lacigf Reunión Preparatoria para el Foro de Gobernanza de Internet

31 de julio al 2 de agosto - Buenos Aires, Argentina

Wednesday, 1 August 2018, 2:30 pm - 4:00 pm

Session 7

Challenges in Managing Internet Identifiers

Part One

Four topics were presented by an expert, each of whom had 7 minutes to introduce the topic and address the challenges and problems it poses. These topics were: Site/network blocking, by Raquel Gatto (ISOC); Disaster preparedness, by Lito Ibarra (SVNET); Privacy under the GDPR approach and its impact on the DNS, by Rodrigo de la Parra (ICANN); and Routing security, by Guillermo Cicileo (LACNIC).

Site/network blocking: Raquel Gatto, ISOC

- Internet blocking is a total or partial interruption of electronic communications which can affect countries, groups of people, or services.
- The Internet Society presented a study of the main techniques used for blocking the Internet: IP-based blocking, blocking based on deep packet inspection (DPI), URL-based blocking, platform-based blocking, and DNS-based blocking.
- Blocking is not always efficient, as it does not always achieve the goal of interrupting the services and generates harmful side-effects for the ecosystem, affecting both human rights and economic and technical aspects.
- An emblematic case was the unsuccessful attempt to block WhatsApp, which had repercussions around the region.

Disaster preparedness: Lito Ibarra (SVNET)

- During LACIGF, different aspects relating to Internet users were discussed, including efforts to connect a greater number of people to the Internet.
- However, network infrastructure remains in place even in case of a disaster. Thus, the promotion of Internet-based applications and services creates greater dependency among users, who now rely on Internet access.
- One of the issues related to natural disasters is the protection of critical infrastructure that allows us to remain connected. Unfortunately, not every natural disaster can be anticipated.
- Systems at risk include domain name servers, Internet exchange points, datacenters, local and international connectivity providers, as well as various infrastructure components (cables, fibers, links, routers, switches, etc.).

- Even though different mitigation measures exist, some of these measures are not adopted until a natural disaster occurs.

Privacy under the GDPR approach and its impact on the DNS: Rodrigo de la Parra (ICANN)

- The privacy and data protection measures adopted in the European Union have long been part of the discussions of the ICANN community. In this case, the topic is discussed in the context of its implications for Internet governance.
- The GDPR was passed by the European Union and came into force on 25 May 2018. It applies to companies that process personal data belonging to subjects residing in the European Union. Large fines apply in case of non-compliance.
- The GDPR affects the Domain Name System in at least two areas:
    - Contracted parties, as they collect, display and process personal data. These actors include registries and registrars.
    - Internally, as ICANN collects and processes some personal data and processes such data for internal services.
- One of the solutions proposed by the ICANN community was the Temporary Specification, which provides a unified interim model to comply with the provisions contained in the GDPR and, at the same time, guarantee the operation of registry services, such as the WHOIS service.
    - In addition, the ICANN multistakeholder community will work to define a policy to address the changes generated by the implementation of the GDPR.

Routing security: Guillermo Cicileo (LACNIC)

- BGP-based routing is one of the pillars of the Internet. However, because it was designed long ago, many security considerations were not taken into account.
- There have been several proposals to address routing security issues, for example, RPKI. However, the adoption of such measures is not yet widespread, so one of the goals is to promote their adoption among relevant actors.
- It is also possible to join the MANRS program to increase security measures among Internet access providers.

Part Two:

The problems and challenges of each topic were displayed on the screens available in the room. The audience was then divided into four groups (each of which was assigned a moderator and a rapporteur) for 30 minutes of constructive and open debate on the problems and challenges considered for each topic. The rapporteurs assigned to each topic were as follows: Site/network blocking, Alexandra Dans (ICANN); Disaster preparedness, Shernon Osepa (ISOC); Privacy under the GDPR approach and its impact on the DNS, Gabriela Ramirez (.AR); and Routing security, Carolina Caeiro (LACNIC).

The following questions were used to trigger the discussions:

Site/network blocking:

- Which Internet users and services are affected by Internet blocking techniques?
- How do these techniques affect human rights, the economy, and network stability?
- What are the roles of the various actors (governments, users, technical community, private sector) in Internet blocking?
- What are their processes and characteristics?

Disaster preparedness:

- What mitigating measures are possible?
- Who should take an interest in damage prevention?
- What is the role of each stakeholder (civil society, government, private enterprise, academia, technical community)?
- What components of the connectivity system should be protected?
- Where should resources be obtained to develop preventive or mitigation measures?
- Should this work be conducted at a national or an international level?
- Should this topic be included under Internet Governance?

The GDPR approach and its impact on the DNS:

- In your opinion, what can we do to find a balance between privacy/personal data protection and security/operational stability?
- What are the lessons learned about the impact of regulations on global aspects of the Internet?
- The multistakeholder model and the challenge of providing an effective reaction to external events.

Routing security:

- What problems can affect end users if the routing system fails?
- Are there any measures to mitigate such problems?
- What can we do so ISPs will adopt such measures?
    - Validation: hard work with NOGs, IXPs, etc.
    - RPKI adoption:
        - operator training;
        - greater dissemination throughout the Internet ecosystem;
        - adherence to MANRS (ISP reputation).
    - Adoption and monitoring of standards on the part of operators.

Part Three:

The four groups gathered once again, and each rapporteur shared the results of the discussions.

Site/network blocking: Alexandra Dans, ICANN

- A variety of reasons were mentioned as the cause of Internet blocking, including the following examples:
    - In Uruguay, there was an attempt to implement a block on gambling websites. While gambling is legal in the country, it is a regulated activity.
    - Several cases were reported in Venezuela, as well as some solutions to avoid

such blocks, including the use of alternative DNS.

- Blocking was also discussed from an ethical perspective, highlighting legitimate motives, such as the fight against child pornography.
- Several questions were brought up concerning what should be considered a legitimate reason for ordering an Internet block, particularly regarding the legitimacy of the authorities who are competent to order such measures. If such legitimacy does not exist, blocking would be legal but not ethical.

Disaster preparedness: Shernon Osepa, ISOC

- One of the experiences shared in the group was what happened in Mexico after the earthquake that took place in September 2017, when many people tried to use Internet-based services and exceeded the capacity of the country's infrastructure. Some participants suggested disseminating advice on how to use the Internet following a disaster.
- In the case of Guatemala, a country that is susceptible to natural disasters caused by volcanoes, prevention and monitoring is particularly relevant.
- In Haiti, local coordination between the operators and the government became particularly relevant when a disaster occurred.
- As for damage prevention, holistic solutions were proposed to incorporate the concerns and best practices of every stakeholder.
- Participants also agreed that disaster prevention and recovery are important issues for the Internet governance community.

Privacy under the GDPR approach and its impact on the DNS: Gabriela Ramirez, .AR

- Regarding the balance between privacy and security, participants pointed out that these characteristics are not antagonistic and that, to avoid abuses, only relevant information should be collected.
- Mention was also made of the differences between ccTLDs and gTLDs, which have a different relationship with ICANN and, consequently, different obligations.
- Local data protection legislations were identified as an important element in the discussion.
- The GDPR was pointed out as an opportunity for the community to review its personal data collection, treatment and protection mechanisms to safeguard the interests of end users.

Routing security: Carolina Caeiro, LACNIC

- Participants presented different examples of routing attacks that occurred in their communities.
- In addition, it was observed that some routing attacks are not perceived by end users.
- Some preventive measures and ways to strengthen routing security such as RPKI and BGPsec were discussed, including concrete aspects such as the need to incorporate passwords to BGP connections for each router.
- The MANRS initiative by the Internet Society was also mentioned as a preventive measure for strengthening routing security.
- There is also a need for cooperation among operators, both nationally and internationally.

- Training was identified as a key element, not only for operators, but also for the different actors that are part of the Internet community.

Rapporteur: Israel Rosas, Outreach Manager LAC, Internet Society