Concordia University College of Alberta

Master of Information Systems Security Management (MISSM) Program

7128 Ada Boulevard, Edmonton, AB

Canada T5B 4E4

# Internet Security Governance : Comparative Analysis of Country Code Top Level Domain (ccTLD) Administration

by

HYACINTHO, Michael B.

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

Master of Information Systems Security Management

**Date: December 2008**

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Dale Lindskog, Associate Professor, MISSM

# Internet Security Governance: Comparative Analysis of Country Code Top Level Domain (ccTLD) Administration

by

HYACINTHO, Michael B.

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Dale Lindskog, 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



**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**

*Master of Information Systems Security Management (MISSM) Program*

*7128 Ada Boulevard, Edmonton, AB*

*Canada T5B 4E4*

# Internet Security Governance: Comparative Analysis of Country Code Top Level Domain (ccTLD) Administration

By

**Michael B. Hyacintho**

*A research paper submitted in partial fulfilment of the requirement for the degree of*

**Master of Information Systems Security Management**

December 2008

**Research Advisors:**

**Pavol Zavarsky (PhD)**

Director of Research and Associate Professor, MISSM

**Andy Igonor (PhD)**

Assistant Professor, MISSM

**ABSTRACT**
Phishing presents a significant security challenge to Internet users, registries and registrars worldwide. The costs of phishing are significant and growing, and the increasing volume of phishing threatens to destroy the fabrics of online transactions. Vulnerabilities in domain registration processes are exploited by phishers leading to distrust for online transactions. These malicious activities are increasing, regardless of the efforts by governments and organizations like IETF, ICANN, and ITU to create policies that regulate the activities of country code Top Level Domains [ccTLD]. While Internet security policies abound, the challenge is the effective implementation of these strategic policies to tackle the issues of security and stability of country domains. To study this problem, 33 countries were selected on the basis of relative severity of phishing activities within their country domain as demonstrated by their phishing scores. The paper also examines the state of Internet Security Governance [ISG] in the operational management of these ccTLDs and the Norwegian domain policy model was used to categorize these ccTLDs. The paper argues further on the need to better integrate ISG with domain management by illustrating with the level of phishing activity in ccTLDs of developing countries like Tuvalu and Tokelau. In these ccTLDs the profitability of the registry operation supersedes the security of the domain registered.

**Author Keywords:** Internet Security Governance, country code Top Level Domain, Phishing and Domain Policy Model

## 1 INTRODUCTION

The Canadian .ca domain until very recently had very restrictive rules as to who could register .ca domain names. As a result, as of November 2000, there were only 98, 000 .ca domains in existence compared to nearly ten million dot-com domains. It was felt that the old rules were too restrictive and had retarded the development of the Internet in Canada, or at the very least had retarded the development of a distinctly Canadian presence on the Internet. Under the revised rules which are already in effect, individual Canadians and not just federally incorporated companies and other organizations may register .ca domains, and there is no longer a limit of one per applicant [1].

The lifting of the restrictive rules transformed the .ca domain from a strictly regulated ccTLD to an unregulated ccTLD. This shift has given room for cyber-squatting, domain tasting, domain slamming and other domain name abuses if adequate Internet security measures are not put in place. The most prevalent abuse in domain registration is "Domain Kiting" or "Tasting"- a practice of repeatedly adding and dropping the same domain name every few days in order to avoid registration fee, in the process registering domain names only after testing their profitability. This practice is an exploitation of the Internet Corporation for Assigned Names and Number [ICANN] 5-days Add Grace Period [ADP], a period where names can be returned and the fees paid will be refunded for any reason.

According to the Anti-Phishing Work Group [APWG] survey [2], the phishing activity in the Canadian country domain has been minimal compared to the Hong Kong ccTLD experience. This could be attributed to the domain registration policy for the Canadian ccTLD. Also, the type of domain policy model and the nature of Internet security policy determine the level of abuse within that country domain. An example is the Norwegian [Norid] domain policy model [3] which has actually worked for Norway in terms of the number of abuse experienced in their domain. This reference model used for this study and it categorizes country domains into four groups, namely strictly regulated, bureaucracy, regulated by quota and unregulated models. This reference models are used to categorize a group of country domains and while an internet security governance framework is suggested to prevent these malicious domain activities.

Furthermore, this paper specifically relied on phishing data from the Anti-Phishing Work Group to explain the different internet security issues that manifest in situations of non conformance to security best practices, in the operational management of ccTLD. And it also suggests ways of incorporating internet security governance [ISG] into the management of the different domain name models. In order to achieve this he research work was conducted on thirty-three country domains selected from Asia, Africa, Europe, America and Oceania. The selection was done based on their respective phishing scores and the relative severity of the phishing activities in their domain.

### 1.1 DOMAIN NAME POLICY MODELS

The categorization of country domains using the Norwegian domain name policy model is based on two factors. One is the number of domain names an applicant may hold and the other is the requirements placed at the time of registration of a domain; like restriction based on local presence and citizenship. The variation of these factors determines the quadrant a country domain will be placed.

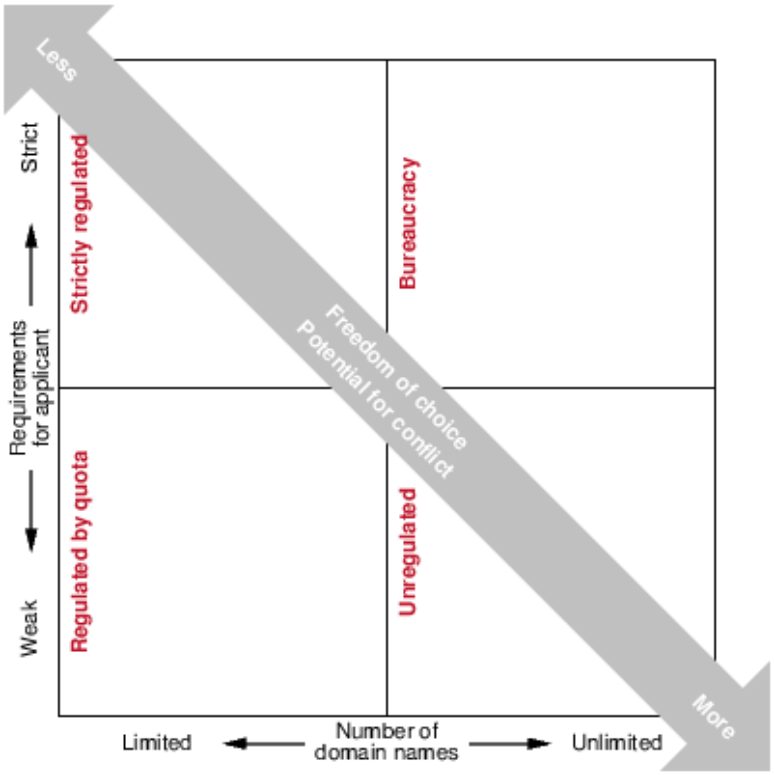


Figure 1: Domain Name Policy Categories
[source: http://www.norid.no/regelverk/rammer/regelverksmodeller.en.html]

For instance, under the strictly regulated category, an applicant may hold a small number of domain names and each domain is evaluated under strict application requirements. In bureaucracy, domain registration by registries involves a manual process of verification of documents; its advantage over the previous is that applicants are not restricted in the number of domain names that they can register. Similarly, Regulated by quota is a process of limiting the number of domain names a registrant can possess by a certain quota. Finally, unregulated is a situation where by there are fewer or no application requirements.

## 2 INTERNET GOVERNANCE

*Internet governance* is defined as "collective action, by governments and/or the private sector operators of the networks connected by the Internet, to establish agreements about the standards, policies, rules, and enforcement and dispute resolution procedures to apply to global internetworking activities"[4]. The goal of this study is the incorporation of security governance to operational management of country code Top Level Domain (ccTLD), through the implementation of an Internet security governance framework.

### 2.1. INTERNET SECURITY GOVERNANCE

Information Security Governance is described as the overall process by which information security is developed to mitigate risks. Internet Security Governance is to protect the integrity and availability of online information and it is a subset of the Internet Governance framework. ISG provides strategic direction, ensures that objective are achieved, manages risks appropriately, uses organizational resources responsibly, and monitors the success or failure of the internet security program. A well implemented program ensures that critical business asset- in this case; the domain name system [dns] is protected, therefore guaranteeing the integrity and availability of this asset throughout its lifecycle. Naturally, Information security requires a balance between sound management and applied technology. In order to achieve this, there is a need to have a framework that will guide the implementation of security best practice in the operational management of country domains.

## 2.2 INTERNET SECURITY GOVERNANCE FRAMEWORK

The proposed Internet Security Governance framework can be used as a starting point by registries to govern Internet security through the development of guidelines and implementing controls to address risks identified by registries, registrars and other stakeholders, such as misuse of web browsing, data corruption, or identify theft.

Ultimately, this governance framework provides Management with the means to implement an effective and comprehensive ISG program that addresses technical and procedural components. The Internet Security Governance framework consists of strategic, managerial [operational] and tactical components. The strategic components provide direction to the managerial components, while the tactical [technical] protection components are controlled by managerial component. The main categories of the ISG framework are:

- **Strategic:**
  - Leadership, governance, resource allocation, strategic vision and coordination
- **Managerial and Operational:**
  - Security management and organization; resource management
  - Security policies
  - Security program management
  - User security management
- **Tactical:**
  - Technology protection and operations

### 2.2.1 STRATEGIC MANAGEMENT

This category comprises executive level sponsorship for information security, as well as commitment from the board and management to protect information assets. This sponsorship is due to the fact that Information Security Governance is accepted as an integral part of good IT and Corporate Governance [5]. This brings to fore the activities of organization like Internet Corporation for Assigned Names and Numbers [ICANN], World Group on Internet Governance [WGIG] and World Summit on the Information Society [WSIS] that are constituted for the promulgation of policies and regulations that govern the internet.

Likewise, individual governments create laws that direct the activities of their respective ccTLD, but from my observation, the problem so far is not the lack of good strategic policies on the security and stability of the Internet but what is grossly inadequate is the effective implementation of these laws. This is shown by the high phishing scores of some developed countries within the unregulated region of the Norid domain model, a reflection of the inadequacy of the strategic policy implementation. Likewise, in third world nations like Nigeria, Tokelau, Tuvalu etc with high phishing scores, this attributed to the drive for web presence, in order to bridge the digital divide, without actually having a strategic policy that will address the operational management of their Internet infrastructure. This is due to the fact that their respective country domains are managed by non-governmental organization or privately owned registries that are either profit oriented or humanitarian in nature as such pay little or no attention to the internet security aspect of the registry operations.

This situation can be addressed by the introduction of the concept of metrics and measurement to measure how effectively the registries are addressing threats to the internet. The implementation of best practices for registrars and ISP/Mailbox providers will also help reduce the incidence of domain name abuse [22], [23]. Likewise, proper execution of registry and stakeholder's strategic vision will go a long way in strengthening the security posture of the country domain. Finally, an appropriate coordination of the available resources would contribute immensely to achieving the registry's strategy.

### 2.2.2 OPERATIONAL MANAGEMENT

The operational management components of the ISG framework consist of the following:

#### 2.2.2.1 SECURITY MANAGEMENT AND ORGANIZATION

Program organization and legal and regulatory considerations are covered in this category. The objective of the category is to manage information security within the registry. Program organization refers to the information security organizational design, composition and reporting structures. Different pieces of national and international legislation needed to be considered for internet security.

#### 2.2.2.2 SECURITY POLICIES

Security policies, procedures, standards, and guidelines are key to the implementation of information security in order to provide management with direction and support [ISO 27002]. The comprehensive security policy should include policies on user awareness, malware protection, incident response management, forensic analysis, phishing domain takedown, fraudulent registration management etc. For instance ICANN has put forward various suggestions for improving the privacy of internet users' whois data, but many have been rejected for being overly complex or unfair. The introduction of official proxies to handle domain registrants' information and accounts could be an option, but adding a layer of security could frustrate law enforcers' efforts to catch fraudsters and scammers online. But a little bit of frustration is better than no security measure.

#### 2.2.2.3 SECURITY PROGRAM MANAGEMENT

Monitoring and compliance as well as auditing are included in this category, which involves management of the security program. It is essential to measure and enforce compliance [5], and both internet technology and registrars along with registrants' activities should be monitored to ensure compliance with internet security policies and to respond effectively and timely to incidents that are detected. Technology monitoring could relate to capacity and network traffic monitoring. For instance the taking down quickly of compromise websites that are used for malicious activities is a way of managing the domain name system. Likewise internet security auditing is necessary to ensure that the policies, processes, procedures and controls are in line with the objectives, goals and vision of the domain registry.

#### 2.2.2.4 USER SECURITY MANAGEMENT

This category addresses user awareness; education and training; ethical conduct and trust and privacy. ISO/IEC 27002 states that the organization must have plans and programs in place to implement, maintain, and effectively promote information security awareness and education throughout the organization. A body that is involved in awareness campaign is the "Coalition Against Domain Name Abuse, Inc." [CADNA] [6]. CADNA is dedicated to building awareness about and advocating action to stop illegal and unethical infringement of brands/trademarks online. Its mission is to decrease instances of cyber-squatting in all its forms by facilitating dialogue, effecting change, and spurring action on the part of policymakers in the national and international arenas.

As part of the ISG framework, ethical conduct must be addressed by the organization to minimize the risk of invasion of privacy, selling of registrants' information and unauthorized altering of data. A trusting relationship should also be established between a registrar and registrant in the process contributing to the registry's reputation and create a safe online environment. One possible way of establishing such a relationship could be for the registrar to illustrate that registrants' information are secured and that registry complies with relevant requirements. Privacy is an essential issue of trust when it comes to good relationships with clients and business partners [7]. If there is no privacy in business, there will be no trust [8]. When implementing information security privacy, both registrars and registrant must be considered and controls must be implemented to protect their respective interest.

User Awareness program should be developed and implemented aggressively to enlighten registrants and internet users on the activities of phishers. A recent survey conducted in U.S on a group of internet users on their awareness of the activities of phishers shows that less than 48 percent have heard of phishing while only 30 percent have any idea of what it is.

### 2.2.3 TACTICAL MANAGEMENT

The technology protection and operations category relates to the traditional focus of information security. It involves the technical and physical mechanisms implemented to secure an internet infrastructure. When implementing the security governance framework, the technology controls applicable to the country domain environment and identified risks must be implemented. These include asset management, system development requirements, incident management, technical operations such as network security, physical, environment, and business continuity controls. It is essential that the technology environment be monitored on a constant basis and that the risks of technology changes in the market are addressed. Also, at this level issue about application security, database security, host security, internal network security and network perimeter security are addressed. The implementation of best practices for cctld administrations [25] is at this stage of domain management.

## 3 STUDY OF OPERATIONAL MANAGEMENT OF SELECTED CCTLD

The rules and policies used to administer ccTLDs domain names vary significantly. This section provides comparative analysis on management practices of ccTLDs in some selected countries. For this research the Norid Policy model was used for the comparison, unfortunately there is no "Perfect Policy" that will satisfy all needs. All categories have their advantages and disadvantages. Model is chosen depending on what the local Internet community judges to be the most important criteria.

### 3.1 OBJECTIVES

The primary aim of this research is to compare the operational management of some selected countries with phishing activity within their country domain. More specifically the objectives include:

- To compare the different country code top level domain regulations employing the following criteria:
  - Whether there is a local presence or related requirement to qualify for the right to register a domain name.
  - Whether there is a limit in the number of domain names for which any entity can apply.
  - The effect of price on domain name registration.
- To categorize the country code top level domains of these countries in to the different policy models.
- To argue that an effective application of Internet Security Governance is a sine-qua-non in the administration of country code Top Level Domain.

### 3.2 METHODOLOGY

In order to understand the nature of the type of domain policy model implemented by a country domain, there is the need to compare the respective domain registration policies and correlate it with the level of phishing activity with within its country domain. For this reason the countries that makeup Table 1 was selected based on the criteria of having either a very low or very high phishing score. The source of this secondary data that was used for comparison is the Anti-phishing Work Group Survey: Domain Name Use and Trends in 2007[9]. Also, the corresponding domain registration policies for these countries will be compared employing the following criteria:

- Whether there is a local presence or related requirement to qualify for the right to register a domain name.
- Whether there is a limit in the number of domain names for which any single entity can apply.
- The prices of the domain name.

Furthermore, in the process of trying to fully understand the outcome of the categorization of the different country domains into strictly regulated, bureaucracy, regulated by quota and regulated, the effect of internet penetration within a particular country is considered through the correlation of the total internet users, the number of domain used for phishing, cost of registration..

### 3.3 DATA COLLECTION

The data shown in column 3 of Tables 1 and 2 relating to Price for domain registration were sourced from the websites of domain registrars; 101Domain.com [10] and RWGusa.net [11] and OECD [19]. While the data shown in columns 4, 5, 6 and 7 of Table 1 are analysis from the respective domain registration policies [12], and the data shown in columns 4, 5, and 6 of Table 2 are from the APWG [9]. Lastly, the data in column 7, 8, and 9 of table 2 are derived from the following websites respectively; InternetWorldStats.com [13] and APWG [2]. Note that the phishing scores for countries like Tonga, Tuvalu, Tokelau and Nigeria were not stated in the APWG listing but with the help of the expression below and information from WebHosting.info website[14] regarding the total domains, the phishing scores for the respective countries was computed.

* Note: *Phishing score is computed using the following expression*: $\frac{10,000}{A1} \times A2$

Where: *A1 = Total Domain,* *A2 = Domain Used For Phishing*

**TABLE 1: DOMAIN NAME POLICY COMPARISON**

| Country | ccTLD | Price | Location Requirement | | Restriction on Number of Domains and Policy Category | |
|---|---|---|---|---|---|---|
| **Europe** | | | | | | |
| Albania | .al | 159 | Yes | Registrant be a citizen or have company ID. | No | Unregulated |
| Bulgaria | .bg | 261 | Yes | Registrant must have presence. | No | Bureaucracy |
| Denmark | .dk | 72 | No | | No | Unregulated |
| Finland | .fi | 288 | Yes | Registrants must be judicial persons and properly registered in Finland. (No private person or foreign companies can be registered.). | No | Registrants can only get one domain name per registered name. Unregulated |
| Germany | .de | 19.95 | Yes | The domain holder or administrator must have his residence in Germany, or state his serving address. | No | Unregulated |
| Moldova | .md | 249 | No | | No | Unregulated |
| Norway | .no | 259 | Yes | The applicant must be an organization registered in Norway. The organization must have a Norwegian post address. Individuals may register domain names only under "priv.no". | No Depends on SLDs | Up to 20 .no domain names per organization directly. Up to 5 domain names under each geographic domain. Up to 5 domain names under each generic domain to which it belongs. Regulated by Quota |
| Romania | .ro | 75 | No | | No | Unregulated |
| Sweden | .se | 68 | Yes | NIC-SE only registers domain names for organizations and individuals with permanent business or operation within Sweden. | No | Unregulated |
| UK | .uk | 18 | No | | Depends on SLDs) | Unregulated |
| **Oceania** | | | | | | |
| Australia | .au | 49 | Yes | Domain name licenses may be allocated to an applicant who is Australian, registered or incorporated in Australia as defined under the eligibility and allocation rules for each SLD. | No | Seven second-level domains (SLDs): asn.au, com.au etc. Bureaucracy |
| Tonga | .to | 199 | No | | No | Unregulated |
| Tuvalu | .tv | 29.95 | No | | No | Unregulated |
| Tokelau | .tk | 50 | No | | No | Unregulated |
| **Asia** | | | | | | |
| China | .cn | 30 | No | | No | Unregulated |
| Japan | .jp | 79 | Yes | Any single person, group or organization that has an address within Japan is eligible. Second level JP domains, such as ".co.jp" have additional requirements. | No | Unregulated |
| HongKong | .hk | 65 | No | | No | Unregulated |
| India | .in | 39 | No | | No | Unregulated |

| | | | | | | |
|---|---|---|---|---|---|---|
| Iran | .ir | 99 | Yes | Copy of company registration from any country. | No | Unregulated |
| Russia | .ru | 54 | No | | No | Unregulated |
| Saudi Arabia | . sa | 209 | Yes | Registrant must have a registered trademark in Saudi Arabia matching the domain name to register. | No | Strictly Regulated |
| Thailand | .th | 98 | Yes | Copy of Company registration in Thailand including a full address, phone number or Thai trademark is required. | No | Strictly regulated |
| **North/South America** | | | | | | |
| Canada | .ca | 51 | Yes | Canadian citizens, corporations under the laws of Canada or any province or territory of Canada, Canadian trademark holders, educational institutions, unions, political parties, and archives etc can register domain names. | No | Unregulated |
| United States | .us | 17.50 | Yes | A natural person i) who is a citizen or permanent resident of the United States of America or any of its possessions or territories or ii) whose primary place of domicile is in the United States of America or any of its possessions etc | No | Unregulated |
| Mexico | .mx | 59 | Yes | No local presence required for .com.mx. (But local presence is required in the other classifications.). | | Unregulated |
| Ecuador | .ec | 99 | Yes | Registrant must have a current passport and ID number from any country. | No | Unregulated |
| Chile | .cl | 84 | Yes | Must have a local contact in Chile. | No | Unregulated |
| Cuba | .cu | 999 | No | | No | Bureaucracy |
| Guatemala | .gt | 99 | No | | No | Unregulated |
| **Africa** | | | | | | |
| Kenya | .ke | 149 | No | | No | Unregulated |
| Libya | .ly | 199 | Yes | Registrant must show proof of company or trademark registration from any country. | No | Unregulated |
| Morocco | .ma | 145 | No | | No | Unregulated |
| Nigeria | .ng | 150 | Yes | For commercial organizations only. Only one domain is allowed per organization. Organization must have physical presence in Nigeria. | No | Regulated by Quota |

**TABLE 2: SELECTED PHISHING DOMAINS**

| Country | ccTLD | Price $ | Total Domains in Nov. 2007 [9] | Domain names used for Phishing in Nov. 2007 [9] | Score: Phishing Per 10,000 domain [9] | Internet Users [13] | Score: Phishing per 10,000 Domain [2] | Average Uptime 1H2008 [HH:MM] [2] | User Growth (2000-2008) [13] |
|---|---|---|---|---|---|---|---|---|---|
| **Europe** | | | | | | | | | |
| Albania | .al | 159 | 250 | 2 | 80.2 | 471,200 | 66.7 | 5:15 | 18,748.0% |
| Bulgaria | .bg | 261 | 7,500 | 13 | 17.3 | 4,000,000 | 10.8 | 10.27 | 830.2% |
| Denmark | .dk | 72 | 862,000 | 239 | 2.8 | 3,762,500 | 1.0 | 10.56 | 92.9% |
| Finland | .fi | 288 | 165,000 | 38 | 2.3 | 3,600,000 | 1.2 | 10.23 | 86.8% |
| Germany | .de | 19.95 | 11,524,091 | 1,798 | 1.6 | 52,533,914 | 0.6 | 11.02 | 118.9% |
| Moldova | .md | 249 | 2,200 | 15 | 68.2 | 700,000 | | 7.42 | 2,700.0% |
| Norway | .no | 259 | 357,722 | 92 | 2.6 | 4,074,100 | 1.5 | 10.31 | 85.2% |
| Romania | .ro | 75 | 242,484 | 316 | 13.0 | 12,000,000 | 5.0 | 11.04 | 1,400.0% |
| Sweden | .se | 68 | 685,000 | 127 | 1.9 | 7,000,000 | 0.7 | 10.18 | 72.9% |
| UK | .uk | 18 | 6,445,465 | 992 | 1.5 | 41,817,847 | 1.3 | 10.24 | 171.5% |
| **Oceania** | | | | | | | | | |
| Australia | .au | 49 | 985,548 | 314 | 3.2 | 16,355,427 | 1.9 | 10.19 | 147.8% |
| Tonga | .to | 199 | 3,035[8] | 29 | 95.6* | 8,400 | | 9.37 | 740.0% |
| Tuvalu | .tv | 29.95 | 5,482[8] | 144 | 262.7* | 4,000 | | 9.34 | 0.0% |
| Tokelau | .tk | 0 | 186[8] | 102 | 5483.9* | 540 | 0.8 | 8.46 | 718.2% |
| **Asia** | | | | | | | | | |
| China | .cn | 30 | 8,459,174 | 1.853 | 2.2 | 253,000,000 | 0.7 | 10.29 | 1,024.4% |
| Japan | .jp | 79 | 972,584 | 359 | 3.7 | 94,000,000 | 1.5 | 10.58 | 99.7% |
| Hong Kong | .hk | 65 | 150,799 | 1,707 | 113.2 | 4,878,713 | 142,2 | 10.59 | 113.7% |
| India | .in | 39 | 331,495 | 168 | 5.1 | 60,000,000 | 3.3 | 10.41 | 1,100,0% |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Iran | .ir | 99 | 72,906 | 26 | 3.6 | 23,000,000 | 2.3 | 10.42 | 54.8% |
| Russia | .ru | 54 | 1,104,572 | 684 | 6.2 | 32,700,000 | 2.5 | 11.44 | 954.8% |
| Saudi Arabia | .sa | 209 | 12,478 | 8 | 6.4 | 6,200,000 | 4.6 | 6.33 | 14.8% |
| Thailand | .th | 98 | 33,000 | 171 | 51.8 | 13,416,000 | 23.5 | 11.35 | 483.3% |
| **North/South America** | | | | | | | | | |
| Canada | .ca | 51 | 935,000 | 286 | 3.1 | 28,000,000 | 1.4 | 10.10 | 120.5% |
| US | .us | 17.50 | 1,362,805 | 661 | 4.9 | 220,141,969 | 1.8 | 9.55 | 130.9% |
| Mexico | .mx | 59 | 230,177 | 189 | 8.2 | 23,700,000 | 3.2 | 11.36 | 773.8% |
| Ecuador | .ec | 99 | 14,941 | 29 | 19.4 | 1,109,967 | 8.6 | 12.36 | 516.6% |
| Chile | .cl | 84 | 195,513 | 222 | 11.4 | 240,000 | 0.7 | 10.57 | 300.0% |
| Cuba | .cu | 999 | 1,455 | 2 | 13.7 | 7,387,000 | | | 320.3% |
| Guatemala | .gt | 99 | 6,262 | 9 | 14.4 | 1,320,000 | 7.1 | 10.16 | 1,930.8% |
| **Africa** | | | | | | | | | |
| Kenya | .ke | 149 | 8,011 | 5 | 6.2 | 3,000,000 | 2.2 | 10.22 | 7.9% |
| Libya | .ly | 199 | 3,100 | 84 | 271.0 | 260,000 | 122.6 | 13.42 | 4.2% |
| Morocco | .ma | 145 | 25,873 | 9 | 3.5 | 7,300,000 | 1.6 | 9.27 | 21.3% |
| Nigeria | .ng | 150 | 10,198[8] | 2 | 2* | 10,000,000 | | 21.12 | 7.2% |

### 3.3 DATA ANALYSIS

The data obtained from various search statements by following the above methodology are in Tables 1 and 2. The domain policy categorization of these selected countries is based on the comparison of the policies regarding the fulfillment of local presence, limit of the number of domains that could be registered by a registrant at any point in time and the cost of registration. It can be seen that countries like Bulgaria and Cuba are categorized as operating a model that is Bureaucratic. Honk Kong, Germany, Canada, Iran etc are Unregulated while a country like Nigeria and Norway is Regulated by Quota. None of the countries selected fits the definition of strictly regulated policy model. The above categorization is depicted in the fig1.

Considering the above categorization of country domains, it is easy to assume that country domains like Albania, Hong Kong, China, Germany, UK etc, that are unregulated will have high cases of domain abuse. This assumption is not completely true because when this condition is applied to countries like Germany and China, its Phishing score for 2007 depict a relatively low phishing activity within its country domain vis-à-vis the number of registered ccTLD within their country domain. This situation could be attributed to the application of an effective Internet security governance implementation at different layers of the country domain. But countries like Nigeria which has relatively low phishing score at the moment but can has a high phishing site uptimes, is a reflection

attributed to absence of an Internet security governance framework. This is an indication of a non-existent strategic management policy for Internet governance as a whole. Furthermore, the categorization of Nigeria as operating a regulated by quota policy model is only a means regulating the number of domain names registered since the Internet infrastructure available can only accommodate a fewer number of registration at a time. But without the development of an Internet security governance framework for the operational management of the country domains, the abduction of APWG anti-phishing best practices recommended for registrars and Internet Service providers [22], [23] and also the implementation of country code Top Level Domain best practices [26] the domain name abuses will persist.

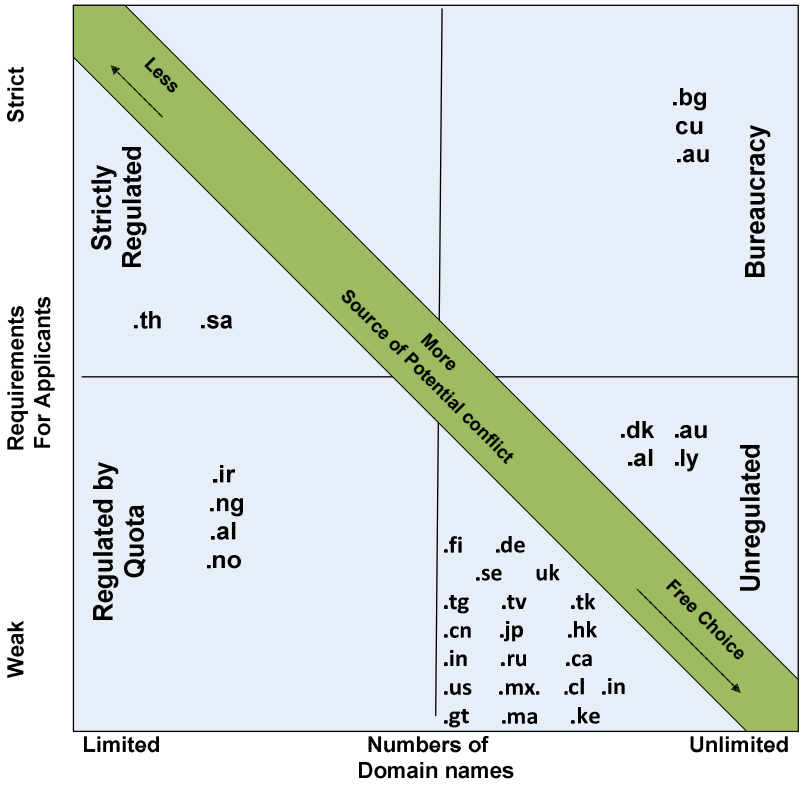


**Fig 1: Domain Policy Models**

In addition, the present state of poor Information technology infrastructure creates a negligible web presence for Nigeria, but in future when the necessary Internet infrastructures are put in place and with the seemingly lack of internet security governance framework, the situation will be different from what it is now. Also, the phishing activity within the .ng country domain will be a cause of concern, considering the average phishing website uptimes for Nigeria, which is a clear indication of the consequence of lack of strategic policy on Internet domain management [2].

Countries like Libya [.ly] and Hong Kong [.hk] with the highest Phishing scores, 271.0 and 113.2 respectively suffered from the systematic registration of domain names by phishers. Most of the .ly phishing domains were maliciously registered in the sub-domain biz.ly, while the .hk's registry anti-abuse capabilities weaknesses were exploited by phishers. In "Mapping the Mal Web Revisited" [15], the reasons given for the relatively high phishing score of .hk Includes:

- "The enhancement of their online domain registration process thus making it more user-friendly. This resulted in the capability for registering several domains at one time, auto-copying of administrative contact to technical contact and billing contact, etc. Phishers usually registered eight or more domain at one time.

- The offer great domain registration discounts such as buy-one, get-two domains.
- Overseas service partners promote .hk domain in overseas markets."

Similarly, the high phishing score for.hk in 2007 is also attributed to the activities of the Rock Phish Gang [2] who systematically exploited weakness in the .hk registry anti-phishing capabilities. But, from Table 2 the phishing score of .hk dropped by almost 50% due to the implementation of anti-phishing best practices within their domain.

Similarly, in contrast to Nigeria which operate a regulated by quota policy model, large country domains like .de, .cn and .uk are unregulated. But regardless of the fact that they are unregulated the level of phishing activities within the top level domain is still low. This is an evidence of the application good governance through the implementation best practices. For instance, the .cn ccTLD had started coordinating registrars within its domain in anti-phishing efforts, APWG [2]. But, due to the larger number of domain names with the registry, the phishing site takedown time is still high, this situation is attributed to the imperfection in their incidence response program. This problem is wide spread, as shown by the average uptimes of 10Hours for a large portion the survey cctld.

In Table 2, Tokelau, .tk, with a phishing score of "5438" is one of the most risky, this is attribute to the fact that domain registration is relatively cheap and the domain is owned by an entrepreneur that some time offer promotional sells to attract client. The promotional offer could be inform of unlimited free anonymous registration, with free URL and email forwarding. This practice businesswise is awesome, but in terms of security it is a bad practice, since the whois database generated during this process will contain false data of fraudulent registrants. A situation like this gives phishers the avenue to register phishing websites that will be used to perpetrate the hideous crime.

Another domain that is of interest is the Romania; .ro ccTLD which has a phishing score of 13.0 and considered a risky domain. Romania's high phishing score is attributed to high number of internet users (relative to its population) with malicious intention. A problem that can be explained by the high number of internet users that are technically knowledgeable and, thus, there exist the likelihood that a higher number of them could use the knowledge for malicious activity [16].

.

### 3.4 RESEARCH LIMITATION

A limitation of this research is the use of APWG data to illustrate malicious activities associated with registration of domains. The incidence of phishing activities is not solely the result of the exploitation of vulnerabilities in the registration process, but also other factors like server vulnerabilities exploit, phishing websites up-time, internet penetration etc. An instance is Thailand's country domain, .th, where phishers systematically took advantage of insecure institutional servers to mount phishing attacks [2]. Similarly, a study by Symantec [16] suggests that the pervasiveness of phishing activities in Romania is related to the culture surrounding computer usage over there vis-à-vis the technical knowledge of internet users. Likewise, a study [16] suggests that the United States has the largest number of bot-compromised computers with approximately 14 percent of the total number of computers infected. These sighted cases of phishing exploit are perpetrated within a country domain and would form part of the phishing data compiled by APWG.

## 4 CONCLUSION AND FUTURE WORK

Domain names have become highly valued assets that are choice targets for attackers. To counter this, it is desirable for country domains to be more proactive in tackling the abuse ongoing within the domain name system. This can be achieved through the development of a comprehensive Internet security governance framework that includes strategic, operational and tactical policies that guides operational management of country domains. This framework should also include the implementation of the anti-phishing best practices for both registrars and ISP/mailbox providers as suggested by APWG, the ccTLD best practices and an aggressive user awareness program to sensitize the registries, registrars, registrant and the average internet user to the activities of groups like the 'Rock Phish Gang'.

Overall, this research has shown that the categorization of domain names into strictly regulated, regulated by quota, bureaucracy and unregulated is basically a business decision that affects the number of domain names been registered. While the security of domain names depends on the nature of Internet Security programs that are implemented, any of these domain models cannot guarantee a phishing free country domain without the implementation of an ISG program; they only promote a web presence that is relative to the form of registration restriction obtainable.

Further research is needed to gain better understanding of the importance registrars and registries place on securing the DNS infrastructure and also, the correlation between the growth in number of internet users and the registration of domain names within a country domain.

**REFERENCES:**


1. Cyber-squatting in the ccTLDs: A Case study of Canada, http://www.auda.org.au/pdf/sub-davidson.pdf
2. Global Phishing Survey: Domain Name Use and Trends in 1H2008, http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey1H2008.pdf
3. Domain name policy models, http://www.norid.no/regelverk/rammer/regelverksmodeller.en.html
4. Rodolfo Noel S. Quimbo,: Internet Governance: Issues and Prospects for Asia and the pacific , UNESCAP, October 2004.
5. Von Solms, S. H. (2005). Information Security Governance— Compliance management vs. operational Management. *Computers and Security*, *24* (6), 443–447.
6. CADNA - The Coalition Against Domain Name Abuse, http://www.cadna.org/
7. Tretic, B. (2001 January). Can you keep a secret? Intelligent Enterprise.
8. Ross, B. (2000). New directives beef up trust in e-commerce. Computer Weekly News.
9. Greg Aaron, Rod Rasmussen, http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey2007.pdf
10. 101 Domain.com Registrar, http://www.101domain.com/
11. RWGUSA.NET Global Domain Registration, http://www.rwgusa.net/
12. ccTLD Governance Project, http://www.cctldinfo.com/country.php
13. Internet Usage in Europe, http://www.internetworldstats.com/stats4.htm
14. Country-wise Total Domain, http://www.webhosting.info/domains/country_stats/
15. Mapping the Mal Web Revisited, http://us.mcafee.com/en-us/local/docs/Mapping_Mal_Web.pdf?cid=45044
16. Romania - European leader when it comes to phishing, http://news.softpedia.com/newsPDF/Romania-European-Leader-When-It-Comes-To-Phishing-83447.pdf
17. Rock Phish gang adds second punch to phishing, http://www.computerworld.com/action/article.do?command
18. Internet Governance: The State of Play, http://www.internetgovernance.org/pdf/ig-sop-final.pdf
19. Comparing Domain Name Administration in OECD Countries, http://www.itu.int/itudoc/itu-t/workshop/cctld/cctld043.pdf
20. S. Possthumus, R. von Solms; A framework for the governance of information security, http://www.sciencedirect.com/science
21. A Da Veiga, J.H.P. Eloff, An information Security Governance Framework
22. Working Party on Telecommunication and Information Services Policies, http://www.oecd.org/dataoecd/46/38/2505946.pdf
23. Anti-Phishing Best Practices for ISPs and Mailbox Providers, http://www.antiphishing.org/reports/bestpracticesforisps.pdf
24. Anti-phishing Best Practices for Registrars, http://www.antiphishing.org/reports/APWG_RegistrarBestPractices.pdf
25. Evolution in the management of country code top level domain names, http://www.oecd.org/dataoecd/8/18/37730629.pdf
26. Country code best practices, http://www.nsrc.org/netadmin/wenzel-cctld-bcp-02.html
27. http://www.icann.org/en/committees/security/sac024.pdf
28. http://www.icann.org/en/announcements/hijacking-report-12jul05.pdf
29. OECD Report (2006) 'Evolution in the Management of Country Code Top Level Domain Names', Working Party on Telecommunications and Information Services Policies, DSTI/ICCP/TISP(2006)/FINAL, 17/11/2006
30. Internet Governance, http://web.ebscohost.com.ezproxy.aec.talonline.ca/ehost/pdf
31. The Internet and Global Governance: Principles and Norms for a New Regime, http://www.atypon-link.com/LRP/doi/pdf/
32. ISO/IEC 27002 (2005). Information Technology. Security Techniques. Code of practice for information security management, http://www.iso27001security.com/html/27002.html#Section5
33. Leslie A. Pal, Tatyana Teplowa: Domain Games: Global Governance of the Internet, http://www.carleton.ca/spa/Publication/Pal%20Teplova%20chapter%203.pdf