

**Securing critical Internet resources: Influencing standards through delegation and social networks**

**Brenden Kuerbis**  
Syracuse University, USA

The Internet is successfully interconnected through the global coordination of 1) the underlying technical protocols or “standards” and, 2) management of critical Internet resources (CIRs).<sup>1</sup> It is widely perceived that the decentralized governance institutions that determine Internet protocols and coordinate CIRs are insulated from, or even resistant to the state influence. However, this view has come under increasing scrutiny. Several powerful governments have conveyed concerns about critical Internet resources. The United States government has long expressed its desire to secure the Internet’s Domain Name System (DNS) and routing system.<sup>2</sup> And the World Summit on the Information Society and U.N. Internet Governance Forum highlighted other governments, notably the BRICs, concerns about the management of critical Internet resources.<sup>3</sup> But, despite this attention, little is understood about how governments actually influence the development of Internet protocols affecting CIRs.

*Research questions*

My dissertation research focuses on the security of critical Internet resources, specifically efforts to develop protocols to secure the Domain Name System and Internet routing.

*RQ1:* How do USG gov’t agencies, as politically driven actors, integrate domestic objectives into Internet standards dealing with security of CIRs?

*RQ2:* What is the impact on and response by other actors to these efforts?

---

<sup>1</sup> CIRs are globally unique logical network identifiers, including top-level domain names (TLDs) and their associated resource records, Internet protocol (IP) addresses, and Autonomous System Numbers (ASNs).

<sup>2</sup> Includes the 1998 Presidential Decision Directive No. 63 (PDD-63), superseded in 2003 by Homeland Security Presidential Directive No. 7 (HSPD-7), which required federal agencies and departments to develop methods and technologies to protect all critical infrastructures and key resources of the government and economic sector. The 2003 *National Strategy to Secure Cyberspace* (available at [http://www.dhs.gov/xlibrary/assets/National\\_Cyberspace\\_Strategy.pdf](http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf)), and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (available at [http://www.dhs.gov/xlibrary/assets/Physical\\_Strategy.pdf](http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf)) explicitly call for securing the DNS as well as Internet routing.

<sup>3</sup> For discussions of the World Summit on the Information Society and how U.S. control of the DNS root became a geopolitical controversy, see Mueller, M., *Networks and States: The global politics of Internet governance*, MIT Press (2010); David Souter, (2004) *The view from the summit: a report on the outcomes of the World Summit on the Information Society*. Info - The journal of policy, regulation and strategy for telecommunications, 2004, 6, 1, 6-11.

*RQ3*: How are global IG arrangements adapting to accommodate differing objectives in securing CIRs?

These questions are informed by several bodies of literature, including the economics and political economy of standardization<sup>4</sup>, network economics (e.g., bottlenecks and externalities)<sup>5</sup>, and the history of national security influence in communications networks<sup>6</sup>. But, given the decentralized nature of Internet governance, the principal-agent literature on delegation<sup>7</sup> and social networks is particularly useful. I argue that the concept of delegation, including maintaining *ex-ante* and *ex-post* controls, is integral to the social networks that coalesce around Internet governance institutions. By identifying and delegating to individual agents within these social networks, principals (i.e., government agencies) can accomplish outcomes consistent with their objectives. In this manner, “multiple principal–multiple agent constellations matter for the way in which control can be exercised...in interactions between government and governance.” (Heritier and Lehmkuhl 2008, pg. 5)

#### *Working hypotheses*

We should expect to see USG agencies influence Internet standards and policy efforts affecting the security of CIRs in ways that reflect and reinforce the existence of resource bottlenecks controlled by the United States, thereby allowing it to maintain control over those critical Internet resources. To accomplish this, USG agencies engaged the social networks that coalesce around the relevant Internet standards and policymaking institutions dealing with securing critical Internet resources (i.e., IETF, ICANN, RIRs). USG agencies identified influential individuals in these social networks and delegated decision-making authority to them. Therefore, we should observe that:

*H1*: Individual centrality in these social networks will be positively related to instances of a USG agency establishing a contract with that individual (or their employer) to provide services related to Internet standards work concerning the security of CIRs.

*H2*: Authorship of IETF Working Group documents by these individuals will be positively related to the advancement of those documents to RFC status.

By engaging these social networks and delegating to individuals, USG agencies influence Internet standards and achieve outcomes concerning critical Internet resources consistent with its multiple and often conflicting interests, while simultaneously mitigating claims to sovereignty

---

<sup>4</sup> For economics of standardization see Farrell and Saloner 1988; Besen and Saloner 1989, 1994; Greenstein 1992; Besen and Farrell 1994. For examinations of the political economy of standardization see e.g., Crane 1979; Hart 1994; Galperin 1992; Fromkin 2002; Camp and Vincent 2004.

<sup>5</sup> See Katz and Shapiro 1985, 1986; David and Greenstein 1989; Arthur 1989; Mueller 2002; Cowhey & Mueller 2008.

<sup>6</sup> See Deasai 2008; Headrick 1993; Snow 1985; Mueller 1991; Diffie and Landau 1998.

<sup>7</sup> See Hawkins, Lake, Nielson and Tierney 2006

expressed by other governments. However, delegation to individuals in social networks as a method of influence and control over the global Internet standards that impact critical Internet resources is limited in its usefulness. As the Internet continues to grow as a global communications medium and in economic importance for other countries and non-state actors, those parties affected by the outcomes of delegation pursue tactics to compensate for imbalances in the distribution of power among governments and between states and non-state actors, thereby challenging its effectiveness. Because of this we should additionally expect to observe the following corollaries:

*C1*: Pressure to renegotiate the relationships that govern resource bottlenecks, or more likely,

*C2*: Other parties adapt Internet protocols or policies governing critical Internet resources to preclude resource bottlenecks and meet the preferences of a larger set of impacted actors.

#### *Research design*

Two exploratory case studies, examining the IETF's DNSEXT and SIDR/RPSEC Working Groups, will be used to evaluate the above hypotheses (see Table 1, below). In both cases, the protocols developed implement globally unique digital signatures to secure CIRs and rely upon a hierarchical "chain of trust" which follows the organization of the extant governance structure(s) to authenticate the signatures, therefore raising issues of control.<sup>8</sup> Archival material will be collected and participants interviewed, with social network analysis conducted to identify central individuals and affiliated organizations.

#### *Preliminary results*

Internet-Drafts (I-Ds) and Request For Comments (RFCs) produced by the participants of the DNSEXT and SIDR Working Groups between 1999-2008 and 1998-2009 respectively were examined. Initial results are consistent with a theory that United States government agencies are learning to influence Internet standards that secure critical Internet resources through delegation relationships and engaging the social networks that coalesce around Internet standards and policy institutions. Highly central individuals, and the organizations they were affiliated with, were identified and played key roles in the formation and deployment of the DNSSEC and RPKI standards.

---

<sup>8</sup> For the DNS, this is ICANN/IANA, TLD registries, registrars, registrants. For IP addresses this ICANN/IANA, regional Internet registries (ARIN, RIPE, APNIC, LACNIC, AFNIC), LIRs and enterprises.

<b>Case (CIR)</b>	<b>IETF Working Group(s)</b>	<b>Main Protocol(s) Developed</b>	<b>Protocol(s) Purpose</b>	<b>Period of Study</b>
1. Securing the Domain Name System (TLDs)	Domain Name System Extensions (DNSEXT)	DNS Security Extensions (DNSSEC); NSEC3	Add data integrity and source authentication to DNS query responses	1999-2008
2. Securing Inter-Domain Routing (IP addresses, ASNs)	Secure Inter-Domain Routing (SIDR); Routing Protocol Security Requirements (RPSEC)	Routing Public Key Infrastructure (RPKI); Secure Border Gateway Protocol (sBGP); Secure Origin Border Gateway Protocol (soBGP)	Provide data integrity and authentication for IP address blocks; provide data integrity for ASN routing objects (i.e., IP address advertisements)	1998-2009

**Table 1: Cases Selected**