Audiência Pública para discutir a suspensão dos serviços de WhatsApp pela justiça brasileira

Thiago Tavares Nunes de Oliveira
Conselheiro do CGI.br
Presidente da SaferNet Brasil
INHOPE Board Member

Brasília, 15 de junho de 2016

cgi.br

1 2 3 4 5 6 7 8 9 — GOVERNO e SOCIEDADE CIVIL — 10 11 12 13 14 15 16 17 18 19 20 21

Representantes do Governo:

1 Ministério da Ciência, Tecnologia e Inovação (coordenador)
2 Casa Civil da Presidência da República
3 Ministério das Comunicações
4 Ministério da Defesa
5 Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 Ministério do Planejamento, Orçamento e Gestão
7 Agência Nacional de Telecomunicações
8 Conselho Nacional de Desenvolvimento Científico e Tecnológico
9 Conselho Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia

Representantes da Sociedade Civil:

10 Notório saber em assunto da Internet
11 a 14 Representantes do setor empresarial
- provedores de acesso e conteúdo da Internet
- provedores de infra-estrutura de telecomunicações
- indústria de bens de informática, de bens de telecomunicações e de software
- setor empresarial usuário

15 a 18 Representantes do terceiro setor
19 a 21 Representantes da comunidade científica e tecnológica

CGI.br/RES/2009/003/P - PRINCÍPIOS PARA A GOVERNANÇA E USO DA INTERNET NO BRASIL

Considerando a necessidade de embasar e orientar suas ações e decisões, segundo princípios fundamentais, o CGI.br resolve aprovar os seguintes Princípios para a Internet no Brasil:

1. Liberdade, privacidade e direitos humanos
O uso da Internet deve guiar-se pelos princípios de liberdade de expressão, de privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática.

2. Governança democrática e colaborativa
A governança da Internet deve ser exercida de forma transparente, multilateral e democrática, com a participação dos vários setores da sociedade, preservando e estimulando o seu caráter de criação coletiva.

3. Universalidade
O acesso à Internet deve ser universal para que ela seja um meio para o desenvolvimento social e humano, contribuindo para a construção de uma sociedade inclusiva e não discriminatória em benefício de todos.

4. Diversidade
A diversidade cultural deve ser respeitada e preservada e sua expressão deve ser estimulada, sem a imposição de crenças, costumes ou valores.

5. Inovação
A governança da Internet deve promover a contínua evolução e ampla difusão de novas tecnologias e modelos de uso e acesso.

6. Neutralidade da rede
Filtragem ou privilégios de tráfego devem respeitar apenas critérios técnicos e éticos, não sendo admissíveis motivos políticos, comerciais, religiosos, culturais, ou qualquer outra forma de discriminação ou favorecimento.

7. Inimputabilidade da rede
O combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos.

8. Funcionalidade, segurança e estabilidade
A estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas.

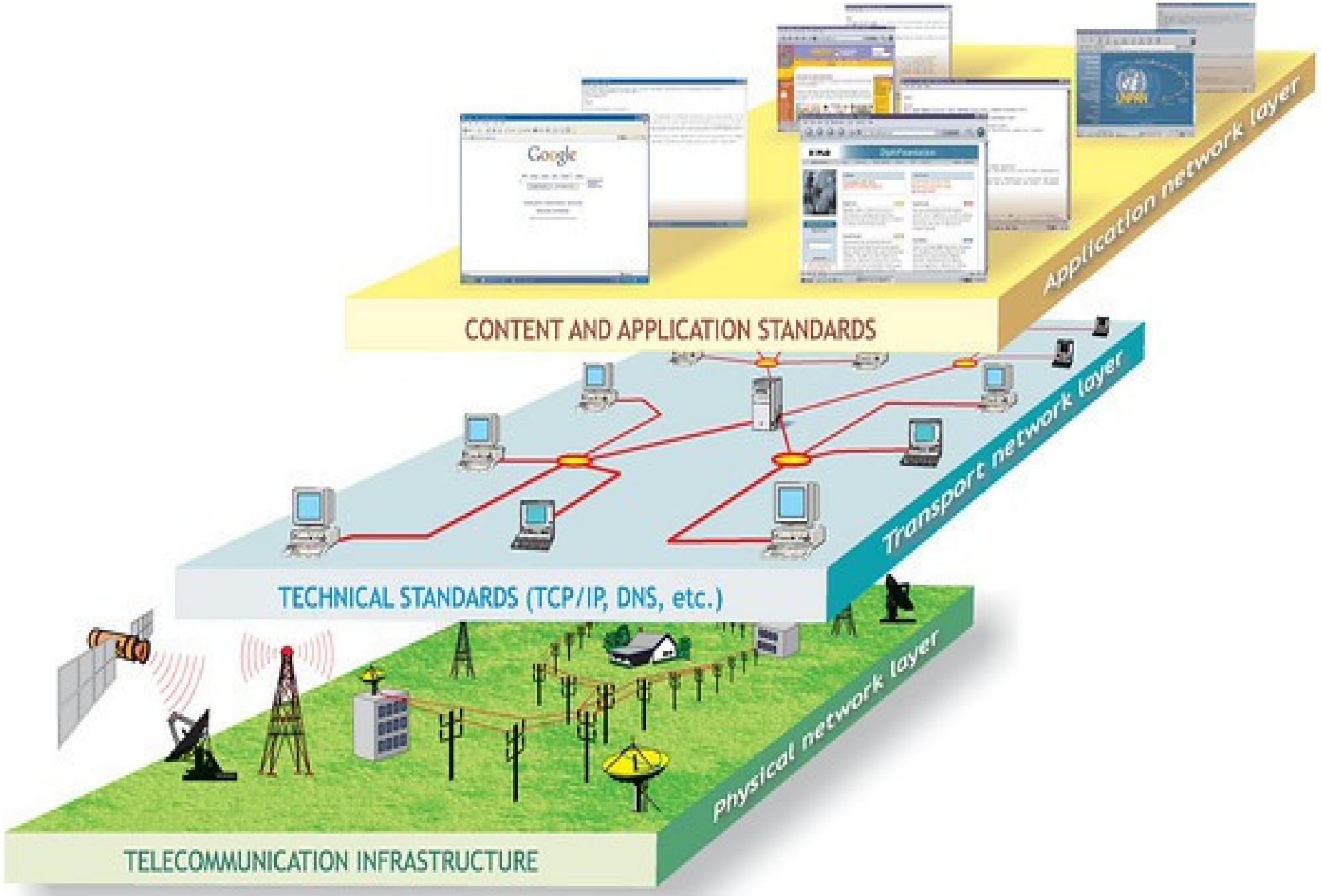
9. Padronização e interoperabilidade
A Internet deve basear-se em padrões abertos que permitam a interoperabilidade e a participação de todos em seu desenvolvimento.

10. Ambiente legal e regulatório
O ambiente legal e regulatório deve preservar a dinâmica da Internet como espaço de colaboração.

7

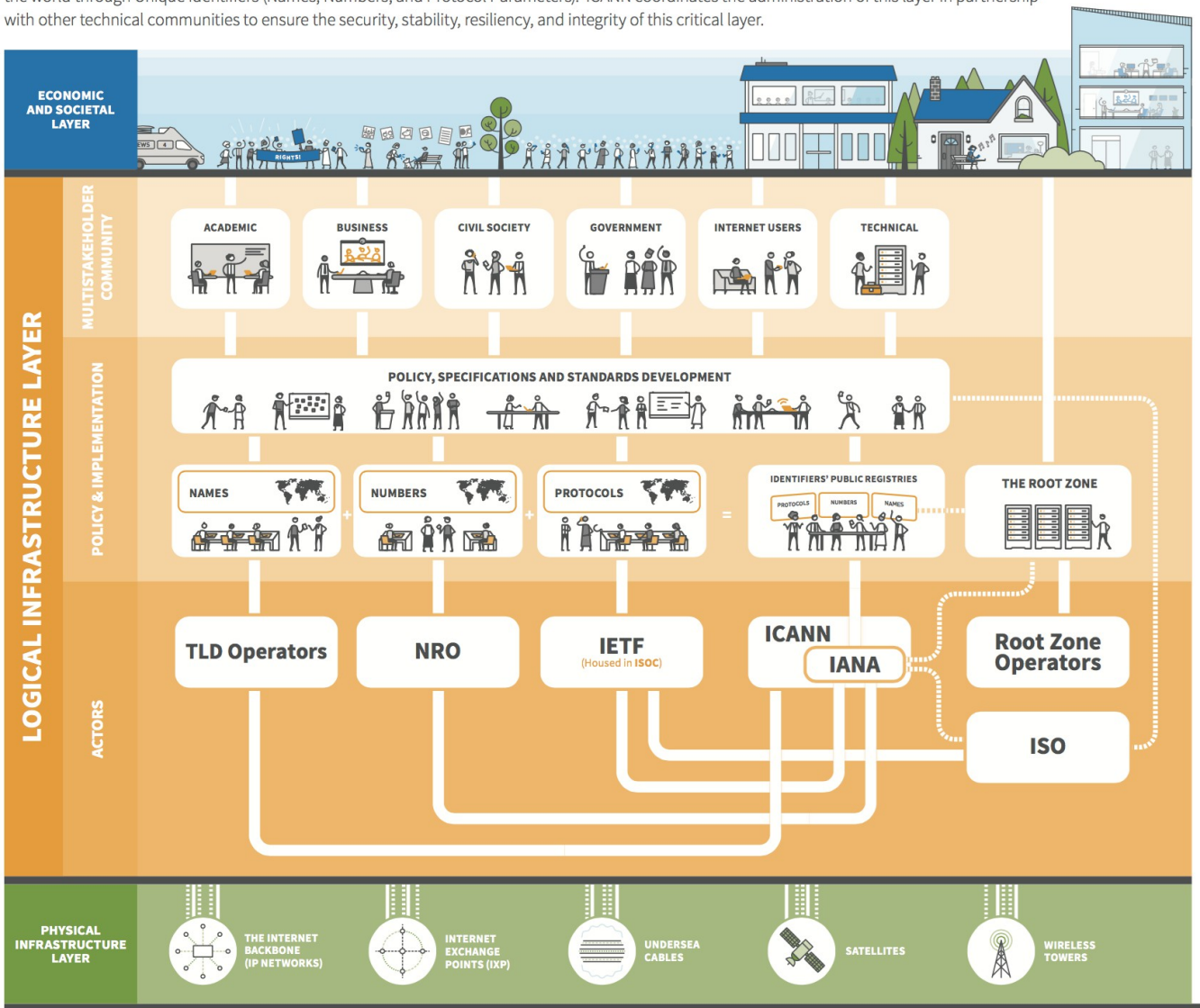
Inimputabilidade da rede

O combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos.


Google
CONTENT AND APPLICATION STANDARDS
Application network layer
TECHNICAL STANDARDS (TCP/IP, DNS, etc.)
Transport network layer
TELECOMMUNICATION INFRASTRUCTURE
Physical network layer

WHO GOVERNS THE INTERNET'S LOGICAL INFRASTRUCTURE?

Layered on top of the Physical Infrastructure's thousands of networks and satellites, the Internet's Logical Infrastructure is what delivers One Internet for the world through Unique Identifiers (Names, Numbers, and Protocol Parameters). ICANN coordinates the administration of this layer in partnership with other technical communities to ensure the security, stability, resiliency, and integrity of this critical layer.



DRAFT

TECHNICAL OPERATIONS

The technical Operating Community comprises multiple independent actors bound by common principles and mutual commitments that ensure its security and stability of the Logical Infrastructure of the Internet. Each actor's community develops policies and standards in an open, inclusive, and consensus-based approach.

ACTORS

ICANN *Internet Corporation for Assigned Names and Numbers*

Helps coordinate the Internet's systems of unique identifiers including domain names and IP addresses, as well as manages the IETF's protocol parameters.
IANA, the Internet Assigned Numbers Authority, is a function housed and operated within ICANN. It acts as the top-level allocator for blocks of IP addresses and AS numbers, proposes creation of and changes to DNS top-level domains, and manages lists of unique identifiers used in Internet protocols.
www.icann.org
www.iana.org

IETF *Internet Engineering Task Force*

Develops and promotes a wide range of Internet standards dealing in particular with standards of the Internet protocol suite. Their technical documents influence the way people design, use, and manage the Internet. The IETF operates under the Internet Society (ISOC) with architectural oversight provided by the Internet Architecture Board (IAB).
www.ietf.org

ISO *International Organization for Standardization*

Standardizes, among many other things, the official names and postal codes of countries, dependent territories, special areas of geographic significance.
www.iso.org

NRO *Number Resource Organization*

A coordinating body for the five Regional Internet Registries (RIRs). The RIRs manage the distribution of IP addresses and Autonomous System Numbers in their regions of the world.
www.nro.net

AFRINIC	*www.afrinic.net*
APNIC	*www.apnic.net*
ARIN	*www.arin.net*
LACNIC	*www.lacnic.net*
RIPE NCC	*www.ripe.net*

TLD Operators *Top Level Domain Operators*

Organizations responsible for the management of the Top Level Domains such as: Generic TLDs (.com, .biz, .edu), Country Code TLDs (.fr, .us, .cn) operators, and Internationalized Country Code for non-latin alphabet systems (Chinese, Arabic)—among others.
www.wikipedia.org/wiki/Top-level_domain

Root Zone Operators

12 independent organisations operate the 13 authoritative name servers (A through M) that serve the Domain Name System (DNS) root zone. The name servers are a network of hundreds of physical servers located in many countries around the world.
www.root-servers.org

MULTISTAKEHOLDER COMMUNITY

Academic
- Institutions of higher learning
- Academic thought leaders
- Professors & students

Business
- Private-sector companies from across industries
- Industry and trade associations

Civil Society
- International organizations
- Non-governmental organizations
- Non-profit organizations
- Think Tanks

Government
- National governments
- Distinct economies recognized in international fora
- Multinational governmental and treaty organizations
- Public authorities (with a direct interest in global Internet Governance)

Internet Users
- Private citizens interested in regional or global Internet Governance

Technical
- Internet engineers
- Computer engineers
- Software developers
- Network operators

DRAFT

THE THREE LAYERS OF DIGITAL GOVERNANCE

No one person, government, organization, or company governs the digital infrastructure, economy, or society. Digital governance is achieved through the collaborations of Multistakeholder experts acting through polycentric communities, institutions, and platforms across national, regional, and global spheres. Such Digital Governance is stratified into three layers to address infrastructure, economic, and societal issues with solutions. For a map of Digital Governance Issues and Solutions across all three layers, visit *https://map.netmundial.org*

MULTISTAKEHOLDER COLLABORATIONS

Solutions to issues in each layer include policies, best practices, standards, and specifications developed by the collaborations of expert stakeholders from actors in business, government, academia, technical, and civil society.

ECONOMIC AND SOCIETAL LAYER

LAWS, POLICIES, AND REGULATIONS

Governing bodies in local, national, regional, and international spheres are engaged with their citizens and with other bodies to develop and apply laws, policies, and/or regulations. The transnational nature of the Internet must be synchronized with the established International system of governance and laws.

INDUSTRY AND TRADE

Manufacturing, retail, supply chain/logistics, healthcare, finance, etc.

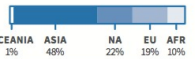
Such as Amazon, eBay, Alibaba, Rakutan, Sony, Toyota, Coca-Cola, Boeing, Alcatel-Lucent

NEWS AND INFORMATION

Newspapers, broadcast, personal & professional blogs, social media.

USERS

There are over 3 billion users worldwide. Most users connect to the Internet through their mobile phone.



www.internetlivestats.com/internet-users/#byregion

EDUCATION

Online universities, research, tutorials, classroom engagement.

APPLICATIONS

World wide web, email, cloud, VoIP, mobile apps.

ENTERTAINMENT

Music, movies, television, games.

Such as iTunes, Spotify, YouTube, Amazon, Netflix

CIVIC AND HUMAN RIGHTS

Privacy, identity, access to content, freedom of expression, cybercrime, consumer protection, cultural diversity, and many more.

SOCIAL MEDIA

Sharing photos, videos, ideas and information.

Such as Facebook, Twitter, Instagram, Tencent QQ, Whatsapp

SECURITY

Cybersecurity, cyber warfare, cyber espionage, cyber terrorism, and many more.

MOBILE

Smart phones, tablets, cars. There are now more mobile devices on the planet than people.

KEY ACTORS

- IGF
- Technical Organizations (ISOC, W3C,...)
- NETmundial
- World Econommic Forum
- National Governments
- Civil Society
- International Governmental Organizations (OECD, UNESCO,...)
- Law Enforcement Agencies

LOGICAL INFRASTRUCTURE LAYER

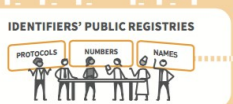
DOMAIN NAMES

~300 Country Code Top-Level Domains (ccTLDs) such as .fr, .br, .us, ...

~600+ Generic Top-Level Domains (gTLDs) such as .com, .biz, .realtor, ...

~1500+ Domain Name Registrars such as GoDaddy, Network Solutions, Register, ...

NAMES + NUMBERS + PROTOCOLS = IDENTIFIERS' PUBLIC REGISTRIES



THE ROOT ZONE

IP ADDRESSES

IPv4: 4.2 billion addresses. IPv6: 340 undecillion (trillion, trillion, trillion) addresses. 5 Regional Internet Registries (RIRs) who oversee the global number resources.

PROTOCOL PARAMETERS

Protocol parameters are the commands and identifiers that are used inside protocols, the structured communications used for the web, email, etc., to transfer the information.

Such as HTTP, TCP/IP, VoIP

ROOT SERVICES

13 Root Servers run by 12 organizations in 4 countries.
~500 Anycast copies worldwide.

KEY ACTORS

- ICANN / IANA
- IETF
- ISO
- NRO
- TLD Operators
- W3C

PHYSICAL INFRASTRUCTURE LAYER

THE INTERNET BACKBONE (IP NETWORKS)
90% is privately owned by global companies like:
Level 3 Communications, TeliaSonera International Carrier, CenturyLink, Vodafone, Verizon, Sprint, AT&T

INTERNET EXCHANGE POINTS (IXP)
~550 points worldwide.

UNDERSEA CABLES
~300 cables that transmit 99% of all international Internet data.

SATELLITES
~2000 communications satellites in use, many used now for Internet data.

WIRELESS TOWERS
~824,000 wireless towers worldwide.

KEY ACTORS

- GSMA
- IEEE
- IETF
- ITU
- National ICT Ministries
- Network Operator Groups

Spy Files 3

Today, Wednesday 4 September 2013 at 1600 UTC, WikiLeaks released 'Spy Files #3' – 249 documents from 92 global intelligence contractors. These documents reveal how, as the intelligence world has privatised, US, EU and developing world intelligence agencies have rushed into spending millions on next-generation mass surveillance technology to target communities, groups and whole populations. Read the full press release here

WikiLeaks Counter Intelligence Unit (WLCIU) Location Tracking Map

Spy Files released so far: 574

Spy Files 1: 2011-12-01
Spy Files 2: 2011-12-08
Spy Files 3: 2013-09-04

Media Publishing

Argentina - Pagina 12
Brazil - Publica
Bulgaria - Bivol
Ecuador - El Telégrafo
Egypt - Al-Masry Al-Youm
France - Rue89
Germany - NDR
Germany - Süddeutsche Zeitung
India - The Hindu
Italy - L'Espresso
Italy - La Repubblica
Mexico - La Jornada
New Zealand - Fairfax NZ News
Norway - Dagens Næringsliv
Russia - RT
Spain - Publico
US - CorpWatch
US - McClatchy

Spy Files 3 Documents:

Surveillance Industry Documents WikiLeaks Counter Intelligence Unit (WLCIU) Location Tracking

Surveillance Industry Documents

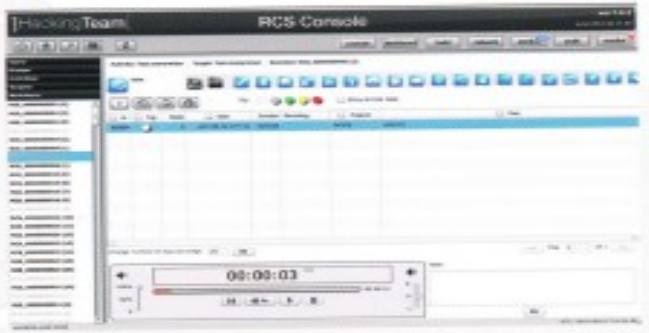
Enter a search term | Select country

Document Title	Company	Year	Document Type	Tags	Target System	Country Codes
10 GigaBit Fiber Taps	NETOPTICS	-	Brochure	NETOPTICS	-	US
10/100 Port Aggregator Tap	NETOPTICS	-	Brochure	NETOPTICS	-	US
10/100/1000 Tap Network Link	NETOPTICS	-	Brochure	NETOPTICS	-	US, FR
10/100BaseT Tap	NETOPTICS	-	Brochure	NETOPTICS	-	US
1U Modular Rackmount Surveillance Simplified	Packet Forensics	2011	Brochure	PACKET FORENSICS, Internet Monitoring, Lawful Interception, Data Retention, VOIP COMINT, HARDWARE	-	US
2 Mercure	OCKHAM	2011	Brochure	OCKHAM, Mass Monitoring, Analysis Software, Traffic Data Processing, SOFTWARE	-	FR
4x1 GigaBit Copper In-Line Regeneration Tap	NETOPTICS	-	Brochure	NETOPTICS	-	US
5-Series Small Devices, Big Opportunities	Packet Forensics	2011	Brochure	PACKET FORENSICS, SIGINT, Tactical Internet Monitoring	-	US

Fonte: http://wikileaks.org/spyfiles3.html

Monitor a hundred thousand targets.

Remote Control System can monitor from a few and up to hundreds of thousands of targets. The whole system can be managed by a single **easy to use** interface that simplifies day by day investigation activities.



Runs everywhere.

Remote Control System can be deployed on any platform.

symbian BlackBerry

Fonte: http://wikileaks.org/spyfiles/files/0/147_HACKINGTEAM-RCS.pdf

Remote Control System

- ***Remote Control System is an IT stealth investigative tool for LEAs.*** *(It is offensive security technology. It is spyware. It is a trojan horse. It is a bug. It is a monitoring tool. It is an attack tool. It is a tool for taking control of the endpoints, that is, the PCs)*
- It permits passive monitoring and ***active*** control of all data and processes on selected target computers.
- Such computers might or might not be connected to the Internet.

Fonte: http://wikileaks.org/spyfiles/files/0/31_200810-ISS-PRG-HACKINGTEAM.pdf

Monitoring and Logging

Remote Control System can monitor and log any action performed by means of a **personal computer**

- Web browsing
- Opened/Closed/Deleted files
- Keystrokes (any UNICODE language)
- Printed documents
- Chat, email, instant messaging
- Remote Audio Spy
- Camera snapshots
- ***Skype*** (VoIP) conversations
- …

Fonte: http://wikileaks.org/spyfiles/files/0/31_200810-ISS-PRG-HACKINGTEAM.pdf

Monitoring and Logging

Remote Control System can monitor and log any action performed by means of a **smartphone**

- Call history
- Address book
- Calendar
- Email messages
- Chat/IM messages
- SMS/MMS interception
- Localization (cell signal info, GPS info)
- Remote Audio Spy
- Camera snapshots
- Voice calls interception
- …

Fonte: http://wikileaks.org/spyfiles/files/0/31_200810-ISS-PRG-HACKINGTEAM.pdf

Smartphones architectures

- Windows Mobile 5
- Windows Mobile 6

- Q109: iPhone
- Q409: RIM/BlackBerry
- Q409: Symbian

Fonte: http://wikileaks.org/spyfiles/files/0/31_200810-ISS-PRG-HACKINGTEAM.pdf

Invisibility

- Allows monitoring (all) PC user's activities
- After the installation, Remote Control System cannot be detected by any bugged computer user
  - Existing files are not modified
  - No new files appear on the computer's hard disk
  - No new processes are executed
  - No new network connections are established
  - **Antivirus, antispyware, anti-key-loggers cannot detect our bug**
    - **E.g., Gartner Endpoint Security Magic Quadrant**

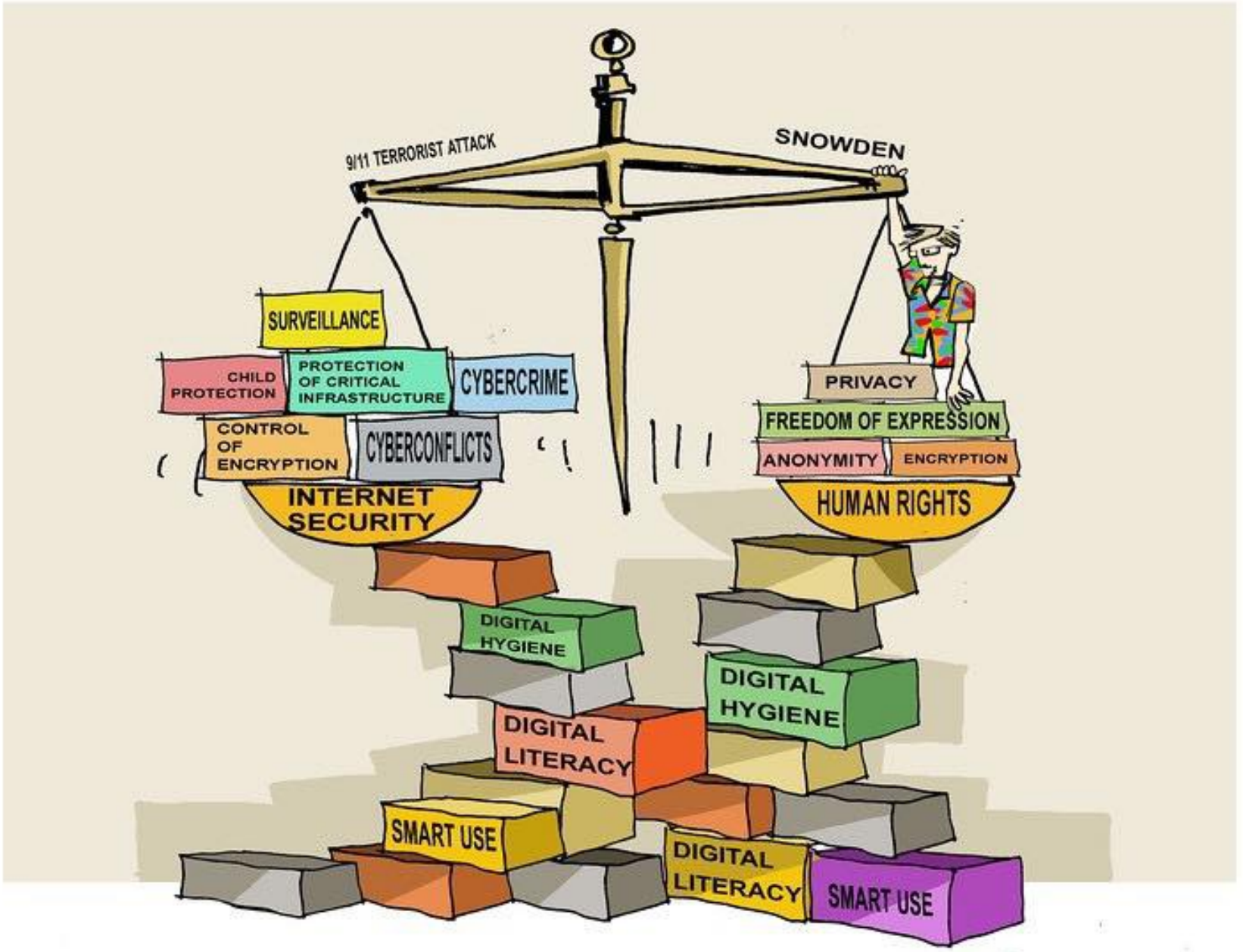
Fonte: http://wikileaks.org/spyfiles/files/0/31_200810-ISS-PRG-HACKINGTEAM.pdf

Attack/Infection vectors

- Remote Control System is software, not a physical device
  - Which can be installed ***remotely***
    - Computer can be bugged by means of several infection vectors
    - Intelligence information about remote target mandatory
  - … but ***local*** installation remains a option
    - Usually very effective

Fonte: http://wikileaks.org/spyfiles/files/0/31_200810-ISS-PRG-HACKINGTEAM.pdf

Conclusão



Concept: Vladimir Radunović Illustration: Vladimir Veljašević

DiPLO www.diplomacy.edu

Obrigado

thiagotavares@cgi.br

nic.br cgi.br

www.nic.br | www.cgi.br