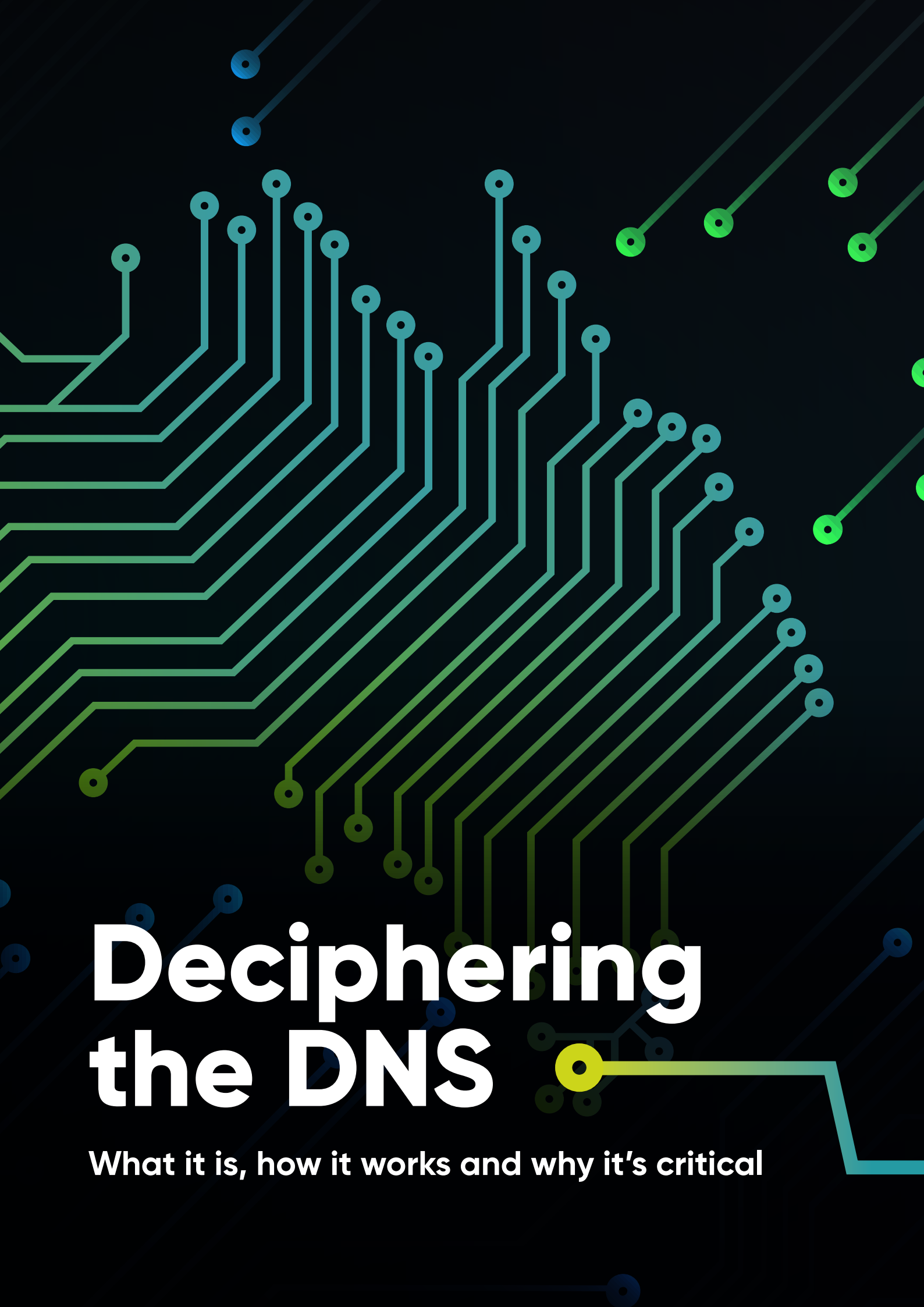


Deciphering the DNS

What it is, how it works and why it's critical

This project was a collaboration between the CSCRC and auDA

CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

With the support of

Australian Government
Department of Industry, Science, Energy and Resources

AusIndustry
Cooperative Research Centres Program

Introduction

Every day across Australian cities and towns, millions of people log on to the Internet, for work and play. Yet, while many Australians rely on the Internet, very few understand how it operates and the vital strategic and security importance of the systems that underpin its operations.

The domain name system (DNS) is the 'directory service' that allows the Internet as we know it to operate effectively. All devices connected to the Internet use numerical Internet Protocol (IP) addresses such as *28.64.198.12* to find and communicate with each other. The DNS acts as a 'directory' for the Internet, translating IP addresses to domain names that can easily be read and remembered, such as *www.example.com.au*.

Without the DNS, Internet users would need to memorise and use IP addresses, making it virtually impossible to easily traverse the Internet. Operators of Internet services frequently change the location where the service is located on the Internet (i.e. the IP address), and users would also need to keep track of changes to IP addresses.

Hence, the DNS is a core service that operates on the Internet that people rely on to connect with others, carry out many common workplace functions, engage in ecommerce and seek information. If the DNS stopped working, the global economy and the digitally connected elements of people's lives would come to a grinding halt.

Given its vital role in supporting the Internet, it is unsurprising the DNS is regarded as a critical infrastructure asset for nations around the globe. In Australia, the importance of the DNS is evidenced by its recent classification as a critical asset in an overhaul of *Australia's Security of Critical Infrastructure Act 2018*.

In an increasingly complex cyber threat environment, securing the DNS is essential to ensuring Australia's connectivity, supporting the growth of the digital economy and protecting Internet freedoms.

Despite its strategic importance, awareness and understanding of the DNS remains limited and possibly underestimated by policy makers, business and the public. Building awareness and a better understanding of the vital role the DNS plays as part of the Internet ecosystem and in supporting Australia's strategic and economic interests will aid future-focussed policy making. It will also help ensure the DNS remains cyber secure as a critical infrastructure asset.

The DNS directory has two defining characteristics:

- It is distributed in nature, stored around the world on domain name servers that 'speak' to each other. This fundamental feature of the DNS's make-up ensures the dynamism and resilience of the Internet, as well as its functionality. This also enables the inherent speed of Internet query responses and access to information, preventing bottlenecks that would occur if the DNS were centrally located and responding to simultaneous demands for the same information.[1]
- The DNS comprises various hierarchical levels, with top-level domains (TLDs) forming the *DNS root zone*, the authoritative name server of the DNS hierarchy. This single, global root and its function as an 'originating source' is fundamental to the resolution of DNS queries ensuring consistent and reliable provision of Internet to billions of users worldwide.[2]

Approaching the issue through a cyber security lens, this report:

Explores the key functions of the DNS and its place in the Internet ecosystem;

Examines the economic and strategic benefits of the DNS in the digital age;

Explores why the DNS is a critical infrastructure asset for Australia; and

Identifies gaps and opportunities in current DNS related frameworks, policy priorities and regulations

1. What is DNS and how does it work? | Network World
2. Brief History of the Internet - Internet Society

Internet vs. World Wide Web

There is often confusion around terms associated with the Internet. For example, many people use 'Internet' interchangeably with the term 'World Wide Web' (or the web), but they are distinct and different technologies.

The Internet is defined by Australian Cyber Security Centre (ACSC) as: "The global system of interconnected computer networks that use standardised communication protocols to link devices and provide a variety of information and communication facilities".[3]

In simple terms, the Internet is a worldwide 'network of networks'[4] that transcends borders and facilitates high-speed global communications and e-commerce at scale.

The Web uses the DNS to name its information servers. Web names change relatively infrequently, whereas the location (IP address) of information servers can change frequently. Information servers with the same domain name, can even be located in different parts of the world, and respond to queries from local users.

What is the DNS?

The DNS is the technical naming system that underpins much of the world's digital communications. All computers connected to the Internet communicate with each other using IP addresses that identify a computer's location. When users type a domain name into a web browser, the DNS translates it so users end up where they want without needing to remember the complex numerical IP address.

Originally developed in the 1980s,[5] the DNS was intended as a globally interoperable and adaptive network, enabling a free flow of information across the network. The .au domain was established in March 1986.

3. Glossary | Cyber.gov.au
4. Networking & The Web | Timeline of Computer History | Computer History Museum
5. Brief History of the Internet - Internet Society

How did the DNS and the Internet come to be?

The evolution of the DNS began within the United States Department of Defense in the early 1960s, when a leading computer scientist at Defense Advanced Research Projects Agency (DARPA) theorised about a vision for a 'galactic network'. This network would allow anyone, anywhere, to quickly access information via globally networked and geographically dispersed computers.[6] This grand theory led to the Advanced Research Projects Agency Network (ARPANET), considered to be the technical precursor to the modern Internet, in 1969.

Importantly, although the Internet has its origins in academia and the US Government, the administration of the global Internet remains free from governmental control and is overseen by multiple stakeholders across civil society, academia, national governments, technical groups and users.[7]

Why is the DNS important to Australia?

The strategic benefits of the DNS are irrefutable: local and global economies, ecommerce and trade, research collaboration, online banking and online learning platforms would collapse if the functionality and security of the DNS was compromised. The virtual world to which many of us have become accustomed would be drastically altered.

In May 2021, the Australian Government published its *Digital Economy Strategy 2030*, setting out ambitions for a strong Australian digital economy.[8] The Strategy notes that 99 per cent of Australians now have access to the Internet.[9] A 2021 report by the Australian Communications and Media Authority (ACMA), also found Australians are voracious Internet users as compared to other nations and economies.[10] These high Internet usage rates signal the reliance, necessity and benefits of the Internet and the DNS to Australians.

This trend has been heightened by the COVID-19 pandemic, with a mass migration to working, studying and socialising from home fundamentally transforming work practices globally at an astonishing pace. A 2020 report by the Australian Trade and Investment Commission (Austrade) and CSIRO's Data61 found digital transformation that previously would have taken a decade to occur happened in a matter of months during the pandemic.[11] This rapid technology adoption has had positive impacts on Australian organisations, increasing resilience, revenue and profitability.[12] And as a result, more organisations have adopted online and hybrid work environments for the long term.

6. Ibid 3
7. https://www.malcolmturnbull.com.au/media/address-to-chatham-house-on-the-future-of-Internet-governance-global-village
8. Digital Economy Strategy (pmc.gov.au)
9. Ibid 6, p. 14.
10. https://www.acma.gov.au/publications/2021-12/report/communications-and-media-australia-how-we-use-Internet
11. *Global Trade and Investment Megatrends* - Data61 (csiro.au), p. 6.
12. https://news.microsoft.com/wp-content/uploads/prod/sites/583/2020/09/AlphaBeta-research.pdf, p. 10

More Australians than ever before are reliant on digital networks for business continuity, employment, education, commerce, banking, healthcare and other essential services.[13] Recent research released by the .au Domain Administration (auDA),[14] indicated that almost all small businesses (98 percent) depend on the Internet as an invaluable tool for generating revenue and connecting with customers. However, auDA's research also revealed Australian consumers and small businesses lack confidence in using the Internet, with cyber security a top concern. Thus, securing the DNS and ensuring its ongoing resilience as a critical infrastructure asset remains a national imperative, given Australia's digital economy relies on it.

98% small businesses depend on the Internet.

Cyber security is a top concern for small businesses

Everyday life – why the DNS matters

The **DNS is part of everyday life** - whether checking your email, working and scrolling on social media sites

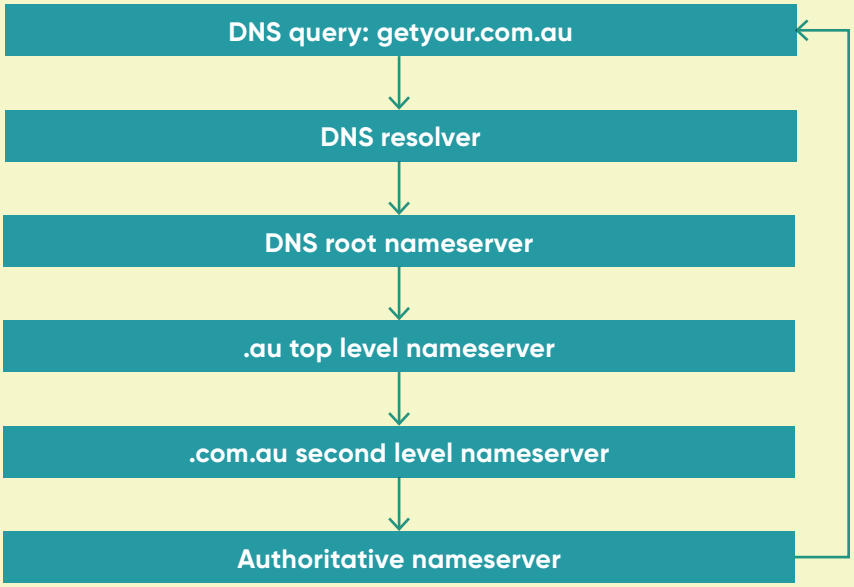
The DNS hierarchy ensures Internet users can **access information quickly** - without it, traversing the Internet would be difficult and onerous

Without the **navigational ease and functionality provided by the DNS**, Internet users would be ill-equipped to access the Internet's vast repositories

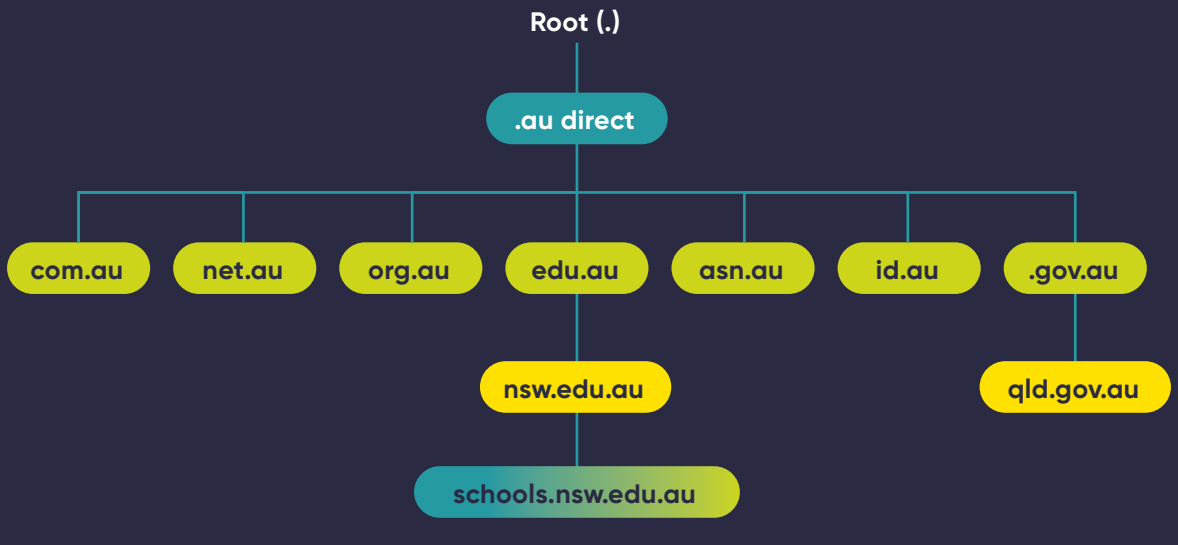
13. Press Release (itu.int)
14. The Digital Lives of Australians 2021 report is available at www.auda.org.au/reports

DNS hierarchy

.au domain name system hierarchy



Source: auDA



Source: auDA

The DNS is a hierarchical system, with names read from left to right. The name at the right following the last 'dot' is called the Top-level Domain, or TLD. For example, in the name cybersecuritycrc.org.au, .au is the TLD.

There are two types of TLDs: generic TLDs (gTLDs) such as .com, .org or .net and country-code TLDs (ccTLDs) like .au or .uk. Each TLD may be operated by a different manager with different rules for registering names within them.

- gTLDs like .com, .org and .net have existed since the early days of the DNS. In 2012, a new gTLD program was launched to allow TLDs relating to cities such as .melbourne or .london, brands such as .bmw or .bbc and other generic words like .art and .bank. There are also gTLDs in foreign scripts, such as Chinese, Arabic and Hebrew. There are about 1239 generic TLDs in use.[15]
- ccTLDs are two-letter TLDs that correspond to two-letter country codes associated with a country or geographical territory, such as .au for Australia or .eu for the European Union. The two letter codes are not arbitrary - but based on the International standard ISO 3166. This standard was first published in 1974 - about 10 years before the DNS was created.

There are hundreds of millions of domain names in use globally and the number keeps growing exponentially. As of June 2021, there are over 4 million domains in .au making it the 9th largest ccTLD in the world.[16] The DNS continues to support the expansion of the Internet now and well into the future.

15. Program Statistics | ICANN New gTLDs
16 Domain Name Industry Brief (DNIB) - Verisign

How is the DNS governed?

Most DNS infrastructure is owned and operated by the private sector, however the Internet is not governed by any one entity or government. The DNS is governed under a decentralised multi-stakeholder model that "places individuals, industry, non-commercial interests and governments on an equal level and allows for community-based policymaking".[17]

The DNS is coordinated globally by a US-based non-government not-for-profit organisation called the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN was established in 1998 and was overseen by the US Government until 2016.

ICANN was established in California under Nonprofit Public Benefit Corporation Law for charitable and public purposes, and is responsible for the introduction of new top-level domains and the withdrawal of existing ones, where required. ICANN also manages the global pool of IP addresses.

Decisions made at ICANN keep the global DNS stable, secure and interoperable. ICANN sets the policy framework for gTLDs but decisions about ccTLDs are made nationally. ICANN is a technical and governance body and issues related to content or the broader use of the Internet remain outside its remit.

ICANN functions according to a 'bottom-up, consensus-driven, multi-stakeholder model'.[18] Its aim is to ensure the continuity of *one global Internet for all*, which is free, open and accessible. This model fosters innovation and helps ensure the growth and social utility of the Internet is not impeded by excessive government oversight or regulation. Importantly, the aim is to ensure global Internet governance remains impartial to the influence of any one stakeholder.[19]

Not all governments support the multi-stakeholder approach, and many would prefer a model that privileges the views of governments over all other stakeholders. The Australian Government's recent *International Cyber and Critical Technology Strategy* reaffirmed Australia's commitment to multi-stakeholder Internet governance and to opposing efforts to bring the technical management and governance of the Internet under government control.

17. Our Work | Australia's International Cyber and Critical Tech Engagement (internationalcybertech.gov.au), p. 82.
18. Welcome to ICANN! - ICANN
19. International Cyber and Critical Tech Engagement Strategy Internet Governance chapter, p. 82.

Oversight of .au

In Australia, auDA is responsible for the management, oversight and maintenance of Australia's .au domain. auDA administers more than 4 million registered .au domain names, ensuring the secure execution and trusted delivery of one of Australia's most vital public resources.[20] This is done through accredited registrars, which offer services to people seeking to register .au domain names. Australia's .au domain is diverse, reflecting Australia's multi-faceted economy, community and industries. The .au domain will play a key role in supporting Australia's ambitions to become a developed digital economy by 2030.[21]

auDA is a not-for-profit community-based organisation, and operates independently of government and is committed to the multi-stakeholder approach.[22] It works with stakeholders from the public and private sector, civil society and the community to ensure the development of Australia's .au ccTLD reflects the priorities of Australian Internet users and to ensure the stable and secure operation of the .au domain.[23]

The DNS and Australia's cyber security

As the DNS continues to evolve and expand, so does the importance of lifting Australia's cyber security posture. The relationship is symbiotic – for the DNS to remain secure effective cyber defences must be in place and vice-versa.

Australia's ccTLD, like other critical infrastructure assets, remains a target for cyber criminals. Therefore, it is important that Australia's domain administrator manages the DNS with cyber security as a lead priority, helping ensure the broader cyber security of Australia's Internet.

Currently, there are 35 registrars accredited to licence .au domain names. Given the fast-moving pace of cyber security threats and the criticality of Australia's ccTLD to internet delivery and connectivity, registrars are required to meet a number of security benchmarks to achieve and maintain accreditation by auDA.[24] These include:

- **ISO 27001 Compliance:** auDA registrars must deploy and maintain an Information Security Management System in compliance with ISO 27001, the leading international information security standard, which is a combination of policies and procedures for organisations to safely secure their systems and data.
- A set of minimum controls based on the Australian Signal Directorate's Essential Eight.[25]

20. .au Domain Names | auDA
21. Digital Economy Strategy (pmc.gov.au)
22. https://assets.auda.org.au/a/2021-09/auDA%20Strategy%202021-2025_0.pdf?VersionId=g1EvNJT532ptJAjEQLtBv7VcuZ-lY7Zld, p. 2.
23. Ibid 23
24. Registrar Accreditation | auDA; these are expressly approved by auDA in writing for this purpose.
25. Registrar Accreditation | auDA, p. 31, Sec. 15.1, (b)

Further stringent security requirements for Australian registrars include:

- Prescribed minimum security controls
- Controlled access to registry data
- Protection of registry data
- Notifications of security breaches.[26]

Registrars' compliance with these obligations is assessed via annual independent audits.

These audits ultimately help ensure Australia's DNS remains secure and helps bolster the nation's cyber security posture. auDA works closely with registrars to ensure high cyber security standards are maintained, and has implemented new registrar agreements with bolstered cyber security requirements and engages with industry to promote cyber security best practice.[27]

2016 Dyn Cyber Attack

The 2016 Dyn cyber attack highlighted the importance of DNS cyber security to the delivery of the Internet. This attack targeted Dyn, a major DNS provider, through a distributed denial-of-service (DDoS) attack via a malware-infected bot. Purportedly the "largest of its kind in history",[28] the October 2016 attack brought the vast majority of the United States' Internet to a standstill for almost a day. Knocking high-traffic sites like Twitter, Netflix and The Guardian offline, the attack had a significant impact on e-commerce and communications globally. The financial repercussions were substantial, with Sony estimating $2.7M in lost revenue[29] and Dyn suffering an eight per cent drop in its customer base post attack.[30]

26. Registrar Accreditation | auDA, p. 32-33, Sec. 15.3 – 15.6
27. https://assets.auda.org.au/a/2021-10/auDA_2020-21_Annual_Report.pdf?VersionId=2pUHN8HL7bOKHhajx5mWVkYBDmv-vULKL, P10
28. DDoS attack that disrupted Internet was largest of its kind in history, experts say | Hacking | The Guardian
29. https://www.engadget.com/justice-department-2016-dyn-cyberattack-plea-183112958.html
30. https://securityledger.com/2017/02/mirai-attack-was-costly-for-dyn-data-suggests/

'Australia's DNS may be used for malicious online activity

The importance of maintaining stringent cyber security standards across Australia's DNS was illustrated in 2021, when a phishing scam targeted .au domain name registrants.[31] Cyber criminals impersonating an auDA employee sent fake emails requesting personal information or asking for confirmation of current details. In this instance, auDA was immediately notified and acted to ensure users were informed of the scam, negating the efficacy of this phishing attempt.

Likewise, the 2018 hacking of an Australian domain name registrar by cyber criminals, who used the company as a backdoor for intellectual property theft, highlights the need for ongoing cyber vigilance concerning Australia's DNS.[32] In the attack, cyber criminals diverted legitimate domains to malicious IP addresses through the creation of fake domain names.

Current Australian DNS policy priorities, regulations and frameworks: the DNS as critical infrastructure

The DNS is essential to preserving Australia's way of life and, due to a recent overhaul of critical infrastructure legislation, is now classed as a critical infrastructure asset.[33]

The identification of the DNS as a critical infrastructure asset, specifically that the .au ccTLD be prescribed as a critical domain name system, reflects rising cyber security threats, a heightened global cyber threat environment and ongoing and sustained malicious cyber activity against critical infrastructure assets globally. Under the new regime, auDA is specified as the entity responsible for the administration of the Australian .au country code.[34]

Leveraging the economic and societal gains provided by the DNS means striking a balance between the protection of Australia's critical infrastructure assets and the preservation of an open and interoperable Internet – one that is market-driven and free from government overreach.

Balancing of these priorities is affirmed in the Department of Foreign Affairs' (DFAT) *2021 International Cyber and Critical Technology Engagement Strategy*. The Strategy is focussed on fostering "cooperative measures, to promote collaboration between countries, based on a mutual commitment to improve resilience and reinforce a peaceful and stable online environment".[35]

31. https://www.auda.org.au/statement/scam-alert-email-scam-targeting-au-registrants
32. https://www.afr.com/policy/foreign-affairs/australian-company-at-centre-of-chinese-hack-to-steal-us-aviation-technology-20181031-h17cd1
33. Advisory report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018 – Parliament of Australia (aph.gov.au)
34. See: Section 12KA, subsection (2) in the Security of Critical Infrastructure Act (SOCI Act).
35. *2021 International Cyber and Critical Technology Engagement Strategy*, P43

Given the DNS's strategic, social and economic importance, there will be an increased role for strategic policy making. Policy must remain adaptive to evolving security challenges while protecting the decentralised nature of the DNS. This requires policy that supports the ongoing agility of the DNS, which is required to respond to current and emerging issues like the exponential growth of the Internet of Things, artificial intelligence and privacy and security concerns.

The global picture

The ecosystem of technologies on which the Internet depends has evolved over time to maintain and improve the security, stability and resilience of the Internet. The global and decentralised nature of the Internet and the DNS is one of its strengths, but it also presents jurisdictional challenges, given it crosses territorial borders.

Increasingly, governments are attempting to regulate the Internet as part of larger regulatory agendas, for example, privacy and data management regulation. However, significant challenges remain when applying a state's laws to a globally distributed network.

As the DNS is a global network, issues that occur on one part of the network can have consequences for infrastructure and end users around the world. An impact on one part of this global network, whether due to a regulatory development or a security incident, may have flow-on consequences for infrastructure and end users in other jurisdictions. Hence, a collaborative, holistic and harmonised approach to global DNS governance as it relates to cross-jurisdictional impacts is required.

Conclusion

The DNS underpins virtually every system and function relied upon in a digital world.

By its very nature it is critical – it ensures connectivity, supports the digital economy and is essential to maintaining an open, free, secure and global Internet. And to support these functions, the security of the DNS is essential.

This report shines a light on the importance of the DNS in the Internet ecosystem and its economic and strategic benefits. It also highlights the role of the DNS as a part of Australia's critical infrastructure, which will only become more vital into the future.

It is important that Australians understand the criticality of the DNS to the effective operation of the Internet and all the systems that rely upon it.

Key points

- The DNS is the technical naming system that underpins much of the world's digital communications and has been designated as 'critical infrastructure' in Australia
- The DNS is like the 'directory' of the Internet and is vital to connect internet users with the websites they are seeking
- Australia's .au domain is managed and maintained by auDA, who administer over 4 million .au domain names
- The DNS is a target for cyber criminals and in Australia auDA accredited registrars have to demonstrate that users of the .au are better protected by adopting high standards set by auDA
- The global and decentralised nature of the DNS is a key strength and there are significant challenges in applying a nation state's laws to the DNS

References

1. What is DNS and how does it work? | Network World

2. Brief History of the Internet - Internet Society

3. Glossary | Cyber.gov.au

4. Networking & The Web | Timeline of Computer History | Computer History Museum

5. Brief History of the Internet - Internet Society

6. Ibid 3

7. https://www.malcolmturnbull.com.au/media/address-to-chatham-house-on-the-future-of-Internet-governance-global-village

8. *Digital Economy Strategy* (pmc.gov.au)

9. Ibid 6, p. 14.

10. https://www.acma.gov.au/publications/2021-12/report/communications-and-media-australia-how-we-use-Internet

11. Global Trade and Investment Megatrends - Data61 (csiro.au), p. 6.

12. https://news.microsoft.com/wp-content/uploads/prod/sites/583/2020/09/AlphaBeta-research.pdf, p. 10

13. Press Release (itu.int)

14. The Digital Lives of Australians 2021 report is available at www.auda.org.au/reports

15. Program Statistics | ICANN New gTLDs

16. Domain Name Industry Brief (DNIB) - Verisign

17. Our Work | Australia's International Cyber and Critical Tech Engagement (internationalcybertech.gov.au), p. 82.

18. Welcome to ICANN! - ICANN

19. International Cyber and Critical Tech Engagement Strategy Internet Governance chapter, p. 82.

20. .au Domain Names | auDA

21. Digital Economy Strategy (pmc.gov.au)

22. https://assets.auda.org.au/a/2021-09/auDA%20Strategy%202021-2025_0.pdf?VersionId=g1EvNJT532ptJAjEQLtBv7VcuZlY7ZId, p. 2.

23. Ibid 23

24. Registrar Accreditation | auDA; these are expressly approved by auDA in writing for this purpose.

25. Registrar Accreditation | auDA, p. 31, Sec. 15.1, (b)

26. Registrar Accreditation | auDA, p. 32-33, Sec. 15.3 – 15.6

27. https://assets.auda.org.au/a/2021-10/auDA_2020-21_Annual_Report.pdf?VersionId=2pUHN8HL7bOKHhajx5mWVkYBDmvvULKL, P10

28. DDoS attack that disrupted Internet was largest of its kind in history, experts say | Hacking | The Guardian

29. https://www.engadget.com/justice-department-2016-dyn-cyberattack-plea-183112958.html

30. https://securityledger.com/2017/02/mirai-attack-was-costly-for-dyn-data-suggests/

31. https://www.auda.org.au/statement/scam-alert-email-scam-targeting-au-registrants

32. https://www.afr.com/policy/foreign-affairs/australian-company-at-centre-of-chinese-hack-to-steal-us-aviation-technology-20181031-h17cd1

33. Advisory report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018 – Parliament of Australia (aph.gov.au)

34. See: Section 12KA, subsection (2) in the Security of Critical Infrastructure Act (SOCI Act).

35. *2021 International Cyber and Critical Technology Engagement Strategy*, P43

36. Full title: the Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM/2020/823 final) (NIS 2), found at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN. The proposal is an update to the first European Union-wide legislation on cyber security from 2016 – the Directive (EU) 2016/1148 on security of network and information systems (NIS Directive). The 2016 Directive encapsulated top-level domain registries (TLDs) and DNS service providers, thereby obliged to undertake more rigorous cyber security practices.

37. https://www.internetsociety.org/blog/2021/10/european-unions-network-and-information-security-directive-threatens-internet-fragmentation-and-creates-security-risks/

38. https://www.icann.org/en/system/files/files/icann-org-comments-proposed-nis2-directive-19mar21-en.pdf

39. https://www.icann.org/en/system/files/files/icann-org-comments-proposed-nis2-directive-19mar21-en.pdf, p. 1.

CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

.auDA