

# DNS STABILITY, SECURITY AND RESILIENCY



---

REPORT OF THE 3<sup>RD</sup> GLOBAL SYMPOSIUM  
ROME, OCTOBER 19-20, 2011

---





**The 3rd Global DNS Stability, Security and Resiliency Symposium  
19-20 October 2011, Rome, Italy**

**Final Report**

Editors:

Emiliano Casalicchio, *University of Rome Tor Vergata*  
Igor Nai Fovino, *Global Cyber Security Center*

Contributors:

R.Arends, J.Crain, P.Koch, P.V.Mockapetris, R.Rasmussen, R.Story, P.Vixie

Sponsors:

Global Cyber Security Center (CSEC)  
Internet Corporation for Assigned Names and Numbers (ICANN)  
Domain Name System Operations Analysis and Research Center (DNS-OARC)



We would like to thank the Global Cyber Security Center for making the symposium possible and for being such gracious hosts. We also wish to thank ICANN and DNS-OARC for their sponsorship and the committees that helped guide the Symposium.

The most thanks of course go to all those who participated and donated their valuable time and thoughts.

We hope this document provides useful input and food for thought for you as the reader.

Sincerely,

Andrea Rigoni & John Crain  
Chairs

## Executive Summary

The Third Symposium on Global DNS Stability, Security and Resiliency was held on October 19-20 2011, at GCSEC headquarters, in the beautiful city of Rome. The purpose for convening a third Symposium were to:

1. Consolidate and further explore topics considered in prior symposiums<sup>1,2</sup>
2. Discuss new issues and challenges related to DNS Security, Stability and Resiliency

The main five symposium objectives were:

- i) Address issues having the potential to globally impact name resolution
- ii) Discuss actions or activities that could speed up the deployment of Domain Name Security Extensions (DNSSEC)
- iii) Speculate on how the DNS and other name spaces used in the Internet might evolve in the coming future
- iv) Determine what metrics are needed to measure the integrity and health of the DNS so that we can formulate a plan to implement these metrics.
- v) Discuss domain name related issues associated with botnet command and control

Each objective was presented and debated in breakout sessions. Objectives (i), (ii) and (iv) stimulated the most interesting discussions and results; specifically,

Objective (i) concentrated on DNS Filtering. The concepts discussed and action items identified at the conclusion of this breakout session are summarized in the following item list.

- Effectiveness of filtering depends on where in the topology filtering is operated.
- Filtering & sophisticated reputation systems may be able to be combined to improve effectiveness.
- Authority and scope of filtering depends on who initiates the process. Filtering is considered to be within remit and scope when applied by the user in its administrative domain or by a government (agency) to combat abuses or fight crimes that are perpetrated within its jurisdiction, but out of scope if applied by ISP for commercial purpose or by government for political reasons.
- Government imposed filtering is an additional cost borne by ISPs (and often an unfunded mandate). The balance between money invested for filtering and effectiveness is subjective (as is the perceived return on investment or justification for the effort).
- Unintended consequences if filters were maliciously replaced (e.g. an ISP child-porn filter replaced with the Alexa 1000 list) are not considered with the full gravity it merits.

Consideration of objective (ii) led to a discussion on enabler and inhibitors for the security of the DNS. The subject of this discussion was DNSSEC adoption, market maturity and value proposition. The concepts discussed and action items identified at the conclusion of this breakout session are summarized in the following item list:

- Adoption of DNSSEC
  - Outsource DNS vs DNSSEC services to overcome technical issues and create incentives.
  - Implement validation as close to the edge as possible – preferably in the application.
  - Design DNSSEC aware operating systems and applications.
  - Simplify DNSSEC management.
- Technology and Market maturity

---

<sup>1</sup> 2009 Global DNS Security, Stability, and Resiliency Symposium <http://www.gtisc.gatech.edu/icann09>

<sup>2</sup> 2010 Global DNS Security, Stability, and Resiliency Symposium <https://www.icann.org/en/topics/ssr/dns-ssr-symposium-report-1-3feb10-en.pdf>

- Refine the validation process and technologies to improve client satisfaction
- Focus on education and outsourcing to sell DNSEC as easy-to-use
- Value proposition
  - DNSSEC doesn't solve all DNS problems so do not make it the *silver bullet*. The integration of cryptography solutions is not the only answer to the wider family of threats to name service.
  - Cost and revenue models are strongly needed, but *"be brave, don't wait too much, the real cost is: if deployment is not quick DNSSEC will remain a curiosity"*
  - Critical end users and operators are the most likely beneficiaries of DNSSEC services. Must find the right selling message/channel.

Objective (iv) was covered in a session on data, measures and metrics. The concepts discussed and the action items identified in this breakout session are summarized below:

- Coordinate efforts to determine what is normal in DNS behaviour. Normality is not always healthy.
- Consider normal behaviour from multiple vantage points (end-user, ISP, name server, ...) and perspectives (academic/business/corporate, security).
- Develop an information sharing model: *when to share; how to share; how to respect legal and privacy constraints; how to incentivize sharing of information.*
- Develop sharing methodologies and standards. The community must move from the simple sharing of errors or warning toward a framework allowing to measure, evaluate and monitor the health of the DNS.
- Consider or adopt a "Program globally, measure locally" strategy to solve legal issues.
- Share synthesized indexes and metrics to provide a high protection against privacy and confidentiality breaches

More than sixty (60) representatives of the global DNS community attended the Symposium to contribute to the improvement of the Security, Stability and Resilience of the DNS. This report contains the results of this fruitful meeting.

# Index

- EXECUTIVE SUMMARY..... 6
- 1. INTRODUCTION ..... 10
  - 1.1. SYMPOSIUM ORGANIZATION AND METHOD ..... 10
  - 2. BREAKOUT SESSION OVERVIEW..... 11
  - 3. BREAKOUT SESSION SPECIFIC RESULTS ..... 13
    - 3.1. SESSION A - DNS FILTERING ..... 13
      - 3.1.1. FILTERING AND DNSSEC..... 13
      - 3.1.2. ETHICS OF DNS FILTERING ..... 14
      - 3.1.3. EFFECTIVENESS AND COSTS OF DNS FILTERING ..... 14
      - 3.1.4. IMPACT OF DNS FILTERING..... 15
    - 3.2. SESSION B - ENABLERS AND INHIBITORS FOR THE SECURITY OF THE DNS ..... 16
      - 3.2.1. DISTRIBUTION CHALLENGES..... 17
      - 3.2.2. TECHNOLOGY AND MARKET MATURITY ..... 18
      - 3.2.3. POTENTIAL DEFINITIONS OF SUCCESS..... 19
      - 3.2.4. VALUE PROPOSITION..... 20
      - 3.2.5. PROCESS AND SIDE ISSUES..... 21
      - 3.2.6. ACTION ITEMS AND RECOMMENDATIONS ..... 22
    - 3.3. SESSION C- EVOLUTION OF THE DNS AND INTERNET NAME SPACES ..... 23
      - 3.3.1. NAME SPACE ISSUES ..... 23
      - 3.3.2. PROTOCOL ISSUES ..... 24
    - 3.4. SESSION D - DATA, MEASURES AND METRICS..... 25
      - 3.4.1. NORMALIZATION ISSUES ..... 25
      - 3.4.2. SHARING AND BASELINE DEFINITION ISSUES..... 26
      - 3.4.3. LEGAL ISSUES ..... 27
    - 3.5. SESSION E - BOTNET COMMAND AND CONTROL ..... 28
  - 4. SUMMARY ..... 29
  - ANNEX1: SYMPOSIUM AGENDA ..... 31
  - ANNEX 2: SYMPOSIUM PARTICIPANTS..... 33

## **Index of tables**

TABLE 1 COMMON THEMES SHARED AMONG THE BREAKOUT SESSION	9
TABLE 2 DRIVER ISSUES FOR SESSION B	15
TABLE 3 DRIVER CONCEPTS FOR SESSION B	16
TABLE 4 TARGET MARKETS FOR DNSSEC	17
TABLE 5 TOPICS OF INTEREST DISCUSSED IN SESSION C	21
TABLE 6 DRIVER ISSUES FOR SESSION D	24

## **Index of figures**

FIGURE 1 FOCUS OF THE SYMPOSIUM IS ON ANALYSE THE MEANING OF DATA AND ACT ACCORDING THE STATE OF THE SYSTEM	23
--	----

## 1. Introduction

DNS has a direct and strong impact on the performance and dependability of nearly all aspects of interactions on the Internet, including web applications, service-oriented architecture based systems, cloud infrastructures and distributed applications in general.

In 2009, experts from the DNS community began meeting annually, to initially discuss the security, stability and resilience of the DNS. In 2010, DNS-SSR Symposium began to consider assessing the health of the DNS, a set of indicators to measure the vital signs of the DNS, and how to assess whether the DNS is fulfilling the needs of the global Internet community.

The third Symposium on Global DNS Stability, Security and Resiliency sought to:

1. Consolidate and further explore topics considered in prior symposiums
2. Discuss new SSR issues and challenges

The Steering Committee identified four main objectives for the 2011 symposium:

- i) Address issues having the potential to globally impact name resolution
- ii) Discuss actions or activities that could speed up the deployment of DNSSEC
- iii) Speculate on how the DNS and other name spaces used in the Internet might evolve in the coming future
- iv) Determine what metrics are needed to measure the integrity and health of the DNS so that we can formulate a plan to implement these metrics.

During the symposium, attendees added a fifth topic of interest:

- v) Discuss domain name related issues associated with botnet command and control

The intent of Objective i) was to stimulate the discussion on new issues that will impact the SSR of the DNS. The natural candidate was “DNS Filtering”.

Objectives ii) iv) and v) pursue work begun in the previous DNS-SSR Symposiums; specifically, the discussion on DNSSEC adoption (objective ii) focused on improving DNS Security and the reducing risks in using DNSSEC (DNS risks were discussed and categorized in the 2009 edition of DNS-SSR). Objective iv) continued the work done in the Kyoto meeting (2010 DNS-SSR) where attendees attempted to rigorously define concept of DNS. The discussion on Botnet command and control (objective v) was added because of the need to consider ways to mitigate risk to the DNS and ways to thwart malicious or abuse of DNS as means to secure the Internet.

Objective iii) was introduced to start a discussion on new applications, if any, which can be enabled by the DNS.

### 1.1. Symposium organization and method

The Symposium motto was: *Interaction, Creativity, and Involvement*.

From its inception, the Symposium was designed to encourage free thinking and brainstorming. Volunteers selected by the Steering Committee moderated breakout sessions. Aside from nominal opening remarks by moderators, participants did not prepare lectures or presentations in advance. Participants were invited to share their perspectives and to collectively build a final common view of the current thoughts related to the DNS issues discussed in each session.

To achieve the objectives mentioned above, the organizers arranged five breakout sessions:

- A. DNS Filtering
- B. Enablers and inhibitors for the security of the domains name system
- C. Evolution of the DNS and Internet name spaces
- D. Data, measures and metrics

## E. Botnet command and control

Breakout sessions A & B ran in parallel during the morning of 19 October 2011. Breakout Sessions C & D ran in parallel in the afternoon. Day one concluded with a series of lightning talks, where participants had a five-minute opportunity to propose a topic for consideration on the morning of day two (October 20, see the agenda in Annex 2). Participants voted by a show of hands. "Botnet command and control" received most votes and was thus the topic discussed on day two.

## 2. Breakout Session Overview

This section provides overviews of the five breakout sessions and describes the themes shared across the topics discussed.

### *DNS Filtering.*

In breakout Session A participants debated about the problem of DNS Filtering, if DNS Filtering via reputation (blacklists, whitelists...) is a necessary function and how should DNSSEC and DNS filtering be integrated.

### *Enablers and inhibitors for the security of the domains name system*

Breakout Session B discussed on what would be the next steps to improve the security of the domains name system. The main issues covered are the barriers to DNSSEC introduction and the unpredictable consequences of signed, malicious registrations.

### *Evolution of the DNS and Internet name spaces*

Session C opened a discussion on the evolution of the DNS and Internet name spaces. In the specific were discussed new applications (e.g. a new PKI) that can be enabled by the DNS.

### *Data, measures and metrics*

Next steps and open issues in DNS data, measures and metrics were discussed in Session D. DNS statistics or trace data are useful information and this breakout session explored what is needed to accelerate the process of defining metrics for DNS Health and Security.

### *Botnet Command and Control*

Session E stimulated a discussion on what is the role of DNS community on botnet mitigation and prevention, what are the solution used today and what new solution can be used.

Breakout sessions share three themes:

- DNS security
- DNS as a means to improve the security of the Internet
- DNS health

**Table 1** summarizes how the breakout sessions are linked to the general symposium themes.

Session A (DNS Filtering) and Session C (Evolution of the DNS and Internet name spaces) considered how the DNS can be used to improve the security of the Internet. While in the former session filtering as a means to

**Table 1 Common themes shared among the breakout session**

		Breakout Sessions				
		A	B	C	D	E
Common Themes	DNS security		✓		✓	
	DNS as a mean to improve the security of the internet	✓	✓	✓		✓
	DNS health		✓		✓	✓

fight abuses and crimes was discussed, the later mainly addressed the quality assurance level that DNS operators should be provided.

Session B (Enablers and inhibitors for the security of the domains name system) is orthogonal to all themes 1, 2 and 3. The main focus was on DNSSEC as a mechanism to improve DNS security *per se* but also as an opportunity to secure the Internet (e.g. for critical end-users). The key concepts emerged from Session B was also related to the health of the DNS.

Session D (Data, measures and metrics) discussed issues related both to health and security of the DNS with a main focus on the concept of “normality of DNS behaviour” and sharing issues.

Session E (Botnet command and control) dealt with one of the main Internet threat and how the DNS community can contribute to mitigate the phenomenon (therefore Session E is related to themes 2 and 3).

### 3. Breakout Session Specific Results

In this section we provide an overview of the five sessions.

#### 3.1. Session A - DNS Filtering

The breakout session leaders raised the following points to stimulate discussion:

1. DNSSEC deployment has begun. Its purpose is to detect alteration of data between the authoritative source and the consumer.
2. DNS filtering applied to avoid the access to certain content is fairly common today (Although not without some controversy)
3. Filtering alters DNS data, therefore:
  - a. should filtering via reputation (blacklists, whitelists, categories, etc.) be standardized, encouraged or discouraged?
  - b. how can/should filtering be integrated with DNSSEC?

The discussion continued along the following thematic areas:

- Filtering and DNSSEC
- Ethics of the filtering practice
- Effectiveness
- Filtering impact
- Unintended Consequences

#### Key Concepts

- **Effectiveness** of filtering depends on where filtering is performed. Filtering after DNSSEC validation prevents end systems from detecting that validation was performed
- Filtering can **always be circumvented** by technically adept users who wish to do so
- **Filtering & sophisticated reputation** systems can be combined to improve effectiveness
- **The authority and scope of the filtering party or entity influence ethics of filtering.** Filtering is ethical if applied by the user in its admin domain or by government to fight abuses and crime (and if the filtering conforms to prevailing law). **Not ethical** if applied by ISP for commercial purpose or by government for political reasons
- Government imposed filtering is an **additional cost** ISPs must bear. The balance between money invested for filtering and effectiveness is subjective
- Filtering is likely to result in users who object to seek alternative name resolution services or methods
- **There may be unintended and harmful consequences** if filters were to be maliciously altered

##### 3.1.1. Filtering and DNSSEC

Fundamentally, filtering and DNSSEC achieve conflicting ends. DNS filtering alters DNS response messages (by returning a non-existent domain or synthesized response). DNSSEC detects these forms of alteration: cryptographic checks will determine that neither response is authentic. When DNSSEC sees compromised digital signatures, it marks the related DNS message as symptomatic of malicious activity, error, misconfiguration, or filtering. Moreover, marking a message as having been altered without determining or signaling the exact cause is by design.

Whether filtering takes place before or after DNSSEC has completed its inspection of a message plays an important role in deployment without conflict or interference. For example, DNSSEC can be deployed at the end system (e.g., any device that supports Internet applications). Here, it protects against DNS message alteration but would detect any DNS filtering performed along the resolution path from the authoritative source to the end system. However, the common practice in today's early deployment is that DNSSEC validation is done on behalf of the end system by a *last hop DNS caching server* (e.g. an ISP's or enterprise's DNS server). The end system relies on the last hop server for DNSSEC verification, hence if filtering is performed *after* DNSSEC the last hop DNS caching server performs validation, the user and end system will see the effects of the DNS filtering.

Providing the end user with an opportunity to detect that his DNS queries were filtered is allows for greater transparency of the filtering policies: the user can be made explicitly aware

that filtering is taking place if he violates a policy. However, policy transparency is in fact a policy decision and transparency may be an issue. Moreover, users may object when they are made aware that their DNS queries (or generally, access to content) are being filtered. If the enforcement mechanisms are not wholly effective, some users may try to circumvent the filter. And if they succeed in circumventing the filter, the circumvention method is easily and often made widely known or available.

### 3.1.2. Ethics of DNS filtering

A fundamental question that participants agree must be clarified when speaking of the *ethics of filtering* is “by what authority is filtering approved or justified?”. Three authorities were discussed:

- Government mandated DNS filtering
- Filtering as part of the ISP’s service
- Self-inflicted filtering (e.g. parental control)

Government or law enforcement mandated filtering caused some debate. Participants agreed that DNS filtering is ethical when used to fight against botnets, malware, child porn or specific crime and citizen threats. Participants also agreed that DNS filtering is not ethical when used for political purposes; for example, when the intent is to suppress free speech. But using free speech as an example, participants observed that free speech is not embraced by all governments, that certain nation states mandate DNS filtering, that the government can exert the filtering policy on its own citizens within its sovereignty, but that advocates of free speech can and do circumvent them, even at the risk of breaking the law.

DNS filtering performed by an ISP in support of that ISP’s policy (e.g., a terms of service agreement as opposed to that mandated by governments) is much less clear. The general consensus was that this was ethical only in very narrow circumstances. Even in those circumstances, ISPs should offer public notice that they filter DNS and what they filter, so that customers can decide if opt-in or opt-out on the basis of this information. Some participants think ISPs could offer DNS filtering as a service. This would give customers the choice of having their DNS messages filtered, and presumably choice of what is filtered (similar to “parental controls”).

Participants agreed on a general principle emerged that DNS filtering is always ethical when applied by the “user” in his own administrative domain. Participants agreed that parents can filter their children’s DNS traffic (but not to what age), and many agreed with scenarios where an employer filters employees. Participants agree that ethical questions can be raised when DNS filtering in your “domain” impacts the freedom of third party; for example, is it ethical for a coffee shop to filter its customers DNS filters? The principle on which participants agreed here seems based on the opt-in opt-out freedom principle.

### 3.1.3. Effectiveness and costs of DNS filtering

There was general agreement that nearly all DNS filtering can be easily circumvented. This can be accomplished by using a different last hop DNS server that does not implement the objectionable filters. DNS servers of this kind are available today, they can be deployed with relative simplicity and agility, and in certain configurations they can be used in stealth. Some ISPs and jurisdictions attempt to restrict DNS traffic that can transit a network (so called port 53 management). Participants agreed that few countermeasures are effective and that technically adept users can probably always evade DNS filtering when they wish to do so.

Government imposed DNS filtering imposes an additional cost onto ISPs, particularly in the management of such filters. The balance between resources invested for filtering and

effectiveness is subjective, but most participants were skeptical. However, in cases such as child abuse material or drive-by malware downloads, participants agreed that DNS filtering is one of the possible ways to attempt to mitigate malware distribution and access to objectionable material or innocently downloaded criminal material is to help non technical users avoid access to domains that host such. Participants observed that a government might be satisfied by less than perfect enforcement (as in driving speed limits). Prohibition against alcohol in the United States, for example, was judged successful from a government perspective: while alcohol consumption was not eliminated but it was reduced enough that the US government concluded the measure was effective. The conclusion? While a technical community can point out that DNS filtering can be circumvented, the government perspective may be different, as even a small change resulting from DNS filtering would qualify as a success.

During the discussion, the idea of using more sophisticated reputation systems to replace simple blacklists was debated. All agreed that reputation systems' output could be used as input for DNS filtering systems.

### **3.1.4. Impact of DNS filtering**

The impact of DNS filtering depends on the scale of the enterprise (i.e. how much filtering is applied) and on the number of persons trying to circumvent it. Circumvention techniques might impact the DNS in different ways (e.g. increase of bandwidth consumption).

One scenario is that DNS filtering could bring people to rely on alternative root servers, DNS services, filtering bypass plug-ins, VPNs as means of circumvention. If these are adopted by large populations, they could affect the coherence, stability and resilience of the DNS; for example, alternative DNS services are unlikely to have the capacity or resiliency of the current, authoritative root system infrastructure. They may not be "well dimensioned and maintained" due to lack of expertise or resources. A worst-case scenario is that they are co-opted or run by criminals.

DNS filtering can have "unintended consequences". Overzealous application of DNS filters might cause an entire top-level domain to be filtered instead of specific delegations.

DNSSEC adoption would be likely be affected by DNS filtering; the two will interact, some think to the detriment of DNSSEC adoption. In theory, DNSSEC will make covert DNS filtering difficult, but when mandated by governments, today in last hop DNS servers, it will be awhile before it will be defeated. DNSSEC improves DNS filtering in that it provides a means for reliably distributing reputation data that is known to be authentic. One participant thought filtering of all sorts could prove beneficial since it would motivate DNSSEC deployment to end systems, rather than last hop servers, where it should have been in the first place.

### 3.2. Session B - Enablers and inhibitors for the security of the DNS

The following questions were raised to stimulate the discussion:

1. What are the next steps and open issues related to advancing the security of the DNS?
2. What are the remaining barriers to DNSSEC introduction?
3. What are the unintended consequences of signed, malicious registrations?
4. How are legal seizures affected when domains listed in a court order are signed?
5. What can and should we be doing to facilitate the security of the domains name system for the purpose of advancing a safer and more secure Internet?

The focus of this session ended up being largely DNSSEC deployment, with some limited discussion of other questions.

An initial brainstorming session led to long list of issues and ideas summarized in Table 2 and Table 3. These are classified into broad, non-exclusive categories. Each category was then enumerated to come up with some key drivers and concepts. These categories overlap, and an issue could belong to more than one category. The issue list also presents a primary dilemma we have in the further roll-out of DNSSEC, distribution needs to be far broader now that we are looking at end-to-end deployment, but there is a lack of awareness/understanding of the value proposition in this wider space. Many of the values cannot be realized without wide adoption, hence a “chicken and the egg” situation. The primary issues and ideas categories identified by the session attendees are:

- Distribution challenges
- Technology/market maturity issues
- Determining and communicating the value proposition to the market
- Process and side issues

Sections 3.2.1 - 3.2.5 expand upon the issues for each category, while section 3.2.6 presents action items and recommendations.

#### Key Concepts

##### • Adoption

- Outsourcing of DNS vs DNSSEC services to defeat technical issues and create incentives
- Implement validation as close to the edge as possible – preferably in the application.
- Design DNSSEC aware OS and Apps
- Simplify DNSSEC management.

##### • Technology and Market maturity

- Refine the validation process and technologies to improve client satisfaction
- Work hard on education and outsourcing (fully-baked solutions) to sell DNSEC as easy-to-use

##### • Value proposition

- DNSSEC doesn't solve all DNS problems, so don't treat it as if it were a *silver bullet*. The integration of cryptography solutions is the only answer to a wider family of threat
- Cost and revenue models are strongly needed, but *“be brave, don't wait too much, the real cost is: if deployment is not quick DNSSEC will remain a curiosity”*
- Strengthen the signing and validation process to improve client satisfaction
- Critical end users and operators are the most likely beneficiary of DNSSEC services. To find the right selling message/channel

### 3.2.1. Distribution challenges

Pushing DNSSEC out beyond publishing within authoritative zones at the TLD and root level is a current challenge. Meeting this challenge requires a multi-pronged effort from domain registrars, DNS service providers, and domain owners on the publishing side and from ISPs, operating system vendors, and Internet aware applications on the validating side.

Unlike the rather small universe of root server and TLD operators, who have similar interests and common industry organizations, the next level of rollout involves a diverse set of industries and interests.

The following challenges to the DNSSEC distribution process were surfaced during the discussion amongst the experts, researchers and stakeholders present at the session.

#### Roll out

The challenge is to roll out of remaining domains TLDs (72%) on the authoritative side. A barrier to achieve this goal is the adoption of DNSSEC by Registrars/domain resellers. Domain registrants look to their domain providers for domain-related services. The open point is to understand if those channels are technically capable and do they have incentives to offer DNSSEC.

A solution to support DNSSEC roll out could be the outsourcing of DNS vs. DNSSEC services. The main related issues are:

- Do domain owners use separate services for “standard” DNS and DNSSEC or a single point?
- What are DNS service platforms offering today, and how is that market incentivized to offer DNSSEC options?

Finally, the choice of the right perspective (End-user, ISP, other operators) can facilitate roll out. The approach could be Top-down (from the root to the edge) or Bottom-Up (from the edge to the root).

Table 2 Driver issues for Session B

Issue	Description
Motivation for DNS security	<p>What is the goal? Why to protect the DNS? Different aspects that must be considered:</p> <ul style="list-style-type: none"> <li>• DNSSEC Adoption: Universal adoption or protection of key sectors and industry segments? Need to define success criteria, target markets, and what they are doing with it</li> <li>• DNSSEC Provisioning: How widely is it distributed, how easy is it to use, how costly?</li> <li>• End-to-end security: Do we get DNSSEC to the edge or is the recursive resolver “good enough”? Alternatively, is the last mile (three feet) to the application covered by some other method derived from the response from the resolver? How is the channel secured end-to-end and specifically the last bit and who is in charge of that last bit?</li> </ul>
Understanding and awareness	Do people truly understand the meaning of DNSSEC? Do people know that if something is signed, it is “authentic” not necessarily “good”?
Top down versus Bottom up	Do we continue rolling out DNSSEC from the “top down” through the ecosystem or do we work “bottom up” from the end user perspective or both. In other words, who is the driver of adoption – end-users/enterprises (registrants), providers or both?

## Validation

"Where" to validate is the second challenge discussed. The common agreement is that the best solution is "as close to the edge as possible – preferably in the application". A solution is to implement validation at ISPs but the issues is "how to stimulate the implementation process". Removal of technical hurdles and establishment of value proposition are the first answer to the issue.

Table 3 Driver concepts for Session B

### DNSSEC aware O/S and Application

Designing DNSSEC aware Operating Systems (OS) and/or application of course will facilitate the adoption. Researcher and practitioners should put an effort in designing standard libraries built into new OS to allow application leverage. The issues remain on the management in legacy OS's. In the same way, DNSSEC aware applications should be capable to directly generate DNSSEC queries or to trust the DNSSEC aware OSs.

### Management of complexity

The complexity of DNSSEC operation must be reduced.

Attendees agreed that methodologies and tools to make easier the management process and to automate some operation are core to mitigate complexity are the right direction to facilitate distribution. For example, automating the signing process should allow for easier adoption. The challenge is to make using DNSSEC "as easy" as standard DNS operations are today. The community (researcher, practitioners, stakeholders) is called to develop methodologies and tools for a *Simple approach to DNSSEC management*.

### Cryptography

Crypto key management and cryptographic algorithms are at the core of DNSSEC. Wide diversity on cryptographic suites can lead to incompatibilities and market confusion. The community should move toward the standardization of cryptographic algorithms used to agree on a cryptographic suite for DNSSEC. Concerning the management of crypto key the open issues are:

- How do you distribute keys?
- How do you roll them?
- How to make simple?

## 3.2.2. Technology and Market maturity

While DNSSEC is not a new technology, the implementations are all fairly new, and undergoing changes as operations ramp-up. The market itself is highly immature, with most entrants coming on-board within the last two years, and many obvious potential providers of services still without offerings. Any "new" market faces similar issues, and our panel of experts, researchers and stakeholders identified the followings, grouped in three categories: Validation, Management of complexity, Cryptography.

Ideas	Description
Positivity	Don't deliver only "obstacles" in these meetings/ discussions about DNSSEC. It is better to promote positive outcomes. Show how DNSSEC solves important problems.
Adoption metric	Look at HTTPS vs. DNSSEC as an adoption metric – if the thing you're communicating is important enough to encrypt for transit, perhaps it should have an authenticated end-to-end resolution for DNS.
Need of DNSSEC	It is important not to jeopardize the overall usability of DNS with overreach on DNSSEC. A lot of people don't need the additional security and the DNSSEC community doesn't need perfection.

## Validation

The validation poses several issues and challenges. The first issue is to identify where is right place to validate. A prevailing idea is that validation should be done at the edge of the DNS, within application themselves, but *has this been proven to be the right solution?*

A second issue is related to the consistency of the validation in various implementations and across them. Participants confirmed that they still see failures based on implementation interactions. Therefore a challenge is to fix the problem and move toward mechanisms to check, manage and enforce the consistency of the validation.

## Management of complexity

Ease-of-use is one of the barriers to widespread adoption that must be overcome. The complexity of the processes in general defeats DNSSEC adoption. The common perception (and often reality) is that is too hard to deal with the management of the processes unless you are an expert. "*Simplicity*" is the keyword substantial barrier to DNSSEC distribution. The community must work on methodologies and tools to simplify the management and adoption of DNSSEC. Different measures are proposed:

- Put more effort in education and new tools to make adoption easier.
- To promote fully baked solutions. The Outsourcing of processes/services is an option. The point is to understand if already exists solutions in a robust enough state
- To promote/facilitate one-stop shopping provider of DNSSEC. Must be investigated the feasibility and technical/legal/process obstacles for an organization to be a one-stop shopping provider of DNSSEC related services.

## Cryptography

Key management process is not yet mature and it remains a challenge. Communication between parties for managing keys and other aspects of the process is core and needs to be easier. Both incentives and more sophisticated tools must be provided.

### 3.2.3. Potential definitions of success

What are we shooting for? Can we measure it? Participants expressed different opinions on this. Here are some proposed definitions for "successful" DNSSEC adoption

- Universal adoption - everyone you communicate with and every device they use can validate throughout the global DNS infrastructure
- Overall end user experience and confidence in the DNS is enhanced - "I trust the Internet and I trust name service"
- Seamless and transparent use - the user blissfully unaware and benefits from DNSSEC irrespective of provider and geographic location.
- All financial and sensitive/critical transactions are secured from origin to destination
- Flexibility - end user chooses to be "more secure" or not as he deems appropriate
- DNSSEC provides a platform to transfer liability issues

**Table 4 Target markets for DNSSEC**

#### Target markets

- Registrants as main driver to provide "secure" connections to users
- ISPs and enterprises running resolvers as a security feature for users
- Registrars, domain resellers, and DNS platform providers for publishing infrastructure (providing security for registrants)
- Applications and O/S vendors

### 3.2.4. Value Proposition

During the session participants identified two concepts considered essential elements of the value proposition of DNSSEC:

1. *The community is spending too much time looking at obstacles versus thinking about opportunities*
2. *DNSSEC doesn't solve all DNS problems, so don't make it out to be a silver bullet*

The participants spent a large portion of their time discussing the value proposition for DNSSEC, as the feeling was that making the value better understood will accelerate adoption, and without it, widespread adoption is less likely. Participants identified target markets (listed in the box on the right) and the factors these markets see as needs and values.

Potential messaging (marketing) and communications plans were discussed in order to expose the target markets to these value propositions. What are the objections, and how can we get "market leaders" to drive key sectors in adoption?

Needs and Values were grouped into five categories: Evangelism/communication and education; cost and return on investment models; Outsourcing models; End-user satisfaction (or end-to-end validation); Critical end users and operators.

**Evangelism/communication and Education** are of paramount importance to scatter the value proposition of DNSSEC and therefore to facilitate rollout. The first issue shared by attendees is related to *who is the audience for selling DNSSEC, what are the key messages, and who are the messengers?* Some possible messages, solutions and related issues are listed below:

- Overselling is a problem – DNSSEC doesn't solve all DNS problems (for example it doesn't prevent domain name hijacking. Don't talk about DNSSEC as if it were a silver bullet. Rather, identify problems DNSSEC does not solve, define cryptographic solutions for these remaining problems and promote the overall objective with a message like *"the incorporation and integration of a family of cryptographic security solutions is the best solution to mitigate the wider family of threats against the DNS"*
- Statistics on spoofing are needed to help show that there is an actual threat to protect against. Of course, DNSSEC is the solution providing a trusted and trustable platform for delivering services.
- Simplify processes to manage DNSSEC to accelerate adoption. The common perception is that implementing DNSSEC is hard – is it, and must it remain so? Can we develop and promote simple solutions?

**Cost and return on investment (ROI).** Identify and disseminate model for cost and is a need and, right now it still a challenge. Costs to be quantified include cost of initial deployment, cost to maintain capacity, and cost of ongoing administration.

Concerning the ROI or revenue model, a question for the distribution network is whether it is possible to generate sufficient revenue to maintain the process and infrastructure. One idea is to generate revenue to pay for assignment and management but the dispute is on the real cost for this operation: adopting a wait-and-see strategy and concluding that "There a little or no cost for doing nothing" has to be considered alongside the consequence of doing too little or nothing. If deployment has insufficient stimulus, DNSSEC will remain a curiosity."

Another revenue generating opportunity may be to design and develop DNSSEC aware applications and operating systems and accelerate adoption by infusing the community with enabling technology. The issue is "what is that market going to look like?"

**Outsourcing** of DNSSEC services is another market opportunity. Outsourcing relieves clients from the responsibility of staffing and managing DNSSEC processes. Outsourcing providers are also highly encouraged to study and develop scalable, automated solutions to crypto key management. However, certain issues would remain unsolved:

- What options are available?
- What are the right choices for various organizations?
- How do we make this simple?

**End-user satisfaction.** Demonstrating the ability to consistently and cost-effectively maintain the customer's desire to sign DNS data and provide end-to-end validation is essential for market value. Issues participants considered include:

- Do ISP's have an obligation to the support DNSSEC? Do they have a larger (unfair?) exposure in the chain of trust (for example, ISPs receive the first helpdesk call when customer experience signing or validation problems)? Collect feedback by distributing questionnaires directly from target market operators or end users.
- The most usable value in DNSSEC comes with end-to-end validation.
  - The community must work on making end-to-end validation widely available.
  - A consistent definition and APIs are needed to make validation available in user applications we needs (should these be opened or closed?).
  - Is the application layer the only or most appropriate place to focus effort?
- Should it be up to the user (case-by-case) to choose what is important to protect?

End users with "critical "application services, intellectual property or trademarks, and large-scale private network operators are the most likely beneficiaries of DNSSEC services. Within Critical Infrastructures (Financial Institutions, Government agencies, Energy and transportation companies, and more...) many critical applications rely on DNS. E-commerce services (at large) are vulnerable to spoofing. To stimulate the adoption in these sectors it is necessary:

- to identify the appropriate individual or unit in the organization to sell the concept (e.g. Potentially reduced liability for critical operators) and
- to explain the DNSSEC value proposition to management.

### 3.2.5. Process and side Issues

The participants identified several issues that are not central for DNSSEC adoption, but are important nonetheless.

- Seizure of signed domains - what happens to key management and other policy issues?
- Consistency of validation - still seeing differences depending on crypto, publishing and resolving software (goes to technology maturity).
- Signed malicious zones - How will the user know that he is safe (e.g. visual indicator)?
- Liability issues - who is exposed to litigation and for what cause when DNSSEC fails?
- Reputation is just as important as authenticity.
- Enterprise/intranet leakage: how do we build defences for real-world scenarios to prevent leakage across zone where compartmentalization was intended?
- Key management issues when signed domains are transferred from one registrar to another? Several process issues must be done correctly and in correct sequence, else domains will be and remain invalid for some period during a registrar or DNS server transfer.
- Communication between parties for managing keys and other aspects of the process needs to be easier.
- Registries having to force data into the system when a registrar cannot or will not do the job.

### 3.2.6. Action Items and Recommendations

Several actions the community should implement emerged from brainstorming sessions:

- Prioritize the issues described in Section 3.2.5 and coordinate actions to cope with them.
- Conduct exercises on market adoption. The exercise should investigate the following:
  - Understand of differences among stakeholders and trying to manage them. Stakeholders to be considered: registry, registrant, and registrar. These could be seen as “successful” by providing DNSSEC. These parties can do more to promote DNSSEC, DNS service platform providers, ISPs, O/S vendors, Software developers (Internet aware applications).
  - Identify incentives and risks and address them.
  - Identify friction points and alleviate them. For example: registrants want to sign zones but registrars don’t want to support it. Community has to promote cooperation among Registrars and Registrants.
- Share ways to get registrars and resellers to adopt and support DNSSEC - use success stories to stimulate interest.
- Working group to look at registrar-registry cooperation for getting zone signing managed smoothly.
- Commit to “Get the word out” initiatives - build the value proposition cases
- Develop “common message” promotional marketing and awareness-raising material for DNSSEC
- Identify technical precursors that parties outside the DNSSEC (DNSSR) community must develop:
  - Consistent API (note: standards IETF project underway)
  - Work on DNS-based Authentication of Named Entities (DANE)
  - Develop a bridge between crypto subsystems and DNSSEC (O/S)
  - Develop configuration settings that are flexible depending on end user

### 3.3. Session C- Evolution of the DNS and Internet name spaces

Internet has changed many facets of modern society. As society becomes accustomed to the Internet as an omnipresent service and influence, it will demand a broader range of services and even greater integration. In this session,

participants discussed the evolution of the DNS and Internet name spaces; specifically whether and how it may need to change to satisfy new demands.

#### Key Concepts

- **Quality Assurance** must be improved and aligned with those provided by CERTs. However it is debated the real need of more assurance
- **Using the DNS to identify “objects” independently from hosts** merits additional study. This is a big challenge but may become more important as use of cloud computing and virtualization become more widespread
- **Methods that enable an authority to invalidate records** associated with a certain domain name merits addition study.

The following questions were selected to stimulate the discussion:

1. What is next in the evolution of the DNS and Internet name spaces?
2. Which new applications, if any, can the DNS enable? A new PKI is a commonly discussed candidate, but are there others?
3. Is the Internet domain name space the only name space the Internet needs?
4. What can we learn from X.509 and existing PKI systems to guide future DNSSEC development?

Topics identified at the opening of the session are listed in Table 5 and described in the following sections.

#### 3.3.1. Name space issues

Two name space issues were debated: quality assurance levels and new uses of DNS as global identifiers/

##### Quality assurance levels

The idea of quality assurance might be interpreted as a way for auditing registry providers. Participants pointed out that no single organization exercises administrative control over the entire chain of trust in the name space and identified this as a considerable barrier to development.

There is currently only one level of assurance in a domain name. In contrast, CERTs provide three levels of quality assurance. Some participants questioned whether there was truly a need for additional assurance levels. The group agreed on the fact that there's a wish, maybe a need, for better quality assurance, better ownership assertion, but doesn't need to be a flag day: can be iterative, compartmentalized.

##### New identifiers and name spaces

Participants discussed possible new uses of the DNS. Participants suggested that using the DNS to identify “objects” independently from hosts merits consideration. Some argued that since DNS already basically is used to identify a certain host, that generalization would be reasonable. Others pointed out that the advent (onset) of “cloud generation” applications has illustrated the need to be able at one level to know or constrain where an object at rest is geo-

Table 5 Topics of interest discussed in Session C

Topic	Issues
Name Space	Quality assurance level
	Ownership assertion and validation
	Other name spaces / other things to name <ul style="list-style-type: none"> <li>• Identifiers in DNS</li> <li>• Use of DNS in non-URLs</li> </ul>
Protocol	ANY queries
	Cache invalidation
	Geo-identifiers and beyond

located (basically, which host) but at another level, to simply be content that the object exists somewhere (possibly at rest in multiple locations) in the cloud. Some participants believe that domain names satisfy the latter but not the former and that some host-independent attributes could be associated with an object identifier that would identify “where the object is permitted to travel and where it is permitted to rest”. Participants agreed that some cryptography could have a role here, but it is not yet clear whether or how the DNS might be used for this purpose.

### **3.3.2. Protocol issues**

In this session, participants discussed protocol issues, in particular focusing on ANY query, cache invalidation and Geo-identification.

**ANY query** should be eliminated. This query appears to be used only for debugging and has few other uses in production environments. It was suggested to associate a permit/deny switch to this query type.

**Cache invalidation.** Participants introduced a concept of “vertical NOTIFY”. This notification would permit an authority to signal that any cached information for the domain name indicated in this new form of notification is invalid. Conceptually, an authoritative name server would keep track of name servers from which it has received queries. If an event were to merit invalidating a domain name, the authoritative name server would send this “vertical NOTIFY” message to all name servers on the list, and those name servers would remove resource records associated with the indicated domain name from their local caches.

The proposal raised some issues related for example to the use of NAT and to the risk of re-enabling the Kaminsky attack.

**Geo-identification.** Participants discussed that certain content distribution providers could benefit from having the ability to direct users to the geographically “nearest” host that can serve up that content (i.e. to the closest server).

### 3.4. Session D - Data, measures and metrics

This breakout session was intended as the next step after the Kyoto's meeting<sup>3</sup> toward the definition of DNS Health and Security metrics. The community agreed on the "clinical" definition of DNS Health. However there was a common agreement about the need to improve the "clinical" approach established in Kyoto.

DNS statistics or trace data are useful information to assess the Health and Security level of the DNS but it was expressed the need for a further discussion on what is required to accelerate the process of defining metrics for DNS Health and Security and how such metrics can be implemented. To stimulate the discussion, the following questions were proposed:

- What methods are available for data analysis?
- What can we see?
- What are we (should we be) looking for?
- Are there data protection and anonymization issues?
- Aggregating data and cumulative views swarm effects?
- What challenges do (new) application and/or (new) behaviours pose?

The DNS community is capable of collecting data and DNS traffic has been characterized in various ways. Participants agreed that is time to shift the focus to behaviour characterization and to how to deal with data collected. The challenges lie in the areas of analysis and action (how to react or respond) and therefore the session opened with a brainstorming on these issues. The brainstorm produced the list of topics summarized in Table 6. The issues were grouped into four main categories and discussed separately:

- Normalization issues
- Sharing and baseline definition issues
- Legal issues
- Survey, quality check issues

#### 3.4.1. Normalization issues

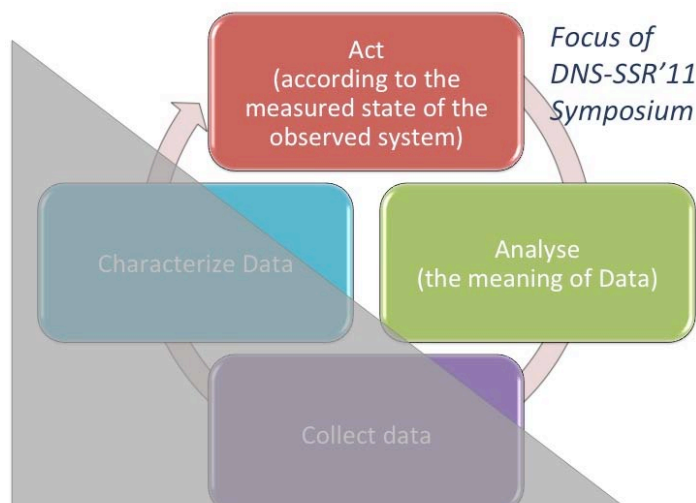
A key concept emerged during the session and largely debated is the "possibility to determine what is normal in DNS behaviour" or better "what should be healthy".

#### Key Concepts

- Coordinate efforts to determine **what is normal** in DNS behaviour. **Normal is not always healthy**. Definition of what is normal must be based on the experience and periodic monitoring.
- **Different perception of normal**: vantage point (end-user, ISP, name server, ...); academic understanding; companies understanding
- **Sharing Model**: *when to share; how to share; how to respect legal and privacy constraints; how to incentive*
- **Sharing Methodologies and standards**: the community must move from the simple sharing of errors or warning toward a framework allowing to measure, evaluate and monitor the health of the DNS.
- Early warning function should be integrated
- **Program globally, measure locally** to solve legal issues. **Community must move toward a DNS-CERT** as coordination entity
- **Sharing of synthesized indexes** and metrics should provide a high protection against privacy and confidentiality breaches

<sup>3</sup> <https://www.icann.org/en/topics/ssr/dns-ssr-symposium-report-1-3feb10-en.pdf>

**Figure 1 Focus of the Symposium is on Analyse the meaning of data and Act according the state of the system**



Periodic monitoring allows us to understand traffic behaviour and compare present to historical data. Spikes and noises are occasional as well as periodic (occurring at regular intervals) -- *traffic indexes that are in the average, spikes that I can see every day* – is what usually operators observe. This behaviour is normal, but can we say the system is normally behaving? Can we accept that? Is that healthy? Normality is not always healthy. There is indeed a need for a proper index to deal with anomalies that fall almost into normal behaviours.

“What is normal?” is difficult to define. In fact it depends on several aspects that must be considered:

- What is normal can be perceived differently depending on the vantage point
- There are differences in academic understanding and companies’ understanding of what is normal or not.

The common agreement is that from collected data must be extracted knowledge on the “normal” and “abnormal” DNS behaviour.

To complete our understanding of normal behaviour we should differentiate between genuine traffic and normal traffic. There is not only the need to monitor network traffic but also internal server behaviour (not only usual performance indexes).

It could be useful to set up some thresholds of “attention” while capturing data, i.e., some measurement that could distinguish traffic that is useful (i.e., beneficial to users) and what is not (e.g., DNS abuse traffic, traffic resulting from configuration error). Thresholds can be helpful also to choose *when* it is appropriate to share collected traffic. To do this, we must define what behaviours (also users’ behaviours) are normal or not and then control what traffic they generate. Once normal behaviour is defined, it is important to understand how the local behaviour, normal or abnormal, affects third parties and other perspectives. Abnormalities must be studied from different points of view. An open issue is *“How we can correlate measures from different observation points”*.

### **3.4.2. Sharing and baseline definition issues**

Sharing is always a big challenge, technical issues are marginal with respect to: business, privacy, confidentiality and legal issues.

The need for data to be analyzed implies suggest that there is also a need for a model for circumstances where operators (or generally, anyone who is collecting or analyzing data) benefit from sharing both raw information and analyses. The sharing model issues to be solved include when to share; how to share; how to respect legal and privacy constraints; and how to incentive.

Information is often most usefully shared when DNS operations are not behaving as intended or expected. It could be useful to define a set of aggregated indexes, describing the local state of a DNS component/subsystem, to be constantly shared. These indexes can be aggregated, back propagated and analysed in order to identify if quasi-normal behaviours at local level might impact other elements, or, worst, the entire infrastructure

Effective sharing requires more than casual or academic discussions among “the usual suspects” (respected members of the DNS community, critical path DNS operators). There is a need for methodologies and standards. Phone calls and newsletters are not powerful enough.

Table 6 Diver issues for Session D

A recommended solution is to set up monitors or tools (e.g. tools allowing to signal errors or warnings) working on the OARC portal (the natural candidate). The community must move from the simple sharing of errors or warning toward a framework allowing to measure, evaluate and monitor the health of the DNS. A set of aggregated indicators must be continuously monitored and shared. A third party, as OARC or a global DNS computer emergency or crisis response team should integrate local measures to come up with a big picture of the DNS behaviour. The MENSA project, as many other projects, is developing the foundation for that view.

### 3.4.3. Legal issues

The final challenge is related to privacy and confidentiality: *“is it possible to distribute information and speculate on what is happening while also assuring that data confidentiality and of the privacy of the data owners is respected and that legally protections are not violated?”*

Determination of jurisdiction (prevailing law) influences whether sharing raw data violates data confidentiality in a legal context and similarly whether sharing of synthesized indexes and metrics provides necessary protections against unlawful disclosure of what is private information.

Issue	Description
<b>Normalization</b>	There are many network tools to measure the DNS but very few way to transform numbers in meaningful information
	Noise in measurement. How we can characterize noise and anomalies
	Homogeneous language to describe the collected data. Standardized approach to measure and to interpret numbers
	Global view of DNS traffic, there is the need to define a way/methodology to compare data
	TLD, registry and registrar point of view in metrics and measurements
	Misconfiguration & anomalies detection
<b>Sharing and baseline definition</b>	Counting capture characterize
	Traffic characterization: netflows, dnsflows
	Shared observation and data
	Active vs passive measurement
	Data exchange format (and data anonymization)
	What should be the focus? There are a lot of data collected by TLD and ISP. A coordinated analysis is needed
	Baseline dataset as reference. (There is no common baseline. Nobody can say how the system should look like. No common reference)
	What are the right things to look at.
How “end-user” perceive the ISP services, service monitoring (SLA)	
<b>Legal</b>	Legal issues with capture
<b>Other</b>	Characterization => analysis
	Health
	Not jet the moment to automatize the measurement model
	Top down approach, from health definition to data collection can pay.
	Local data view

The key concept to solve part of the legal and privacy issues is: *“Program globally, measure locally”*.

### 3.5. Session E - Botnet Command and Control

A typical type of botnet command and control is performed using algorithmically generated domains (a Domain Generation Algorithms, DGA). Common examples are conficker<sup>4</sup> and Srizbi. The participants discussed the following issues:

- Botnet blocking and alternatives
- Effects of takedown by courts
- High Security Zones

#### Botnet blocking and alternatives

The first issue discussed is how to work out the DGA time parameters being used and how the DGA clock is set in order to block the botnet. Participants agreed that:

- Disabling botnets by blocking algorithmically generated domain names is a stopgap measure. It creates operational, contractual challenges and has poor scaling properties. Conficker was a demonstration of how the scales don't work for the good guys. The blocking process doesn't scale because it takes time.
- Generating "Security feeds" for known DGA in various formats including Resource Policy Zones (RPZ) can help deal in real time with algorithmically generated domain names.

OS vendors must continue to improve the security of their systems and to continue to study ways to improve (accelerate) remedial processes (patch distribution). The Internet community and OS vendors must fix botnet related issues and vulnerabilities. From the discussion emerged two considerations:

- Solution must be implemented in DNS, because that is where control is happening (the finger of doom is pointing at DNS industry), and
- Protection mechanisms must be put close to the user because that's where people care.

Dealing with botnets shares poses of the same challenges as DNS filtering?

- ISP and DNS operators are blocking DGA names and users seem to like the free protection.
- ISP and DNS operators could also use this as a reporting mechanism for combating infection. There exist already some examples of this solution in place.
- What happens when the bad guys decide to move on? Attacks against filtering can produce a net loss.
- Botnet mitigation (once detected) can be expensive.

#### Effects of takedown by courts

*How is the takedown by courts affecting industry, including ability to remediate?*

- Netherlands has a platform for take down, but DNS is last resort.
- There are processes for takedowns in some countries.
- Having a wall of shame for TLDs might not work

**High security zones experience** demonstrated that, sometimes, users don't want to be protected.

#### Key Concepts

- **Blocking names** has operational and scaling limitations. It can be somewhat improved through development of enhanced processes.
- **RPZ with DGA filters** can be combined for blocking and infection discovery.

---

<sup>4</sup> Phillip Porras, Hassen Saidi, and Vinod Yegneswaran, *An analysis of Conficker's logic and rendezvous points*, 2009, <http://mtc.sri.com/conficker>

## 4. Summary

Breakout sessions conducted during the Symposium share three themes:

- 1) DNS security
- 2) DNS as a means to improve the security of the Internet
- 3) DNS health

Session A (DNS Filtering) and Session C (Evolution of the DNS and Internet name spaces) considered how the DNS can be used to improve the security of the Internet (theme 2). Session A mainly discussed filtering as a means to fight against abuses and crimes. Effectiveness, Ethics and costs of DNS filtering were the main issues considered. Session C concentrated on the quality assurance levels operators should provide.

The main focus of Session B (Enablers and inhibitors for the security of the domains name system) was DNSSEC as a mechanism to improve DNS security but the session also created an opportunity to discuss complementary ways to promote the need to secure the name service. Participants discussed ways to accelerate adoption of DNSSEC; how to mature the market and technologies; and the need to assert a value proposition for DNSSEC.

Session D (Data, measures and metrics) considered issues related both to health and security of the DNS (themes 2 and 3) with a main focus on understanding what constitutes “normal DNS behaviour”. Participants also discussed data collection, data analysis, and data sharing issues.

Session E (botnet command and control) dealt with one of the main Internet threat and how the DNS community can better contribute to mitigate the phenomenon (therefore Session E is related to themes 2 and 3).

The key concepts and takeaway messages developed during the sessions include:

### Session A – DNS Filtering

- **Effectiveness** of filtering depends on where filtering is performed. Filtering after DNSSEC validation prevents end systems from detecting that validation was performed
- Filtering can **always be circumvented** by technically adept users who wish to do so
- **Filtering & sophisticated reputation** systems can be combined to improve effectiveness
- **The authority and scope of the filtering party or entity influence ethics of filtering.** Filtering is ethical if applied by the user in its admin domain or by government to fight abuses and crime (and if the filtering conforms to prevailing law). **Not ethical** if applied by ISP for commercial purpose or by government for political reasons
- Government imposed filtering is an **additional cost** ISPs must bear. The balance between money invested for filtering and effectiveness is subjective
- Filtering is likely to result in users who object to filtering to seek **alternative name resolution** services or methods
- **There may be unintended and harmful consequences** if filters were to be maliciously altered

### Session B – Enabler and inhibitors for the security of the DNS

- **Adoption**
  - Outsourcing of DNS vs. DNSSEC services to defeat technical issues and create incentives
  - Implement validation as close to the edge as possible – preferably in the application.
  - Design DNSSEC aware OS and Apps
  - Simplify DNSSEC management.

- **Technology and Market maturity**
  - Refine the validation process and technologies to improve client satisfaction
  - Work hard on education and outsourcing (fully-baked solutions) to sell DNSSEC as easy-to-use
- **Value proposition**
  - DNSSEC doesn't solve all DNS problems, so don't treat it as if it were a *silver bullet*. The integration of cryptography solutions is the only answer to a wider family of threat
  - Cost and revenue models are strongly needed, but *"be brave, don't wait too much, the real cost is: if deployment is not quick DNSSEC will remain a curiosity"*
  - Strengthen the signing and validation process to improve client satisfaction

Critical end users and operators are the most likely beneficiary of DNSSEC services. To find the right selling message/channel

### Session C – Evolution of the DNS and Internet name spaces

- Quality Assurance must be improved and aligned with those provided by CERTs. However it is debated the real need for more assurance
- Using the DNS to identify "objects" independently from hosts merits additional study. This is a big challenge but may become more important as use of cloud computing and virtualization become more widespread
- Methods that enable an authority to invalidate records associated with a certain domain name merits additional study.

### Session D – Data, measures and metrics

- Coordinate efforts to determine **what is normal** in DNS behaviour. **Normal is not always healthy**. Definition of what is normal must be based on the experience and periodic monitoring.
- **Different perception of normal**: vantage point (end-user, ISP, name server, ...); academic understanding; companies understanding
- **Sharing Model**: *when to share; how to share; how to respect legal and privacy constraints; how to incentive*
- **Sharing Methodologies and standards**: the community must move from the simple sharing of errors or warning toward a framework allowing to measure, evaluate and monitor the health of the DNS.
- Early warning function should be integrated
- **Program globally, measure locally** to solve legal issues. **Community must move toward a DNS-CERT** as coordination entity
- **Sharing of synthesized indexes** and metrics should provide a high protection against privacy and confidentiality breaches

### Session E – Botnet Command and Control

- **Blocking names** has operational and scaling limitations. It can be somewhat improved through development of enhanced processes.
- **RPZ with DGA filters** can be combined for blocking and infection discovery.

# Annex1: Symposium Agenda

---

*Day One, October 19, 2011*

---

**8:30 Registration**

**9:00 Welcome message (Sarmi/Rigoni/Crain)**

**9:15 Introduction of SSR topics**

**10:00 Breakout sessions, in parallel:**

**Session A:** How should DNSSEC and DNS filtering be integrated?

Questions to consider include:

1. Is DNS filtering via reputation (blacklists, whitelists...) a necessary function?
2. If yes, how it should be integrated with DNSSEC usage?

(Moderator: Paul Mockapetris)

**Session B:** What are the next steps and open issues to advancing the security of the domains name system?

Questions to consider include:

1. What are the remaining barriers to DNSSEC introduction?
2. What are the unintended consequences of signed, malicious registrations?
3. How are legal seizures affected when domains listed in a court order are signed?  
What can and should we be doing to facilitate the security of the domains name system for the purpose of advancing a safer and more secure Internet?

(Moderator: Rod Rasmussen)

**11:15 Coffee break**

**11:45-13:00 Continue Sessions A & B**

**13:00-14:00 Lunch**

**14:00 -16:30 Breakout sessions, in parallel:**

**Session C:** What is next in the evolution of the DNS and Internet name spaces?

Questions to consider include:

1. What new applications, if any, can the DNS enable? A new PKI is a commonly discussed candidate, but are there others?
2. Is the Internet name space all it is and can ever be?
3. What can we learn from X.509 and existing PKI systems to guide future DNSSEC development?

(Moderator: Roy Arend)

**Session D:** Data, measures and metrics: next steps and open issues. DNS statistics or trace data are useful information but what is needed to accelerate the process of defining metrics for DNS Health and Security? Questions to consider include:

What methods are available for data analysis?

What can we see?

What are we (should we be) looking for?

Are there data protection and anonymization issues?

Aggregating data and cumulative views swarm effects?

What challenges do (new) application and/or (new) behaviours pose?

It is recommended that participants make themselves familiar with the output of the previous SSR symposium on the topic of health.

<https://www.icann.org/en/topics/ssr/dns-ssr-symposium-report-1-3feb10-en.pdf>

(Moderator: Peter Koch)

**16:30 Coffee break**

**17:30- 18:30 Lightning Talks: Topic Setting for Day 2**

Participants get 5 minutes to present a topic he or she would like to have discussed on Day 2.

Topics will be selected using a Doodle poll conducted overnight.

(Moderator: Dave Piscitello)

**18:30 Closing remarks, social events or dinner**

---

## ***Day Two, October 20, 2011***

---

**8:30 Coffee**

**9:00 Topics for the day announced**

**9:15-10:45 Breakout sessions, in parallel.**

Sessions E and F will be chosen using an overnight Doodle poll. The two lightning talk topics that receive the most votes will be the subjects of these two sessions.

**10:45 Coffee Break**

**11: 00-1200 Continue sessions E and F**

**12:00-1300 Summary reports from session moderators (10 mins each)**

Formal presentation materials are not required. However, we ask that moderators please submit a summary of reasonable detail by email to [john.crain@icann.org](mailto:john.crain@icann.org) or [dave.piscitello@icann.org](mailto:dave.piscitello@icann.org) by November 15 so that we can include these in the Symposium report. Include in your summary,

- Main discussion points
- Issues raised
- Solutions proposed
- Actions recommended
- Parties upon whom the task of performing recommended actions would fall

**13:00 Closing remarks**

**13:30 Adjourn**

## Annex 2: Symposium Participants

LAST NAME	FIRST NAME	ORGANIZATION
Akkerhuis	Jaap	NLnet Labs
Andreev	Peter	MSK-IX
Archbold	Richard	Amazon
Arends	Roy	NOMINET
Armas	Carlos	Network Startup Resource Center (NSRC)
Balla	Emanuele	CURBL
Blumenthal	Don	.ORG, the Public Interest Registry
Bond	John	RIPE NCC
Bortzmeyer	Stephane	AFNIC
Carli	Carlo	AGEIE
Castro	Sebastian	.nz Registry Services
Cocco	Antonello	ISCOM (substitute for Rita Forsi)
Crain	John	ICANN
Cudazzo	Raffaele	Aubay
D'Agostino	Gregorio	ENEA
Damas	Joao	ISC
Davids	Marco	SIDN
Deccio	Casey	Sandia National Laboratories
Deri	Luca	NIC.IT (substitute for Domenico Laforenza)
Diaz	Marco	NIC Chile
Ermert	Monika	eLance Journalist
Frosini	Nicola	Register.it
Fukuda	Kensuke	National Institute of Informatics
Gall	Alexander	SWITCH
Galvin	James	Affilias
Garofalo	Michele	Selex Sistemi Integrati
Gieben	Miek	SIDN
Gijsen	Bart	TNO
Groeneweg	Marc	SIDN
Hagnell	Staffan	.SE
Ihrén	Johan	Netnod
Jung	youchan	Catholic Univ.
Kato	Akira	Keio University/WIDE Project
Fukuda	Kensuke	National Institute of Informatics
King	Adam	.AU
Koc	Yakup	Delft University of Technology
Koch	Peter	DENIC
Kohmanyuk	Dimitry	INTUIX LLC
Kumari	Warren	Google
LA Young-Sun	LA Young-Sun	NIDA/KRNIC
Lamb	Richard	ICANN

Larson	Matt	Verisgn
Liu	Ziqian	China Telecommunications Corporation
Lloyd	Sion	Nominet
Long	Lei	Shanghai Huanlei Information Technology Co., Ltd.
Manning	Bill	Retired
Matsuzaki	Yoshinobu	IJ
Mikle	Ondrej	CZ.NIC
Mockapetris	Paul	Nominum
Pagnozzi	Sergio	Telecom Italia
Phonsen	Tanut	EGA
Pisanty	Alejandro	UNAM
Piscitello	Dave	ICANN
Rasmussen	Rod	Internet Identity
Robachevsky	Andrei	ISOC
Ruberti	Stefano	NIC.IT (substitute for Domenico Laforenza)
Shaw	Cloe	Othello Technology Systems
Slaný	Karel	CZ.NIC
Story	Robert	SPARTA
Surý	Ondřej	CZ registry
Vaughn	RL	Baylor University
Vixie	Paul	ISC
Wallström	Patrik	.SE
Yoshinobu	Matsuzaki	Internet Initiative Japan
Zamparelli	Fabio	Telecom Italia
Ziqian	Liu	China Telecommunications Corporation