nic.br cgi.br | 20 years cert.br

LAC-CSIRTs & FIRST Technical Colloquium

Rosario, Argentina

September 26, 2018

From Professionals to Policy Makers: Challenges and Opportunities in Educating about Cybersecurity and Incident Handling

Dr. Cristine Hoepers
General Manager, CERT.br/NIC.br
cristine@cert.br

cert.br nic.br cgi.br

Internet Governance in Brazil:
The Brazilian Internet Steering Committee – CGI.br

CGI.br is a **multi-stakeholder organization** created in 1995 by the Ministries of Communications and Science and Technology to **coordinate all Internet related activities in Brazil**.

Among the diverse responsibilities reinforced by the Presidential Decree 4.829, it has as the main attributions:

- to propose policies and procedures related to the regulation of Internet activities
- **to recommend standards for technical and operational procedures**
- to establish strategic directives related to the use and development of Internet in Brazil
- **to promote studies and technical standards for the network and services' security in the country**
- to coordinate the allocation of Internet addresses (IP) and the registration of domain names using <.br>
- **to collect, organize and disseminate information on Internet services, including indicators and statistics**

https://www.cgi.br/about/

cgi.br

1 2 3 4 5 6 7 8 9

GOVERNMENT (Appointed)

and

10 11 12 13 14 15 16 17 18 19 20 21

CIVIL SOCIETY (Elected)

Government Representatives:

1 Ministry of Science and Technology (Coordination)
2 Presidential Cabinet
3 Ministry of Communications
4 Ministry of Defense
5 Ministry of Development, Industry and Foreign Trade
6 Ministry of Planning, Budget and Management
7 National Telecommunications Agency
8 National Council of Scientific and Technological Development
9 National Forum of Estate Science and Technology Secretaries

Civil Society Representatives:

10 Internet Expert
11 General Business Sector Users
12 Internet Service Providers
13 Telecommunication Infrastructure Providers
14 Hardware and Software Industries
15 a 18 Non-governmental Entity
19 a 21 Academia

Brazilian Network Information Center – NIC.br

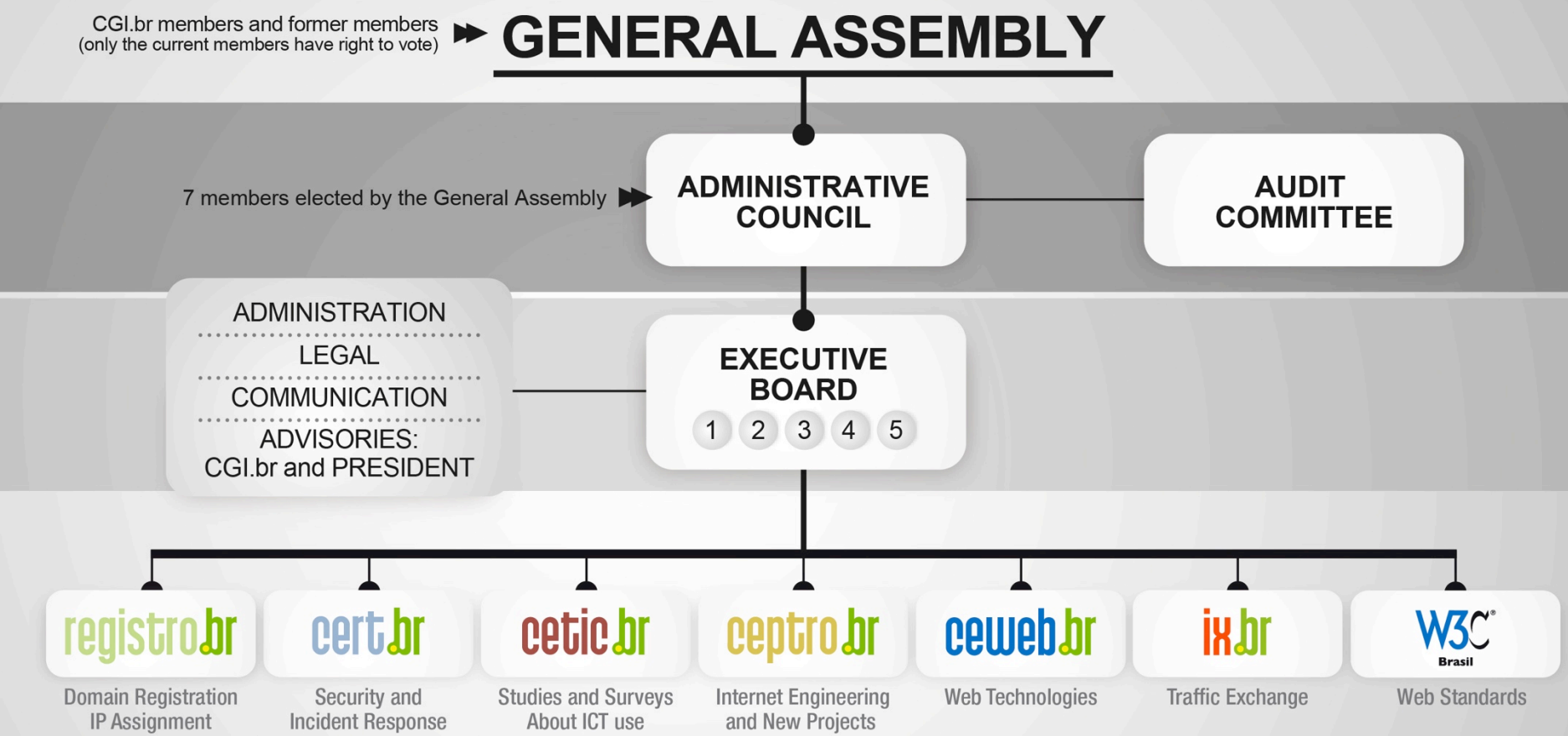
A **private not for profit** organization, created to **implement the decisions and projects designed by the Brazilin Internet Steering Committee – CGI.br**.

Its mission involves certain rights and obligations, which include:

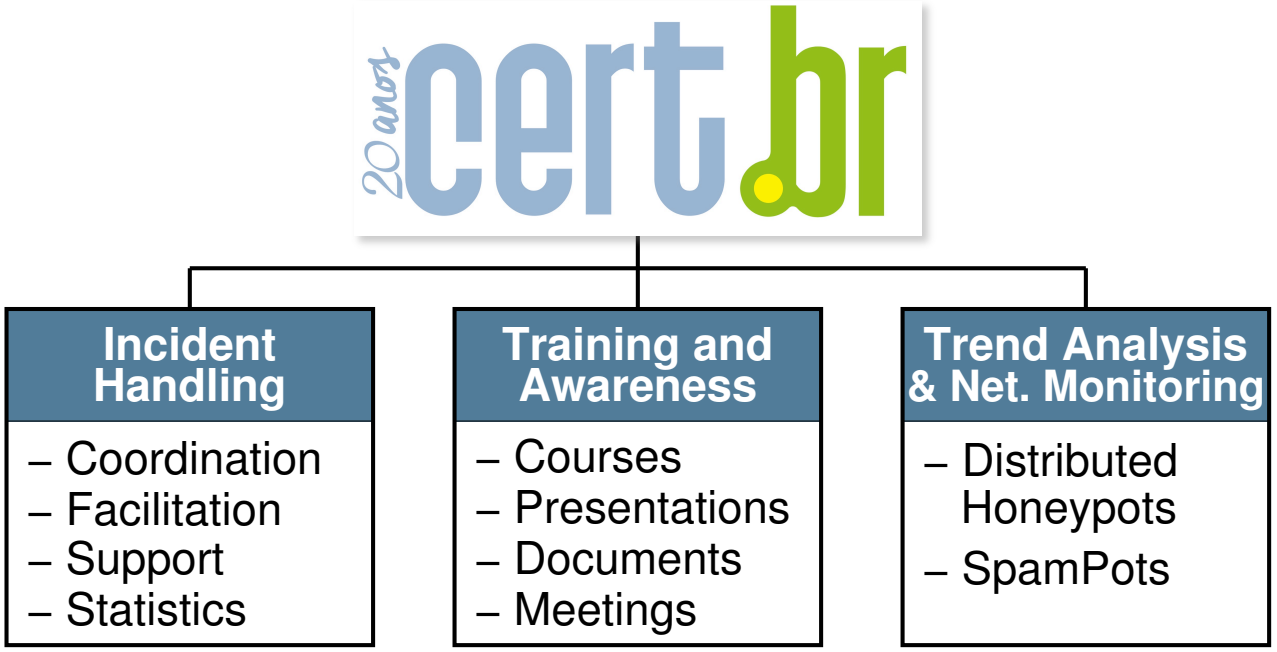
- registering and maintaining <.br> domain names, as well as allocating Autonomous System Numbers (ASN) and IPv4 or IPv6 addresses in the country through Registro.br;
- **handling and responding to computer security incidents involving networks connected to the Brazilian Internet, which are activities to be carried out by CERT.br;**
- projects that support and improve the network infrastructure in the country, such as the direct interconnection between networks (IX.br) and the distribution of the Brazilian Official Time (NTP.br). These projects are the responsibility of CEPTRO.br;
- promoting studies and recommending procedures, norms and technical and operational standards that will improve network and Internet service security, as well as ensure its increased and adequate use by society.

https://nic.br/who-we-are/

Brazilian Network Information Center – NIC.br



1 Chief Executive Officer
2 Administrative and Financial Director
3 IT and Services Director
4 Director of Special Projects and Development
5 Consulting Director for CGI.br activities



FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

SEI Partner
Carnegie Mellon.

Created in 1997 to handle computer security incident reports and activities related to networks connected to the Internet in Brazil

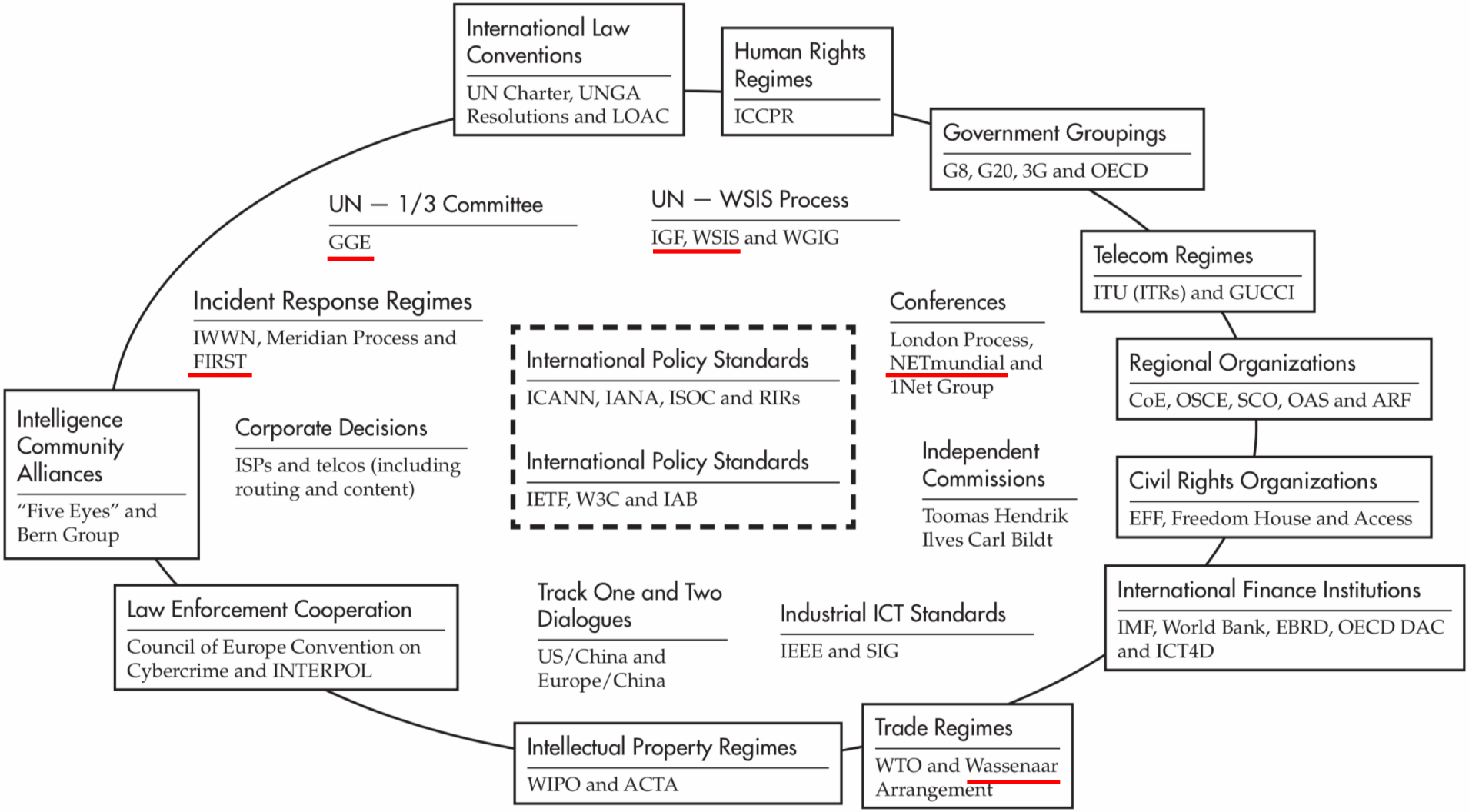
- National focal point for reporting security incidents
- Collect and disseminate information about threats and attack trends
- Increase the country's security awareness and incident handling capacity
- Develop collaborative relationships with other entities
- Help new CSIRTs to establish their activities

https://www.cert.br/about/

1996 CGI.br study that defined the needs and mission of CERT.br (in Portuguese):
http://www.nic.br/pagina/grupos-de-trabalho-documento-gt-s/169

Policy Makers and Cybersecurity

cert.br nic.br cgi.br



The Regime Complex for Managing Global Cyber Activities
Global Commission on Internet Governance Paper Series No. 1
May 20, 2014, Joseph S. Nye Jr.
https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities

World Summit on the Information Society (WSIS): **Declaration of Principles**

Document WSIS-03/GENEVA/DOC/4-E

12 December 2003

[...]

B5) Building confidence and security in the use of ICTs

35. Strengthening the trust framework, **including information security and network security, authentication, privacy and consumer protection**, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs.

[...]

http://www.itu.int/wsis/docs/geneva/official/dop.html

Led to the creation of the Internet Governance Forum (IGF) in 2006

IGF Internet Governance Forum

CGI.br:
Principles for the Governance and Use of the Internet

CGI.br/RES/2009/003/P - Principles for the Governance and Use of the Internet

February 2009

[...]

8. Functionality, security and stability

The **stability, security** and overall functionality of the network must be actively preserved through the **adoption of technical measures that are consistent with international standards and encourage the adoption of best practices**.

[...]

https://www.cgi.br/resolucoes-2009-003-en/

The CGI.br principles lead to a new legislation: **The Brazilian Internet Bill of Rights (MCI)**

2009 – 2013

- Open consultation process for a new legislation
- Active participation of all sectors of the society
  - All contributions via an online platform

Early 2013

- Legislation draft sent to Congress

Mid 2013

- “Snowden revelations”

2013 – 2014

- Legislation proposal got traction in Congress
- NETMundial meeting was called

April 2014

- MCI was signed into law by the President at the NETmundial opening ceremony

https://igarape.org.br/marcocivil/assets/downloads/igarape_brazil-the-internet-and-the-digital-bill-of-rights.pdf

NETmundial:
Internet Governance Principles

Global Multistakeholder Meeting on the Future of Internet Governance

NETmundial

NETmundial Multistakeholder Statement

April, 24th 2014, 19:31 BRT

[...]

SECURITY, STABILITY AND RESILIENCE OF THE INTERNET

Security, stability and resilience of the Internet should be a key objective of all stakeholders in Internet governance. As a universal global resource, the Internet should be a **secure, stable, resilient, reliable and trustworthy network**. **Effectiveness** in addressing risks and threats to security and stability of the Internet **depends on strong cooperation among different stakeholders**.

[...]

http://netmundial.br/netmundial-multistakeholder-statement/

UN GGE

UNODA
UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS

UN General Assembly, Group of Governmental Experts, Document A/70/174

22 July 2015

[...]

States should not conduct or knowingly support activity to **harm the information systems of the authorized emergency response teams** (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

[...]

https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf

Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies

Group of 42 countries, created after the Cold War, to control the export of weapons and dual-use technology

Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, **Mexico**, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom and United States.

2013 – inserted "*intrusion software*" in the list of controlled technologies

Scope of the New Entries:

Systems, equipment, components and software specially designed for the **generation, operation or delivery of, or communication with, intrusion software** include **network penetration testing products** that use intrusion software to identify vulnerabilities of computers and network-capable devices. Certain penetration testing products are currently classified as encryption items due to their cryptographic and/or cryptanalytic functionality. Technology for the development of intrusion software **includes proprietary research on the vulnerabilities and exploitation of computers and network-capable devices**.

https://www.federalregister.gov/documents/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items

Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies – December 2017

4. E. 1. "Technology" as follows:

a. "Technology" according to the General Technology Note, for the "development", "production" or "use" of equipment or "software" specified by 4.A. or 4.D.

[...]

c. "Technology" for the "development" of "intrusion software".

Note 1 **4.E.1.a. and 4.E.1.c. do not apply to 'vulnerability disclosure' or 'cyber incident response'**.

Note 2 Note 1 does not diminish national authorities' rights to ascertain compliance with 4.E.1.a. and 4.E.1.c.

Technical Notes

1. **'Vulnerability disclosure' means** the process of identifying, reporting, or communicating a vulnerability to, or analysing a vulnerability with, individuals or organizations responsible for conducting or coordinating remediation for the purpose of resolving the vulnerability.
2. **'Cyber incident response' means** the process of exchanging necessary information on a cyber security incident with individuals or organizations responsible for conducting or coordinating remediation to address the cyber security incident.

[...]

https://www.wassenaar.org/app/uploads/2018/01/WA-DOC-17-PUB-006-Public-Docs-Vol.II-2017-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf

We have Statements and Several Fora
Do all stakeholders understand the technology?

UNODA
UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS

IGF Internet Governance Forum

Global Multistakeholder Meeting on the Future of Internet Governance

NETmundial

"Without 'exceptional access' it is impossible to investigate crimes"

"Routers should not inspect packet headers"

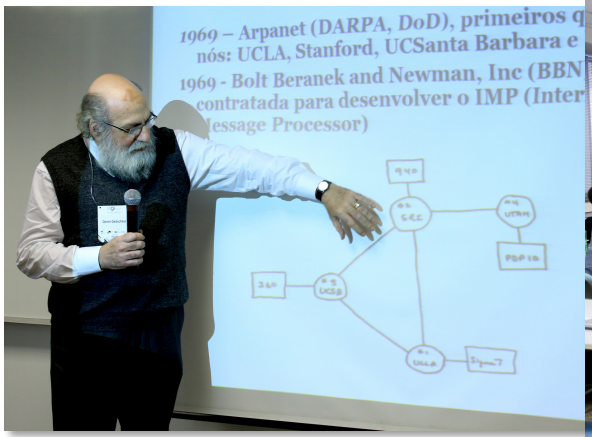
"Using crypto is enough to ensure privacy"

"Cookies harm privacy, we should get rid of cookies"

Brazilian Internet Governance School (EGI) 2014–present: **Educate policy makers about technology**

https://www.flickr.com/photos/nicbr/albums

Brazilian Internet Governance School – Legal Focus: **Educate LEAs, judges, prosecutors, lawyers, etc**



https://www.flickr.com/photos/nicbr/albums

Training Different Audiences: **Major Challenges**

Technical community

- Lack of foundations
  - TCP/IP, operating systems, networking
- Believe that tools should be the focus
- Don't care about policy implications
- Resistance to new technologies
  - Delay in acknowledging them
  - Resistance to adopt them

Policy makers, activists and legal personnel

- They don't think they need to understand a minimum about the technology
  - Mismatch of expected behavior vs. unintended consequences of a given policy being proposed
- Have preconceptions
- Different "language" is still a main barrier
  - To describe their view of how the technology works they rely on metaphors, not always the best ones ☹

Training Different Audiences:
Major Opportunities

Technical community

- Provides a structured way to deliver our message
- Creates a pool of knowledgeable professionals
- Fosters a trusted community

Policy makers, activists and legal personnel

- Highlights our own misconceptions and preconceptions
- Helps us to better shape our message
  - Avoid “taboo” words (like monitoring and deep packet inspection!)
  - Create our own metaphors ☺
- We can get them acquainted with our language and acronyms
  - CSIRT, CERT, FIRST, IETF, ICANN, ISOC, RIR...
  - AS, ASN, BGP, IXP, ISP, Peering...
  - TCP/IP, UDP, Service Port, TLS, DNSSEC, PGP...

Security is Inheritably Multi-stakeholder: **Cooperation for a Healthy Ecosystem**

No organization or agency alone will be able to secure the digital environment – everyone has a role, specially:

Academia
- needs to include security thinking in all disciplines
- secure development has to be a priority from the beginning

Developers / companies
- security needs to be a requirement from early development stages

Managers / executives
- think about security as in investment and allocate appropriate resources

System and network administrators and security professionals
- care about which type of traffic is leaving your network
  - mindset: do no harm, do not pollute the Internet
- adopt best current practices

End users
- understand the risks and follow security practices
- keep all devices updated and apply all patches

Final Thoughts

Technical professional qualification

- How to entice young people to learn “hard skills”?

Policy makers

- Need to learn to listen to the technical community
  - Maybe case studies of what went well and what went wrong?

Please, get engaged! Two places to start:

- **FIRST Internet Governance Initiative**
  https://first.org/global/governance/
- **United Nations Internet Governance Forum**
  Best Practice Forum on Cybersecurity
  https://www.intgovforum.org/multilingual/content/bpf-cybersecurity-1

See also:

An Internet of Governments: How Policymakers Became Interested in “Cyber”

https://first.org/resources/papers/conf2018/Van-Horenbeeck-Maarten-Aiken-Klee_FIRST_20180626.pdf

Obrigada!
¡Gracias!
Thank You!

www.cert.br

cristine@cert.br

@certbr

September 26, 2018

nic.br cgi.br

www.nic.br | www.cgi.br