.CO Internet S.A.S.

How .CO ccTLD handles cybersecurity matters

Agenda

1. *About us*
2. *.CO Security*
   - *Motivation*
   - *Relationship*
   - *Strategy*
   - *Policies*
   - *Process*
3. *.COllaboration*
   - *Efforts in Colombia*
4. *Q&A*

About us

- .CO Internet
  - *Started in 2010 to promote and manage the ".CO" ccTLD*
  - *Concession contract with the Colombian Government (ITC Ministry)*
- .CO Statistics and Milestones
  - *From 1991 to 2010 there were only 28,000 registered domains*
  - *Today: +2.2 million domain names registered in +200 countries*
    - *+70 Registrars and their resellers*
- Credibility and Awareness
  - *All Colombian government agencies have at least one ".CO" domain name.*
  - *90% of Top-100 Colombian enterprises use ".CO" as their primary online domain name*
  - *URL shorteners*
    - *T.CO (Twitter), G.CO (Google), O.CO (Overstock)*
  - *A lot of startups worldwide using ".CO"*
    - *500.co, vine.co, up.co (Startup Weekend)*

.CO Security: Our Motivation

We are committed to supporting initiatives, projects and activities which contribute to the security, stability, and reliability of both the .CO namespace and the Internet in general.

.CO Security: Our Relationship

- *Identification of trustworthy sources/feeds and sharing information agreements with relevant cybersecurity partners and stakeholders*

- *__Memberships__ to security related organizations*
  - *APWG (AMDoS program)*
  - *FIRST (NEUCIRT)*
  - *DNS-OARC*
  - *NCMEC*
  - *EU-CICILE*
  - *TSDF*
  - *WEF-PCR*
  - *And others*

.CO Security: Our Strategy

1. *High-level IT operation, based on industry standards and best practices*
2. *Active participation as stakeholders in national, regional and worldwide cybersecurity communities, positioning the ccTLD*
3. *Generate mechanisms of collaboration with the community at national, regional and global levels*
4. *Take specific actions in regard to legal compliance and safety issues*
    - *.CO ccTLD namespace is under Colombian applicable law*
5. .CO security policies

.CO Security: Our Policies

1. **Good practices in IT, Security and Business Continuity**
2. **Promotion and active participation in initiatives, communities, and joint efforts in-country, regionally and worldwide**
   - *Knowledge Transfer and Security Awareness*
   - *Joint projects and campaigns with public/private stakeholders*
   - *(in-country) Support to the IT and Security industry*
3. **Collaborative action with our Registrar's channel**
   - *Cybersecurity: "added-value" for .CO Registrants*
   - *Registrars: our best partners*
4. **Higher price in order to discourage domain name registrations for fake, illegal, abusive, malicious or criminal use**

.CO Security: Our Process

- ***Rapid Domain Compliance Process (RDCP)***
  - ***Defined:*** *Verification/Validation of contractual obligations (Terms & Conditions) compliance of all our .CO Registrants*
  - ***Tool:*** *Registry Threat Mitigation Service (RTMS): Operational workflow for RDCP infringements or violations*

.CO Security: Our Process

- Registry Threat Mitigation Service (RTMS)
  - *Alert management related to .CO domains and URL’s*
    - Multiple *sources*: communities and security companies, SOC’s, CERT’s, CSIRT’s
    - *Incident* follow-up: actions between *Registry, Registrars and Registrants (“Terms & Conditions”)*
  - *RTMS Incident’s scope*
    - Phishing, Pharming, Malware distribution, Malicious Hacking, CP, Defacements
    - We do NOT focus on *content*, *rogue-pharma*, *e-piracy*, *cyber-squatting*, etc.

.CO Security: Our Process

- **If an alert is *actionable* (validated via NEUCIRT .CO Team), incident is reported and followed-up on by the respective entity, based on the domain type**
  - ***EDU.CO, GOV.CO, ORG.CO or MIL.CO domains:***
    - ***Registry to Registrant (CC'ing Colombian LEA's)***
  - ***COM.CO, NET.CO or .CO domains:***
    - ***Registry* to *Registrar***
    - **Registrar handles case with *Registrant* (based on "*Terms* and *Conditions*")**
  - ***URL shorteners, subdomains, ISP's, Hosting Providers***
    - **Registry to *Registrant***

.CO Security: Our Process

- Rapid Domain Compliance Process (RDCP)
  - *Continuous improvement*
    - Terms & Conditions
      - Policies and procedures review with
        - » (a) Our *Registrars* channel
        - » (b) the Colombian ITC Ministry

  - *Special (non-RTMS) cases like SPAM, content, Rogue-Pharma, e-Piracy, Cyber-squatting, etc.*
    - We always escalate these cases to Colombian Law Enforcement Agencies (LEA's) and ITC Ministry so that they can investigate and take action.

Our Process: Lessons Learned

- **After 5 years of RTMS operation, 97% of alerts are non-actionable**
  - ***44% dead links***
  - **56% *not malicious* after research**
- **Therefore:**
  - **We review *every single alert* we received**
    - **Based on RDCP / RTMS's incident scope**
  - **We only notify after exhaustive investigation**
  - **.CO special (non RTMS) cases:**
    - **Escalate to LEA's and ITC Ministry for investigation and action**
    - **We are NOT a LEA and we're very conscious of it**
    - **Local LEA's: our partners in cybersecurity (collaboration).**
  - **Every country has its own perspective on cyber-crime**

.COllaboration

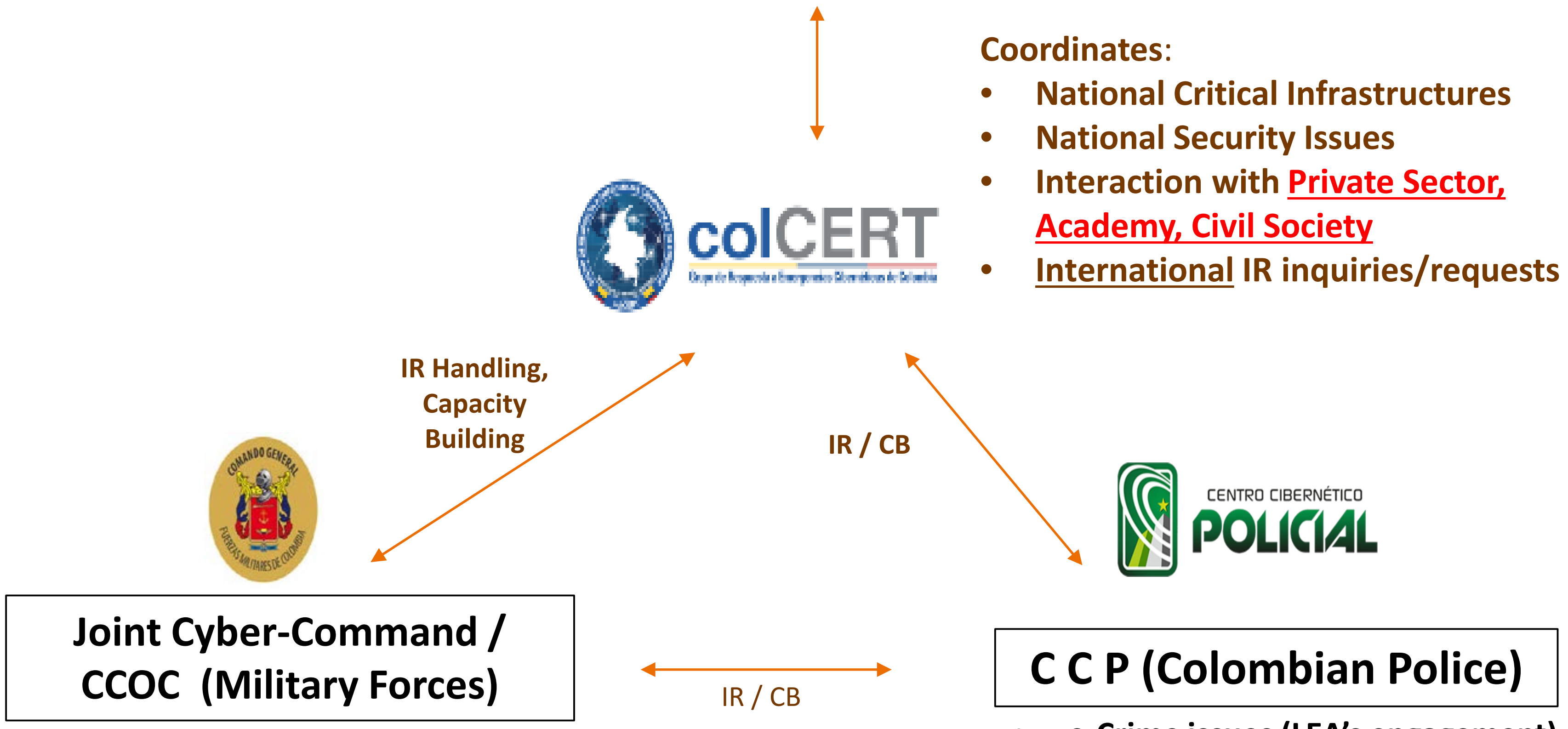
- Related to Security Policies
  - *ICANN (ccNSO, current LATAM's SSR and Security projects), LACTLD, LACNIC, APWG, ISOC, OAS/IDB, WEF, DNS-OARC*
- Related to Incident Management
  - *RDCP / RTMS*
    - Colombia: *Ministry of Defense* (National CERT and Cyberdefense Command, National Police), Ministry of ITC and *child protection communities/organizations (REDPAPAZ)*
    - Worldwide: FIRST, APWG, SOC's, CERT's and CSIRT's
  - *Permanent networking and exchange with world-class cybersecurity stakeholders.*

Digital Security – National *Policy*

(CONPES 3854 / 2016)

President, Ministers, External Affairs:

- ***Political*** **and *Strategic* management**



Coordinates:

- **National Critical Infrastructures**
- **National Security Issues**
- **Interaction with Private Sector, Academy, Civil Society**
- **International IR inquiries/requests**

IR Handling, Capacity Building

IR / CB

Joint Cyber-Command / CCOC (Military Forces)

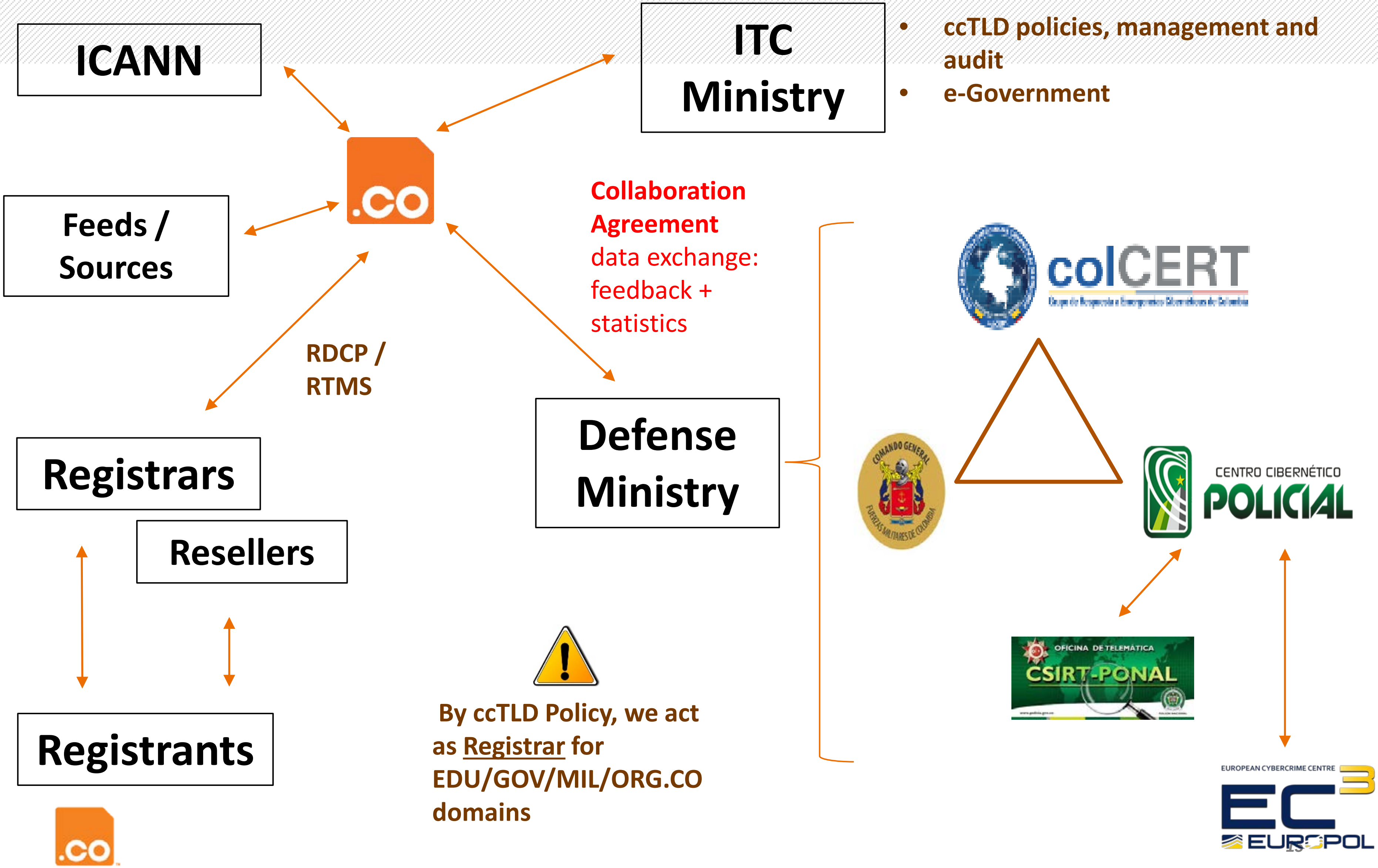
IR / CB

C C P (Colombian Police)

- **National Critical Infrastructure framework**
- **Cyberdefense issues**

- **e-Crime issues (LEA's engagement)**
- **Individuals & Companies Awareness and Protection**

How everything is linked to us



ICANN

ITC Ministry

- ccTLD policies, management and audit
- e-Government

Feeds / Sources

Collaboration Agreement
data exchange:
feedback +
statistics

RDCP / RTMS

Registrars

Resellers

Defense Ministry

Registrants

By ccTLD Policy, we act as <u>Registrar</u> for EDU/GOV/MIL/ORG.CO domains

.COllaboration: Efforts in Colombia

COLOMBIA CSIRT-CCIT
Centro De Coordinación Seguridad Informática Colombia

FIRST
Improving Security Together

- **2010**: Colombian ITC Chamber (CCIT)
  - *Our first cybersecurity cooperation agreement*
  - *Support for CSIRT-CCIT to be the 1st national member of the FIRST community*
    - *Via NeuStar's NEUCIRT (site visit sponsor)*
- **Today**: Nine (9) Colombian CSIRT's in FIRST
  - *Including .CO Team from NEUCIRT*

.COllaboration: Efforts in Colombia

colCERT
Grupo de Respuesta a Emergencias Cibernéticas de Colombia

MinDefensa
Ministerio de Defensa Nacional

- National Government CERT (colCERT)
  - *.CO incidences exchange and follow-up*
    - *GOV/MIL/EDU/ORG.CO domain names*
  - *Support knowledge transfer, cyber-hygiene and awareness campaigns in public entities*
    - *WHOIS.CO contact info updates from GOV/MIL/EDU/ORG.CO Registrants*
  - *DNSSEC for GOV.CO's project*
  - *HONEYPOT project*
  - *Incident Management System*
    - *Joint software development project*

.COllaboration: Efforts in Colombia

- **National Cyber-Police Center (CCP)**
  - ***.CO incidences exchange and follow-up***
    - ***GOV/MIL/EDU/ORG.CO domain names***
  - ***Support to knowledge transfer, cyber-hygiene and awareness campaigns in public entities***
    - ***WHOIS.CO contact info updates from GOV/MIL/EDU/ORG.CO Registrants***
  - ***“Cyber experts Coffee” active attendance***
  - ***PANGEA (Rogue Pharma) and IOS-II (e-Piracy) operations (INTERPOL): currently working together, under Colombian Applicable Law***

.COllaboration: Efforts in Colombia

- National Police CSIRT (CSIRT-PONAL)
  - .CO incidences exchange and follow-up
    - GOV/MIL/EDU/ORG.CO domain names
  - Support to knowledge transfer, cyber-hygiene and awareness campaigns in public entities
    - WHOIS.CO contact info updates from GOV/MIL/EDU/ORG.CO Registrants
  - Active attendance in Crisis Meetings
    - Incident handling during national holidays

.COllaboration: Efforts in Colombia

- **Joint Cyber-Command (CCOC)**
  - ***Active participation in their Critical Infrastructure’s meetings***
    - **We are aware and conscious of being a *critical asset* for the global and country’s Internet stability and reliability**
  - ***DNSSEC for MIL.CO’s project***
  - ***Training and knowledge transfer program to military forces***
    - ***Internet Governance matters***
    - ***Domain and Internet industry trends***
    - ***Cyberdefense related topics***

.COllaboration: Efforts in Colombia

FISCALIA
GENERAL DE LA NACION

República de Colombia
Ministerio de Justicia y del Derecho

- National General Attorney (FGN)
  - *Training and knowledge transfer program to investigators and attorneys*
    - *Internet Governance matters*
    - *Domain and Internet industry trends*
    - *Cybercrime related topics*

.COllaboration: Efforts in Colombia

- **National ITC Ministry (MinTIC)**
  - ***Active participation in their multi-stakeholder meetings to generate a new version of the National Cybersecurity and Cyberdefense Public Policy and Strategy (CONPES 3854/2016)***
  - **Support to knowledge transfer, cyber-hygiene and awareness campaigns in government entities**
    - **WHOIS.CO contact info updates from GOV.CO Registrants**

.COllaboration: Efforts in LATAM

ICANN

Organization of American States

- *Paraguayan Cybersecurity Strategy*
  - 2015: .CO invited by OAS to participate in its construction

- *Peruvian Cybersecurity Strategy*
  - 2016: .CO invited by ICANN and Peruvian External Affairs to make two (2) awareness trainings for Government entities

Some Lessons Learned

- **Active collaboration between us (ccTLD as a Critical Infrastructure) and LEA’s**
  - ***Exhaustive joint research, follow-up and feedback when complex cases are submitted by trusted sources***
  - ***Legal and tech expert advice before generate official requests to take any action***
  - ***Continuous training to in-country LEA’s in regard to domains (expiration/suspension) and DNS management matters and issues***
  - ***Continuous review to ccTLD policies and domain registration’s terms and conditions***
    - **Registrar’s follow-up is KEY for success.**

.COnclusions

- TRUST is KEY!
  - Domain Registration Channel: our best partners
  - Global Law Enforcement Authorities
    - Our most capable friends and supporters in cybersecurity
- Cybersecurity communities
  - Most fruitful and valuable relationships
    - Need to be permanently nurtured by attending meetings and events
  - *Friends* trust *Friends*
    - Having a strong network of partners and friends in the industry leads to better results than complex MoU's and signed agreements.

.CO Internet S.A.S.

Q & A

Thanks!