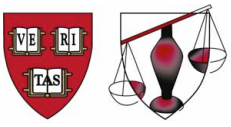
Accountability and Transparency at ICANN
An Independent Review

Appendix E: The DNS-CERT Proposal
October 20, 2010



Berkman
The Berkman Center for Internet & Society
at Harvard University

Abstract

ICANN's DNS-CERT proposal advocates the creation of an organization to analyze, assess, and respond to global DNS security threats. This case study begins with an overview of ICANN's DNS security mandate as described in its Memorandum of Understanding with the United States Department of Commerce, its Bylaws, and its 2009 AoC. A summary of the DNS-CERT proposal follows, based on ICANN's "Proposed Strategic Initiatives for DNS Security, Stability, and Resiliency" and its "DNS-CERT Business Case." The study then traces the origins of the controversy surrounding the DNS-CERT proposal, beginning with ICANN's publication of the proposal and the remarks made in Nairobi by its CEO, Rod Beckstrom, and the controversy's development through public comments, correspondence, and material gathered in interviews with the DNS community.

The review of these materials suggests three key issues underlying the controversy: (1) the merits and clarity of ICANN's assessment of the current state of DNS security and its proposal for the creation of a centralized CERT; (2) varying interpretations of ICANN's DNS security mandate; and (3) procedural issues related to openness, transparency, public input, and stakeholder participation.

Case Study Sources and Methodology

For more information on our sources and methodology, please see Appendix A.

This case study is based on publicly available materials, including public comments, ICANN documents, academic studies, media reports, and expert opinions. It provides a summary of the facts regarding ICANN's DNS-CERT proposal. As per Exhibit B, section 1 of the Services Agreement between the Berkman Center and ICANN, its goal is to help identify key issues, challenges, and areas of disagreement related to ICANN's DNS-CERT proposal. The observations below will contribute to the Berkman team's final report.

In addition to publicly available sources, this case study includes statements, opinions and perceptions of those we interviewed in the course of developing this case. These perceptions and opinions play an important role in the interpretation of ICANN decisions and their reception by the community. The statements of interviewees do not reflect the opinions or conclusions of the study team. While we have made every effort to remove factual inaccuracies, we do not attest to the accuracy of the opinions offered by interviewees. The interviews were conducted on the condition of confidentially.

Note: As per the Services Agreement, this case study focuses on events prior to June 17, 2010. However, the DNS-CERT proposal and related events are still evolving. As such, this study may not reflect the most recent developments in this case.

Disclosure: Professor Jonathan Zittrain, Berkman Center Faculty Co-Director and Co–Principal Investigator of this review, is on the Board of Directors of the Internet Society (ISOC). This study refers to a letter from Lynn St. Amour, President and CEO of ISOC, in establishing the factual basis of the DNS-CERT controversy.

Table of Contents

1 Background: ICANN's Role in DNS Security

In its original Memorandum of Understanding (MoU) with the United States Department of Commerce, ICANN was tasked with the technical management of the Domain Name System (DNS). ICANN assumed responsibility for four areas of DNS management: "stability, competition, bottom-up coordination, and representation."[1] ICANN's commitment to DNS stability was reflected in its original Bylaws, in which the Root Server System Advisory Committee (RSSAC) was established to "examine and advise on the security aspects of the root name server system."[2]

In 2001, ICANN extended its commitment to DNS security when the Board directed ICANN's President "to appoint a President's standing committee on the security and stability of the Internet's naming and address allocation systems."[3] A year later, in May 2002, the Board resolved to convert the standing committee into the permanent "Security and Stability Advisory Committee" (SSAC), which remains a cornerstone of ICANN's DNS security efforts.[4] The "new Bylaws," published soon thereafter, confirmed DNS security as one of ICANN's central organizational goals. The first of ICANN's "Core Values," according to the revised Bylaws, is "[p]reserving and enhancing the operational stability, reliability, and global interoperability of the Internet."[5]

ICANN's Affirmation of Commitments (AoC), published in September, 2009, once again reaffirmed ICANN's commitment to DNS security. "ICANN has developed a plan," it reads,

> *to enhance the operational stability, reliability, resiliency, security, and global interoperability of the DNS, which will be regularly updated to reflect emerging threats to the DNS. ICANN will organize a review of its execution of the above commitments no less frequently than every three years. The first such review shall commence one year from the effective date of this Affirmation.*[6]

The ICANN plan for preserving DNS security, stability, and resiliency has three areas of focus: (1) general attention to physical and network security of the DNS, (2) contingency planning, and (3) "maintaining clear processes."[7]

---

[1] ICANN, "Memorandum of Understanding Between the United States Department of Commerce and Internet Corporation for Assigned Names and Numbers," November 25, 1998, http://www.icann.org/en/general/icann-mou-25nov98.htm.

[2] ICANN, "Bylaws," November 6, 1998, http://www.icann.org/en/general/archive-bylaws/bylaws-06nov98.htm.

[3] ICANN, "Third Annual Meeting of the ICANN Board in Marina del Ray Preliminary Report," November 15, 2001, http://www.icann.org/en/minutes/prelim-report-15nov01.htm#StandingCommitteeonSecurityandStability.

[4] ICANN, "Special Meeting of the Board Preliminary Report," May 13, 2002, http://www.icann.org/en/minutes/prelim-report-13may02.htm#SecurityCommittee.

[5] ICANN, "Bylaws," December 15, 2002, http://www.icann.org/en/general/archive-bylaws/bylaws-15dec02.htm.

[6] ICANN, "Affirmation of Commitments by the United States Department of Commerce and the Internet Corporation for Assigned Names and Numbers," September 30, 2009, http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm.

[7] Ibid.

2 Overview of ICANN's DNS-CERT Proposal

Pursuant to the commitments described in the AoC, ICANN published a draft of its "Plan for Enhancing Internet Security, Stability, and Resiliency" in May 2009.[8] The draft plan describes ICANN's high-level security objectives, clarifies its role within the broader Internet security community, and provides an overview of its anticipated security-related projects for the 2009–2010 operating year—including the implementation of DNSSEC for the authoritative root zone, enhanced security measures for new gTLDs and IDNs, and active collaboration with a wide range of security stakeholders.

In December 2009, ICANN published a draft of its 2010–2013 strategic plan. The draft plan makes reference to "DNS CERT concept development" as a plan under the heading of "[p]reserve DNS stability and security," but provides no additional detail. The final draft of the plan, published on February 22, 2010, includes a brief overview of the anticipated project:

> *ICANN will work in partnership with other organizations to develop an approach to the establishment of a DNS CERT in order to address one of the broader issues of Internet security. This system would enable a more coordinated and effective response to incidents and attacks on the DNS. In addition, ICANN will be working with the Internet community to enhance contingency planning and exercises to address risks and threats to the DNS.*[9]

On February 12, 2010, ICANN published two additional security-related documents: the "Proposed Strategic Initiatives for Improved DNS Security, Stability and Resiliency"[10] and the "Global DNS-CERT Business Case."[11] Taken together, these two documents define the contours of ICANN'S DNS-CERT initiative, which aims to facilitate the creation an independent organization to anticipate, evaluate, and respond to the full range of DNS security threats.

2.1 Proposed Strategic Initiatives

The Proposed Strategic Initiatives document begins with a series of statements about the current state of DNS security. First among them is the observation that the DNS—a fundamental component of the majority of user applications on the Internet—exists "in an environment of increasing threats and risks."[12] The increase in the "frequency and serious nature" of calls to action within the DNS security community, it argues, indicates a growing need for system-wide response capabilities. It claims that current efforts, however, are "not systemically focused." Overall, ICANN takes the position that the DNS "lacks system-wide focal points for accountability

---

[8] ICANN, "Plan for Enhancing Internet Security, Stability, and Resiliency," May 16, 2009, http://www.icann.org/en/topics/ssr/ssr-draft-plan-16may09-en.pdf.

[9] ICANN, "July 2010–June 2013 Strategic Plan," February 19, 2010, http://www.icann.org/en/strategic-plan/strategic-plan-2010-2013-19feb10-en.pdf.

[10] ICANN, "Proposed Strategic Initiatives for Improved DNS Security, Stability and Resiliency," February 12, 2010, http://www.icann.org/en/topics/ssr/strategic-ssr-initiatives-09feb10-en.pdf.

[11] ICANN, "Global DNS-CERT Business Case: Improving the Security, Stability and Resiliency of the DNS," February 12, 2009, http://www.icann.org/en/topics/ssr/dns-cert-business-case-19mar10-en.pdf.

[12] ICANN, "Proposed Strategic Initiatives," 2.

related to key capabilities in risk assessment, contingency planning and exercises, and dedicated, sustained response."[13]

The document argues that ICANN's obligation to DNS security (as defined in the AoC and other policy documents) compels it to "ensure establishment of system-wide approaches to assess risk, to plan and exercise contingencies against potential threats and to orchestrate collaborative incident response capabilities to improve the overall security, stability and resiliency of the DNS system."[14]

ICANN outlines three types of current DNS security risks: malicious activity risks (including DDoS and cache poisoning attacks), technical risks (including the DNS protocol vulnerabilities identified by Dan Kaminsky), and organizational failures (such as when a root server operator, registry, or registrar can no longer perform its function).[15]

The document proposes two initiatives in response to these risks. The first is a program to coordinate "system-wide DNS risk analysis, contingency planning, and exercises."[16] An expert advisory group, composed of DNS operators and the broader cybersecurity community, would oversee risk assessment and contingency planning activities. A DNS root-system information-sharing mechanism would facilitate analysis and incident response. Finally, ICANN would lead a series of multi-stakeholder exercises to identify weaknesses in current DNS security response practices.[17]

The second proposed initiative is the creation of a DNS-CERT organization, to serve as a central point of contact in coordinating responses to DNS security incidents. The DNS-CERT proposal is described fully in the DNS-CERT business case.

2.2 DNS-CERT Business Case

The DNS-CERT business case begins with a detailed evaluation of the current state of play in DNS security. It begins with an overview of the structure and importance of the DNS. The essential role of the DNS, it argues, has driven an increase in malicious activity aimed at disrupting or compromising the system's security. At the same time, the increasing importance of the DNS to a range of vital applications has raised the stakes of other structural risks, such as technical and organizational failures.

Citing a report from the 2009 Global DNS Security, Stability, & Resiliency Symposium (a gathering of the global community of DNS security stakeholders held in Atlanta in February 2009), the proposal contends that "information sharing within the DNS community is sorely

[13] Ibid., 3.
[14] Ibid., 4.
[15] Ibid., 4–8.
[16] Ibid., 9.
[17] Ibid., 9–11.

lacking" and that security response capabilities are "limited at all levels."[18] Such limitations are not necessarily due to any ineptitude or torpor within the DNS community, but rather may result from geographic constraints or limitations in resources, as well as the fact that loosely coordinated responses to security threats have, until recently, worked adequately well.

The proposal lists a series of previous DNS security incidents—including the Conficker worm, the Kaminsky vulnerability, domain hijacking, and the Avalanche attacks—to make the case that a centralized body is needed to coordinate responses to such events.[19] The proposed DNS-CERT organization would meet this need. The organization would represent the interests of broad and highly diverse range of stakeholders, including DNS root operators, TLD registries and registrars, ISPs, existing CERTs, governments, vendors, and end-users.[20] Its mission would be the following:

> *Ensure DNS operators and supporting organizations have a security coordination center with sufficient expertise and resources to enable timely and efficient response to threats to the security, stability and resiliency of the DNS.*[21]

Three goals, with accompanying objectives, would to support the mission:

> **1**. **Goal:** Gain situational awareness and share information.
>
> **Objective:** Establish communications means and procedures to maximum number of players; exercise regularly.
>
> **2. Goal:** Improve coordination within the DNS operational community.
>
> **Objective:** Enable measurement and facilitate information sharing about the health, stability and resiliency of the DNS. Engage in appropriate situations: support contingency planning and exercises; undertake After Action Reporting (AAR). Engage with DNS-OARC and RISG, among others collaborators, to leverage expertise and existing operational response capabilities related to information sharing and analysis.
>
> **3. Goal:** Improve coordination with the broader security community.
>
> **Objective:** Establish relationships with key partners (CERTs, security researchers, key security lists, vendors, antivirus companies, law enforcement and governments); participate in contingency planning and exercises; engage in appropriate situations; undertake After Action Reporting (AAR).[22]

The proposed DNS-CERT's core responsibilities would be to provide proactive services—including education, training, contingency exercises, and continuous monitoring of DNS health—

---

[18] ICANN et al., "The Global DNS: Security, Stability & Resiliency Symposium: Summary, Trends, and Next Steps," April 2, 2009, http://www.gtisc.gatech.edu/pdf/DNS_SSR_Symposium_Summary_Report.pdf.

[19] ICANN, "DNS-CERT Business Case," 7–10.

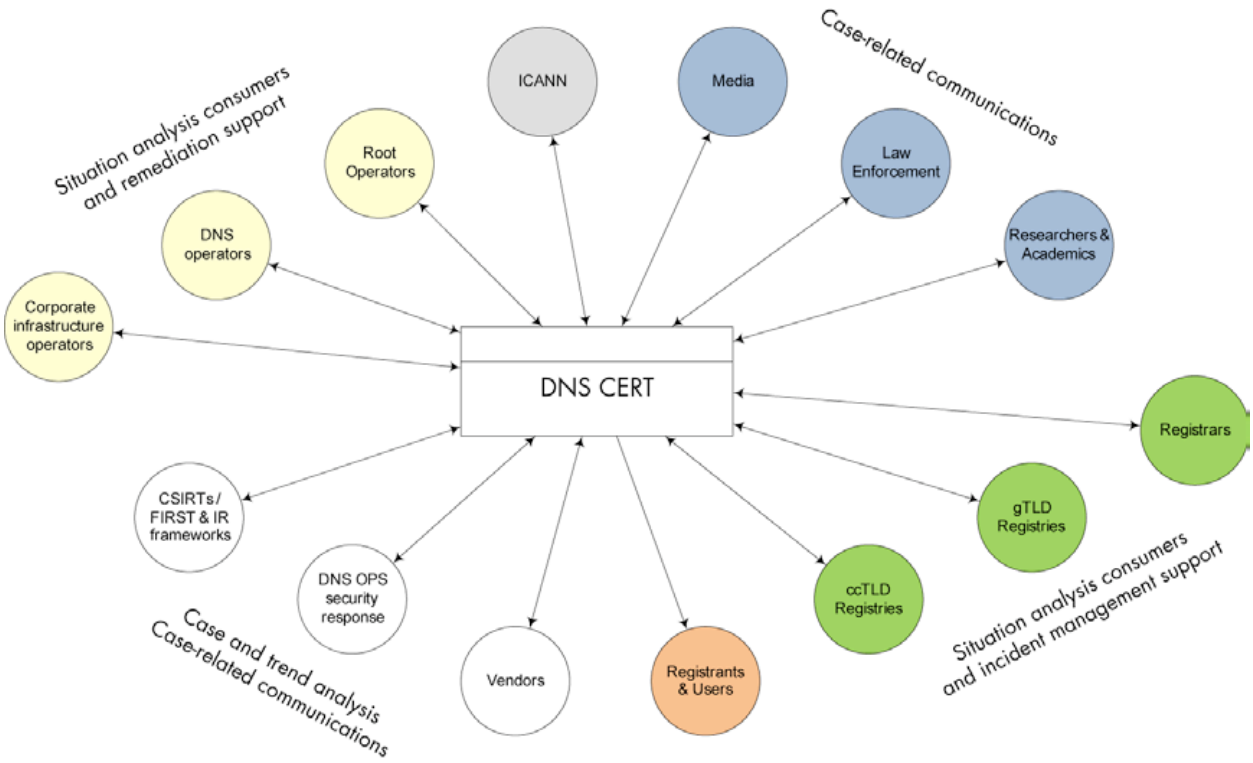
[20] Ibid., 9–10.

[21] Ibid., 11.

[22] Ibid., 10–11.

and reactive services, including serving as a hub for coordinating responses to DNS security incidents.[23]

Although the precise relationships with constituents and stakeholders remain undefined, the proposal envisions DNS-CERT as a central node in the gathering and distribution of information about DNS security threats, which it illustrates in the following diagram:[24]



ICANN lays out a series of steps to establish the organization, based on guidelines published by CERT/CC.[25] These steps—beginning with the identification of stakeholders and participants, and ending with the definition of roles and responsibilities—are described in the remaining portion of the proposal, although, as it notes, the proposal is intended as "the basis for further development of this effort through community support and feedback."[26]

---

[23] Ibid., 12.

[24] Ibid., 14.

[25] CERT/CC has published a set of guidelines for the establishment of new Computer Security Incident Response Teams (CSIRTs). See CERT/CC, "How does an organization start a CSIRT?," http://www.cert.org/csirts/csirt_faq.html#16.

[26] Ibid., 15.

The document ends with a brief overview of DNS-CERT's proposed funding sources, governance model, and organizational structure. An estimated $4.2 million annual budget is suggested for the organization, along with a staff of fifteen, a steering committee, and a Board of Governors. ICANN would serve as the project's initial sponsor "until the organization can stand on its own."[27] ICANN's role in the governance and operations of the proposed organization is not clearly articulated in the proposal. It reads:

> *Although we envisage the organization being established with initial support from ICANN, the DNS-CERT is intended to operate as much as possible as a freestanding organization, not directly dependent upon any one organization for its direction and operation. Therefore, to be successful, the DNS-CERT must be created with a governance structure that makes it accountable to key stakeholders and to the public at large.*

3 Timeline: Origins of the Controversy

ICANN began formal discussions with stakeholders about the DNS-CERT proposal in December 2009 (see pp. 4–5 above), when it was first included in the draft 2010–2013 strategic plan. Although the need for an organization similar to DNS-CERT had been identified at the February 2009 DNS symposium, there was no indication of a direct role for ICANN until December 1 of that year. ICANN has indicated that ten private consultations centered on DNS-CERT occurred during the following week, with a handful more taking place in January.[28]

The draft 2010–2013 ICANN Strategic Plan was posted for public comment on December 1, 2009 and closed on January 21, 2010.[29] Seven of the twenty-nine public comments received in response to the 2010–2013 strategic plan directly addressed DNS-CERT proposal.[30] These comments are generally supportive of ICANN's stated intention to develop a specific proposal related to DNS-CERT; the comments mainly address the overall need for better coordination in DNS security response efforts. The only openly critical comment came from Eric Brunner-Williams, who wrote:

> *I am concerned by the detail–free plan to copy–a–Cert....The point is, CERTs are not a given thing, they are a box into which some money and some purpose is put. We should decide how much money and what purposes, not just 'start a CERT'....If we are not careful, an 'ICANN CERT' will [be] captured, much like the ICANN SSAC function during the fast–flux hosting effort, by retail cops–and–robbers concerns that missed the fundamental issues of rapid update by registries as a fundamental tool of modern dns exploiting systems, and zero effective cost of registration, again by modern dns exploiting systems. At that point we*

---

[27] Ibid., 16.

[28] ICANN, "Summary of Consultations and Comments related to the ICANN Global DNS-CERT Business Case," May 24, 2010, http://www.icann.org/en/public-comment/summary-analysis-strategic-ssr-initiatives-and-dns-cert-business-case-24may10-en.pdf.

[29] ICANN, "Public Comment Requested on Draft 2010-2013 Strategic Plan," December 1, 2009, http://www.icann.org/en/announcements/announcement-01dec09-en.htm.

[30] See received public comments: ICANN, "[stratplan-2010] Chronological Index," http://forum.icann.org/lists/stratplan-2010/.

> *would have a 'CERT' which 'makes the suits smile' but does us no good when competent and motivated programmers target infrastructure.*[31]

ICANN published its "DNS-CERT Business Case" and its "Proposed Strategic Initiatives" for public comment on February 12, 2010. Until March 25, however, only one comment had been submitted, correcting a factual detail in the strategic initiatives document.[32]

At least as far as publicly accessible materials are concerned, the DNS-CERT proposal remained largely uncontroversial until ICANN's meeting in Nairobi in March 2010. During a joint GAC–Board meeting on March 9, the CEO of ICANN, Rod Beckstrom, conveyed a series of warnings about the health of the global DNS.[33] "What I want to share with you," he said,

> *as a representative of many countries of the world is that the domain name system is under attack today as it has never been before. I have personally consulted with over 20 CEO's of the top Registries and Registrars globally, all of whom are seeing increasing attacks and complexity of attacks and who are extremely concerned.*
>
> *The domain name system is more fragile and vulnerable today than it has ever been. It could stop at any given point in time literally. It has never stopped, it has been slowed down through attacks and the Kominsky exploit that was disclosed only 18 months or so ago could have been used to fundamentally cripple the domain name system. That system is used 1 trillion times per day and your economies depend upon it. It can stop or it can materially be damaged and harmed. It is under attack. . . .*
>
> *I'm sharing this because I'm gravely concerned and we need your help. So we're going to be asking you for your advice on domain name security and on the DNS SERT and what can be done and particularly to learn the lessons from you as well. What has been accomplished in your countries?*[34]

Mr. Beckstrom's remarks provoked strong reactions from the ICANN community. After the Nairobi meetings, ICANN extended the public comment period on the DNS-CERT Business Case and its Proposed Strategic Initiatives documents to April 14, 2010.[35] In total, ICANN received 13 comments on the strategic initiatives document and 25 comments on the DNS-CERT proposal. Included in the comments were formal letters from the GNSO, ccNSO, and ALAC. (See below,

---

[31] Eric Brunner-Williams, "On 'DNS-CERT concept development' and '100% uptime,'" January 28, 2010, http://forum.icann.org/lists/stratplan-2010/msg00027.html.

[32] Till Doerges, "Comment: Proposed Strategic Initiatives for Improved DNS Security, Stability and Resiliency (SSR)," February 27, 2010, http://forum.icann.org/lists/strat-ini-ssr/msg00000.html.

[33] ICANN, "Transcript of the GAC Board Meeting," March 9, 2010, http://gac.icann.org/system/files/transcript-gac-board-meeting-09mar10-en.pdf, 26.

[34] This passage is copied verbatim from ICANN's unedited transcript of the meeting.

[35] The original source of the request to extend the public comment deadline is unclear. The ICANN summary of the public comments cites "requests from the community" with no further detail (see below, n. 40). The first public comment submitted on the DNS-CERT business case—a joint letter from the Chairs of the gNSO, ccNSO, and ALAC—reads, "We welcome the extension of the current public comment periods on ICANN's proposed strategic initiatives for improved DNS security, stability and resiliency and the global DNS-CERT business case document to 14 April 2010" (see above, n. 57).

"Reactions from the ICANN Community," for an overview of the substance of commentary from the ICANN community.)

The comments generally take the form of formal input from organizations of various types. Only four individuals submitted comments. Three of ICANN's advisory committees and supporting organizations submitted comments: ALAC, ccNSO, and gNSO. Five commercial stakeholders submitted comments: AT&T, Net Choicer, PayPal, PRESENSE Technologies GmbH, and USCIB. Governments, national CERTs, registry operators, TLD associations, and other Internet organizations submitted the remainder of the comments.

On April 6–7, ICANN hosted a private, invitation-only workshop on DNS security in Washington, D.C..[36] Workshop participants—comprised of representatives from various corners of the DNS security community—discussed a series of real and hypothetical DNS security scenarios in order to identify gaps in existing security response mechanisms. A draft of the findings of the workshop was posted for public comment on May 24, 2010.[37] The draft report includes a summary of the workshop proceedings, a list of takeaways, and a dissenting "minority report" from other workshop participants. ICANN solicited public comments on the draft report through July 2, during which it received six comments in total.[38]

On May 24, ICANN published two additional documents related to DNS-CERT.[39] The first was a sixteen-page summary of public comments received in response to the strategic initiatives and the DNS-CERT business case.[40] This summary provides synopses of all public comments received, highlighting three overarching themes: (1) the need for a "deeper understanding of the threats and risks to the DNS" before a specific DNS-CERT proposal can be usefully proposed; (2) the need for more information about existing security response mechanisms and opportunities to enhance existing efforts; and (3) the view that establishing a DNS-CERT may be beyond ICANN's mission as a technical coordinating organization.[41]

The second document published on May 24th was a 26-page record of ICANN's consultations regarding DNS-CERT, divided into three areas: (1) consultations prior to the publication of the business case; (2) consultations related to the draft 2010–2013 strategic plan, of which DNS-CERT was a part; and (3) inputs received after the business case was posted for public review.[42] The consultation record shows several private consultations with DNS stakeholders prior to the

---

[36] ICANN, "April 2010 DNS-CERT Operational Requirements and Collaboration Analysis Workshop Report," May 24, 2010, http://www.icann.org/en/topics/ssr/dns-cert-collaboration-analysis-24may10-en.pdf.

[37] ICANN, "Public Comment: April 2010 DNS-CERT Operational Requirements & Collaboration Analysis," May 24, 2010, http://www.icann.org/en/announcements/announcement-24may10-en.htm

[38] ICANN, "dns-collab-analysis," May 24, 2010, http://forum.icann.org/lists/dns-collab-analysis/.

[39] ICANN, "Public Comment: April 2010 DNS-CERT Operational Requirements & Collaboration Analysis," May 24, 2010, http://www.icann.org/en/announcements/announcement-24may10-en.htm.

[40] ICANN, "Summary & Analysis of Comments on the Security Strategic Initiatives and Global DNS-CERT Business Case paper," May 24, 2010, http://www.icann.org/en/public-comment/summary-analysis-strategic-ssr-initiatives-and-dns-cert-business-case-24may10-en.pdf.

[41] Ibid., 1–2.

[42] ICANN, "DNS-CERT Consultation record," May 24, 2010, http://www.icann.org/en/topics/ssr/dns-cert-consultation-record-24may10-en.pdf.

publication of the business case, as well as seven public comments regarding the initial suggestion for DNS-CERT in the 2010–2013 strategic plan.

4 Reactions from the ICANN Community

The following sections describe three areas of the ICANN community's reactions to the DNS-CERT proposal and Mr. Beckstrom's Nairobi remarks: (1) issues of substance, including ICANN's assessment of the current state of DNS security and the details of the solution it proposes; (2) the extent to which DNS security operations fall within ICANN's mandate; and (3) issues of procedure, including openness, transparency, public input, and stakeholder participation.

4.1. Substantive Issues

The most immediate substantive issue is the CEO's characterization of the fragility of the DNS. Many stakeholders—including participants from the Nairobi meeting—felt that ICANN's CEO exaggerated the threats facing DNS security and understated the effectiveness of existing security response mechanisms. Two days after the meeting, for instance, Chris Disspain (on behalf of the ccNSO) published a sharply-worded letter, calling Mr. Beckstrom's remarks "inflammatory" and "alarming."[43] The next month, Lynn St. Amour wrote to the ICANN Board on behalf of the Internet Society (ISOC), stating that Mr. Beckstrom's warning about the fragility of the DNS "has raised concern among many, yet the facts to substantiate that statement have not been made available to the community."[44] "[M]any recognized experts in DNS security," she wrote,

> *…are on record saying that they do not agree that the Internet is suddenly experiencing dramatically greater or new types of attack, or that the DNS, or the Internet itself, are likely to collapse at any moment.*

Kevin Murphy at *Domain Incite* unsympathetically called the remarks "part call to arms, part Chicken Little."[45] Mr. Byron Holland, CEO and President of the Canadian Internet Registration Authority, wrote:

> *the tone of the message could be considered somewhat inflammatory….Many people in the room felt that Beckstrom was speaking out of turn and disregarding the work the community is already undertaking to ensure the stability and the security of the DNS."*[46]

Reactions to the substance of the DNS-CERT proposal—as expressed in public comments to ICANN and observations made in interviews for this case study—have varied substantially,

---

[43] ICANN, "Letter from Chris Disspain to Rod Beckstrom", March 11, 2010, http://www.icann.org/correspondence/disspain-to-beckstrom-11mar10-en.pdf, 1.

[44] ICANN, "Letter from Lynn St. Amour to ICANN Board of Directors," April 14, 2010, http://www.icann.org/correspondence/amour-to-dengate-thrush-14apr10-en.pdf, 1.

[45] Kevin Murphy, "Beckstrom: DNS is under attack," *Domain Incite*, March 11, 2010, http://domainincite.com/beckstrom-dns-is-under-attack/.

[46] Byron Holland, "DNS-Community Emergency Response Team, or CERT," *Public Domain*, March 26, 2010, http://blog.cira.ca/2010/03/dns-community-emergency-response-team-or-cert/.

ranging from cautious support on one end of the spectrum to vigorous skepticism on the other. These reactions center on two main questions: first, whether an organization such as DNS-CERT is necessary, given the current landscape of DNS security risks; and second, whether the proposed organization, as specified in ICANN's business case, is appropriately conceived.

ICANN's argument—as expressed in the Proposed Strategic Initiatives and the DNS-CERT business case, and outlined by its CEO in Nairobi—is straightforward: an increase in the frequency and complexity of attacks on the DNS has led to the need for a centralized body to coordinate proactive and reactive responses to DNS security threats. Community members, in contrast, display a range of reactions to ICANN's characterization of the risks facing DNS security as the following statements illustrate.

The Council of European National Top-level Domain Registries ("CENTR") wrote that "ICANN should focus first on sharing information" about security threats and existing response capabilities "in order to build a common assessment of risks and weaknesses."[47] Lynn St. Amour, quoted above, questioned whether ICANN's assessment aligned with the judgment of the DNS security community. In his response to Ms. St Amour, Mr. Beckstrom echoed the call for more information, but shifted some of the burden to the DNS community: "We have…been informed," he writes,

> *that many registries have experienced increases in botnet attacks; but none have, so far, been willing to come forth and share their data….It would be very helpful if we could work together to gather additional data on attacks on registries, and on how that information is being shared and measured on a global basis. It would greatly contribute to our joint efforts to evaluate the seriousness of the threat and coordinate our forces more effectively to meet it.*[48]

Numerous community members have expressed the view in interviews and public comments, which ICANN appears to share, that further information is needed before the fragility of the DNS can be accurately assessed.

The second point of contention is whether, given existing knowledge about the threats to DNS security, a centralized DNS-CERT–like organization should be established. As ICANN's CEO made clear in his letter to ISOC, ICANN considers existing security response mechanisms to be largely inadequate: "I am not convinced that we are yet doing enough," wrote Mr. Beckstrom, "or moving quickly enough."[49] Many, however, expressed concern that the model ICANN describes in its DNS-CERT proposal is not an optimal approach. For instance, the Registries Stakeholder Group, in a unanimously-approved statement, argued that existing DNS security response mechanisms are well-established and often highly robust. The responses to the Conficker worm and the Kaminsky

---

[47] CENTR, "CENTR Comment in response to the consultation on the Domain Name System-Computer Emergency Response Team (DNS-CERT) Business Case," March 24, 2010, http://forum.icann.org/lists/dns-cert-proposal/pdfPZE4i_GvRI.pdf.

[48] Rod Beckstrom, "Letter from Rod Beckstrom to Lynn St. Amour," June 18, 2010, http://www.icann.org/correspondence/beckstrom-to-st-amour-18jun10-en.pdf.

[49] Ibid.

vulnerability, as one example, "demonstrated a very effective level of coordination, information sharing, and action."[50] Similarly, CENTR argues in its comments that the community's response to Conficker is

> *a perfect illustration of the fact that security relies fundamentally on cooperation and collaboration amongst different experts and that's how the current security network is build up. In such a framework different security incidents can be addressed more effective [sic] and on the long run much more efficient than with the proposed concept of a CERT focusing on one single area with potential security problem, like DNS.*[51]

Ms. St. Amour agrees with Mr. Beckstrom about the importance of DNS security, but, regarding the specifics of ICANN's DNS-CERT proposal, notes that "we are concerned that the current proposals do not show convincingly that there has been a full analysis of alternate approaches."[52]

On the other hand, some interviewees from the cybersecurity and DNS operational communities have endorsed the idea of a centralized CERT.[53] Much of the impetus for the idea derived from the first "Global DNS Security, Stability, & Resiliency Symposium" of February 2009. The report from the symposium argues that

> *the DNS technical, operational, and security communities are disjointed and in need of a dedicated information sharing and incident response capability. These functions are generally performed by CERTs, but no such capability exists expressly for the DNS community."*[54]

Similarly, Paul Vixie, founder of DNS-OARC, has advocated publicly for the creation of a DNS-CERT organization: "We need a 24x7 monitoring and response and coordination function," he writes, "with full time analysts looking at real time DNS events and participating in a global mesh of DNS NOCs."[55] Although DNS security was originally a component of OARC's mandate, Mr. Vixie writes that "Somewhere along the way we got distracted. . . . DNS-OARC was a huge undertaking, and one that I significantly underestimated."

4.2 ICANN's DNS Security Mandate

ICANN proposes to oversee the governance, operations, and funding (of the nontrivial $4.2 million annual budget) of the organization "until the DNS-CERT's initial operational capability is

---

[50] RySG, "Registries Stakeholder Group Statements Regarding the 'Proposed Strategic Initiatives for Improved DNS Security, Stability and Resiliency (SSR)' and 'Global DNS-CERT Business Case,'" April 14, 2010, http://www.gtldregistries.org/webfm_send/79.

[51] CENTR, "CENTR Comment," 1.

[52] Lynn St. Amour, "Letter from Lynn St. Amour to Rod Beckstrom," 2.

[53] Interview, September 2010.

[54] ICANN et al., "The Global DNS Security, Stability, & Resiliency Symposium: Summary, Trends, and Next Steps," April 2, 2009, http://www.gtisc.gatech.edu/.../DNS_SSR_Symposium_Summary_Report.pdf.

[55] Paul Vixie, "Perspectives on a DNS-CERT," March 12, 2010, http://www.isc.org/community/blog/201003/perspectives-dns-cert.

achieved."[56] However, the proposal does not stipulate how ICANN will determine when this capacity has been reached; in addition, the permanent structure of the organization's governance, operations, and funding remain undefined.

Many community members have rejected the idea of ICANN playing an operational role in DNS security. In a joint letter, the gNSO, ccNSO, and ALAC wrote that "In general terms, ICANN plays a coordinating, non-operational role in managing Internet naming and numbering resources. However, we are concerned that, in this particular case, ICANN's proposed role remains unclear."[57] Ms. St. Amour writes, "we continue to be concerned that ICANN may be broadening out from its principle mandate as coordinator of the global resource that is the domain name system into the management of new and peripheral operational functions."[58] The Registries Stakeholder Group provides a similar argument:

> *ICANN points to its Bylaws and the Affirmation of Commitments (AoC) to define its responsibility to ensure the stable and secure operation of the Internet's unique identifier systems. In general terms, ICANN plays a coordinating, non-operational role in managing Internet naming and numbering resources. However, in the SSR and DNS-CERT documents, ICANN's proposed role seems both unclear and over-broad. The RySG shares the concern already voiced by some in the community that ICANN's role in these potential initiatives and undertakings not cross over into an operational capacity. ICANN should undertake activities that are consistent with its limited technical coordination role. There should be a systematic examination of that role in relation to the SSR and DNS-CERT, using existing community processes. ICANN must be able to explain its remit and work within it, rather than expanding its mission to meet unrealistic or uninformed expectations, or into areas best filled by other entities.*[59]

The Registries Stakeholder Group points to the third of ICANN's core values, as stated in the ICANN Bylaws, to substantiate its argument that ICANN should avoid playing an operational role wherever possible.[60] This core value is:

> *To the extent feasible and appropriate, delegating coordination functions to or recognizing the policy role of other responsible entities that reflect the interests of affected parties.*[61]

The concerns regarding ICANN's DNS security mandate may also stem from uncertainty surrounding its intentions. One interviewee described DNS security as an issue on which ICANN has "real legitimacy" and an area where it could successfully facilitate a bottom-up decision-making process among its full range of stakeholders. Lack of clarity regarding ICANN's

---

[56] ICANN, "DNS-CERT Business Case," 15–16.

[57] gNSO, ccNSO, and ALAC, "Joint letter from Chairs of the gNSO, ccNSO and ALAC," March 25, 2010, http://gnso.icann.org/correspondence/chairs-letter-re-dns-cert-25mar10-en.pdf.

[58] Lynn St. Amour, "Letter to Rod Beckstrom," 2.

[59] RySG, "Registries Stakeholder Group Statements," 2.

[60] RySG, "Registries Stakeholder Group Statements."

[61] ICANN, "Bylaws," Section 2.3.

motivations, however, has made the DNS-CERT proposal "feel like a land grab," causing a "missed opportunity" in the realm of DNS security, according to this interviewee.[62]

The ambiguity surrounding ICANN's role in the proposed organization is displayed in the ICANN CEO's letter to ISOC. "[W]e have never proposed that ICANN should be the operator of such a CERT," he wrote, "but rather have asked the community for their view on the proposal that such a global DNS CERT should be established."[63] In the same paragraph, however, he wrote, "I think that ICANN should probably have a role in the operation of such a CERT, if required by the community, but in any case, we look forward to the continuing discussions." The DNS-CERT business case does not clearly describe whether ICANN should be the operator or merely have a role in the operation of the CERT.

4.3 Procedural Issues

The review of a diverse set of publicly available materials (see above), as well as a series of interviews, suggests that the root of the DNS-CERT controversy is—to varying degrees—attributed to factors such as limited transparency in the development of the DNS-CERT proposal, the perceived absence of opportunities for public input prior to the publication of the detailed business case, and the apparent lack of adequate prior consultation with the community of DNS security stakeholders.

4.3.1. Openness and Transparency

As the above reactions indicate, a perceived lack of openness appears to have fueled additional concerns. Reportedly, DNS stakeholders were not informed that Mr. Beckstrom would be making any remarks related to DNS security issues prior to the Nairobi meeting.[64] This claim is supported by the fact that DNS security was not mentioned on the GAC meeting agenda.

ICANN's CEO opened his remarks with the claim that he had "personally consulted with over 20 CEO's of the top Registries and Registrars globally." As one interviewee noted, however, Mr. Beckstrom has refused to disclose the names of the registry and registrar members with whom he consulted. Furthermore, ICANN has conducted surveys within governments about DNS security issues, unbeknownst to members of the DNS communities within those countries.[65] As Mr. Disspain expressed in his letter from March 11, 2010, the Nairobi remarks have, to varying degrees, undermined the credibility of ccTLD operators on DNS security issues in the eyes of governments, implanting unnecessary barriers to DNS policy goals. One interviewee suggested that ICANN's handling of the process led to the demise of an idea that otherwise carried a good amount of legitimacy and may have led to productive collaborations between ICANN and the DNS security community.[66]

---

[62] Interview, September 2010.

[63] Rod Beckstrom, "Letter to Lynn St. Amour," 2.

[64] Interview, September 2010.

[65] Interview, September 2010.

[66] Interview, September 2010.

Several public comment submissions expressed similar concerns about a general lack of openness and transparency throughout the DNS-CERT process, generating confusion and mistrust about ICANN's intentions.

4.3.2 Public Input and Stakeholder Participation

Interviews and public materials have raised the issue of the degree to which ICANN solicited and addressed input from DNS security stakeholders and the public at large during the DNS-CERT process. Mr. Disspain, for instance, wrote:

> *Our concerns lie not with your focus on security issues, but with your precipitated unilateral analysis of such an important issue and the public and inflammatory manner by which your views have been communicated.*
>
> *We agree that, as CEO of ICANN, it is your responsibility to address these issues, but it is equally your responsibility to do so through ICANN's bottom-up, consensus-based multistakeholder model. It is also the responsibility of those in positions of influence within ICANN to show due care when making statements on complex, cross-cutting issues to ensure effective analysis and stakeholder engagement without unnecessary confusion or concern.*[67]

Ms. St. Amour echoes Mr. Disspain in expressing "strong concerns" about the means by which the DNS-CERT proposal was developed, arguing that ICANN has failed to demonstrate a commitment to "open, freely accessible, multi-stakeholder, and knowledge-based processes."[68] In addition to a lack of stakeholder involvement, Ms. St. Amour also contends that ICANN's security-related proposals:

> *do not show convincingly that there has been a full analysis of alternate models. ISOC believes that the proposals have been put forward prematurely—without the full backing of the supporting organizations and advisory committees in ICANN, nor with the broader community, including the technical community.*[69]

At the *Internet Governance Project*, Milton Mueller blogged:

> *One moral of this story is that there is still a residue of suspicion within the traditional internet technical community about ICANN and its ambitions. Another is that an ICANN CEO who challenges them or who makes them look as if they aren't doing their jobs right will have hell to pay.*

One interviewee commented that "ICANN's openness is commendable," referrring particulary to the public comment period for both the "Proposed Strategic Initiatives" and the "DNS-CERT Business Case" and ICANN's willingness to extend the deadline at the public's request. The

---

[67] Chris Disspain, "Letter from Chris Disspain to Rod Beckstrom."

[68] Ibid., 2.

[69] Ibid.

interviewee expressed concern, however, that ICANN "hasn't done much to show that it's responsive to input from the public."[70]

Some DNS stakeholders have expressed strong concern about the lack of opportunities to participate prior to the Nairobi meeting. For instance, the ccNSO's letter to the ICANN CEO reads:

> *Although ICANN's DNS-CERT business plan acknowledges existing security stakeholders such as CERT/CC and the CERT network, FIRST and DNS-OARC and other involved parties such as RIRs, DNS Root Operators, registrars and ccTLD and gTLD registries, little effort appears to have been made to engage these groups in developing the DNS-CERT proposal. This lack of dialogue leads to the potential for duplication of efforts and confusion, rather than clarification, of specific roles and responsibilities.*[71]

Interviews and written submissions by ICANN staff solicited for this case study offer a markedly different perspective on the opportunities for input and stakeholder involvement during the development of the DNS-CERT proposal. ICANN staff point to a long series of consultations and public submissions dating to early 2009, during which they consulted with numerous networking and security experts (see Appendix 1 for a timeline and references). In the 2009 DNS symposium held in Atlanta, participants explicitly identified the need for a centralized CERT-like coordinating body. The report from the 2010 DNS symposium, however—which occurred prior to the Nairobi meeting—took a more measured position, emphasizing above all the need for further research and information-sharing before a specific program could be proposed.

ICANN's consultation records show that, prior to the Nairobi meeting and the publication of the DNS-CERT proposal, participation from the ICANN community at large was minimal. ICANN consulted with a range of DNS security stakeholders, but the majority of interactions with the DNS community took place in private consultations. The draft 2010–2013 strategic plan suggests the creation of a DNS-CERT project, but offers no details to which the public could respond.

After Nairobi, many stakeholders continued to be dissatisfied with the lack of opportunities to participate.[72] ICANN's April 6–7 workshop in Washington, D.C. aimed to convene a range of participants from the DNS security community specificially to share information and identify the gaps in current DNS security measures. However, the workshop was held privately, and fewer than thirty participants were invited,[73] causing some to view the workshop with skepticism rather than enthusiasm.

---

[70] Interview, September 2010.

[71] ccNSO, "Comments on ICANN DNS-CERT Proposal," 1.

[72] Interview, September 2010.

[73] ICANN, "April 2010 DNS-CERT Operational Requirements and Collaboration Analysis Workshop Report" (see the list of participants at the end of the report).