

KnujOn (nûj-ôn)



Research Report on the ccTLD Space

Prepared by Garth Bruen, CEO KnujOn.com LLC

May 18, 2009

KnujOn ccTLD Research Index

- I. Intent
- II. Top-Level ccTLD Administrative Bodies
- III. General Observations
- IV. Whois Access Policies and Law Enforcement Data Request Policies
- V. Conditions of Concern
- VI. Known Trouble Spots
- VII. Problematic
- VIII. At-Risk ccTLDs
- IX. Sun-setting ccTLDs with continued Domain Traffic
- X. ccTLDs Administered by U.S. Companies
- XI. ccTLDs DNS Partially Hosted by U.S. Universities
- XII. Who is Randy Bush?
- XIII. Other ccTLD DNS Supporting Groups in the U.S.
- XIV. Latin and Non-Latin Whois
- XV. Experimental TLDs for Non-Latin Character Sets
- XVI. ccTLDs For Territories with No Indigenous Population
- XVII. Recommendations
- XVIII. Chart Values
 - 1. ccTLD and Country Name
 - 2. Active
 - 3. Notes
 - 4. GAC Rep
 - 5. Sponsoring Organization
 - 6. DNS Information
 - 7. CERT Contact
 - 8. ISOC Chapter
 - 9. Registries/Registrars/Agents
 - 10. Open or Closed Registrations
 - 11. KnujOn Spammed Domains
 - 12. KnujOn Instance Count
 - 13. KnujOn Spam Index
 - 14. Thick Whois URL and condition
 - 15. Thin Whois ULR and condition

I. Intent

The purpose of this report is to analyze the current structure of the Country Code Top-Level Domain space (ccTLD) for policy failures, abuse, potential threats, validity of published contacts, availability of Whois data, quality of infrastructure, depth of documentation, and other related issues. The report also specifically records how much of the ccTLD space is supported from the United States, whether by private companies or universities. This report is also intended to develop a series of recommendations for abating threats, limiting potential abuse, and exposure of such to the Internet in general. These recommendations should also be made available to the concerned ccTLD sovereign governments for their own protection and education. It is generally recommended that this type of report be issued regularly since national policy and administration for each ccTLD may change frequently and without notice. A chart of all the analyzed ccTLDs and detailed data concerning each is attached to this report. The values are described in the section called "Chart Values". The opinions contained within are purely those of KnujOn and the author. We understand that many of these topics are controversial and welcome international debate and discussion for the purpose of improving security for the entire structure.

II. Top-Level ccTLD Administrative Bodies

The Internet Corporation for Assigned Names and Numbers (ICANN)

<http://www.icann.org/tr/english.html>

Internet Assigned Numbers Authority (IANA)

<http://www.iana.org/about/>

Country Code Names Supporting Organisation (ccNSO)

<http://ccnso.icann.org/about/>

III. General Observations

"Websites operating from the two-letter country-code top-level domains (ccTLDs) are likely to become increasingly important to our Internet fraud efforts. Websites operating from ccTLDs are viewable by U.S. consumers, and an increasing number of our actions involve foreign-based websites targeting U.S. consumers." - 2002 House Subcommittee on Courts, the Internet, and Intellectual Property: *"ACCURACY AND INTEGRITY OF THE WHOIS DATABASE"*

(http://commdocs.house.gov/committees/judiciary/hju79752.000/hju79752_0.htm)

This quote is possibly more even more accurate now than it was in 2002. As new ccTLDs become active and existing ccTLDs are delegated to private and/or foreign management, concerns over abuse and a lack of accountability should be openly discussed and researched. This is not an issue for the U.S. only, but all participating countries.

ccTLDs are two-letter domain extension codes intended to represent a specific country (i.e., ".US" for United States). These codes are issued to the sovereign government of the particular country by the Internet Corporation of Assigned Names and Numbers (ICANN) and administered by Internet Assigned Numbers Authority (IANA). In theory, once a ccTLD is issued to a sovereign government it is under their complete control and no other body or government may interfere with its use. There is still much confusion and discussion over who is ultimately responsible for the ccTLD space. IANA oversees ccTLDs and IANA is a division of ICANN. Additionally, ICANN has a contracted "ccTLD Compliance Program (<http://www.icann.org/en/compliance/ccTLD-compliance.htm>)" which includes the following obligations for ccTLD operators:

1. Operate name servers for ccTLD in a stable and secure manner (4.1)
2. Ensure that zone file and registration data are continually available to ICANN (4.2)
3. Establish a data escrow or mirror site policy for registry data (4.3)
4. Obtain approval from Governmental Authority for data escrow or mirror site operator (4.3)
5. Establish proper agreement among Sponsor, GA and escrow agent (4.3)
6. Notify ICANN of changes in contact info within 7 days (4.4)

7. Abide by ICANN consensus policies that concern interoperability or other topics as applicable (4.5)
8. Make financial contributions to ICANN (4.6 and Attachment E)
9. Notify ICANN of proposed subcontractors (6.11.1)

It is unclear how often, if at all, these conditions are monitored and what remedies are available in case of compliance failure. Many ccTLDs researched here may currently be non-compliant.

Due to the complex international distribution of Internet communication, policy and legal confusion may emerge. An example situation would be an Internet criminal in **Country A** using a proxy domain registration in **Country B** that refuses to issue data to **Country A's** law enforcement. Police in Country A may never know their suspect is a citizen due to international sovereignty issues. Law Enforcement may have to go through a series of high-level diplomatic procedures only to learn about a "homegrown" criminal. This is not speculation as KnujOn has recorded illicit networks distributing their operations throughout the globe to avoid detection and policy enforcement. In short, the ccTLD space requires much more study and discussion.

KnujOn surveyed the existing 257 ccTLDs, excluding .INT and the five experimental internationalized-character set TLDs. We found that the ccTLD space is in general poorly documented. We found contradicting statements concerning ccTLD policies and in most cases no posted policies at all.

The U.S. sponsorship or access to foreign ccTLDs is possibly larger than commonly known. 17 ccTLDs are managed outright by U.S.-based companies (see: ccTLDs Administered by U.S. Companies). 20 have a portion of their DNS at an American university (see: ccTLDs DNS Partially Hosted by U.S. Universities). 64 have a portion of their DNS at an American private company (see: Other ccTLD DNS Supporting Groups in the U.S.); surprisingly Cuba is among this group. American companies are also offering domain registrations for known trouble spots like Moldova (.MD), Niue (.NU) and the defunct Soviet Union (.SU).

In this report KnujOn also reviewed law enforcement Whois access & registrant disclosure policies, assessed conditions that make ccTLDs vulnerable to abuse, detailed abused ccTLDs, and listed U.S. connections to many ccTLDs. The final sections are list of recommendations and a guide for the attached chart.

IV. Whois Access Policies and Law Enforcement Data Request Policies

As expected, Whois access policies vary from country to country with some having no stated policy at all. **Canada's cctLD (.CA)** adopted a new Whois access policy in June, 2008 which requires notification to a domain registrant if private Whois data is requested by law enforcement.

"5. Notice to Registrant. If CIRA approves a request hereunder, CIRA shall, unless prohibited by law, not less than thirty (30) and not more than sixty (60) days after disclosure of the Information, use reasonable efforts to send an email to the Administrative Contact of the Registrant indicating: (a) that CIRA has disclosed the Information; and (b) to whom CIRA has disclosed it.
(http://www.cira.ca/assets/Documents/Legal/Registrants/disclosure_law.pdf)"

Requests should be directed to:

Disclosure Requests
Canadian Internet Registration Authority
306-350 Sparks Street
Ottawa, Ontario K1R 7S8
Facsimile: (613) 237-0534 or 1-800-285-0517
Email: disclosurerequests@cira.ca

Law Enforcement has 30 days to act on the information before the notice is sent to the registrant via email. The "unless prohibited by law" clause could be taken to mean that certain situations would prevent disclosure to the registrant, and, as would be expected, the law and national security trump privacy policy. Law enforcement would need to make the case to CIRA that sharing a disclosure with the registrant violated the law or constituted a public safety threat. This policy is more likely intended to prevent regular or mass surveillance and not to hinder police investigations. Some police may argue that 30 days is not long enough to complete an investigation. However, a disclosure could likely be halted by a judge's order under the right circumstances.

Additionally, the CIRA Whois policy states the following: "*The new dot-ca WHOIS contains changes that apply primarily to individual Registrants. Private information about individual Registrants will no longer be accessible through the dot-ca WHOIS. The private information of corporate Registrants will be displayed by default." Rogue Internet pharmacies, pirated software download sites, and other illicit enterprises are not protected by this policy. If an individual has registered a site claiming personal use and is in fact engaging in commercial transactions they have violated their agreement with CIRA. This case could be made for any domain engaging in transactions.*

Mexico's cctLD (.MX) policy stipulates no notification is required.

The more common policy is to inform registrants that their information is made public intentionally or provided upon request to law enforcement. **Australia (.AU)** is a good example of this:

"c) the interests of law enforcement agencies in accessing information about domain names for consumer protection and other public interest purposes. (<http://www.auda.org.au/policies/auda-2002-06/>)"

Arab Emirates (.AE) policy requires law enforcement cooperation and makes no mention of registrant notification:

"6.3. Law enforcement or other national agencies may require access to all the information that is held regarding certain Domain Names. The .aeDA will handle all such requests where the request is legal and appropriate.

(http://www.aeda.ae/eng/policies/AEDA-POL-005_WhoIs_Data_Collection_and_Display_Policy.pdf)"

The United Kingdom (.UK) Offers "Whois2" which is a permissions-based Whois service that avoids the querying party from being blacklisted for excessive requests: <http://www.nominet.org.uk/other/whois2/>. However, EU customers may opt-out of personal Whois disclosure. The law enforcement policy is as follows:

"11.3 if they ask in writing, give your personal data to people with a legitimate reason for asking for it (based on the exemptions in the Data Protection Act 1998 or similar laws that replace or follow it), including government or law enforcement agencies;

(<http://www.nominet.org.uk/registrants/aboutdomainnames/legal/terms/>)"

The UK policy of registrant disclosure is similar to the CIRA but does not give a timeline and seems more deferential to police:

"From 11 January 2005 where data about a registration, in excess of that available by inspection of the WHOIS and/or PRSS, is passed by Nominet to a third party, then Nominet shall inform the registrant by email at the registrant's email contact address (or if no such address exists, Nominet shall use reasonable endeavours to use an alternative contact mechanism) of the identity of the third party and the information passed to that third party. This shall not apply:

- (a) where the passing of such information is prohibited by law, or
- (b) where it has been, prior to the passing of such information, shown by the third party, to Nominet's reasonable satisfaction, that there is a very substantial likelihood that the rights of others will be damaged by disclosing the fact that such information has been passed, or that law enforcement would be prejudiced. (<http://www.nominet.org.uk/registrants/aboutdomainnames/legal/dataprotection/>)"

The Cocos Islands (.CC) Policy is similar to the CIRA policy but suggests disclosure would not occur if specifically requested by the police:

"5.5 If [Country Code Administrator] uses or discloses Personal Information under this Use and disclosure paragraph 5, it shall make a written note of the use or disclosure, and except where

requested by a law enforcement agency, inform the Registrant by email of the identity of the requesting entity and stated reasons for the release of the information. These reasons must be one of the stated reasons in paragraph 5.1(2).

(<http://www.coccaregistry.net/index.php/home/policy-recommendations/privacy-and-whois-policy.html>)"

Niue (.NU) policy is leaning towards the CIRA policy:

"Under the .NU Domain Privacy Policy, if someone such as a law enforcement organization or a trademark attorney, needs contact information about a domain name holder, the person is required to submit a statement to .NU Domain Ltd identifying who they are, and why they need the information, before private information is provided to them. If they can not justify a valid need for this information, the information is withheld.

(<http://www.nunames.nu/Press/privacypolicy.cfm>)"

It should be noted that this policy is being set not by the sovereign government of Niue but by the technical operator, J. William Semich, who is a U.S. citizen. .NU is also noted as a "trouble spot" below.

Poland (.PL) also blocks access to personal Whois records and does not post a method or policy for police contact:

"Data of a private person such as the name and the address are protected by The Personal Data Protection Act of the 29th August 1997. (<http://www.dns.pl/english/whois.html#7>)"

The ccTLD Best Practices recommend cooperation and no notice to the registrant:

"3.2.2.6 Co-operation with law enforcement. A ccTLD Manager receiving a complaint from a relevant and recognized authority (e.g. branches of security agencies that concern themselves with mass media) of harmful or illegal (i.e. activity that is prohibited by local laws on disseminating certain kinds of information [national security-related data, pornography, etc.]) activity being conducted on a domain registered with the ccTLD, should share with that authority information on the holder of the domain name. (<http://www.wwtld.org/ongoing/bestpractices/bp.16aug00.html>)"

The 33 problem ccTLDs (described in sections below) and their whois privacy policies (or lack of) are listed in this table:

.bs Bahamas	No public whois, no stated policy
.bz Belize	No public whois, no stated policy
.CD Democratic Republic of the Congo	Open whois, no stated policy
.CM Cameroon	Unknown
.CO Colombia	Open whois, no stated policy
.cv Cape Verde	Limited whois, no stated policy
.dj Djibouti	No public whois, no stated policy

.ec Ecuador	Open whois, no stated policy
.fm Federated States of Micronesia	Policy to comply with subpoenas, no registrant notification (http://www.dot.fm/policy.html)
.GG Guernsey	Policy to comply with subpoenas, no registrant notification (http://www.channelisles.net/tandc.shtml#14)
.hn Honduras	Open whois, no stated policy
.IR Iran	Policy to comply with subpoenas, no registrant notification (http://www.nic.ir/Terms_and_Conditions_ir_Appendix_2_WHOIS_Policy)
.kz Kazakhstan	Open whois, no stated policy
.LA Laos	Open whois, no stated policy
.ls Lesotho	No public whois, no stated policy
.ly Libya	Open whois, no stated policy
.MD Moldova	Open whois, no stated policy
.me Montenegro	Open whois, no stated policy
.mn Mongolia	Policy to comply with subpoenas, no registrant notification (http://www.nic.mn/content.php?action=mypages&page=privacy.html)
.MS Montserrat	Open whois, no stated policy
.na Namibia	Policy to comply with subpoenas, no registrant notification (http://www.na-nic.com.na/attachments/011_aup.pdf)
.NR Nauru	Open whois, no stated policy
.NU Niue	Policy similar to CIRA (http://www.nunames.nu/Press/privacypolicy.cfm)
.PL Poland	Blocks access to personal Whois
.RU Russia	Open whois, no stated policy
.sc Seychelles	Open whois, no stated policy
.SG Singapore	Open whois, no stated policy
.sm San Marino	Unknown
.SU Soviet Union	Unknown
.sy Syria	No public whois, no stated policy
.tj Tajikistan	Open whois, no stated policy
.tt Trinidad and Tobago	Open whois, no stated policy
.ws Samoa	Open whois, no stated policy

V. Conditions of Concern

Some ccTLDs have already been targeted for abuse because of ease of access and lack of oversight. Hong Kong (.HK) became a primary target for phishing in the last few years, called "epidemic" in 2005 (<http://www.smh.com.au/news/Breaking/HK-says-spam-cost-US770m-in-2004/2005/02/25/1109180080931.html>). Combating a wave of malicious attack using .BS (Bahamas) domains, abuse handlers were frustrated by the lack of published contacts for the ccTLD. Internet criminal networks are constantly looking for new areas to exploit and will abuse certain ccTLDs until security is tightened and then move on to weaker targets.

A country with an unstable government, open registrations, and no Whois is an attractive target for criminals and rival intelligence services. "False flag" operations could be launched from these nations. Abuse and attacks using these ccTLDs would be effectively shielded from recourse or even investigation. The best option for handling these is to (1) forbid ISPs from hosting these ccTLDs and (2) block Internet traffic to and from these countries. This may seem an extreme measure, but any nation wishing to benefit from global Internet traffic would quickly remedy the problems.

By examining the policies and structure of all the ccTLDs, we have been able to determine sets of conditions that make a ccTLD vulnerable. Many smaller countries have opened registrations of their ccTLD to non-citizens as a source of potential revenue. This is their prerogative, but when it is combined private Whois or no Whois it becomes an open invitation to the world's criminals to abuse the ccTLD with anonymity and impunity. Closing a ccTLD to non-nationals drastically reduces potential abuse. Having a public Whois allows international anti-abuse efforts and police to mitigate problems. We have developed a simple matrix for determining risky ccTLD policies.

Risky Conditions

	Open Registration	Closed Registration
Public Whois	Ok	Ok
Private/No Whois	Bad	Ok

Of course, in the above matrix we are assuming that a government or ccTLD authority is responsible and responsive. In cases where the authority or government could not be contacted or could not effectively address the situation other conditions would be less important since public Whois and registration policies are only useful if monitored and enforced.

Worst Case Scenario

Responsible Party	Public Whois	Closed Registration	Ok
Responsible Party	Private Whois	Closed Registration	Ok
Responsible Party	Public Whois	Open Registration	Ok
Responsible Party	Private Whois	Open Registration	Problematic
No Responsible Party	Public Whois	Closed Registration	Problematic
No Responsible Party	Private Whois	Closed Registration	Problematic
No Responsible Party	Public Whois	Open Registration	Bad
No Responsible Party	Private Whois	Open Registration	Worst

In the above matrix we see that a ccTLD with no Whois access, registrations open to non-nationals, and no contactable governance creates a disastrous situation. This is the type of arrangement that criminals hope for, a freely accessible space with no accountability and no oversight. We found more than 20 ccTLDs that potentially fit this description.

In respect to national sovereignty, the United States cannot mandate that another country open its Whois or close its registrations, but we can assist them in gaining representation and accountable infrastructure. KnujOn has identified three bodies that all ccTLD should participate in for the sake of their own stability: The ICANN Government Advisory Committee (GAC), to participate in Internet policy development; CERT, to assist and cooperate on Internet attacks; and The Internet Society (ISOC), to represent interests of the citizen user. Having one or more of these affiliations can greatly reduce the chances of being targeted and increase the possibility of successfully defending against abuse. Unfortunately, the number of countries with representation is drastically outnumbered by those who do not (see: VIII At-Risk ccTLDs).

Beyond ccTLDs with poor oversight and representation that may be victimized there are ccTLDs which, for whatever reason, seem to tolerate or even welcome illicit activity. These are listed in the next section.

VI. Known Trouble Spots

.CN - China: Use of .CN domains for rogue pharmacies are increasing. Phishing, typosquatting, and brandjacking through "COM.CN" has become pervasive. Whois results for .CN domains are returned in Chinese which obscures the name of the Registrar and other details. Standard Whois queries cannot parse the character set so results are often returned with blank fields. Because of the obfuscated Whois results for .CN and the general lack of contacts or cooperation it is extremely difficult to address abuse issues. The Chinese Registrars Xin Net, Bizcn, OnLineNIC, and HiChina have frequently been cited for tolerating illicit pharmacy, software piracy, and spam as well as for weak security that has allowed criminals from Eastern Europe and elsewhere to abuse the space, using the Chinese connection to obfuscate the true source of cyber attacks and illicit traffic. In the last three months KnujOn has recorded 122,248 .CN domains advertised with 2,280,839 spam emails which is an average of 18 spams per domain. .CN has the highest percentage of illicit pharmacy domains of all other ccTLD.



.CN Registry WHOIS Data

Domain Name	0018my.cn
Domain Status	ok
Registrant Name	王勇清
Administrative Email	domainwang@126.com
Registrar	北京众鑫乾坤网络科技有限公司
Name Server	ns5.namerich.cn
Name Server	ns6.namerich.cn
Creation Date	2009-01-11 04:24
Expiration Date	2010-01-11 04:24

.CD - Democratic Republic of the Congo: Registrations by non-nationals are officially closed but we have recorded software piracy sites being registered by a known spammer based in Eastern Europe.

.SU - Soviet Union: While this ccTLD is allegedly being phased out, there are several locations offering new registrations and specifically promoting the "Soviet" aspect, displaying the Hammer & Sickle as advertising. The company claiming Registration authority is a U.S.-Based ICANN-accredited Registrar: 10ldomain.com, AKA Rightway Gate Inc, 5858 Edison Pl. Carlsbad CA 92008.

101domain.com

QUESTIONS? CALL TOLL FREE
877.983.6624
 Int: ++1.760.444.8674



gTLD Domains
Premium Domains
International Domains
IDNs
Trademark
B2B
Rules & Prices
Hosting

Register .SU - Register Soviet Union Domain - Register Soviet Union Domain Name .SU



SEARCH AND REGISTER

DOMAINS

Enter the desired domain name, select the extension and click search.

WWW. .SU Search

ALL SOVIET UNION DOMAINS

.SU - Soviet Union

PRICE AND REQUIREMENTS

1 Year Registration \$ **69.00**


2 Years Registration \$ **129.00**

.SU Soviet Union Domain
>Select Domain Extension ▾



SU Domain Name Registration - Soviet Union Domain .SU

.SU Soviet Union Domain - .su domain name - Soviet Union .SU - domain name su - .SU Soviet Union Domain Registration - Register .SU Soviet Union Domain - Register Url .SU

Soviet Union Domain Name .SU	
Facts:	
Country Domain:	Domain Name Soviet Union .SU
Application Fee:	Included
Maintenance Fee:	Variable
Domains Per Applicant:	Unlimited
Sub Domains:	.SU ▾
Popular Sub Domains:	
Local Presence:	Local presence is not required
Requirements:	no restrictions
Provide Local Presence:	
Multiple Domains:	Allowed
Registration Contract:	2 Years
Registration Fee for most domains:	\$ 150.00
Whois Server	Soviet Union .SU Domain Name Registration
Renew Your Domain Here:	Renew Domain .SU



Whois Server Information

.MD - Moldova: .MD is being used to market "medical professional" domains by Max.md in Fort Lee, NJ and several unlicensed pharmacies have been discovered in this space.

Register or check availability of a .md domain name:

www. .md

Establish your Online Identity using our FREE tools.

The cornerstone of the offering is the .md domain name, .mdEmail® and .mdSecureIM™. [\(more...\)](#)

[.mdFeatured Sites](#) | [Testimonials](#) | [Learn more](#)

[.mdEmail® REACHMD Podcast](#)

dave.md choice.md osna.md hernias.md

.NU - Niue: "Nu" means "nude" in some languages and illicit domainers have been using .NU to register prostitution (possibly human trafficking) and illegal pornography domains. .NU is administered by a company in the U.S.: J. William Semich .NU Domain Ltd/IUS-N, 266 Main St. Suite 31, Medfield Massachusetts 02052.



EliteGirls.Nu
the best girls only

Марина
возраст - 21
рост - 175
телосложение - нормальное
размер груди - 2

[объявление](#)
услуги
цены: 1 час - 13000руб.
м. Кутузовская
☎ +7 (916) 734.4444

"Services"

13,000 Rubles Per Hour

.RU - Russia: Spammers and Internet criminals in Russia are frequently observed registering domains through other countries and generally within the gTLD space. Spamming within Russia often has a local aspect, with Russians spamming other Russians concerning local businesses and services, not necessarily illegal businesses. However, .RU is a heavily

abused ccTLD internationally. KnujOn has recorded in the last three months 14,573 domains spammed with 814,724 messages making it one of the highest spam-to-domains ratios at 56/1.

.IR - Iran: It has recently been noted that Iran's government-controlled ISP is hosting space for the so-called Russian Business Network. It is not clear yet how much influence they have within the ccTLD space, but it should be discussed.

VII. Problematic

.CO - Colombia: Because .co is used in by some ccTLDs as a sub-domain to represent "company", i.e. co.uk, and typos leaving off the "m" in .com, .CO may be used for phishing and brandjacking.

.CM - Cameroon: Being used for typosquatting and phishing for users who omit the "O" in .COM. Their official Whois page redirects to a parking page: agoga.com.

.PL - Poland: .pl is also the extension of a web script (Perl). Internet users may be tricked into thinking they are visiting a Polish site when they are in fact running malware.

.NR - Nauru: Nauru has 40,000 registered corporations and 400 shell "brass plate" banks for a population of 12,000. .NR could be used for online money laundering operations that would be difficult to trace.

.MS - Montserrat: May be abused to misrepresent "Microsoft" (MS)

.GG - Guernsey: Frequent favorite of online gambling

.LA - Laos: Being marketed exclusively at the "Los Angeles" TLD, there is no mention of Laos anywhere on the ccTLD website, they even post the current weather for Los Angeles on the home page.

.SG - Singapore: Officially closed to non-residents but KnujOn has recorded many rogue pharmacy sites in the .SG space that have been tracked to Eastern Europe.

VIII. At-Risk ccTLDs

The following ccTLDs are rated as "At-Risk" for potential abuse. They all have registrations which are open to non-nationals while at the same time lack a GAC Representative, a CERT center or an ISOC Chapter. Additionally some also have non-functioning or private Whois. It is our opinion that selling domains to non-citizens while also lacking standard Internet contacts, and additionally not providing information on domain ownership, creates conditions that make a ccTLD attractive to criminals.

.bs	Bahamas*
.bz	Belize
.cv	Cape Verde*
.dj	Djibouti*
.ec	Ecuador
.fm	Federated States of Micronesia
.hn	Honduras
.kz	Kazakhstan
.la	Laos**
.ls	Lesotho*
.ly	Libya
.me	Montenegro
.mn	Mongolia*
.ms	Montserrat
.na	Namibia
.nr	Nauru
.sc	Seychelles
.sm	San Marino
.sy	Syria*
.tj	Tajikistan
.tt	Trinidad and Tobago
.ws	Samoa

It is recommended that each of these countries be contacted and encouraged to seek a GAC seat, create a CERT center, and apply for an ISOC chapter. While opening ccTLD registrations to non-citizens may seem like a lucrative opportunity, doing so without global connections or crisis management centers is a dangerous idea.

**No Whois or non-functioning Whois*

***While Laos' ccTLD is operated by an U.S. company, this is somewhat obfuscated. IANA's contact list for .LS makes no mention of the U.S.-based contacts and only lists the Laotian administrators.*

IX. Sun-setting ccTLDs with continued Domain Traffic

Several ccTLDs have been closed over the years because the countries no longer exist or have changed their names. These ccTLDs have been purged of domain names: .CS "Czechoslovakia" is now Czech Republic (.CZ) and Slovakia (.SK); .DD "Deutsche Demokratische Republik", the former East Germany reunified with West Germany; .TP East Timor, now .TL; .ZR "Zaire", now Democratic Republic of the Congo .CD.

.SU - Soviet Union: While it is claimed this ccTLD is being phased out Registrations are still being accepted. Unlike the phase-out of .YU there is no published timetable or transparent process for decommissioning .SU.

.YU - Yugoslavia: According to nic.yu all .YU domains will cease functioning after September 30, 2009.

X. ccTLDs Administered by U.S. Companies

The following non-U.S. territorial ccTLDs are administered within the United States:

Ukraine (.UA)

Technical Contact ,Igor Sviridov ,CS/MONOLIT Network Centre ,650 Castro Street ,#120-335 ,Mountain View California 94041-2055 ,United States ,Email: sia@nest.org, Voice: +1-877-570-5414 / +1-415-672-3654 Fax: +1-978-359-5830

Tanzania (.TZ)

Randy Bush ,PO Box 128 ,Kapa`au Hawai`i 96755 ,United States ,Email: randy@psg.com

Tuvalu (.TV)

Verisign Global Registry Services ,21345 Ridgetop Circle ,Dulles Virginia 20166 ,United States ,Email: info@verisign-grs.com, +1 703 925-6999 Fax: +1 703 421-5828

Niue (.NU)

J. William Semich, .NU Domain Ltd/IUS-N,266 Main St., Suite 31, Medfield MA 02052

Nigeria (.NG)

Randy Bush, PO Box 128 ,Kapa`au Hawai`i 96755 ,United States ,Email: randy@psg.com

Lebanon (.LB)

Randy Bush, PO Box 128 ,Kapa`au Hawai`i 96755 ,United States ,Email: randy@psg.com. Also sponsored by the American University of Beirut.

Cayman Islands (.CY)

Stephen Bernacki ,Perimeter eSecurity ,440 Wheelers Farms Road #202 Milford, Connecticut 06461 ,United States ,Email: kysupport@perimeterusa.com , +1 800 234 2175

Guinea (.GN)

Randy Bush, PO Box 128 ,Kapa`au Hawai`i 96755 ,United States ,Email: randy@psg.com

Eritrea (.ER)

Craig Harmer, Punchdown Vintners ,110 Clayton Street ,San Francisco California 94117

Cocos (.CC)

Verisign Global Registry Services ,21345 Ridgetop Circle ,Dulles Virginia 20166 ,United States ,Email: info@verisign-grs.com, +1 703 925-6999 Fax: +1 703 421-5828

Democratic Republic of the Congo (.CD)

There is little internal management of the ccTLD, they have liaison in Switzerland and a portion of the DNS in run through Princeton University 87 Prospect Ave. Princeton NJ 08540

Laos (.LA)

Administrators are reported from multiple locations including Laos, Guernsey, and England. But the company seemly running it is CentralNic USA Ltd. Suite 1030, 21700 Oxnard St. Woodland Hills, California 91367

Liberia (.LR)

Randy Bush, PO Box 128 ,Kapa`au Hawai`i 96755 ,United States ,Email: randy@psg.com

Moldova (.MD)

Max.md handles domain registration and is in Fort Lee, NJ and is being marketed for medical professional websites.

Federated States of Micronesia (.FM)

BRS Media Inc., 55 New Montgomery St Ste 622 · San Francisco CA 94105. Similar to Laos and Moldova, this ccTLD seems exclusively marketed for commercial purposes, namely online radio.

Palau (.PW)

EnCirca Inc. P.O. Box 164 Reading MA 01867 Email: pwtech@encirca.com
Voice: +1 781 942 9975

Samoa (.WS)

Global Domains International, Inc. 701 Palomar Airport Road, Carlsbad, CA, 92011

XI. ccTLDs DNS Partially Hosted by U.S. Universities

Princeton University:

Burundi (.bi)
Democratic Republic of the Congo (.cd)
Republic of the Congo (.cg)
Switzerland (.ch)
Haiti (.ht)
Liechtenstein (.li)
Luxembourg (.lu)
Rwanda (.rw)

University of Oregon:

Ivory Coast (.ci)
Dominican Republic (.do)
Ethiopia (.et)
Guyana (.gy)
Jamaica (.jm)
Comoros (.km)
Libya (.ly)
Tajikistan (.tj)

University of California, Berkeley:

Fiji (.fj)
Hong Kong (.hk)

Purdue University:

Sri Lanka (.lk)

Columbia University:

Colombia (.co)

XIII. Who Is Randy Bush?

Randy Bush is listed as the technical administrator for five ccTLDs: Guinea(.GN), Lebanon (.LB), Liberia (.LR), Nigeria (.NG), and Tanzania (.TZ). He is a founding member of the Network Startup Resource Center (NSRC) which is a non-profit organization that has worked since the late 1980s to help develop and deploy networking technology in various projects throughout Asia/Pacific, Africa, Latin America and the Caribbean, the Middle East, and the New Independent States (nsrc.org). He is a Senior Researcher at the Internet Initiative Japan (iij.ad.jp). He was a member of the founding boards of ARIN and AfNOG, and also served as an IVTF Ops Director. He was the founding engineer of Verio, now NTT/Verio. He maintains a free peering site, psg.com, which provides technical support for small, underfunded countries.

PSG also provides partial DNS support for the following ccTLDs:

Albania (.al)
Armenia (.am)
Azerbaijan (.az)
Botswana (.bw)
Central African Republic (.cf)
Switzerland (.ch)
Cuba (.cu)
Egypt (.eg)
Fiji (.fj)
Ghana (.gh)
Guinea (.gn)
Israel (.il)
Lebanon (.lb)
Liechtenstein (.li)
Lesotho (.ls)
Liberia (.lr)
Malawi (.mw)
Nigeria (.ng)
Palestine (.ps)
Saudi Arabia (.sa)
Swaziland (.sz)
Tunisia (.tn)
Tanzania (.tz)

XIII. Other ccTLD DNS Supporting Groups in the U.S.

Several ccTLDs also have DNS servers or some support from these organizations located in the United States.

isc.org
Internet Systems Consortium, Inc.
950 Charter Street
Redwood City, CA 94063

Andorra (.ad)
United Arab Emirates (.ae)
Armenia (.am)
Antarctica (.aq)
Canada (.ca)
Catalonia (.cat)
Chile (.cl)
Guyana (.gy)
Israel (.il)
Iceland (.is)
Moldova (.md)
Mali (.ml)
Malta (.mt)
Namibia (.na)
Netherlands (.nl)
Nauru (.nr)
Nepal (.np)
Philippines (.ph)
Pitcairn Islands (.pn)
Portugal (.pt)
Serbia (.rs)
Thailand (.th)
Ukraine (.ua)
Uruguay (.uy)
Venezuela (.ve)
South Africa (.za)

pch.net
Packet Clearing House
572-B Ruger Street, Box 29920
The Presidio of San Francisco
San Francisco, California 94129-0920

Bahamas (.bs)
Catalonia (.cat)
Cyprus (.cy)
Guyana (.gy)
Heard Island and McDonald Islands (.hm)
Hong Kong (.hk)
Haiti (.ht)
Sri Lanka (.lk)
Lesotho (.ls)
Montserrat (.ms)
Malta (.mt)
Maldives (.mv)
Namibia (.na)

Nepal (.np)
Puerto Rico (.pr)
Palestine (.ps)
Serbia (.rs)
Saudi Arabia (.sa)
Solomon Islands (.sb)
Trinidad and Tobago (.tt)

dyntld.net
Dynamic Network Services Incorporated
1230 Elm Street, Fifth Floor
Manchester, NH, 03101

Christmas Island (.cx)
South Georgia and the South Sandwich Islands (.gs)
Kiribati (.ki)
Montserrat (.ms)
Mauritius (.mu)
Namibia (.na)
Solomon Islands (.sb)
East Timor(.tl)

sprintlink.net
6391 Sprint Parkway
Mailstop: KSOPHT0101-Z2100
Overland Park, Kansas 66251

Costa Rica (.cr)

XIV. Latin and Non-Latin Whois

Most countries in the world use the Latin(Roman) Alphabet or a variation. Non-Latin character sets are predominately used in North Africa/Middle East(Arabic), China/Mongola/Southeast Asia(Vietnam excluded)/Korea/Japan, and Russia/Ukraine/Belarus/Kazakhstan. The ccTLD countries that use Arabic generally offer Whois results in English, as do the Pacific Rim nations. At the moment China returns a mixed character set Whois result with the Registrar and registrant in Chinese only.

XV. Experimental TLDs for Non-Latin Character Sets

There are five experimental ccTLDs for non-Latin character sets: Simplified Chinese, Hindi, Russian Cyrillic, Korean(Hangeul), Hebrew, Traditional Chinese, Farsi, Tamil, Greek, Arabic, and Japanese(Kana). These are currently administered by ICANN.

XVI. ccTLDs For Territories with No Indigenous Population

.AQ Antarctica
.BV Bouvet Island
.HM Heard Island and McDonald Islands

XVII. Recommendations

1. The closure of .SU (Soviet Union) should be placed on a published timeline and monitored regularly. Registration services offering .SU domain names should be contacted and prevented from issuing new domain names.
2. ccTLDs for non-states, incorporated regions of other countries and unpopulated locations, should no longer be issued and existing ones merged.
3. Use the next ICANN e-crime session to address potential threats to ccTLDs and incorporate discussions within the ccNSO working groups.
4. Reach out to countries lacking GAC representation, CERT centers, and ISCO chapters to encourage them to participate more and gain representation.
5. Expand research on trouble-spot ccTLDs and continue to build on this report.
6. Convert the attached chart into a regularly updated online database.
7. The legality of various cross-border Internet business arrangements should be carefully analyzed by experienced attorneys.

XVIII. Chart Values

These brief explanations refer to the values in the attached spreadsheet for each ccTLD. In this chart you should find all Thin and Thick Whois where available, the names and contact information for all GAC representatives, the DNS information for the ccTLD, technical contacts, and a variety of statistical and policy data. We hope to expand this data set into an online "fact book" for the ccTLD space.

1. **ccTLD and Country Name:** The two-letter ccTLD and the sovereign country responsible.
2. **Active:** Indicates if the ccTLD is operational or actually in use. Some have been tagged with a "U" for unknown or unclear.
3. **Notes:** Additional information about the country or status of the ccTLD.
4. **GAC Rep:** The ccTLD Country's delegation to the Governmental Advisory Committee (GAC) at ICANN, if available.
5. **Sponsoring Organization:** What body is ultimately responsible for the ccTLD. Governments, universities and telecommunications companies are typical.
6. **DNS Information:** Underlying root server information for the ccTLD.
7. **CERT Contact:** A DOD sponsored Carnegie Mellon University group chartered to respond to Internet emergencies and serious security incidents. There are currently 43 other CERT centers in different countries. <http://www.cert.org/>
8. **ISOC Chapter:** The Internet Society (ISOC) represents the interests of the Internet users across the globe. 66 countries are currently represented by ISOC.
9. **Registries/Registrars/Agents:** Common location for registering domain names for the ccTLD.
10. **Open or Closed Registrations:** A ccTLD may decide to reserve domain registrations to its own citizens and businesses or to open registrations to residents of any country. This is a complex situation. Some counties with officially closed registrations were found to have non-citizens with registrations or services were found that seemed to ignore the policy. In many cases closed registration countries allow in-country businesses to act as proxy agents for non-citizens, which effectively opens registration to all.
11. **KnujOn Spammed Domains:** Number of domains with this ccTLD spammed in the last 3 months, as recorded by KnujOn
12. **KnujOn Instance Count:** Number of times domains with the ccTLD have been spammed in the last three months, as recorded by KnujOn

13. KnujOn Spam Index: The average ratio between spammed domains and the number of instances of spamming within this ccTLD. A small ratio may indicate anomalies and not real spam campaigns. Ratios of 10/1 or higher indicate high spam traffic and repeated attempts to exploit domain names.

14. Thick Whois URL and condition: The GUI interface for requesting domain owner information. Most of the Whois URLs published by ICANN/IANA were not accurate or not functioning. Many were found at alternate locations. Some ccTLDs simply provide a list or spreadsheet of domain names and contacts because the number is so small.

15. Thin Whois URL and condition: The command-line query interface for retrieving domain owner information. Some published thin whois locations were not functioning.

Sources and more information:

<http://www.iana.org/domains/root/db/>
<http://gac.icann.org/index.php?name=Representatives&mode=4>
<http://www.cert.org/csirts/national/contact.html>
<http://www.isoc.org>
<http://ran.psg.com/~randy/>
<http://www.icann.org/en/cclds/agreements.html>
<http://www.iana.org/reports/>