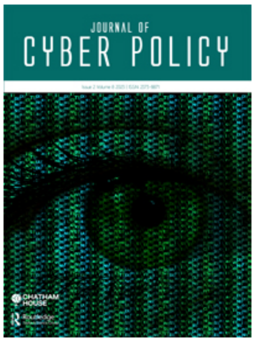

Journal of Cyber Policy

ISSN: 2373-8871 (Print) 2373-8898 (Online) Journal homepage: www.tandfonline.com/journals/rcyb20

Special issue on domain name system (DNS)

James Burrell

To cite this article: James Burrell (2023) Special issue on domain name system (DNS), Journal of Cyber Policy, 8:2, 137-141, DOI: 10.1080/23738871.2024.2312922

To link to this article: https://doi.org/10.1080/23738871.2024.2312922

Published online: 09 Feb 2024.

JOURNAL OF CYBER POLICY
2023, VOL. 8, NO. 2, 137–141
https://doi.org/10.1080/23738871.2024.2312922

Routledge
Taylor & Francis Group

GUEST EDITORIAL

Special issue on domain name system (DNS)

ARTICLE HISTORY Received 28 January 2024; Accepted 29 January 2024

Advancements in technologies that utilise global information infrastructures remain dependent on foundational technical standards, protocols and services to establish and maintain network communications. These foundational components were devised during the developmental stages of the internet and, despite incremental improvements, there are challenges with the ability to support the technology and policy requirements for expanding internetworking services and applications.

This special issue of the *Journal of Cyber Policy* focusses on the Domain Name System (DNS) and the factors that impact governance, resilience, security and privacy. The DNS provides critical internetworking services responsible for the translation or resolution of internet domain names to corresponding Internet Protocol (IP) addresses that enable the reliable exchange and delivery of network data. The DNS operates as a decentralised open-source hierarchical model that was designed to provide some degree of scalability, reliability and resiliency. As with other decentralised models, these characteristics provide significant advantages, but also present certain limitations with respect to control, validation and trust. They therefore contribute to broader consolidation, security and privacy issues. The recent occurrences of malicious attacks, malfunctions and misconfigurations of DNS services that resulted in global internet outages that directly and indirectly lead to economic and national security concerns related to stability and security. Despite having one of the most critical roles in the reliable operation of the internet, the DNS operates in relative transparency with no foundational level of security.

The continued reliance of existing and emerging internet services on this foundational infrastructure requires the re-evaluation of the technologies and governance essential to support digital technology transformation and the global digital economy. The development of emerging internetworking services and applications that include mobile, cloud, wearable and the Internet of Things (IoT) devices are blockchain and non-fungible token (NFT) services. An article in this special issue by Georgia Osborn and Nathan Alan explores the increasing use blockchain technology, specifically blockchain domain names, that are currently non-interoperable with the DNS. This research highlights how blockchain and other technologies are outside the traditional scope of internet governance and provides recommendations to address the challenges introduced by this technology.

The governance of the DNS is complex. Its multi-stakeholder consensus-based processes include transnational government, private sector, academic and research communities. Differing views on internet governance have been debated for decades and, although alternative models have been contemplated, many would represent increased intergovernmental control, influence or alignment. In some instances, the increased governmental control of DNS or other functions of the internet could lead to actions that prioritise alignment with certain national laws that could result in global policy implications related to censorship, security and privacy. The article by James Mortensen and Samuel Bashfield examines the administration, management and regulation of top-level domains in several colonial territories and the observed implications of increased centralised government management.

The United States initially had an influential role in internet governance based primarily on the development of the ARPANET and subsequently the internet. As a national government, the US maintained oversight and a level of control over the Internet Assigned Number Authority (IANA) and subsequently ICANN, which were responsible for management of the IP address and domain namespace. In 2016, the US transitioned its oversight and control in its entirety to ICANN which currently operates as an independent global organisation with a distributed governance model. In furtherance of the evaluation of DNS governance, the article by Derrick Cogburn, Theodore Ochieng and Haiman Wong analysed ICANN Uniform Domain-Name Dispute Resolution Policy (UDRP) using data available from the DNS Research Federation Data Analytics Platform that validated the increase in the number of disputes and stability of UDRP processes.

The complexities associated with DNS governance extend beyond the development and improvement of technical specifications that define the functionality and interoperability of internet communications. The Internet Engineering Task Force (IETF) is responsible for the development and recommendations for technical standards and protocols with a structure that supports open participation and coordination with other governance organisations. The implementation of these technical recommendations can significantly influence the development, support and advancement of policy related considerations. As an example, the technical specifications for encryption standards and protocols have a significant impact on the formulation of policies that impact security and privacy for governments, organisations and civil society.

The DNS was designed to provide substantial resiliency, with various technical and configuration measures crucial to effective operation and recovery of DNS. There are significant threats to the operation of DNS from malicious activities, but DNS vulnerabilities have been demonstrated by both intentional and unintentional actions. In 2021, a global interruption of access to specific social media services impacted approximately three billion users for over five hours. The incident extended to multiple social and messaging services attributed to cascading DNS and networking routing protocol configuration failures of interconnected systems. This service interruption was the most significant disruption at this scale since 2019, demonstrating the continued vulnerabilities of the DNS and internet routing protocols.

However, the potential impact of similar failures could be even higher. In instances where DNS routing or records must be updated for remediation, the complete remediation could take up to 48 hours to propagate changes to servers before service is restored to the impacted networks. There have been similar DNS disruptions impacting global cloud service providers, which further illustrate potential impacts on trust and reliability, especially where there is a consolidation of services under the control of a single entity. The article by Carolina Aguerre examines the changes introduced by ICANN over a decade ago that eased regulations for the structural separation between DNS registries and registrars and provides a retrospective of the potential implications of increased consolidation on geographical competition and diversity.

Widespread abuse and exploitation of the DNS by nation states, organisations and criminal enterprises has introduced additional concerns related to integrity, reliability and resilience of networks and services. In terms of quantifying the current state of DNS security, the 2023 Global DNS Threat Report published by the International Data Corporation (IDC) indicated that 90 per cent of the participating organisations experienced a DNS security attack with an average of over seven DNS related incidents per organisation during the most recent one-year period and an average cost estimated to exceed $1 million in addition to the theft of sensitive data and intellectual property. The statistics further indicated that 80 per cent of respondents recognised the criticality of DNS security, 59 per cent have not adopted auto-remediation solutions, and 36 per cent do not collect or analyze DNS data.[1] In addition, ICANN and other organisations and researchers publish DNS security reports.

Numerous DNS enhancements have been proposed and adopted, most notably DNS Security Extensions (DNSSEC) which describes a specification adopted by the IETF to enhance security based on an open standard approach to public key infrastructure that provides end-to-end authenticity and integrity for transaction data. The implementation of DNSSEC is voluntary and while there has been a high adoption rate associated with Top Level Domains (TLDs), the adoption rate for second level domains remains significantly lower – primarily due to configuration and management complexities.

In the absence of significant adoption of DNSSEC or other security specifications, online users and organisations must rely on existing cybersecurity protections that may not be effective against certain categories of malicious actor. An attempt to quantify the prevalence of DNS related security incidents is certainly underrepresented in survey statistics and require the implementation of proactive defence methods and policies to reduce the number and severity of these incidents. As previously described, security enhancements provide a level of defence if properly implemented but in order to achieve an increased level of protection against current and emerging threats to the DNS infrastructure proactive methods should consider the inclusion of passive and active DNS monitoring and analysis to identify patterns of malicious activities.

The adoption and use of threat information could assist in the detection of distributed denial of service (DDoS) attacks, data exfiltration and other DNS infrastructure abuses and provide actionable intelligence that may be used to reduce the probability of occurrence and impact severity of active threats. In addition, security, data protection and privacy concerns have extended to DNS query information. DNS queries are unencrypted by default, enabling network service providers to monitor, collect, and potentially monetise the data. The primary risks to user privacy involve a historical record of browsing activities and geolocation based on the DNS server information. There are regional regulatory restrictions, such as the EU General Data Protection Regulation (GDPR), which prohibit the collection of personal data without prior consent. Elsewhere, these protections are non-existent or governed by applicable privacy policies. For example, in the US, most network service providers allow users to opt out of the collection and potential sale of certain user generated data on their network, but the default opt-in model still creates concerns. The risk to privacy could also increase significantly with consolidation or collaboration of network and service providers where a more comprehensive view of user activates could be collected, shared and analysed.

The impact of these privacy related issues has resulted in the increased use of virtual private networks (VPNs) and encryption and authentication of DNS queries using DNS over TLS (DoT), DNS over HTTPS (DoH) and DNSCrypt network protocols. There have been regional initiatives by national governments related to the security, privacy and resilience of internet content and services. In 2022, the European Union introduced the DNS4EU, a regional DNS service designed primarily to protect the sovereignty, security and privacy of EU citizens. While the use of the service is currently voluntary, it could present consolidation and censorship concerns for citizens in EU member countries. The article by Roxana Radu provides a comprehensive overview of the DNS4EU initiative intended to address issues of DNS resilience, security and privacy with an analysis of the advantages, limitations and the future of DNS resolution.

Domain Name System governance entities could enact stricter measures to reduce the occurrence and effects of DNS abuse. In 2018, in compliance with the provisions of the GDPR, the amount of information available for domain name owners was limited for public purposes. While this measure provided a level of privacy protection, it could slow down lawful government requests. In October 2023, ICANN proposed amendments to accreditation agreements, based on concerns expressed by the international community that would require immediate action to mitigate detectable instances of DNS related abuses defined in part as involvement of botnets, malware, phishing and spam. Despite a requirement to initiate action if adopted, this amendment provides signatories the discretion to select and implement specific mitigation actions. A review of articles published in leading international technical research journals and proceedings over the past year identified articles that provided insight into complex issues related to DNS encryption, malicious domain and traffic detection, security risk evaluation and privacy and usability. The article by Mark Datysgeld provided further insight into a specific problem of illegitimate online sale of health-related products and the impact on vulnerable populations. In the absence of jurisdictional uniformity and accepted international guidelines the author proposes the DNS as a possible pathway for the identification of legitimate providers, based on health and pharmaceutical standards, and to reduce the threat to human safety posed by illegitimate actors.

Overall, there is a need for transdisciplinary academic research in engineering, computer science, and public policy programmes related to DNS governance, resiliency, security, privacy and other societal concerns. More concretely, advancing strategic governance and policies for the DNS and other internet services requires the increased availability of relevant, accurate, accessible and actionable data. This would support a data-driven governance and policy process that could help identify and detect anomalies and trends to reduce and mitigate current and emerging threats to the DNS infrastructure. This information may include DNS threat data, passive and active monitoring, and data from a combination of other sources with the recognition that each may have respective legal, policy, contractual or other restrictions.

The following recommendations are presented for consideration that promote strategic data-driven policy and governance decisions and enhance the ability to identify, analyse, and develop mitigation approaches to counter active methods of DNS abuse:

(1) availability of relevant, accurate, accessible and actionable data to assist in the prevention and mitigation of the increasingly sophisticated level of complex threats that could include threat information, passive and active monitoring, and other data sources in compliance with applicable legal, policy, contractual or other regulations;
(2) examination of the integration of privacy preserving technologies for analytical data sets that maximise the values of data usability and personal privacy;
(3) promoting the development and enhancement of DNS analysis platforms with the following capabilities:
    - authoritative global source of abuse data and statistics;
    - improved detection and prediction of DNS abuse activities;
    - advanced predictive analysis and artificial intelligence models;
    - innovative data visualisation methods;
    - access to multi-source data repositories in standard formats;
    - open-source software modules;
    - auditable processes and functions;
(4) advancing the level of awareness for DNS governance, security, and privacy issues in transdisciplinary public policy and technical academic programmes and research.

The articles presented in this special issue are representative of the range of policy topics related to DNS and highlights a significant opportunity for scholarly evidence-based research and analysis to identify trends, behaviours and insights to improve the understanding of complex interdependencies and issues and to inform international governance and policy processes.

Note

1. International Data Corporation (2023). 2023 Global DNS Threat Report. https://www.idc.com

Disclosure statement

This editorial was prepared by the author in their personal capacity and does not represent the views, opinions, or endorsement of any organisation, institution, the United States Government, or any agency of the United States Government.

Notes on contributor

James Burrell has served in distinguished leadership positions as a US senior federal government executive, corporate c-level executive and academic/research professional. He has extensive international and national policy experience serving as a delegate to multinational organisations and senior representative to US government policy committees on national security, terrorism and technology. He maintains advisory and board affiliations with governmental, non-governmental and private organisations, to include the US National Academies of Sciences, Engineering and Medicine.

ORCID

James Burrell http://orcid.org/0000-0002-7386-4665

James Burrell
✉ james.burrell@bc.edu http://orcid.org/0000-0002-7386-4665