Stichting Digitale
Infrastructuur Nederland

Report on Open Forum "Protecting the public core of the Internet"

Towards a framework for sustainable Interaction of Governments with the Internet ecosystem

Date/time: November 10 2015, 11:00 AM, room 3
Organiser: DINL - the Digital Infrastructure Association Netherlands
Chair: Mr. Michiel Steltman, Director of DINL
Speakers/Panelists:

- Mr. Bastiaan Goslings , Governance and Policy Officer at AMS-IX, Netherlands
- Mr. Pranesh Prakash , Policy Director, CIS, India
- Mrs. Marília Maciel , Researcher and Internet policy analyst - Coordinator of the Center for Technology and Society - FGV, Brasil
- Mr. Dennis Broeders, Professor of Technology and Society at Erasmus University Rotterdam; and Senior Research Fellow and Project coordinator at the Scientific Council for Government Policy ; Netherlands

Summary

DINL sees a unique opportunity to further define and design generic principles for protection of the Public core of the Internet, and for developing generic concepts for operational Interaction between Governments and Intermediaries for the purpose of law enforcement.
Such an approach does not address specific forms of crime ; nor does it touch or affect local legislation in any form. Such an approach could offer the world a substantial degree of protection of an important international public good : the Public core of the Internet, whilst offering (any) government the ability to optimally enforce and execute its laws with respect to activities on – or enabled by the Internet.

About DINL

The Digital Infrastructure Netherlands (DINL) foundation was set up almost a year ago to promote the strong and continuous development of the Netherlands as one of *the* major hubs hub within the global digital infrastructure. DINL represents the parties in the Netherlands that provide the underlying technical facilities and services necessary for a digital society and economy to thrive: founding fathers are the DDA (datacenter association), the DHPA and ISPconnect (representing the hosting sector), NLNet, SURFnet (the academic network), AMS-IX (one of the world's largest Internet Exchange points) and SIDN (the ccTld registry for .nl), and NL ICT - The national IT sector organisation.

DINL has four focus areas:

1. Information sharing and advocacy
2. Investing in excellent IT-education
3. Building trust and transparency
4. Drive cooperation both within the sector as well as with other stakeholders

Stichting Digitale Infrastructuur Nederland
Overgoo 13 / Postbus 262
2260 AG Leidschendam

T: +31707621070
E: info@dinl.nl

DINL aims to create structure in complex themes and educates stakeholders about developments that affect the Dutch digital ecosystem. As such DINL works closely with government, politics, industry, NGO's and press. DINL emphasizes the importance and benefits of an open, reliable and safe digital infrastructure sector for the economy and society as a whole. DINL promotes continuous cooperation between all involved stakeholders as an essential mechanism.

Recently the Dutch Digital Infrastructure sector has been named by the Dutch Parliament as Holland's third mainport. Following Amsterdam Schiphol airport and the Rotterdam Harbor it is considered as a prerequisite for economic growth and the future of Netherland's digital economy.

Forum Description

A free, open and secure internet is seen by the internet infrastructure organizations united in DINL as an essential condition for long term economic growth and socioeconomic development. Obviously, these conditions are determined by the actions of many public and private organizations active in the global internet ecosystem. Today, we see an increase in government engagement with "the internet" to protect their citizens against crime and abuse and to protect economic interests and critical infrastructures. Also, states assert themselves on the internet for reasons of national security through the presence of the military and intelligence and security agencies.

The fact that the benign neglect of states towards the internet is increasingly replaced with political interest has positive and negative effects. States have an important role in fighting cybercrime, safeguarding civil liberties and fundamental human rights and creating a level playing field for the internet economy to thrive. However, heavy handed interventions by governments may also lead to privacy violations, pressures on economic development and innovation and even securitization or militarization of the internet.

In this open forum we are particularly concerned with those state interventions that impact on the technical and logical 'core' of the internet ecosystem – such as interventions in the DNS - and in the impact on organizations and businesses that are traditionally thought of as 'technical' and whose roles are in danger of being politicized, such as ISPs, CERTs and hard- and software developers. There is a growing need to separate out the legitimate interests of states from political overreach into the technical and logical core of the internet.

The interests of business, governments and end users all have to be taken into account in matters of internet governance and there is a substantial risk that a too proactive and one-sided approach of governments, even from those who have traditionally been preaching the benefits of an open and free internet, disturbs this delicate balance. Traditionally the technical Internet community rejects and resents the involvement and interaction of governments with the Internet, but it can be argued that this is also a counterproductive approach. A cooperative or constructive approach towards interaction, founded in firm principles, may strengthen the balance and lead to a sustainable protection of Internet values.

In this open forum we will present ideas about an agenda for the international protection of 'the public core of the internet' and seek to collect and discuss ideas for the formulation of norms and principles and for the identification of practical steps towards that goal. In doing so DINL aims to build on the insights that the Netherlands Scientific Council for Government Policy laid down in its 2015 report 'The public core of the internet. An international agenda for internet Governance'. More specifically we aim to discuss:

- A definition of a so called neutral zone: this comprises the core protocols and infrastructure of the internet which all governments should consider as a global public good, governed by the Internet community and protected from unwarranted interventions by governments
- Definitions of proper interfaces: outlining norms and mutual expectations that should govern the relations between governments and various central actors in the technical and economic internet ecosystem, such as ISPs, CERTs and hard- and software developers when it comes to fighting cybercrime, retrieve information , mandate takedowns, request information and more.

In this IGF open forum DINL wants to explore these ideas and discuss them with thought leaders from other countries. The goal is to develop this into a model and an inventory of viable norms, standards and initiatives that can be shared with stakeholders in governments and politics in the participating countries. We believe that IGF provides the ideal environment to develop and challenge these ideas – since knowledge and expertise is present and the goals and ambitions of a free, open and secure internet are widely shared.

Forum report

The forum started with a presentation of the DINL association by the chair, followed by a presentation of the key principles and conclusions of the 2015 Report of Netherlands Scientific Council for Government Policy 'The public core of the internet. An international agenda for internet Governance' by Professor Dennis Broeders. Next, AMS-IX's Bastiaan Goslings gave additional insight in de exact scope of the concept of the Public Core, by mentioning the key roles and protocols which constitute the elements to be protected.
The third presentation was by Mr. Pranesh Prakesh, who outlined the Manilla Principles, a set of guidelines and principles for the interaction between public authorities and internet intermediaries. Pranesh made the link between the concept of Intermediaries and companies and other key stakeholders operating in the public core of the internet, and explained how Intermediaries should be treated by Governments with respect to dealing with unlawful activities on the Internet.
Mrs Marília Maciel illustrated the Public Core protection concept by explaining why the DNS system should get an internationally recognized diplomatic status.

Conclusions

The key conclusion of this session are the following:

- The concept of "the Public core of the Internet" : a collection of key roles and key protocols, should be considered as an International, public good. It should therefore be protected from unwarranted interventions by governments.

- Key Protocols such as DNS, BGP ; and Key functions that affect the stability and safety of the whole Internet, such as Internet exchanges , root zones etcetera – and perhaps also Encryption, should be protected from unwarranted government interventions.
- Interactions between such entities and national or international law enforcement, for information requests or takedown purposes, should follow clear policies, guidelines and procedures – as to be agreed upon in an International setting.
- Companies and other entities operating in the Core of the Internet who can be considered as Intermediaries , must be protected from liability for activities that are not under their control; as described in the Manilla principles
- Key Internet protocols, and entities responsible / or appointed to operating the technical mechanisms that may affect the stability and safety of these protocols on a global scale, should be protected, perhaps by granting them diplomatic status

Next steps

First, there is a need to refine definitions core protocols and of Intermediaries and their roles that are within the Public Core. This can be achieved by creating an internationally recognized Taxonomy. Such an initiative for the interaction between public authorities and intermediaries is underway within the scope of the Manilla Principles project. DINL will connect to this initiative.

Second, the exact nature and scope of protection of such Intermediaries and protocols must be defined in more detail. Such an initiative may follow the line of thought of assigning diplomatic status to DNS, as presented by Center for Technology and Society - FGV, Brasil. Perhaps other legal protection mechanisms can be inventoried, researched, designed. DINL will initiate contacts with these institutions to start this process up.

Third, there is a need to define generic principles, policies and perhaps even procedures, for interaction by Governments with such Intermediaries. Such a generic solution would ultimately facilitate law enforcement interactions for the purpose of lawful takedowns or lawful information requests – as described by the Manilla principles.
This can be achieved by combining the Manilla principles with successful practical solutions for Takedown and other actions, such as the NTD (Notice and Takedown) policy designed in the Netherlands, and the initiatives of “Internet & Jurisdiction” on transnational due process and transparency. DINL will, again, reach out to seek cooperation on this ambition

DINL proposes to report on the proceedings of these three next steps and the concrete results on the 2016 IGF; where these can be presented by aforementioned stakeholders.

Feedback on attendance and invitation process to the IGF organization

The forum started a bit late due to the fact that the panel and attendees were unfamiliar with the audio setup ; room 3 was an open room which required headsets for all participants to exclude external noise. This setup appeared to be somewhat confusing and little help was available from the organization.

The number of visitors, approximately 15, was a little disappointing. The reason appeared to be the fact that none of the participants was familiar with the organization DINL and that very little

information on the forum was available in advance, due to the possibilities offered by the IGF for describing open forums. The fact that an open forum is identified in the programme with the name of the organisation – as opposed to title and topic, as is the case in workshops – does not help to attract participants

> Open Forums appear to attract visitors predominantly based on past reputation of the organizer and chair. DINL is however a new organization, founded early 2015, and has therefore not participated in IGF events before. Unfortunately the IGF site does not cater for an extended explanation and presentation of the organisation or chair, so this limited possibility to present our organization resulted in a limited attendance.

The session organizers strongly advice IGF to provide more room for descriptions on the event site for Open Forums, and more possibilities to provide information about the participating organizations. This may help to attract more attendees to open forums organized by relatively new or otherwise unknown organizations.

DINL
Michiel Steltman
November 2015