micitt

MINISTERIO
DE CIENCIA, TECNOLOGÍA
Y TELECOMUNICACIONES

Information Security and Cybercrime in Costa Rica – a General Overview

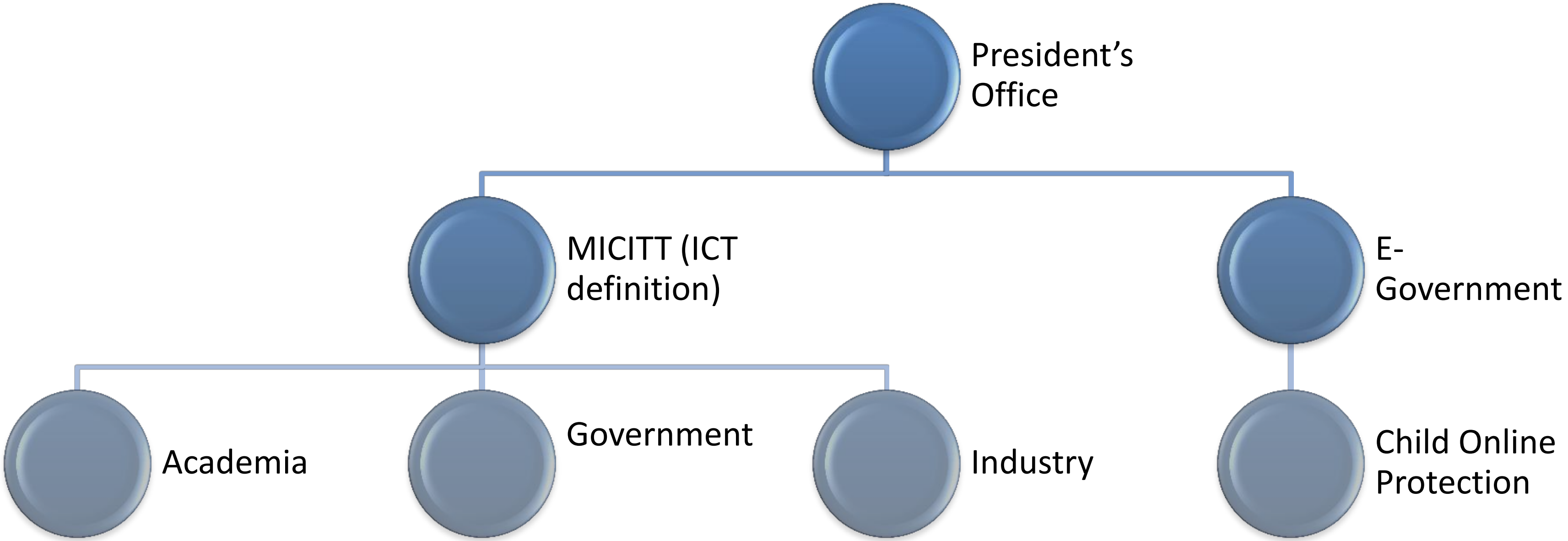
Santiago Núñez Corrales
Director

Directorate of Digital Technology
Ministry of Science, Technology and Telecommunications

ICT in the National Plans

National Development Plan	• General guidelines of ICT for national development in economics, society and public policy development
National Plan for Science, Technology and Innovation	• A plan for seven development areas in STI where ICT is central to academia, government, firms and society
National Plan for Telecommunications Development	• An implementation agenda for the recent telecommunications market opening
E-Government Master Plan	• Definiton of general guidelines for applications development towards digital citizen-orientes services

General ICT Ecosystem



President's Office

MICITT (ICT definition)

E-Government

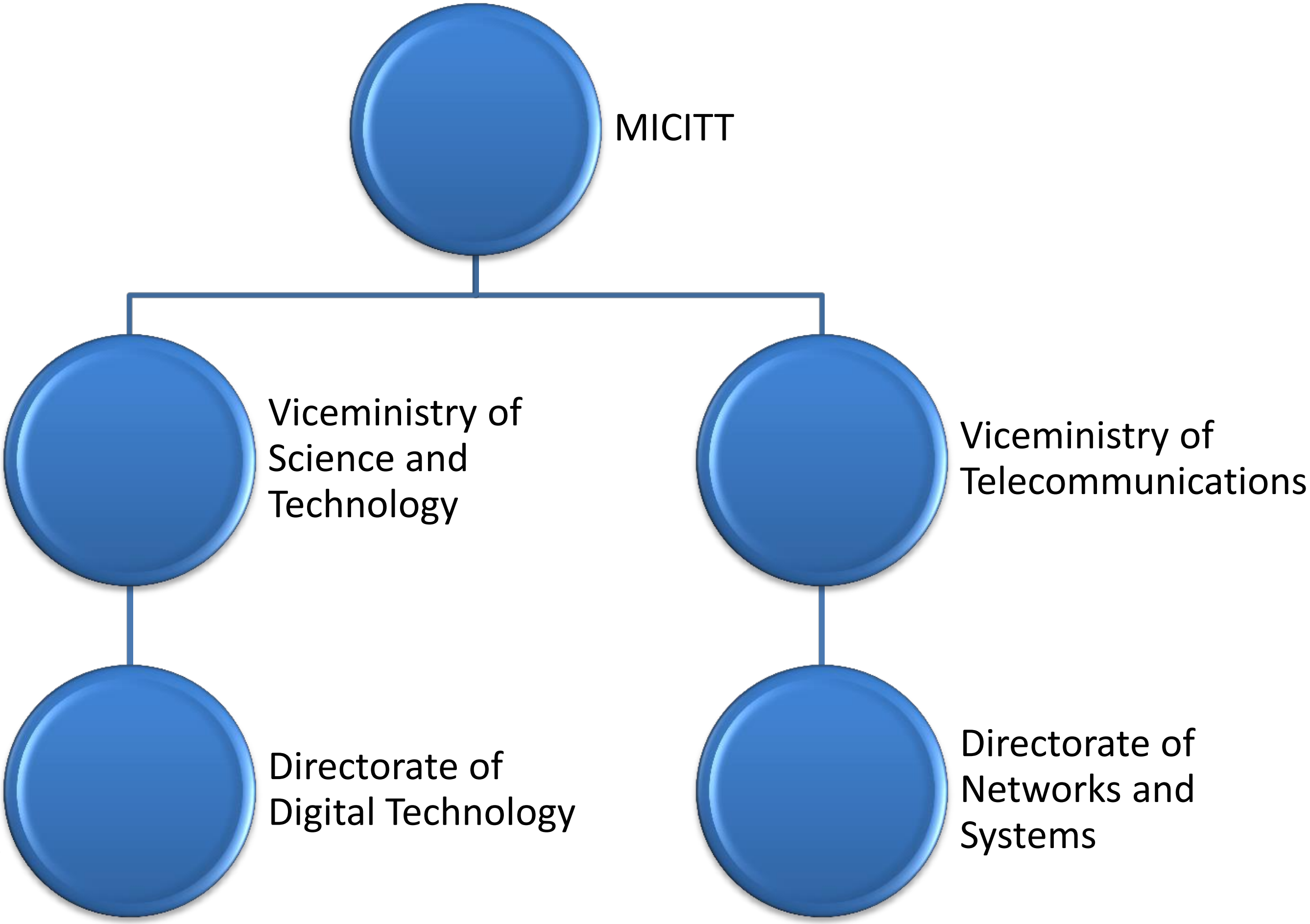
Academia

Government

Industry

Child Online Protection

ICT at MICITT



MICITT

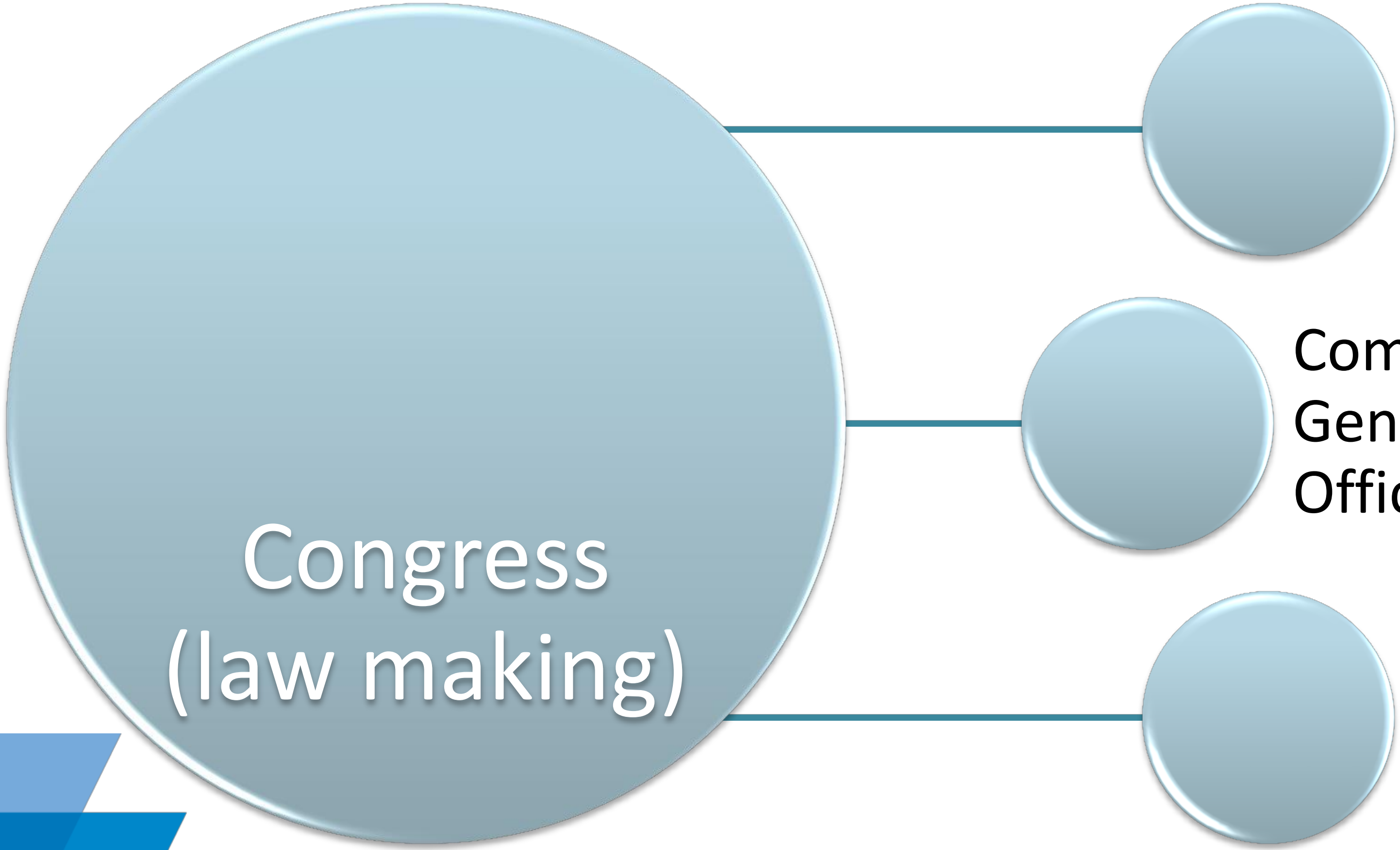
Viceministry of Science and Technology

Viceministry of Telecommunications

Directorate of Digital Technology

Directorate of Networks and Systems

General Policy Regulatory Bodies



Congress (law making)

Attorney-General's Office

Comptroller-General's Office

ARESEP

- SUTEL

ICT organization in the private sector

Chamber of ICT firms (CAMTIC)

- 85% of firms are SMEs (~300 firms)
- Generate 45% of national ICT exports

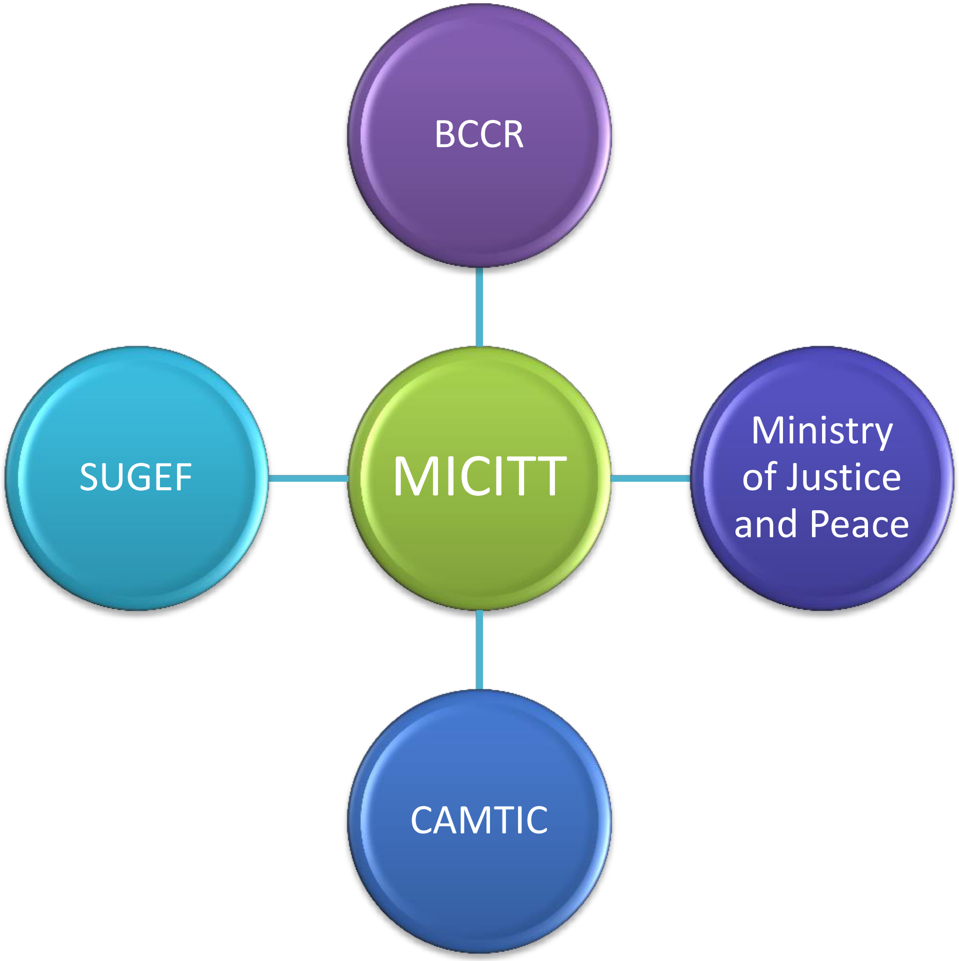
Chamber of Infocommunications (INFOCOM)

- Mostly ICT-enabled services (e.g. digital animation)
- Approx 28% of total national exports

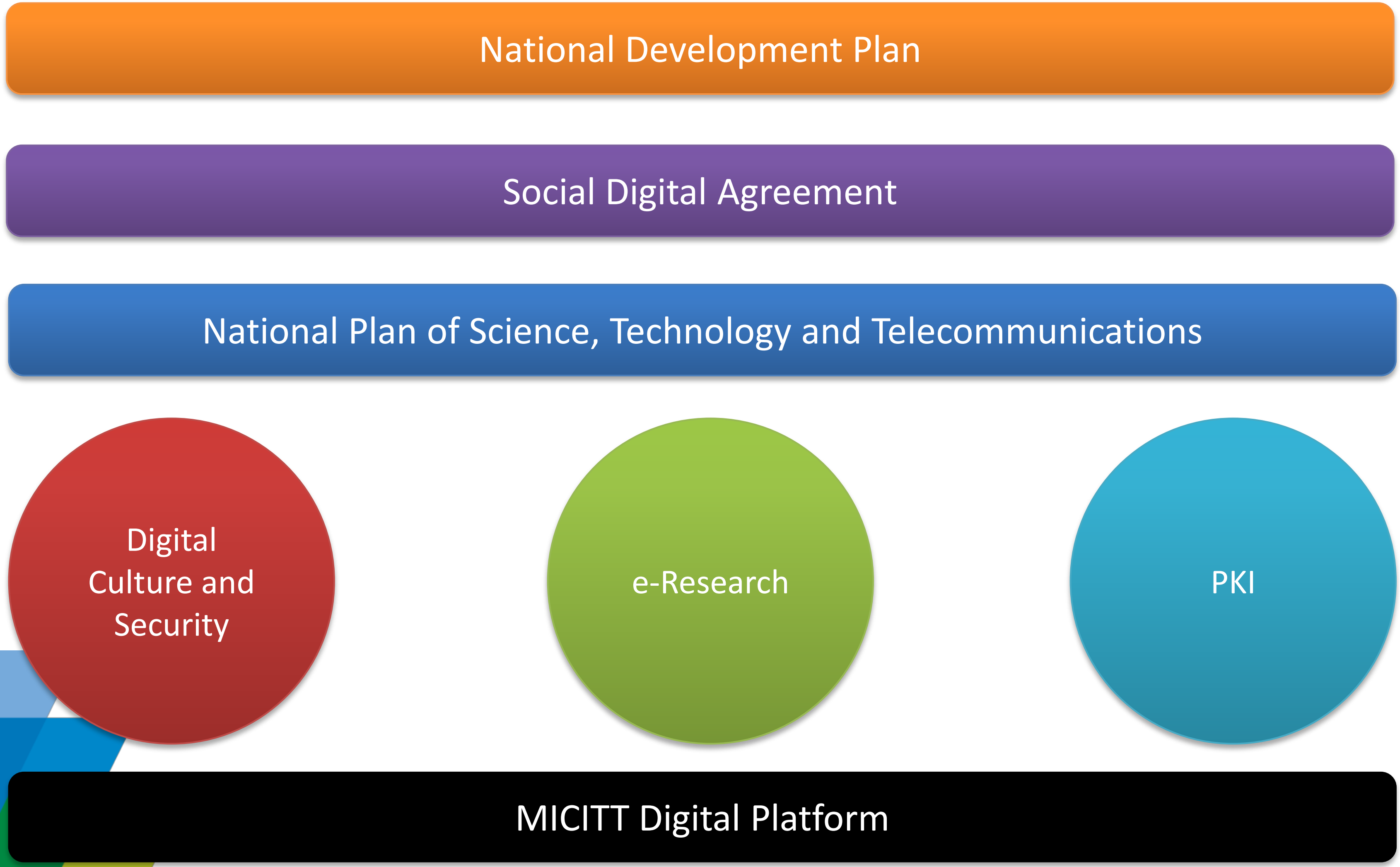
Costa Rica Investment Promotion Agency (CINDE)

- 15% of firms in CR, transnationals
- Generate 55% of national ICT-exports

National PKI infrastructure



Social Perspective of ICT at MICITT



National Development Plan

Social Digital Agreement

National Plan of Science, Technology and Telecommunications

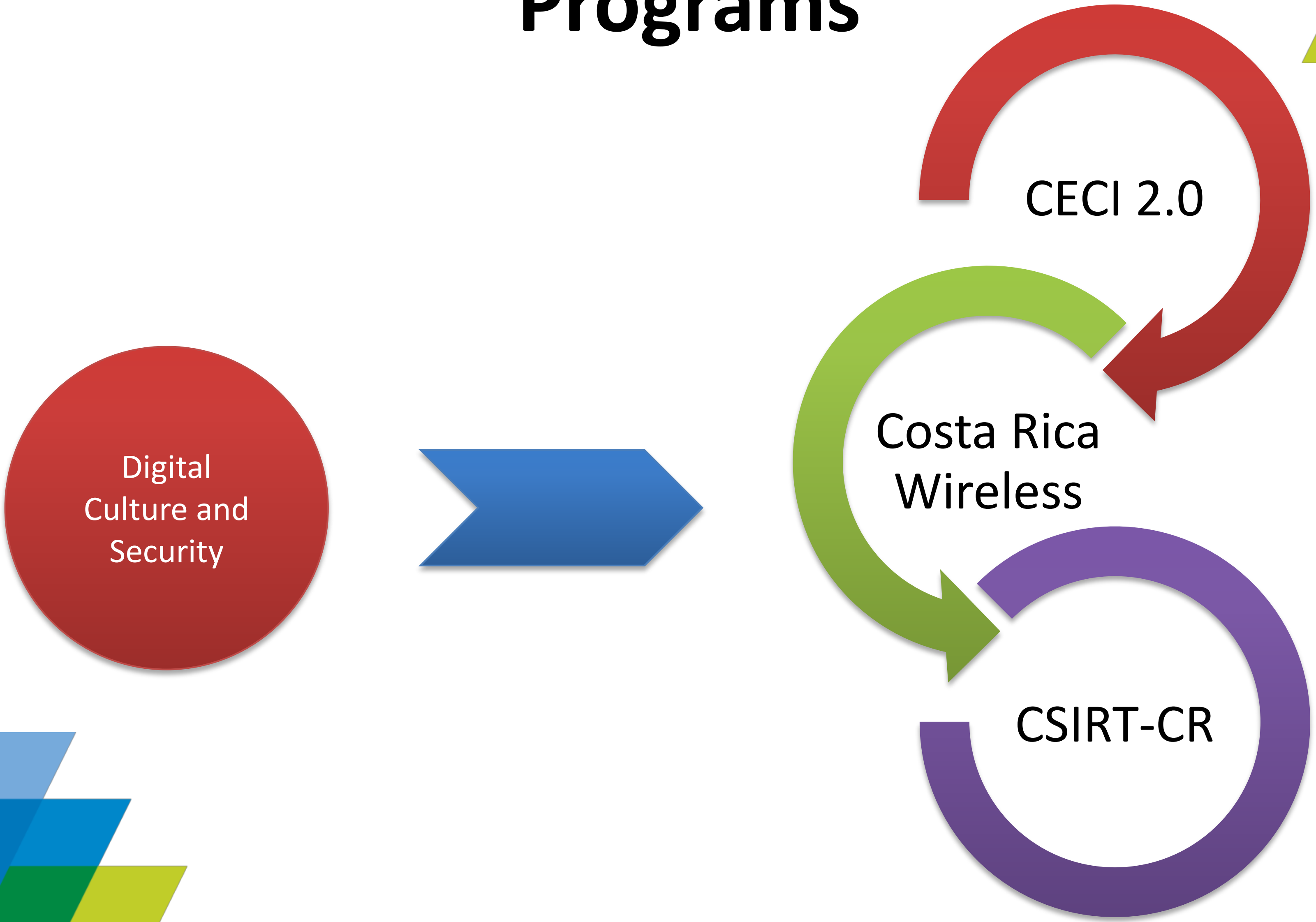
Digital Culture and Security

e-Research

PKI

MICITT Digital Platform

Directorate of Digital Technology: Programs



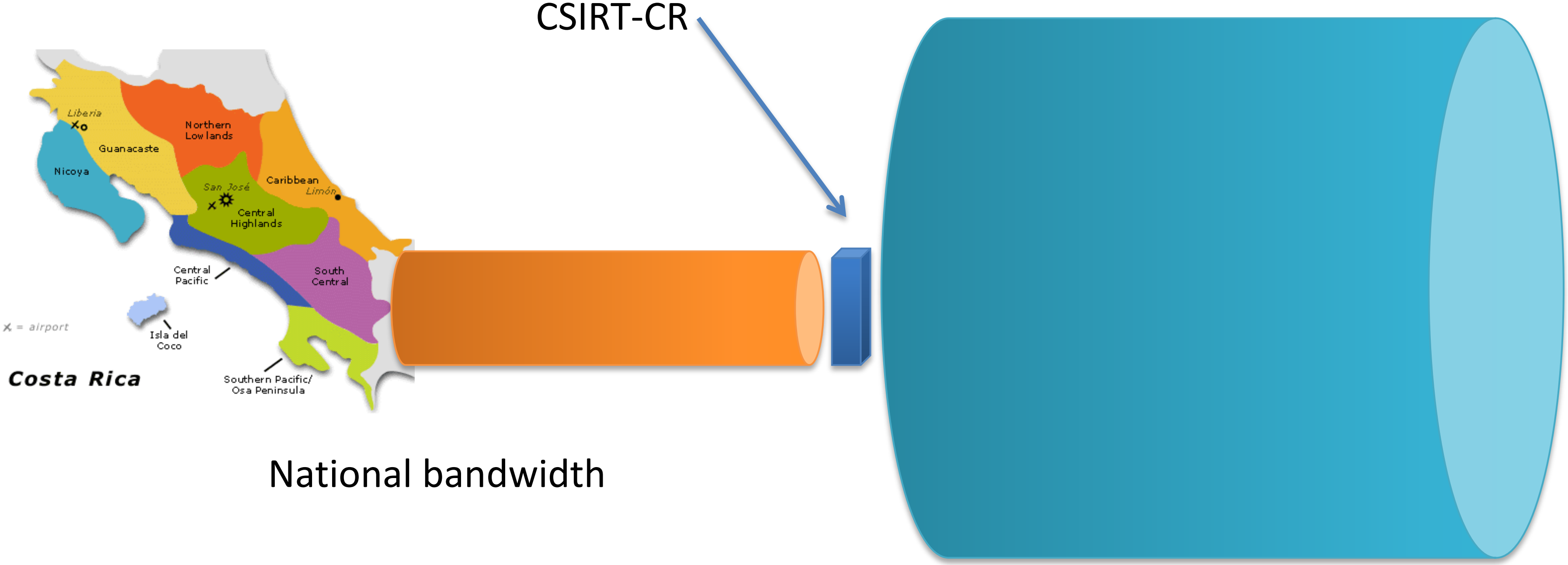
Status on Cybersecurity

CSIRT-CR

Establishment of CSIRT-CR

- **2005**: Adhesion to the international OAS treaty on terrorism
- **2008**: Adhesion to the international treaty on cybercrime
- **2012**: Formal creation by decree of CSIRT-CR, April 13
  - First incident: April 14th
- **Current status**: limited incident response

CSIRT-CR: the need

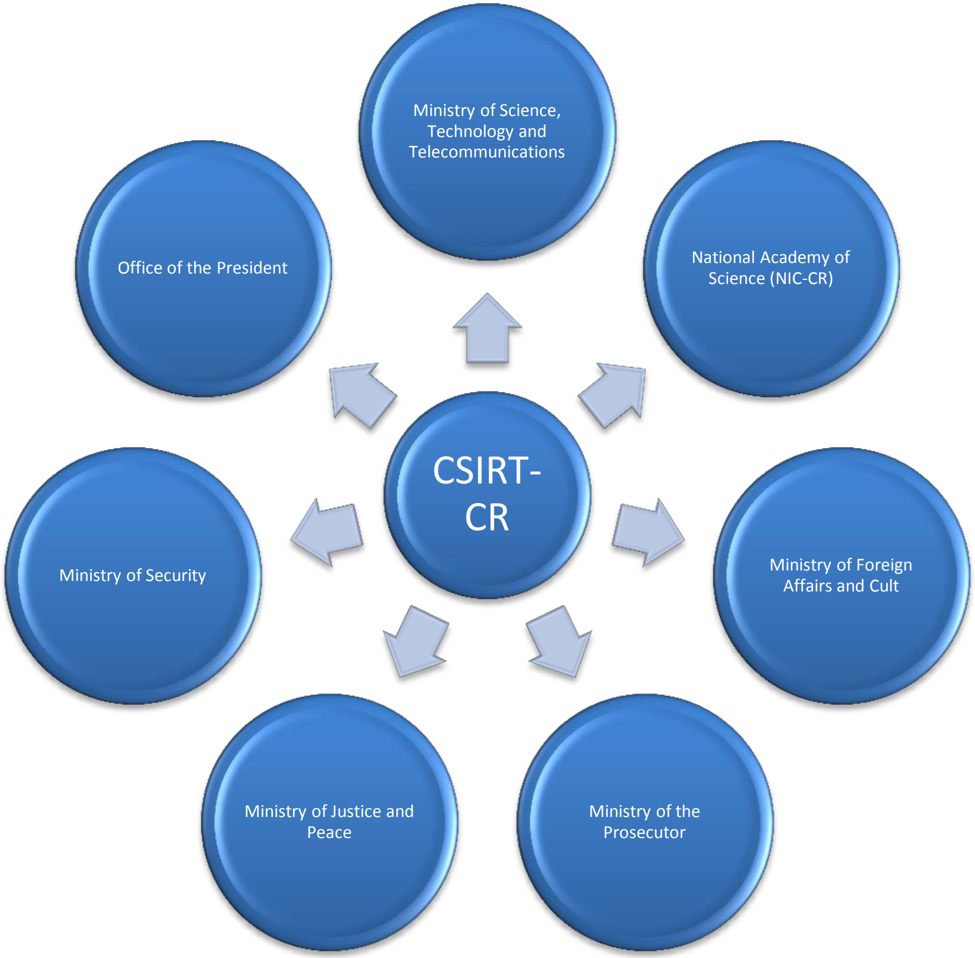


CSIRT-CR

National bandwidth

Anonymous potential attack > 300Gbps

CSIRT-CR: structure



CSIRT-CR

Ministry of Science, Technology and Telecommunications

National Academy of Science (NIC-CR)

Ministry of Foreign Affairs and Cult

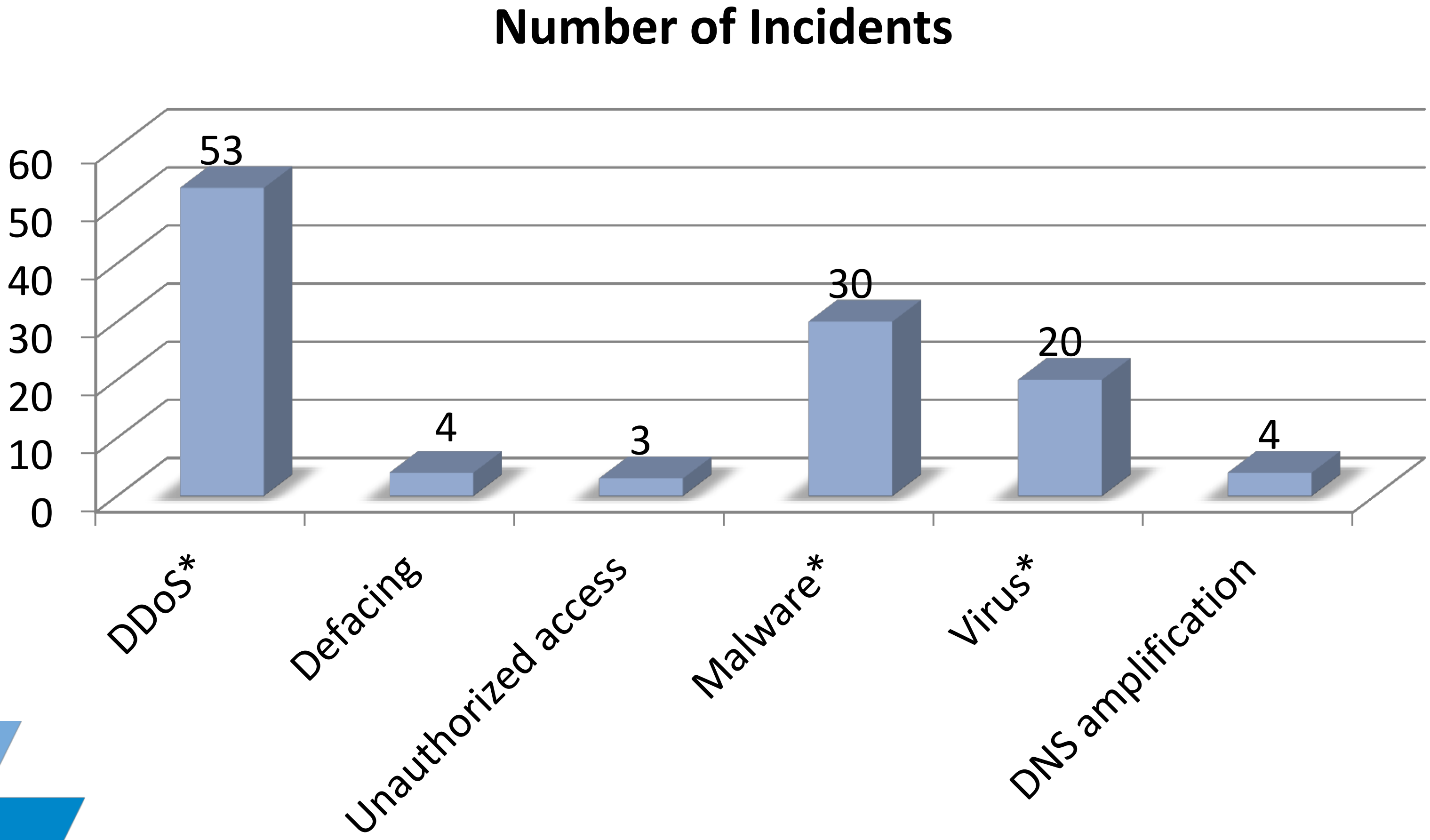
Ministry of the Prosecutor

Ministry of Justice and Peace

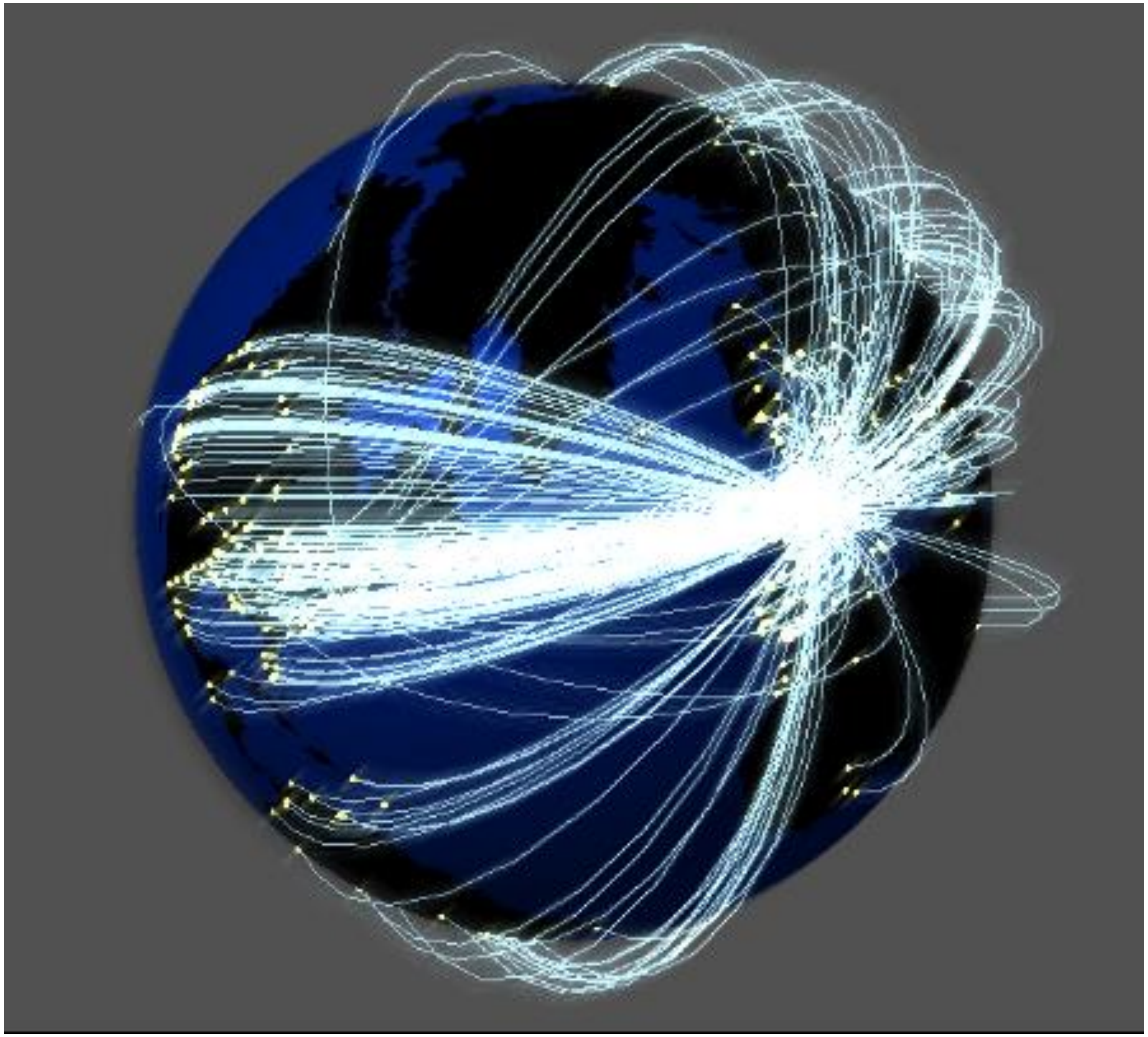
Ministry of Security

Office of the President

Incident Handling Statistics



* Includes only top 5% incidents in relevance. For actual figures, rescale values by 20X.



Incident Handling: Impact

DDoS	• Limited national internet bandwith • Blocking of state websites, no critical assets yet affected
Defacing	• Affectation of public image • Revealed several basic vulnerabilities
Unauthorized access	• One case related to corruption • User profile definition problems
Malware	• Main incident • Botnet related activities
Virus	• Irregular distribution of antivirus availability • Software versioning with little or no control
DNS amplification	• Limited internet bandwidth • Discovery of latent DNS vulnerabilities

Incident Handling: sources of attacks

Asia

- China***
- Vietnam**
- North Korea
- Singapore
- Malasya
- Iran
- Arab Emirates
- Syria
- Afghanistan

Africa

- Egypt***
- Niger
- South Africa
- Libya

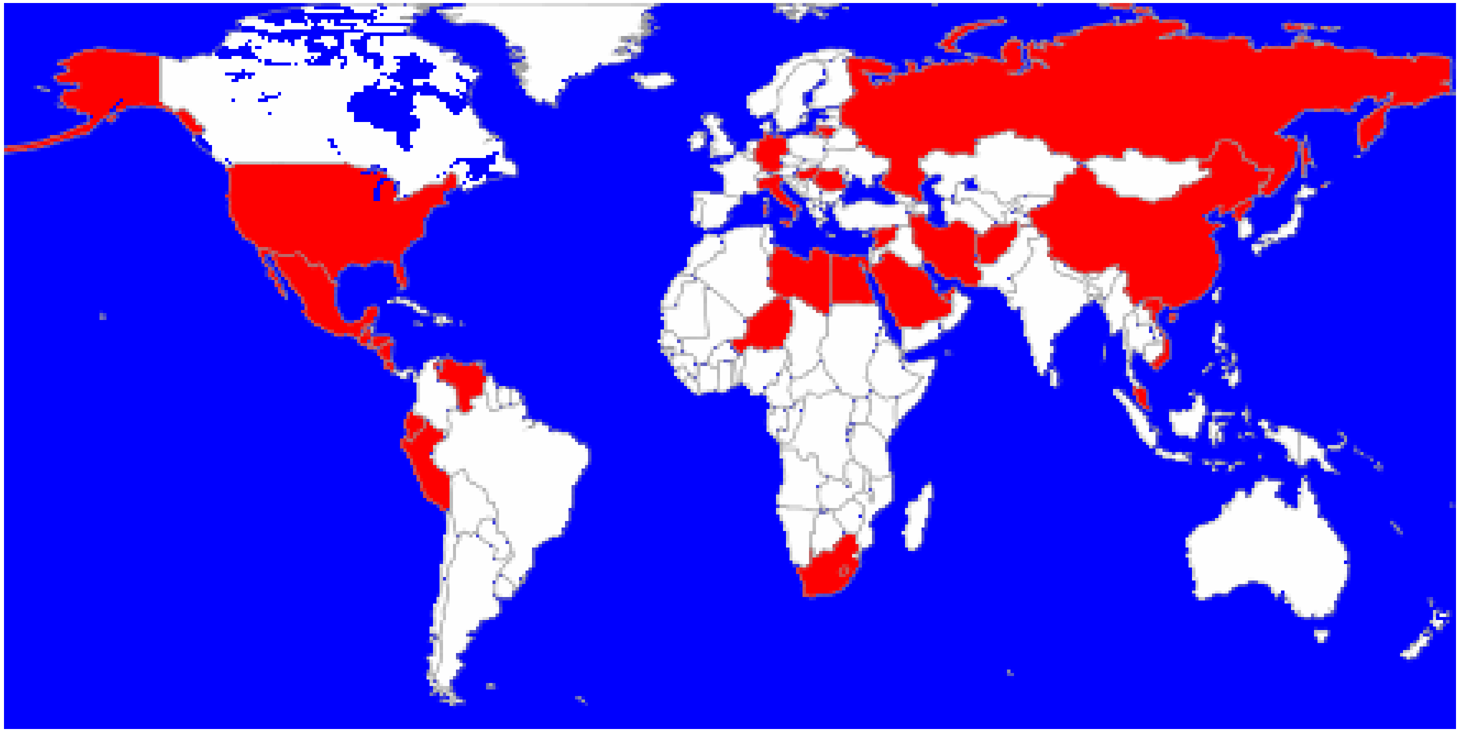
Europe

- Russia***
- Germany
- Italy
- Romania**
- Hungary
- Serbia
- Lithuania

America

- USA
- Mexico
- Ecuador***
- Venezuela
- Guatemala**
- El Salvador**
- Honduras
- Nicaragua
- Colombia
- Peru

Incident Handling: sources of attacks



CSIRT-CR: pending challenges

Limited staff

- Based on voluntary work for anticipated significant events
- Only two permanent collaborations at MICITT, part time (amongst *several* other assignments)

No current funding

- Six positions pending to be enabled
- No independent operational infrastructure

Low awareness in the government sector

- No integrated coordination
- Protocols limited to basic actions

Revamping the judicial system

- Homologation of international legal instruments (e.g. Evidence preservation)
- Improved cybercrime definitions and enacting normative

14/04/2012

The Anonymous Case

The Initial Discovery

- Two local Anonymous groups detected by the judicial police six weeks in advance, coordination started
- The CSIRT-CR decree was being drafted since November 2011 and fast-tracked for that occasion
- An informal group of the most critical institutions gathered together four weeks in advance as a task force

The Attack Strategy

- A massive DDoS attack on several institutional Websites including the Ministry of Finance, the Presidential Office, the Ministry of Security, the Ministry of Justice and the Legislative Assembly
- Correlated with a national protest against a fiscal reform ("Plan Fiscal 2012")
- 3 weeks in advance: recruitment of Anonymous Central America, Italy and Germany observed

The Proposed Mitigation Plan

- Objective: quick detection and response
  - NIC-CR: detection of abnormal DNS traffic patterns
  - MICITT, MH, MS, BCCR, Casapres: six surveillance shifts, 8 hours per shift (covering from the expected day of the attack to one day after)
  - One protocol for calling key people and performing the report
  - Strong coordination with CSIRT-ICE

Tools and Communication

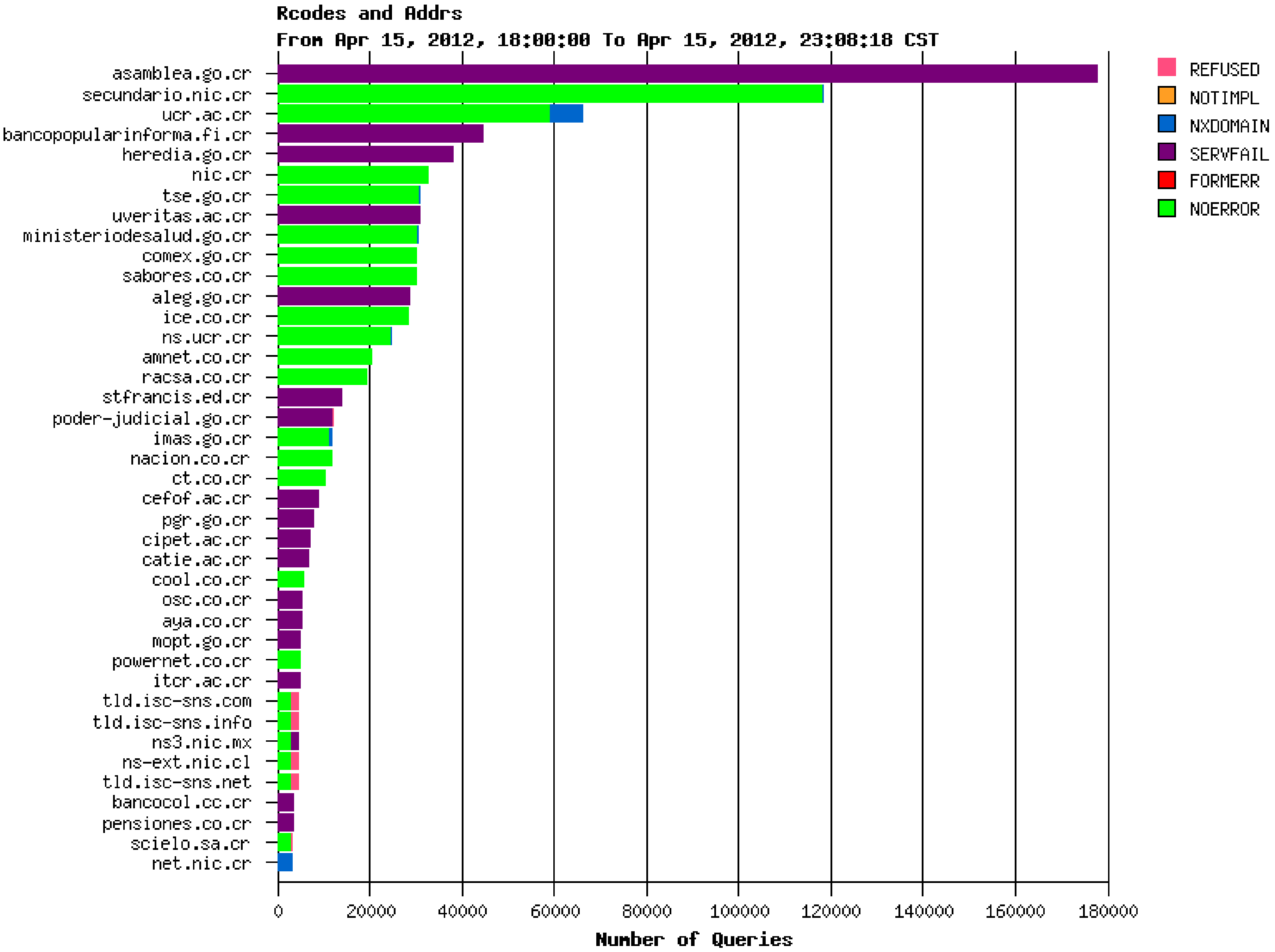
- Single e-mail for incidents created
  - csirt-cr@micit.go.cr
- Usage of servermojo for detecting sites in DOWN state
- Constant DNS query monitoring
- E-mail and phone numbers
- A simple incident logging tool was developed for the occasion
- Casa Presidencial: cloud-based DNS shelter

Initial Prevention

- 40 most critical State institutions
- IT directors were alerted in all of them at different periods before the incident
  - 3 weeks
  - 1 week
  - 3 days
  - 1 day

The Attack

- CSIRT-CR was created on April 13th, 2012
- Anonymous attacked at 17:00h, April 14th 2012
- Target sites
  - Presidential Office
  - Legislative Assembly
- Anonymous used the WEBHIVE DDoS tool
- Initial mitigation started at 17:30h
- A change in the attack strategy was detected at 18:00h and the volume of offenders increased


Rcodes and Addrs
From Apr 15, 2012, 18:00:00 To Apr 15, 2012, 23:08:18 CST
asamblea.go.cr
secundario.nic.cr
ucr.ac.cr
bancopopularinforma.fi.cr
heredia.go.cr
nic.cr
tse.go.cr
uveritas.ac.cr
ministeriodesalud.go.cr
comex.go.cr
sabores.co.cr
aleg.go.cr
ice.co.cr
ns.ucr.cr
amnet.co.cr
racsa.co.cr
stfrancis.ed.cr
poder-judicial.go.cr
imas.go.cr
nacion.co.cr
ct.co.cr
cefof.ac.cr
pgr.go.cr
cipet.ac.cr
catie.ac.cr
cool.co.cr
osc.co.cr
aya.co.cr
mopt.go.cr
powernet.co.cr
itcr.ac.cr
tld.isc-sns.com
tld.isc-sns.info
ns3.nic.mx
ns-ext.nic.cl
tld.isc-sns.net
bancocol.cc.cr
pensiones.co.cr
scielo.sa.cr
net.nic.cr
0
20000
40000
60000
80000
100000
120000
140000
160000
180000
Number of Queries
REFUSED
NOTIMPL
NXDOMAIN
SERVFAIL
FORMERR
NOERROR

The Results

- Casa Presidencial: DOWN time reduced to two periods of no more than 5 minutes on each attack attempt
- Legislative Assembly: site down by 17:20h
- The attack finished at the 23:00h with trailing IP addresses until 15/04/2012 5:00h
- Offenders from the expected countries, a large share from Central America and Europe
- Few IP addresses from Costa Rica
- Extensive use of TOR networks to conceal origin

The Lessons

- Digital surveillance in hacktivism groups is a valuable prospection tool
- It is possible to coordinate a distributed response to a large incident and reduce the final impact (from 10 institutions to 2)
- Offenders are quick to adapt to incident response strategies
- A sustainable structure is required for follow-up
- International coordination is key for a quick response

micitt