006) Report.

Table 5: DOI for Top 25 Economies, 2006



Source: ITU, DOI for the year 2006 published in 2007

The digital opportunity index is the main indicator, alongside data from West (2006), and information from each country ICT policy documents, we use to determine the country maturity level.

In the next section, we undertake an analysis of security governance in an underprivileged part of the World.

[6] International Telecommunication Union; http://www.itu.int/ITU-D/ict/doi/index.html. Retrieved on 28/01/2008

4. ANALYSIS OF INFORMATION SECURITY GOVERNANCE PRACTICES IN THE ECOWAS ZONE

Using the digital opportunity index 2006 from the International Telecommunication Union (ITU) and the e-government ratings computed in West (2006), this section analyzes the issues at stake, to rank the countries. The section gives successively information about the limitation of the data, the assessment methodology, and the results.

4.1 Virtues and Limitations of the Digital Opportunity Index

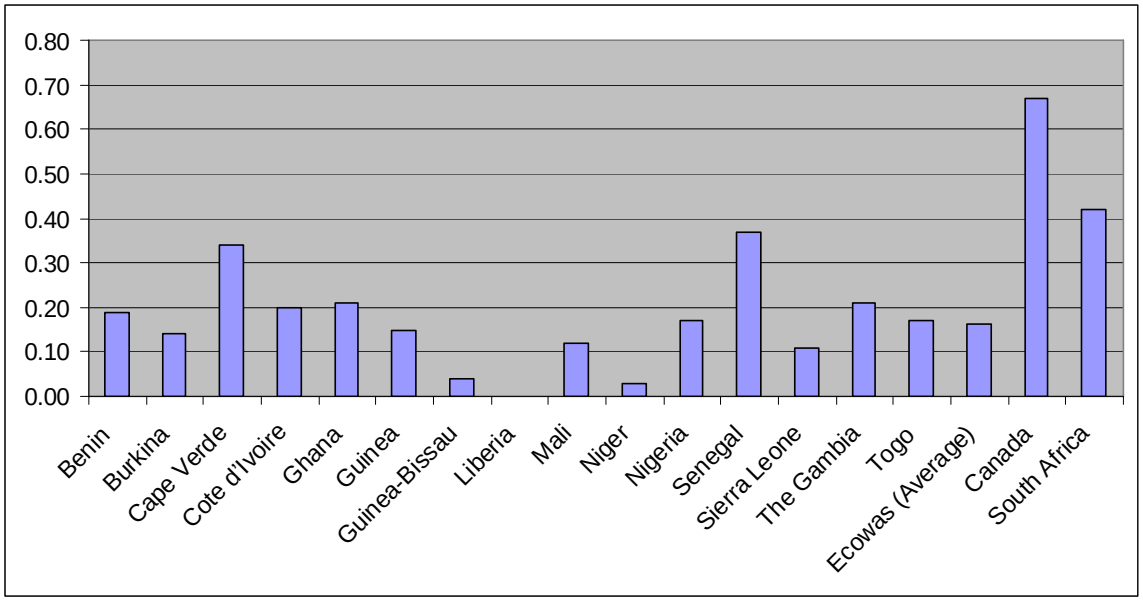
It is straightforward, that the DOI ranks the countries. For example, Canada has a DOI of 0.67, which is higher than that of South Africa (0.42) or Senegal (0.37).

Table 6: Composite Digital Opportunity Index (DOI), 2006

Countries	DOI	Countries	DOI
Benin	0.19	Liberia	0.00
Burkina	0.14	Mali	0.12
Cape Verde	0.34	Niger	0.03
Cote d'Ivoire	0.20	Nigeria	0.17
Ghana	0.21	Senegal	0.37
Guinea	0.15	Sierra Leone	0.11
Guinea-Bissau	0.04	The Gambia	0.21
South Africa	0.42	Togo	0.17
Canada	0.67	Ecowas	0.16

Source: Author's analysis based on data from ITU

Table 7: Digital Opportunity Index



Source: ITU

We are not able to confirm the DOI of Cape Verde, which is like a puzzle. Further research is needed for Cape Verde. So Senegal and Cape Verde win the top Digital Opportunity Indices. Nigeria earns a DOI of 0.17 despite all the heavy investment in ICT. We explain this with our concept of deep intra-country imbalance or disequilibrium later.

The DOI can be employed to compare countries, monitoring progress, urban and rural divide, for example.

Among the virtues of the DOI, it comes to our attention that the DOI is the standard, but flexible indicators, relevant to developing countries, and forward-looking. The DOI ranks the world's nations according to their degree of penetration of ICTs, or their e-readiness. In the framework of the implementation of the WSIS Plan of Action, a composite "Digital Opportunity Index" is based on the base list of indicators agreed by the "Partnership for Measuring ICT for Development" of UN agencies at their meeting on 7-9 February 2005. The methodology is built around eleven indicators in four clusters. The clusters concern:

i) Affordability and coverage, which includes the mobile phone coverage and tariff baskets for mobiles and Internet access.

ii) Access path and device, which concerns the penetration of fixed-lines, mobile phones and PCs.

iii)Infrastructure that is related to the fixed and mobile Internet subscribers and international Internet bandwidth per inhabitant.

iv)Quality, which concerns the penetration of fixed and mobile broadband subscribers.

In West (2006), the data for analysis is from an assessment of 1,782 national government websites for the 198 nations around the world. He analyzes a group of sites within each nation to obtain a full knowledge of the situation in each country. The paper analyzes website of executive offices (those of president, ruler, prime minister, royalty, party leader), legislative offices (such as Parliament, Congress, People's Assemblies), judicial offices (such as major national courts), Cabinet offices, and major agencies serving top functions of government, such as education, health, human services, taxation, interior, economic development, military, administration, natural resources, foreign affairs, tourism, foreign investment, business administration, and transportation. The author does not include websites for sub national units, obscure boards and commissions, local government, regional units, and municipal offices in his research. The study was done during June and July, 2006 at Brown University in Providence, Rhode Island.

Websites are assessed for their protection of multiple characteristics like privacy, security, public access, information availability, and service delivery. Besides, the paper evaluates privacy policy, digital signatures, credit card payments, email address, comment form, automatic email updates, website personalization, and personal digital assistant (PDA) access, amongst others.

The study by West (2006) checks for visible statements highlighting privacy and security measures because it is important to attract weary population. Citizens must trust e-government services and information. People should feel safe and secure in their online information and service activities. If e-government is to be efficient, then information security governance must be taken very seriously by the country’s leadership.

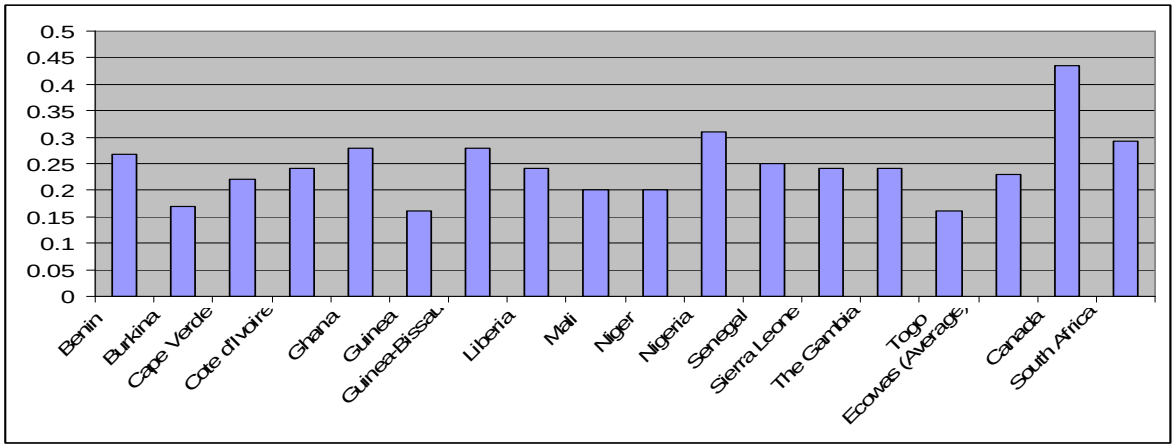
Table 8: E-Government Ratings for Canada, South Africa, and West African Country, 2006
(Converted to a scale from 0 to 1)

Countries	Value	Countries	Value
Benin	0.267	Liberia	0.240
Burkina	0.170	Mali	0.200
Cape Verde	0.220	Niger	0.200
Cote d'Ivoire	0.240	Nigeria	0.311
Ghana	0.280	Senegal	0.251
Guinea	0.160	Sierra Leone	0.240
Guinea-Bissau	0.280	The Gambia	0.240
South Africa	0.292	Togo	0.160
Canada	0.435		

Source: West D; 2006; Global E-Government, Center for Public Policy, Brown University, www.InsidePolitics.org

We choose Canada and South Africa as benchmarks for our study.

Table 9: E-government Country Ratings or Indices as in West (2006)



Source: West D.; 2006; Global E-Government, Center for Public Policy, Brown University, www.InsidePolitics.org

The main limitation of the DOI is the issue surrounding the adaptation of the DOI to account for innovation and technological change.

4.2 Quantitative Methodology

The evaluation includes a quantitative analysis of information security governance based on secondary data from two main sources: ITU and West (2006). We use the secondary data from those sources to compute a composite country index. We use the 80-20% rule to compute the country index. We give a weight of 80% to the Digital opportunity Index and 20% to the secondary data from West (2006) paper.

Country Security Governance Index = 80% DOI + 20% E-government Country Rating

Table 10: Country Security Governance Index for West Africa, Canada, and South Africa, 2006
(Scale of 0 to 1)

Countries	Value	Countries	Value
Benin	0.21	Liberia	0.05
Burkina	0.15	Mali	0.14
Cape Verde	0.32	Niger	0.06
Cote d'Ivoire	0.21	Nigeria	0.2
Ghana	0.22	Senegal	0.35
Guinea	0.15	Sierra Leone	0.14
Guinea-Bissau	0.09	The Gambia	0.22
South Africa	0.39	Togo	0.17
Canada	0.62	Ecowas	0.18

Source: Author's analysis based on data from ITU and West (2006)

With the digital opportunity index, the result will be used to determine the maturity levels, in the rest of our research.

4.3 Towards a New Maturity Paradigm

This research is based on multiple source data and policy documents at both the country level and Ecowas level. In evaluating the maturity level in each country, we only use secondary data. Therefore, the fundamental trend is given by the major secondary data that we use as main indicator, which is the digital opportunity index (DOI) from the International Telecommunication Union (ITU)

Finally, the scale is from one to seven for the maturity levels. The optimized maturity level is the most mature level and the non-existent one the least. The chosen scale allows us to get a more precise evaluation than we would have obtained with a scale from 0 to 5 for example.

From this point, the author uses his knowledge of the Ecowas and the newest ICT policies documents to match each country or a group of countries to its maturity level. We can infer the maturity level from the DOI indicator combined with other determinants.

At a first glance, the country security governance shows that the top performers are Senegal with a score of 0.35, Cape Verde (0.32), and Ghana (0.22). Consequently, in our study, security governance is being well taken care of in Senegal, Cape Verde, and Ghana. This makes, for example, Senegal slightly better ranked than the two others, but well above Liberia. West African nations, though, score well below the benchmark country of Canada and South Africa, which surge respectively at 0.62 and 0.39 on our composite country security governance index. This is due not to chance, but to the superior importance those benchmark countries give to information security matters, to protect their business-critical and government-critical assets.

5. MODELING INFORMATION SECURITY GOVERNANCE PRACTICES IN ECOWAS

In this section, we present the outcome of our research.

5.1 Country Maturity Assumptions

From the start of this research project, we try to find out the maturity level of information security governance in each West African Country. How do West African countries fare on information security governance? This requires a broader knowledge to evaluate at country levels. The IT Governance Institute recommends the Maturity Model[7] to compare organization's security governance. Our goal is to reappraise that model. Our innovation is to revisit it and adapt it to countries in the underprivileged parts of the world like West Africa.

We use an extension to the maturity model to determine the information security governance ripeness in each West African nation. For that matter, our purposely-built Country Governance Security Maturity Model classifies West African nations by the maturity level of their information systems security governance. We consider the six initial steps of the original maturity model. But we believe that we must take account for the intra-country and inter-country disparities to be able to extend the model to geographical entities.

For Canada and the Federal Republic of Nigeria, we must consider the difference in information technology between provinces in the former and states in the latter. For simplicity, we assume that all provinces in Canada have arguably a very similar level of maturity in the technology development, across the board. Our position stems from the facts that there exists a fair equalization process between provinces in Canada. On the contrary, Nigerian states do not encounter such privileged treatment and the disequilibrium can be enormous from The Katsina state in the North to the oil-rich Delta States in the South of the federation. We arguably believe we should account for these discrepancies. By the same token, we also pinpoint major disparities between Senegal, and Cape Verde, on one hand, and the other Ecowas countries on the other hand, as shown by their respective country security governance maturity indices. We must take

[7] IT Governance Institute. Information Security Governance. Guidance for Boards of Directors and Executive Management. 2nd Edition. Page 36

into account this inter-country imbalance as well. For instance, there is a huge dissemblance between the ICT facilities in Guinea-Bissau on one side and Senegal or Ghana on the other.

For the above reasons, we propose and use the following eight levels that form our new Country Information Security Governance model or, using its acronym, simply the CISGM model[8]. As a major innovation, the CISGM model is unique and, most importantly, distinguishes two extra maturity levels on top of the six maturity ones from the initial ISGM model examined previously.

Level 0: non existent i.e. no applied management processes like in case of wars (Liberia, Sierra Leone)

Level 1: initial (adhoc but disorganized processes like Cote d'Ivoire[9], Togo, Cape Verde, Guinea-Bissau, Guinea, Niger)

Level 2: Intra-Country Imbalanced (within a federal poor country like Nigeria with dependent local states)

Level 3: Inter-Country Imbalanced (within underprivileged zone made of independent sovereign states like the Ecowas zone)

Level 4: Repeatable (Processes follow a regular pattern: Senegal and Ghana)

Level 5: Defined (documentation and communication of processes like South Africa)

Level 6: Managed (measurement and monitoring of processes like in Canada)

Level 7: Optimized (Good practices are followed and automated like in the USA).

The Country Information Security Governance (CISGM) Model is applied in the following sections below.

5.2 Modeling of Country Information Security Governance Maturity

The maturity level model is our original model. We derive the extended Model by adding the following two extra levels:

- Intra-Country Imbalanced maturity level
- Inter-Country Imbalanced maturity level

[8] For more detail, please refer to IT Governance Institute. Information Security Governance; Guidance for Boards of Directors and Executive Management. 2nd Edition. Page 36-39

[9] Cote d'Ivoire used to have one of the best ICT. It is now in a political turbulence zone at the moment. It is recovering fast but the intra-communication between the South and the North is not effective yet.

We would like to implement our extended model. We called this new model "The Country Security Governance Maturity Model" to be applied to a country or a group of countries, which constitutes a regional community, specifically the Ecowas zone. Our results suggest that Nigeria is at the Intra-Country Imbalanced Maturity level while Ecowas is at the inter-country imbalanced maturity level. Even though both Nigeria and Ecowas has nearly the same mathematical average index, respectively 0.2222 and 0.2212, we believe that Ecowas has an advantage because of the many community projects it is leading in the region. We believe that we must account for the principle of synergy inherent to pulling together forces in a union.

Applicability of the Maturity Model to the Ecowas Zone

We expect to see the countries like Senegal, Cape Verde, and Ghana to have the most mature security governance since they get the highest marks in our previous country security governance index. Nigeria may present a challenge though because of the structural imbalance within the Nigerian federation itself. On one hand, Lagos States and Delta Oil States are wealthier than Northern poorer States on the other. This extended model is more suitable to the information security fact in West Africa where countries are at very different stage of their ICT development.

Table 11: Matching Country Maturity Levels with Country Security Governance Index

(Indices are on a scale from 0 to 1)

Country Maturity Levels	Corresponding Country Security Governance Index (or Range)
Level 0: Non-Existent	0.0 to 0.049
Level 1: initial	0.050 to 0.299 for most unitary States 0.050 to 0.199 for a federation of States 0.050 to 0.199 for a regional organization of States
Level 2: Intra-Country Imbalanced	0.200 to 0.299 Plus sustainable ICT national projects (endogenous, domestic disequilibrium within the

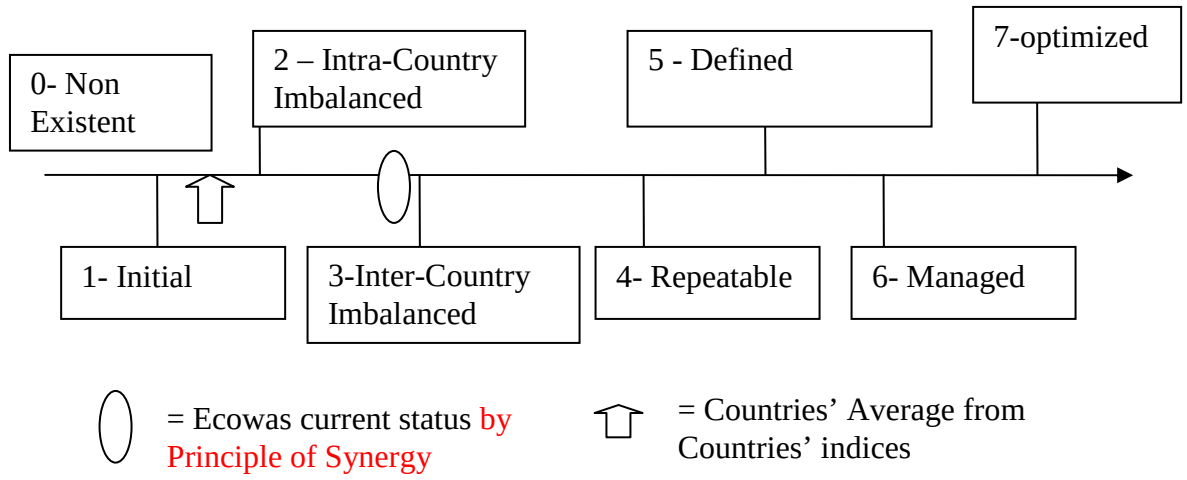
	nation), for a federation like Nigeria
Level 3 Inter-Country Imbalanced	0.200 to 0.299 plus some sound, viable, and successful i.e. sustainable regional ICT projects (exogenous Principle of Synergy originating from the Community of nations with spillover effects on each member country), for a regional organization like Ecowas.
Level 4 : Repeatable	0.300 to 0.399
Level 5: Defined	0.400 to 0.499
Level 6: Managed	0.500 to 0.699
Level 7: Optimized	0.700 to 1

Source: Author's analysis based on data from ITU and West (2006)

Modeling of Ecowas

We use the extended maturity model that we called the "Country Security Governance Maturity Model" to undertake a comparative study of Ecowas. Indeed, we notice that Ecowas is at the inter-country imbalanced maturity level. At this level, countries can communicate at the speed of the least developed nation within the region of Ecowas. But their ICT transactions are executed at a higher speed than otherwise, with Canada or South Africa or other more developed Western nations with better maturity levels. Given its index average and the sustainable, regional ICT project implementations lead by the organization, Ecowas is set at the inter-country imbalanced maturity level. In the long run, that unstable quasi-equilibrium should converge to a more stable state like an optimized steady state.

Figure 12: Synoptic Presentation of our Country Governance Maturity Model



Source: Authors' analysis based solely on secondary data from ITU and West (2006), UNECA, Ecowas, and each country's ICT policy documents

5.3 Analyzing the Results

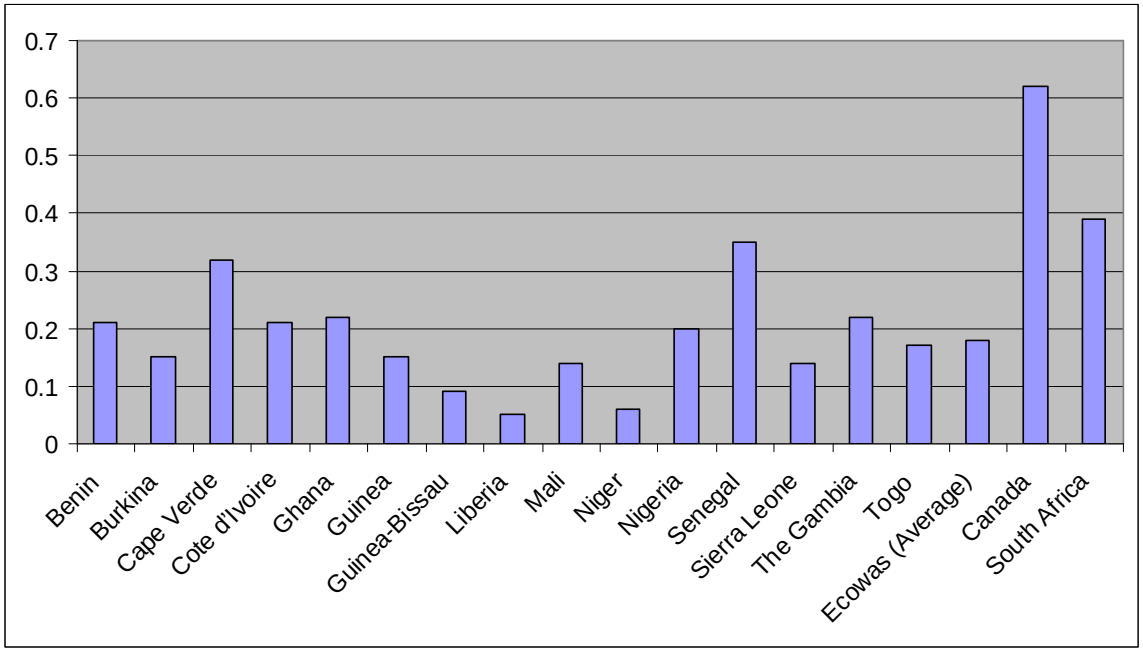
Based on our research, Senegal scores 0.35, which places it at the level 4 or the repeatable country security governance maturity level. Another country at the same level as Senegal is the archipelago of Cape Verde. The Federal Republic of Nigeria is put at the intra-country imbalanced level 2 while Ecowas, the regional organization, is set at the initial maturity level. At the maturity level 1 or the initial stage, there are adhoc but disorganized processes like in most West African nations like Cote d'Ivoire[10], Togo, Guinea-Bissau, Guinea, and Niger, to name a few.

Because Nigeria is a federation of dependent local states, with very different infrastructure maturity or Level 2, we rank Nigeria in the intra-country imbalanced category. Nigeria is a very diverse entity within which the States have their own local governments. The State legislatures and the State government, within the biggest West African country, take independent decisions. In contrast, most of the other West African

[10] Cote d'Ivoire used to have one of the best ICT. It is now in a political turbulence zone at the moment. It is recovering fast but the intra-communication between the South and the North is not effective yet.

countries are at the second maturity level, which is the initial level one. The very first level is level zero, among eight levels in total

Figure 13: Composite Country Security Governance Indices



Source: Authors' analysis based on data from ITU and West (2006)

Besides, at the maturity Level 3, if progress continues, we could have the Economic Community of West African States (ECOWAS), an organization formed by a set of independent sovereign states. Countries are not at the same level of maturity and IT decisions are decentralized. Presently, Ecowas itself is ranked at the initial level, but could be ranked later in the inter-country imbalanced, within this underprivileged zone. Once again, at level 4, we notice that Senegal and Cape Verde are at the repeatable maturity level. South Africa has one of the best Information communication technology systems in Africa and is at the repeatable maturity level 4 but is moving fast towards the level 5, with proactive information security. Since Canada has a country index of 0.62, a better IT system than South Africa, it deserves to be placed at level 6, above South Africa.

All in all, our finding is consistent with both the hierarchical typology previously built and the fundamental, preeminent trend given by the digital opportunity index. It is instrumental to emphasize that the trend is wholly impulsed by our secondary data. The

West African nations with higher DOI are also the ones found to be of higher maturity level than the others. It is the case for Senegal and Cape Verde, for example. In the case of Nigeria, it is at the initial level one but is moving to level two thanks to huge efforts in security governance. Nigeria will reach the intra-country imbalanced level very soon. We would like to conclude to explore the path for future work.

6. Future Work

This research paper is the very first attempt to evaluate information security governance in an underprivileged part of the World like West Africa, using an extension to the information security governance (ISGM) model fathered by the IT Governance institute. We revisited and built an extension to that model. The new model, that we named Country Information Security Governance Maturity (CISGM) model, is groundbreaking. It opens new path for further research in the field of information security governance. The work we did is unique. Its novelty resides in the fact that, before us, no one dares to analyze the information security governance in an underprivileged area like West Africa. Therefore it was a challenging but inspiring task. The author emphasizes that this paper may not be perfect. But it should fire the ambition for further research in the information security governance applied to poor countries. For example, it could be used to explore the state of information security governance in most underprivileged parts of the World. It is suitable for large nations like India or China, federal countries like Nigeria or Brazil, and even small open country like Benin Republic or Senegal Republic. Besides, it could be applied to regional organization like Southern African Development Coordination Conference (SADCC), which unites 9 states with a combined population of 60 million. It can even conveniently be applied to the Association of Southeast Asian Nations, commonly referred to as ASEAN.

Besides, in future work, later, we will go further on the field to collect primary data based on survey or phone interviews, in West Africa. We will also determine the best linear unbiased estimator (BLUE) for a linear multivariate regression model. In case the linear model does not give consistent estimates, then we will proceed with non-linear models. Furthermore, we can derive mathematically the Ecowas estimator and the country estimators using the statistical concepts of proxy variables and instrumental variables.

Along with the other secondary data compiled from West (2006), we can use the composite digital opportunity index (DOI) to derive good estimates for the information security governance data because the DOI establishes an implicit classification of the countries worldwide.

We suggest using the digital opportunity index (DOI) as a good instrumental variable in the modeling of information security governance for the West African country group called Ecowas. Because the digital opportunity has a lower and upper bound (0 and 1), it can be used as a very good ICT policy analysis tool. Unlike the DOI, the ICT opportunity Index (ICT-OI), the other uniquely internationally-agreed index, is a more inclusive index obtained by geometric mean and does not have an upper bound, which precludes it to be used as a policy analysis tool like the DOI is. The DOI is a very good instrumental variable to approximate the information security estimate. Later, in another paper, we can use a linear or non-linear regression model to fit the data. If we use the DOI as a proxy or an instrumental variables for security governance, we can test and estimate information security governance.

The author believes that the composite Digital Opportunity Index is a very good instrument to measure the information security governance. His position stems from the fact that digital opportunity means ideally:

i) Universal, easy access to ICTs at affordable prices;

ii) Universal equipment of all homes with ICT devices;

iii) All citizens having mobile ICT devices;

iv) Everybody using broadband.

In future work, later, we will go further to determine the best linear unbiased estimator (BLUE) for a linear multivariate regression model. In case the linear model does not fit the data well or gives inconsistent estimates, then we will proceed with non-linear models, in a future paper. We can use a mathematical model to validate the model but this is beyond the scope of this work.

7. Conclusion

In our study we give a weight of 80 percent to the digital opportunity index and a weight of 20 percent to the secondary data from the West (2006) Report, because the DOI is an internationally agreed index.

Overall the research project is very challenging. It gives us an opportunity to better comprehend the state of the security governance in West Africa. We identify the maturity levels using a modified maturity model, which we adapt to the political structures.

Our work throws some light on the wide gap amongst West African states. Furthermore, we find a marked discrepancy between Canada and West Africa, that latter still lags far behind in security governance. Our findings are that Senegal and Cape Verde have the highest maturity level. The other must improve on government actions and best practices, government human capacity building, and attract much needed investments to mature.

In the paper, we extend the initial maturity model. Our big innovation is to do what nobody have done before us, that is to evaluate information security governance in underprivileged West African countries, using an extension to the information security governance maturity model. Although not perfect, this work should be seen as a pathfinder. Our pioneering research helps to open up a new line of research in the promising field of information security governance. It was a difficult and challenging task.

Eventually, we should fine-tune the model to capture the positive or negative externalities within each country. Nigeria, because of its federal political structure, seems to be a very good candidate for further research.

8. References

1. Status of Information and Communication Technologies in Africa: the changing regulatory environment. DISD/ICT/2000/NRP/1, December 2000.
Retrieved on 04 January 2008 from
http://www.uneca.org/aisi/nici/documents/status_of_information_and_commun.htm

2. McCarthy K. 2005. Light regulation will beat child porn, says trade minister. Retrieved on January 5, 2008
http://www.theregister.co.uk/2005/11/21/alun_michael_wsis/

3. Agence des Telecommunications de Cote D'Ivoire (ATCI). Retrieved from http://www.atci.ci/pages/loirec.htm, on January 7, 2008.

4. Network Information Center Côte d'Ivoire http://www.nic.ci/. Retrieved on January 7, 2008

5. Tebeje A. 2005. Brain Drain and Capacity Building in Africa Retrieved on January 9, 2008 from http://www.idrc.ca/en/ev-71249-201-1-DO_TOPIC.html

6. Kaberuka D. 2007. Joint statement issued at the end of landmark "Connect Africa" two-day summit in Kigali

7. Economic Community of West African States. http://www.ecowas.info/. Retrieved on January 9, 2008

8. Economic Commission for Africa -Commission économique pour l'Afrique. 1997. Report on a Subregionsl Workshop in Nigeria on the Internet for West African Anglophone Countries, Abuja, Nigeria, 21-23 April 1997

9. Provision from the Regional African Telecommunication Development Conference, Harare 1992, Buenos Aires Declaration in 1994, ECA's Resolution no. 812 (XXXI) of May 1996

10. Houédraogo A. Rencontre sur le net (Meeting on the Internet). 2008. Journal du jeudi| Le Faso http://www.afribone.com/article.php3?id_article=9467. Retrieved on January 8, 2008.

11. The Associated Press. 2007. Australian Farmer Escapes Internet Love Scam from Mali. http://www.iht.com/articles/2007/08/13/africa/mali.1-113940.php. Retrieved on January 8, 2008

12. Status of Information and Communication Technologies in Africa: the changing regulatory environment. DISD/ICT/2000/NRP/1, December 2000. Retrieved on 04 January 2008 from
http://www.uneca.org/aisi/nici/documents/status_of_information_and_commun.htm

13. UNECA. http://www.uneca.org/aisi/nici/Benin/benin.htm. Retrieved on 8 January 2008

14. Burkina-NICI Policy Development Process. Retrieved on January 7, 2008. http://www.uneca.org/aisi/nici/Burkina_Faso/burkina.htm

15. Nuhu R. 2004. *Implication of Economic and Financial Crimes on the Nation's Economy*. Nigeria. Being a paper presented to Defence Adviser Conference in Abuja, on the 10th September, 2004.

16..IT Governance Institute. Information security Governance. Guidance for Board of Directors and Executive Management, 2nd Edition.

17: International Telecommunication Union (ITU)
18. Licensing in the Era of Liberalization and Convergence: the Case Study of the Federal Republic of Nigeria; International Telecommunication Union (ITU)

19. Nigerian National Policy for Information Technology (IT) 'use it', National Information Technology Policy

20. Worldbank 2006, Information Communication for Development: Global Trend and Policies

21. West D.;2006; Global E-Government, Center for Public Policy, Brown University, Providence, Rhode Island 02912-1977 United States, Darrell_West@brown.edu, (401) 863-1163, www.InsidePolitics.org

22. ITU; West African Common Market Project: Harmonization of Policies Governing the ICT Market in the UEMOA-ECOWAS Space Model ICT Policy and Legislation

23. Dada J., Global Information Society Watch (GISW). Nigeria report and other country reports

24. ITU, UNCTAD; 2007; World Information Society Report 2007 Beyond WSIS

9. Appendix One: Digital Opportunity Index 2006 Ranking - Africa

Table 2a Digital Opportunity Index 2005/06 – Africa

Rank in Africa 2005/2006	Economy	Opportunity 2005/2006	Infrastructure 2005/2006	Utilization 2005/2006	Digital Opportunity Index 2005/2006	World Rank 2006/2006
1	Mauritius	0.98	0.43	0.09	0.50	58
2	Seychelles	0.96	0.35	0.14	0.48	62
3	Morocco	0.89	0.16	0.37	0.47	68
4	Algeria	0.93	0.19	0.15	0.42	83
5	South Africa	0.94	0.24	0.08	0.42	86
6	Tunisia	0.97	0.20	0.07	0.41	87
7	Egypt	0.96	0.22	0.04	0.41	91
8	Botswana	0.93	0.15	0.08	0.38	100
9	Gabon	0.92	0.13	0.07	0.37	103
10	Senegal	0.73	0.07	0.31	0.37	106
11	Libya	0.93	0.13	0.02	0.36	109
12	Namibia	0.88	0.14	0.02	0.35	113
13	Cape Verde	0.79	0.16	0.07	0.34	115
14	Swaziland	0.85	0.10	0.02	0.32	120
15	Equatorial Guinea	0.73	0.07	0.01	0.27	131
16	Djibouti	0.74	0.05	0.01	0.26	132
17	Lesotho	0.71	0.05	0.01	0.26	133
18	Sudan	0.66	0.04	0.02	0.24	136
19	Cameroon	0.66	0.04	0.01	0.24	137
20	Angola	0.64	0.03	0.01	0.23	138
21	Ghana	0.56	0.04	0.03	0.21	142
22	Gambia	0.53	0.08	0.01	0.21	144
23	Côte d'Ivoire	0.43	0.06	0.09	0.20	145
24	Benin	0.52	0.03	0.03	0.19	146
25	Togo	0.46	0.03	0.03	0.17	151
26	Congo (Republic of)	0.48	0.04	0.00	0.17	152
27	Kenya	0.46	0.05	0.01	0.17	153
28	Mauritania	0.46	0.06	0.00	0.17	154
29	Nigeria	0.45	0.05	0.01	0.17	155
30	Comoros	0.47	0.03	0.00	0.17	156
31	Zimbabwe	0.37	0.06	0.06	0.16	157
32	Uganda	0.46	0.02	0.01	0.16	158
33	S.Tomé & Principe	0.38	0.06	0.03	0.15	159
34	Guinea	0.43	0.01	0.00	0.15	161
35	Tanzania	0.41	0.03	0.00	0.15	162
36	Zambia	0.40	0.03	0.00	0.14	163
37	Rwanda	0.40	0.01	0.01	0.14	164
38	Burkina Faso	0.38	0.03	0.01	0.14	165
39	Madagascar	0.35	0.02	0.00	0.12	167
40	Mozambique	0.33	0.02	0.01	0.12	168
41	Mali	0.33	0.02	0.00	0.12	169
42	Sierra Leone	0.32	0.02	0.00	0.11	171
43	Ethiopia	0.30	0.01	0.00	0.10	172
44	Burundi	0.27	0.01	0.00	0.09	173
45	Central African Republic	0.25	0.01	0.00	0.09	174
46	Malawi	0.23	0.01	0.01	0.09	175
47	D.R. Congo	0.22	0.02	0.00	0.08	176
48	Eritrea	0.19	0.01	0.00	0.07	177
49	Guinea-Bissau	0.10	0.03	0.01	0.04	178
50	Chad	0.11	0.01	0.00	0.04	180
51	Niger	0.06	0.01	0.02	0.03	181
	Africa	**0.55**	**0.08**	**0.04**	**0.22**	**140**

Source: ITU-UNCTAD; Table 2a from World Information Society Report 2007 Beyond WSIS; p159

10. Appendix Two: Overview of Past, Ongoing and Planned Information and Communications Technology (ICT) Initiatives in ECOWAS

1. INTELCOM II Project is known as ECOTEL.

- ECOWAS plans 10% teledensity, to establish GSM roaming facility
- INTELCOM II launched in 1997 is aimed at establishing 32 interstate fiber-optic links to constitute the regional opto-electronic backbone for the West African region.
- Integrated backbone that can serve the bandwidth requirements of member states of ECOWAS as well as create a good market base for bandwidth in the region.
- The main objective of the INTELCOM II program is to provide the community with a regional telecommunications network that is modem, reliable, and capable of offering a wider variety of services, including multimedia and wide band services. This will reduce transits through countries outside Africa and improve direct links between member states.

2. The decisions previously adopted by the ECOWAS Ministers in charge of Telecommunications and ICTs in Abuja, Nigeria in 2006, were adopted as Supplementary Acts by ECOWAS Authority of Heads of States and Government during its thirty-first session held in Ouagadougou on 19th January 2007.

- Regional telecommunications policy and a regulatory framework covering specific areas, such as interconnection to ICT and services networks, license regimes, management of the radio frequency spectrum.
- Harmonized ICT regulatory decisions were adopted at the 6th Meeting of the ECOWAS Ministers in charge of Telecommunications and ICT, held in Abuja Nigeria on 11th May 2006.

3. The content body of these decisions was derived from the best practice guidelines adopted in Accra, Ghana, in 2005 Sources: (Final Report of the Ministerial meeting, ITUNews article, ECOWAS Press release) and http://www.itu.int/ITU-D/treg/projects/itu-ec/index.html

4. Best practice guidelines developed and adopted in Accra, Ghana, at the 3rd Ordinary General Assembly of the West Africa Telecommunications Regulators Assembly (WATRA) in September 2005. (see http://www.watra.org).

5. In 2004, the EC/ITU West African Common Market Project

6. In 2001, The ECOWAS ministers of information and communication, met in Bamako in October 2001 and adopted a new information and communication policy

7. In 1983-1992, implementation of INTELCOM 1 with 95% completion rate of Intelcom 1, according to the International Telecommunication Union (ITU)

8. May 1979 INTELCOM 1, which delivered 13 interstate telecommunication links to member states of ECOWAS.

improve and expand the sub-regional telecommunication network.

9. ECOWAS Projects Supported by EU

Regional infrastructure was identified by the EU Strategy for Africa as a means of interconnecting Africa for contributing to economic growth, competitive. and regional integration. In this regard, EC had a contract with the ITU to harmonize the telecom & ICT legislation in Western Africa. The Heads of State and Government adopted a new regulatory framework (6 Supplementary Acts) in January 2007 that is more favorable for the development of Telecommunications and ICT in the sub-region. Following the success of this project, the EC started to expand this project to other regions in Africa in the framework of the EU-Africa Partnership on Infrastructure.

- Under EDF9 programme, ICT sector of ECOWAS received 1,000,000 Euros to support 4 projects:

  i) Developing detailed feasibility study for broadband communications infrastructure linking Senegal and several post conflict countries with the greatest demand for communications infrastructure (Guinea Bissau, Guinea, Sierra Leone, Liberia and Cote d'Ivoire)

ii) Capacity building and dissemination at the national level of the regional policy and regulatory guidelines for ICT adopted in January 2007 by the Heads of State and Government ECOWAS Projects Supported by EU

iii) Study to facilitate regional roaming, including recommendations for cross-border interconnection and tariffs, fiscal incentives for roaming

iv) Implementation of a telecommunications management information system (SIGTEL) to facilitate critical statistical data gathering at the national and regional level

---

Source: information compiled through online research by the author, mainly from ITU; West African Common Market Project: Harmonization of Policies Governing the ICT Market in the UEMOA-ECOWAS Space Model ICT Policy and Legislation

11. Appendix Three: Overview of Past, Ongoing, and Planned Information and Communications Technology (ICT) Initiatives in Nigeria

1. ICT4D initiative is being funded by the Economic Commission for Africa (ECA)

2. A new initiative, Virtual Library Project, is being launched within National Open University and is also supported by government.

3. A Presidential Task Force on ICT Harmonization was inaugurated in August 2006.

4. SchoolNet Nigeria

SchoolNet Nigeria was launched in September 2001 with the support of the Ministry of Education, Ministry of Telecommunications the Ministry of Science and Technology and the Education Tax Fund. Nigeria took steps toward increasing ICT access last year, with the launch of the Computer for All Nigerians Initiative. It aims to increase the number of computers in the country, which according to the International Telecommunications Union is as low as seven per 1,000 inhabitants. The government had agreed to remove import duty for the scheme, but this promise has yet to be fulfilled.

5. The Nigerian government sponsored almost US$1million worth of computers for its public servants last year in 2006.

6. Since 2003 UNESCO has been supporting a project for community access to ICTs in Nigeria, by providing FM broadcasting equipment for radio programmes aimed at raising awareness of information and communication technologies.

7. The Federal Government of Nigeria is launching a project called NetPost, which plans to provide post offices with Internet points to bring affordable access to the people of Nigeria.

8. Universal Service Provision Fund (USPF) The Nigerian Communications

Act 2003 provided for the establishment of a USPF, which finally became operational with the inauguration of its Governing Council in September 2006 (NCC, 2003).

9. Broadband Infrastructure. setting up of Galaxy Backbone, a company owned by the Nigerian government. A deployment of 2,000 VSATs (satellite terminals) across Nigeria is planned. This will offer access to remote, underserved locations, and ensure that each of the 774 local governments will have connectivity.

10. Fiber optic cables have been laid from Lagos to Kano, and Zaria to Jos, by Glo Telecoms, as part of its Nigeria to UK project. The National Space Research and Development Agency (NASRDA) launched a second satellite in May 2007. It is being

built by Surrey Satellite Technology, and is expected to aid agricultural and economic planning as well as help in disaster. Nigeria launched its satellite communication in May 2007. Developed with support from the African Union, it is also set to serve telecommunications, broadcasting and broadband communications across Africa.

11. Computers for All Nigerians Initiative (CANI) The aim of this initiative is to improve Nigerians' access to computer hardware. It includes a funding mechanism whereby civil servants will be able to purchase computers and pay back the loan at a low rate of

interest. Launched in July 2006, CANI is a typical example of a public-private partnership. It is being coordinated by NITDA and involves Microsoft, Zinox and Omatek. Related to the initiative is a Petroleum Technology Development Fund (PTDF) plan to build and equip computer centers in higher education institutions across Nigeria.

12. Universities Bandwidth Consortium This is a pilot programme in which six of the nation's universities are able to bulk purchase bandwidth for academic purposes. The scheme holds promise for the over 600 higher education facilities in Nigeria. National Rural Telephony Project (NRTP) The NRTP was expected to provide 500,000 connected lines to 343 local governments in Nigeria within one year. In 2003, the federal government accessed credit from the World Bank's International Development Association (IDA), and a part of the funds obtained was to be set aside to improve national teledensity, as well as to step up telecommunication penetration in rural area

13. Internet exchange points (IXPs). The establishment of internet exchange points will help keep local internet traffic within the country, which reduces the need to use international bandwidth and thus significantly lowers costs. An IXP allows different internet service providers (ISPs) to exchange internet traffic between their autonomous networks without cost. Although the Lagos IXP has been completed, it has not been commissioned. Seven more were expected to have gone live by now.

14. Telecentre Network of Nigeria (TNN) The inaugural meeting of the Network was held at the National Institute for Policy and Strategic Studies, Kuru, on 25-27 January 2007, with the support of the International Development Research Center's (IDRC's) telecentre.org programme. It is hoped that the Network, by leveraging opportunities presented by the USPF, among other initiatives in Nigeria, will attain the goal of one telecentre in each of the country's 774 local government areas.

Source: information compiled through online research by the author, mainly from Dada J., Global Information Society Watch (GISW). Nigeria report and other country reports