FINAL REPORT

Internet Governance System Map

Mapping influence and interactions in the world of Internet governance

Department of Infrastructure, Transport, Regional Development, Communications and the Arts

October 2023

noeticgroup.com

Contact

PO Box 4177
Kingston ACT 2604

Level 4, 42 Macquarie Street
Barton ACT 2600 Australia

T +61 2 6234 7777

Contents

Executive summary

Purpose of the report

This report offers a detailed exploration of the Internet governance ecosystem, emphasising the key actors, their roles, and interrelations. It's an effort to demystify the various elements and dynamics that shape Internet governance, thus influencing policy-making decisions, inciting public dialogue, and identifying avenues for stakeholders to make impactful contributions.

Approach

The approach taken in creating this report is comprehensive and multidimensional, grounded in extensive desktop research and the insightful perspectives of diverse stakeholders. These stakeholders' range across various sectors, each with unique experiences and roles within the Internet governance landscape. Their insights enrich our analysis, providing real-world context and balance to the theoretical aspects of our research.

Simultaneously, this report adopts a specific geographical perspective (Australia) to anchor the global Internet governance landscape within a domestic context. The Australian perspective serves as a practical case study, showcasing how local stakeholders navigate and contribute to the broader global Internet governance ecosystem. This focus also facilitates a more relatable and tangible understanding of the complex dynamics at play in Internet governance.

The Internet: its importance, governance dynamics, and emerging tensions

The significance of the Internet

The Internet has emerged as the most critical infrastructure in human history, significantly impacting daily lives and the global economy. As it becomes even more integral for collaboration, social connection, service delivery, and prosperity, the need for effective governance also grows. However, it presents unresolved challenges that impact users' rights and interests, like privacy, security, and safety.

Governance models and stakeholders

Three overarching approaches to Internet governance exist: multistakeholder, multilateral, and unilateral. The multistakeholder model, currently the dominant approach, has been instrumental in fostering a free, open, and globally connected Internet. Nevertheless, this model faces hurdles in an increasingly intricate Internet governance landscape.

Governments play an essential role in safeguarding their citizens' interests. Their engagement with the Internet has surged due to increased usage, its significant economic impact and the public interests of their citizens. However, governments are only one group among many that influence Internet governance within the multistakeholder model.

The tension in Internet governance

Governments can also wield influence through multilateral channels or unilaterally by enforcing legislation that affects Internet interoperability and the overall governance landscape. This power dynamic creates a tension around the ideal method of governing the Internet. If not resolved to satisfy most stakeholders, there is a risk of increased unilateral regulation or multilateral governance excluding the technical community. This situation could lead to fragmentation of the Internet, undermining its utility and value.

Principal discoveries

The research, grounded in comprehensive literature reviews and stakeholder interviews, underscores the escalating prominence of the Internet in day-to-day life and global commerce. With the Internet's increasing integration into societal structures, challenges such as privacy, security, and safety have been amplified, calling for more effective governance mechanisms.

The multistakeholder model, the dominant strategy for Internet governance at present, has been instrumental in nurturing a free, open, and globally interconnected Internet. Nonetheless, as the landscape grows more intricate, this model is confronting substantial hurdles.

Governments, whose responsibility is to safeguard the interests of their citizens, have become more involved with the Internet due to increased usage, its economic importance and influence on public interests. This increased involvement, sometimes expressed through multilateral or unilateral actions, has introduced stress into the governance structure. Governments have a sovereign right to implement policies and actions that may constrain or prevent certain uses of the Internet to align to its legislation and its citizens' culture, religions and social norms. However, these actions could undermine the functionality and value of the Internet if it results in technical fragmentation of the Internet where the underlying infrastructure no longer allows systems to be fully interoperable and exchange data packets and function consistently at all end points.

Key findings from the research include:

- **The multistakeholder model**, with its capacity to incorporate a diverse range of voices, is a vital determinant in the continued success and equitable benefits of the Internet.
- **Unilateral action resulting in technical fragmentation** poses a threat to the openness and interconnectivity of the Internet, highlighting the need for a harmonised, global approach to Internet governance.
- **The role of governments** is critical in the balance between national interests and the preservation of the Internet as a global public good. The need to delicately balance regulation with innovation emerges as a significant finding.
- **Security and privacy** issues require robust governance mechanisms to balance competing needs. Users are increasingly concerned about their privacy rights amidst the backdrop of cyber threats and data breaches. However, access to user data is needed for activities such as law enforcement, consumer protection, and competition and rights protection.

- **Digital inclusion and capacity building** are significant issues. As the Internet expands, concerted efforts are needed to bridge the digital divide and ensure that all communities have equal opportunities to participate in and benefit from the digital economy.

The report concludes by underlining the need for concerted action and collaboration among all stakeholders. The future of the Internet, its openness, security, and inclusive nature, depends on how effectively we navigate these challenges and capitalise on the opportunities that lie ahead.

Strategic implications and future directions

The Internet governance landscape is characterised by its complexity, diversity, and dynamism, with a myriad of actors each operating with unique interests and facing distinct challenges. Comprehending this multifaceted ecosystem is not merely an academic exercise but is important for effective engagement and strategic planning.

Key implications emerge from this understanding:

- **Strategic positioning:** Stakeholders can better identify their role within the landscape, optimise their influence on policymaking, and align their initiatives with broader governance objectives.
- **Collaborative opportunities:** Understanding the landscape enables the identification of potential partners, synergies, and opportunities for collaboration, fostering a more integrated and effective approach to governance.
- **Risk management:** Recognising the challenges and potential threats within the landscape allows stakeholders to anticipate, mitigate, and manage risks effectively.
- **Future foresight:** A comprehensive view of the landscape equips stakeholders to anticipate and prepare for emerging trends, technologies, and policy issues.

Armed with these insights, stakeholders are better equipped to navigate the complexities of the Internet governance landscape. It allows them to contribute more effectively towards a shared vision of the Internet as a robust driver for innovation, cooperation, and progressive societal transformation. This understanding and the subsequent strategies developed from it will play a crucial role in shaping the future trajectory of the Internet, making it more inclusive, secure, and beneficial for all.

Introduction

Overview

In today's interconnected world, the Internet has become an integral part of our daily lives, enabling communication, commerce, and the exchange of information on a global scale. As the Internet continues to evolve and expand, its governance becomes increasingly critical to ensure its stability, security, and accessibility for all users. The complexity of the Internet governance landscape has grown over time, with a multitude of stakeholders and organisations involved in various aspects of its operation and regulation.

Approach

The methodology employed in this report follows a comprehensive approach to analyse the Internet governance landscape and provide valuable insights. The approach consisted of several key activities, including:

1. **Information Collection Process:**
   - Conducting a thorough literature review of academic articles, policy documents, and reports from international organisations to gather insights into the Internet governance landscape, its evolution, and key issues.
   - Conducting in-depth interviews with experts and stakeholders from various sectors, including government, private sector, civil society, and academia, to gain first-hand perspectives on Internet governance.
   - Performing a comprehensive online search to gather additional information about organisations, initiatives, and forums involved in Internet governance, as well as identify recent developments and trends.
2. **Problem Analysis Approach:**
   - Identifying and categorising the various stakeholders, organisations, processes, and challenges involved in Internet governance to provide a comprehensive overview of the landscape.
   - Analysing the relationships between different components of the Internet governance landscape, highlighting connections, dependencies, and potential points of conflict or collaboration.
   - Assessing the dynamics of the Internet governance landscape, considering the evolving nature of the Internet, the roles of different stakeholders, and emerging challenges and opportunities.
   - Identifying potential areas for intervention by the Australian Government and the broader Internet community based on the analysis of the Internet governance landscape.
3. **Design Principles Applied in the Report:**
   - Structuring the report to provide a logical flow of information, guiding readers from the introduction and context of Internet governance to the in-depth analysis of the landscape and identification of opportunities for intervention.

- Incorporating visual representations, such as diagrams, charts, and tables, to illustrate complex concepts, relationships, and trends for enhanced understanding.
- Ensuring consistency and clarity throughout the report using consistent terminology, formatting, and presentation styles.
- Tailoring the report to meet the needs and interests of various audience groups, addressing specific concerns and questions of stakeholders in the Internet governance landscape, as well as providing broader insights for the public.

By employing this rigorous approach, the report aims to provide a comprehensive, accurate, and accessible analysis of the Internet governance landscape, offering valuable insights for policymakers, industry leaders, and the wider Internet community.

Structure of this report

The table below outlines the structure of the report and maps out the analysis contained within each section.

Table 1: Structure of the report

Section	**Purpose**
Executive summary	Provides an overview of the report's key points, findings, and recommendations.
Introduction	Sets the context and explains the aim and scope of the report.
Fundamentals of Internet and its governance	Discusses the basic concepts and principles related to the Internet and its governance.
How the Internet works	Explains how the Internet works.
History of Internet governance	Summarises key Internet governance milestones and the emergence of the multistakeholder model.
Internet governance landscape: an overview	Analyses the Internet governance landscape, including models of governance, key players, influence and relationships.
Challenges to effective Internet governance	Outlines the challenges related to effective Internet governance such as fragmentation of the Internet and unilateral action.
Opportunities for enhanced Internet governance	Explores the potential areas of advancement and how they could contribute to more robust, inclusive, and effective Internet governance.
Emerging technology trends and their impact on Internet governance	Analyses the influence of evolving technology trends on Internet governance.
Future of Internet governance	Explores the future challenges and opportunities of Internet governance.
Australia's Internet governance landscape	Highlights the unique aspects and challenges of Internet governance in Australia.
Findings and implications	Summarises the key findings from the study and discusses their implications for Internet governance.
Conclusion	Offers a summary of the report's major conclusions and their implications for the future of Internet governance.
Annexes	Provides additional resources and context, including details of the study's methodology, list of references, and a glossary of key terms and concepts used in the report.

Fundamentals of the Internet and its governance

What is the Internet?

The Internet is a network of networks. It is an interconnection of physical networks that can join to create a much larger, decentralised network that allows information to be rapidly sent from one point to another.[1] The Internet is designed to be robust and resilient, with redundant routing and backup connections that ensure that data can still be transmitted even in the face of disruptions or failures in the network. This redundancy allows the Internet to adapt to changes in traffic patterns or network topology, helping to maintain its stability and reliability.

Layers of the Internet

The Internet consists of several layers:

- **Physical infrastructure layer**: the hardware of the network that allows information to move from one point to another (e.g., cables, computers and satellites). This is like the airplanes, trucks and roads used to transport physical mail.
- **Logical layer:** the technical instructions for how information travels through the network (e.g., Domain Name System (DNS), Internet Protocol addresses (IP addresses), routing protocols). This is like managing how physical mail is sent from one point to another based on addresses and rules for routing and package size.
- **Applications layer:** the software and applications that allow us to access the Internet (e.g., Internet browsers, email applications, video conferencing applications and games). This is like the paper and pens used to write letters that are sent via physical mail.
- **Content layer:** the information that exists on the application layer (e.g., website content and social media posts). This is like the messages that are written in the physical mail.

What is Internet governance?

Internet governance is a broad term with many interpretations. The technical community[2] initially used the term 'Internet governance' to refer to the governance 'of' the Internet through the technical management of the DNS, protocols, and root servers (the Physical Infrastructure and Logical layers of the Internet). However, due to the increase in unresolved public policy issues related to the Internet (e.g., concerns about privacy, online safety, cybersecurity and

[1] Lee TB (2015), ' The internet, explained', Vox, accessed 29 August 2023. https://www.vox.com/2014/6/16/18076282/the-internet

[2] Technical Community: In the context of Internet governance, the "technical community" typically refers to a diverse group of individuals and organisations that contribute to the development, deployment, and maintenance of the Internet's technical infrastructure. This includes but is not limited to software developers, engineers, researchers, network operators, and institutions such as the IETF, ICANN, and W3C, which set standards and protocols to ensure the interoperability and functionality of the Internet.

intellectual property), there is an increased interest in addressing these issues by governing the services 'on' the Internet (the Applications and Content layers).

The competing interests in how Internet governance is defined reflects the desire to either retain or gain influence in the landscape. For example, the technical community, involved in managing the Internet's technical infrastructure like the DNS, protocols, and root servers, prefers a "narrow definition". This definition confines Internet governance to the technical management 'of' the Internet. Upholding this narrow definition allows the technical community to retain more influence. On the other hand, some governments lean towards a "broader definition", encompassing policy issues of services 'on' the Internet like privacy, cybersecurity, and intellectual property. By promoting this broader definition, governments aim to expand their influence over Internet governance.

The most widely accepted definition adopted in 2005 comes from the Tunis Agenda for the Information Society:

> *'Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.'*

By this definition, Internet governance is a decentralised, multistakeholder process that involves various actors, such as governments, private sector entities, civil society organisations, academia, and technical communities. These stakeholders contribute to the governance of the Internet through diverse forums, organisations, and processes, addressing issues related to the Internet's infrastructure, protocols, standards and policies.

The way that Internet governance is defined determines the scope of the landscape. This report focuses on the logical layer of Internet governance, noting that there is a level of overlap and interplay between the layers.

Why does Internet governance matter?

Internet governance is pivotal for social, economic, and political reasons. Socially, the Internet has become an integral part of our daily lives, facilitating communication, education, commercial transactions, and entertainment. However, it also presents challenges such as privacy and security concerns, and the spread of harmful content.

Economically, the Internet has opened new markets, fostered innovation, and transformed many traditional industries. However, it also brings about issues such as the digital divide[3], intellectual property rights, and competition matters, especially with the dominance of 'Big

[3] "Digital divide" refers to the disparity in access to and use of information and communication technologies, including the Internet. This divide may exist between socio-economic groups, geographical locations, or demographic groups. The term encapsulates the differences in both physical access to technology and the resources and skills needed to effectively participate as a digital citizen.

Tech'. Internet governance plays a key role in managing these challenges and ensuring a fair and sustainable digital economy.

Politically, the Internet has significant implications for democracy and national security, offering a platform for free expression and political participation. Yet, it introduces challenges like disinformation, state surveillance, and cybercrime, which can undermine democratic processes and human rights.

> *The Internet is the most important infrastructure in human history – it impacts everyone, but no one seems to know much about it.*
> Subject Matter Expert Research Participant

In essence, Internet governance matters because it shapes the rules and principles that support our interaction with the digital world. Its impact is direct and far-reaching, influencing how the digital world affects us and ensuring that the Internet continues to serve the best interests of legitimate users worldwide.

Case Study: New IP

BACKGROUND

In 2019 Huawei, with support from other Chinese technology companies, submitted a set of proposals to the International Telecommunication Union's Telecommunication Standardization Sector (ITU-T). These set of proposals, called 'New IP', proposed to develop new network protocols and architectures by extending and redesigning the traditional IP (Internet Protocol) to support new services for a new Internet by 2030. New IP aims to retain the core advantages of traditional IP while upgrading fundamental capabilities to support future technology requirements.

THE IMPACT

Internet standards are currently developed by the Internet Engineering Task Force (IETF) which operates in a multistakeholder environment that allows anyone to contribute to the development of these standards in an open, bottom-up manner. Submitting the New IP proposals to ITU-T is a departure from the current governance processes for setting Internet standards.

Additionally, the proposed architecture for New IP is not backwards compatible with the existing architecture of the global Internet. This lack of interoperability could result in a fragmented Internet of two global interconnected networks running in parallel which cannot talk to each other.

ACTIONS TAKEN AND LESSONS LEARNED

In 2020 the ITU-T asked for input from the IETF on the New IP proposal. The decision was made in 2020 not to accept the New IP proposals and to stop discussing New IP until at least March 2022. However, elements of the New IP proposals continued to be submitted as new proposals in different ITU-T study groups throughout 2021.

This case study highlights the importance of an agreed approach to Internet governance and related processes to maintain an interoperable Internet.

By understanding the complexities of Internet governance, policymakers, industry leaders, and the wider Internet community can work together to create a more secure, stable, and inclusive digital future for all. This is crucial because the statement below made by the founders of the Internet is as true today as when it was written in 1997:

- If the Internet stumbles, it will not be because we lack for technology, vision, or motivation. It will be because we cannot set a direction and march collectively into the future.
  - A Brief History of the Internet – Internet Society

The pillars of Internet governance

Internet governance plays a crucial role in ensuring that the Internet remains an open, inclusive, and innovative platform for communication, collaboration, and economic growth.

Some critical aspects of Internet governance include:

- **Technical coordination:** Internet governance is essential for maintaining the stability and interoperability of the global Internet. This involves the management of critical Internet resources, such as domain names and IP addresses, as well as the development and implementation of technical standards and protocols that enable the seamless functioning of the Internet.
- **Security and stability:** as the Internet becomes increasingly essential for various aspects of modern life, it is crucial to ensure its security and stability. Internet governance includes improving security measures (e.g., Resource Public Key Infrastructure and Domain Name System Security Extensions) that protect the resilience of critical Internet infrastructure, fostering a secure and reliable online environment.
- **Openness and innovation:** Internet governance supports the open and collaborative nature of the Internet, promoting innovation and the free flow of information. This involves the protection of fundamental rights, such as freedom of expression and privacy, as well as the development of policies and regulations that encourage competition and foster the growth of the digital economy.
- **Inclusivity and access:** Ensuring that the benefits of the Internet are accessible to all is a central aspect of Internet governance. This includes efforts to bridge the digital divide, promote affordable Internet access, and implement the universal acceptance of all valid domain names, including internationalised domain names (IDNs) which are domain names that use non-Latin characters.

Acknowledging the evolving landscape of internet governance, it is evident that the historical four tracks of the Internet Governance Forum (IGF) risk becoming outdated in the face of rapid technological advancements and emerging challenges. In contemporary times, there are eight key tracks that reflect the complexities of the digital age. Although still evolving, it is increasingly acknowledged that the new pillars of internet governance may be:

- Artificial Intelligence and Emerging Technologies
- Avoiding Internet Fragmentation
- Cybersecurity
- Cybercrime and Online Safety
- Data Governance and Trust
- Digital Divides and Inclusion
- Global Digital Governance and Cooperation

- Human Rights and Freedoms
- Sustainability and the Environment.

These evolving pillars of internet governance reflect the complexities of the digital age. The emergence of these eight contemporary tracks highlights the need for a comprehensive approach to address the challenges and opportunities of the digital era. By recognising and engaging with these new pillars, stakeholders can work towards a more inclusive, secure, and sustainable digital future.

How the Internet works

The Internet, a global network of interconnected computers, servers, and devices, facilitates the exchange of information and communication between users worldwide. It's not a single network but rather a network of networks spanning the globe.

Each device connected to the Internet is assigned a unique Internet Protocol (IP) address, which enables it to communicate with other devices over the network. The DNS translates human-readable domain names (e.g., www.example.com) into these IP addresses, simplifying Internet navigation for users.

When data is sent over the network, it's broken down into smaller digital pieces known as 'packets'. These packets traverse the network and are reassembled into a complete file at their intended destination. Protocols, such as the Transmission Control Protocol/Internet Protocol (TCP/IP), guide these data packets, ensuring they arrive where they're supposed to go.

Internet Service Providers (ISPs) play an essential role in this process. They provide users with Internet access and the necessary infrastructure for data transmission, acting as gatekeepers and ensuring efficient traffic routing between networks.

When an Internet user wants to visit a website, they enter a domain name into a web browser. The IP address for that domain name is retrieved from a DNS server, directing the user to the corresponding website hosted on a server. This entire process happens within milliseconds!

The website owner, to facilitate this, would have registered their domain name with a registrar such as GoDaddy, or Tucows. Meanwhile, registries, such as Verisign, maintain records of these domain names to ensure accurate retrieval from DNS servers when users search for a website.

Various commercial and non-commercial organisations play a role to support each element of the Internet. The cooperation of these organisations is what makes the Internet work.

To summarise, the operation of the Internet involves several key elements:

- **Protocols:** These determine how data moves through the network. TCP/IP is one such protocol that guides where a data packet is sent and how it reaches its destination.
- **Domain Name System:** Often referred to as the 'phone book of the Internet', the DNS translates human-readable domain names into IP addresses.
- **Registries and Registrars:** These organisations manage domain names and IP addresses on the DNS.
- **Internet Service Providers:** ISPs connect users to the Internet and provide the necessary infrastructure for data transmission.
- **World Wide Web (WWW):** The WWW is a method of accessing information on the Internet, consisting of interconnected documents and resources, accessed via web browsers using the Hypertext Transfer Protocol (HTTP). It's important to note that the web is just one of many types of applications and services that run over the Internet.

History of Internet governance

The history of Internet governance traces back to the Internet's inception, managed initially by a collective of researchers and engineers. This collaborative approach characterized the early governance model, fostering participation from diverse sectors including governments, private entities, academia, and civil society.

Key historical milestones include:

- The creation of the Advanced Research Projects Agency Network (ARPANET) by the USA Defense Advanced Research Projects Agency (DARPA) in the 1960s, which eventually evolved into the Internet.
- The Internet Assigned Numbers Authority (IANA) was informally established in 1972 by Jon Postel, then a graduate student, who allocated and managed socket numbers for the emerging ARPANET network.
- The establishment of the Internet Engineering Task Force (IETF) in 1986, which fostered open standards ensuring network interoperability.
- The establishment of Regional Internet Registries (RIRs) in the 1990s to manage the allocation of IP addresses across the world.
- The formation of the Internet Corporation for Assigned Names and Numbers (ICANN) in 1998, tasked with global DNS management and IP address allocation.
- The World Summit on the Information Society (WSIS) in 2003 and 2005, leading to the establishment of the Internet Governance Forum (IGF).
- The transition of IANA stewardship from the U.S. government to ICANN in 2016, reinforcing ICANN's multistakeholder, non-profit status.

In the early stages, Internet governance was primarily technical, focusing on core resource management, such as domain names, IP addresses, and protocols. As the Internet expanded, formal structures like the IETF and the Internet Architecture Board (IAB) emerged, overseeing technical development, and promoting voluntary standards.

The rise of ICANN in 1998 marked a significant shift in Internet governance, transitioning towards a more formal, institutional model. Despite this evolution, the principles of openness, collaboration, and consensus-based decision-making remain the cornerstone of Internet governance.

Today, as the Internet continues to grow in complexity and global interconnectedness, the need for effective Internet governance is more pronounced. Challenges around interoperability, particularly regulatory interoperability, necessitate a collaborative approach to preserve the Internet's utility and openness. Additionally, debates surrounding the extent of government control over the Internet continue to shape the governance landscape. Understanding this history is vital for navigating the complexities of today's Internet governance.

Emergence of the multistakeholder model

The multistakeholder model of Internet governance came to prominence in the early 2000s. The model recognised the wide range of actors impacted by the Internet. Under this model, various stakeholders, including governments, private sector entities, civil society organisations, academic and research institutions, and individual users, all have a role to play in shaping the evolution of the Internet. This model was formalised at the WSIS in 2003 and 2005, where it was agreed that Internet governance should be collaborative, transparent, and inclusive.

The multistakeholder approach was seen to balance the diverse interests of different groups and ensure that no single entity could exert undue control over the Internet. It was designed to foster greater participation and democracy in Internet governance, reflecting the Internet's decentralised, distributed nature. Crucial organisations such as ICANN, the IGF, and the IETF operate under this model, promoting global cooperation and consensus-building.

> The Internet is too important to be in the hands of a single entity.
> Subject Matter Expert Research Participant

Multistakeholder governance has been instrumental in promoting innovation, openness, and the free flow of information on the Internet. It has allowed for rapid technological advancement while also addressing critical issues such as concerns about cybersecurity, privacy, and digital inclusion.

Case Study: The Multistakeholder Model Working

BACKGROUND

In the current multistakeholder model, the Internet is governed by non-profit organisations that sit outside commercial and geopolitical interests.

INTEROPERABILITY

This unique arrangement has enabled an interoperable network of networks that is open to everyone. The Internet is based on open standards that are not under patent by a single company. If the creation of the Internet was led by industry, commercial interests would likely have resulted in several companies patenting their own standards, resulting in many networks that were not interoperable. This approach would have deepened the digital divide with companies charging for access to their network to recoup a return on their investment.

Without a multistakeholder approach led by non-profit organisations that sit outside of market forces, the Internet would not exist, and the utility of these networks would be severely limited by the lack of interoperability that has made the Internet so successful.

SERVICE

Most people in the world have never heard of the Internet Corporation for Assigned Names and Numbers (ICANN) or the registries that make the Internet work. In fact, most people have not heard of the Domain Name System (DNS). This is largely due to the excellent service Internet users receive from the DNS. Since the Internet started being used more broadly, there has not been a single service disruption to the DNS, despite intentional attacks on DNS servers to cause service disruptions. No one has ever said "the DNS is down again today; I need to call ICANN to figure out what is going on". This demonstrates the ability of multistakeholder approach led by non-profit organisations to provide better service levels than what is achieved by commercial and public service providers who routinely have outages to Internet services.

IMPARTIAL

On 28 February 2022, following Russia's invasion of Ukraine, ICANN received a letter from the Ukrainian government asking it to 'introduce strict sanctions against the Russian Federation in the field of DNS regulation in response to its acts of aggression towards Ukraine and its citizens.' The requested sanction would remove Russia from the Internet by revoking Russian domain names from the DNS and shutting down root servers in Russia.

ICANN rejected this request because its 'globally agreed [multistakeholder] policies do not provide for ICANN to take unilateral action to disconnect these domains…such a change in the process would have devastating and permanent effects on the trust and utility of this global system'.

In a time when commercial companies were enforcing sanctions on Russia and Russia was losing seats in UN organisations, ICANN continued to operate with impartiality in alignment with its multistakeholder policies. If ICANN had been governed by commercial or multilateral approaches, this request may have been granted. This would have resulted in a loss of trust and credibility in how the Internet is governed because it would set the precedent that any government or commercial company could lose its access to the Internet on which its livelihood now depends if it did not act in accordance with the geopolitical interests of the majority of governments. This demonstrates the importance of the multistakeholder model to operate outside of geopolitical forces to enable an open, trusted and interoperable Internet.

Challenges to the multistakeholder model

Despite its strengths, the multistakeholder model has also faced criticism and challenges. One major concern is the question of representation. While the model aims to be inclusive, not all stakeholders have equal resources or capacities to participate effectively in governance processes. In addition, the current multistakeholder governance mechanisms were created by organisations in countries that pioneered the Internet, which meant that later adopters of the Internet have less influence on the existing governance mechanisms. This can lead to power imbalances, with certain actors, particularly those from the private sector or from developed countries, having a disproportionate influence on decision-making.

Another challenge is the complexity and inefficiency that can arise from the multistakeholder approach. With so many different actors involved with competing interests, decision-making processes can be slow and difficult to coordinate. The lack of formal authority can also make it challenging to enforce decisions and hold stakeholders accountable.

Additionally, the multistakeholder model has faced political challenges. The multistakeholder model is contrary to many existing political and multilateral models where governments have more influence. Some governments have expressed discomfort with the perceived loss of sovereignty and control that comes with this model. They argue for a more state-centric approach to Internet governance, leading to debates over the role of international organisations like the UN (including the International Telecommunications Union (ITU)) in governing the Internet. These tensions reflect broader debates about the balance between openness and control, and freedom and security in the governance of the Internet.

Case Study: Historical Evolution of Internet Governance

BACKGROUND

The Internet, as we know it today, is a global system of interconnected networks that enables billions of devices worldwide to communicate with each other. However, the governance of this complex system has not always been as structured and multi-faceted as it is now. Initially, Internet governance was more centralised and primarily controlled by the United States Government and related entities.

THE CHALLENGE

In the early days, the Internet was a research project funded by the U.S. Department of Defense, and governance was largely in the hands of technical experts who developed the protocols and managed the infrastructure. However, as the Internet grew and became more commercialised and global, the need for a more inclusive and transparent governance model became evident.

THE IMPACT

The shift from a primarily U.S. controlled system to a more global and multistakeholder model has had profound impacts on how the Internet operates and evolves. On the one hand, this transition has allowed for greater inclusivity, with more voices and perspectives being represented in governance discussions. On the other hand, it has also led to increased complexity, with debates around key issues such as net neutrality, digital rights, cybersecurity, and the digital divide becoming increasingly contentious.

ACTIONS TAKEN AND LESSONS LEARNED

Over time, several key organisations have emerged as important players in Internet governance, including the Internet Engineering Task Force (IETF), Regional Internet Registries (RIRs), the Internet Corporation for Assigned Names and Numbers (ICANN) and the World Wide Web Consortium (W3C). These organisations along with national governments, private sector companies, and civil society groups, work together in a multistakeholder model to shape the policies and standards that guide the Internet's operation and development.

However, the evolution of Internet governance is still ongoing, and significant challenges remain. These include debates over the balance of power between different stakeholders, questions around how to ensure fair and equitable access to the Internet, and concerns about how to protect users' rights and privacy in an increasingly digital world.

This case study highlights the complexities of Internet governance and the need for ongoing dialogue and cooperation among a diverse range of actors. It underscores the importance of a multistakeholder approach in navigating these complexities, fostering an Internet that is secure, open and inclusive.

Internet governance landscape: an overview

The Internet governance landscape is an intricate tapestry woven from a diverse array of structures and organisations. Key players include technical standards bodies such as the IETF and the World Wide Web Consortium (W3C), operational entities like ICANN, policy discussion forums like the IGF, as well as governments and inter-governmental organisations such as the ITU. Alongside these global entities, a host of national and regional bodies also play significant roles.

These entities collectively promote a multistakeholder approach to governance, embracing participation from governments, private sector entities, civil society, academia, technical community and the Internet user community. The result is a decentralised, inclusive governance model reflecting the diverse interests of the global Internet community.

Understanding governance models and their tensions

Three primary models characterise the governance landscape: multistakeholder, multilateral, and unilateral. These models exist on a continuum, with each actor in the landscape typically operating within this range, their positions influenced by their interests, influence, and specific issues at hand.

The multistakeholder model, best represented by organisations like ICANN, fosters broad participation across sectors, creating a decentralised and inclusive approach to Internet governance. Conversely, the multilateral model, often represented by inter-governmental organisations such as the ITU, involves a more substantial role for state actors in decision-making[4]. Over the past two decades, these two models have seen an underlying tension, with some advocating for a more significant government influence over Internet governance.

The unilateral model, typically enacted by national governments, supranational organisations like the European Union (EU) or Big Tech companies, involves independent decision-making that can significantly impact the governance of the Internet. Such actions often necessitate adaptations from other countries and organisations to ensure regulatory interoperability.

An additional factor impacting the tension between models is that the multistakeholder model is unusual and unique to Internet governance. Governments and Big Tech companies, which typically operate using a top-down approach, are required to adjust their approach when contributing to the bottom-up multistakeholder approach for Internet governance. Governments and Big Tech may disregard the multistakeholder model when making unilateral decisions or may be reluctant to engage in the multistakeholder approach where they may have less influence on outcomes.

The table below illustrates key players representing these three models.

[4] Stakeholders can contribute to multilateral processes in some capacity through consultations or through joining onto national delegations, but they have less influence in multilateral processes compared to the multistakeholder model.

Table 2: Stakeholder representatives

Model	Key representative stakeholder	Influence Mechanism
Multilateral	United Nations	Treaties and capacity building (which influences governments' legislation and regulation)
Unilateral	National Governments	Legislation and regulation (which influences multistakeholder policies and standards)
Multistakeholder	ICANN	Technical expertise

In this intricate web of influences and interests, the IGF, despite not having decision-making powers, serves as a crucial bridge. The IGF fosters dialogue and understanding among these three models, mediating tensions and promoting cooperation in the ever-evolving landscape of Internet governance.

Case Study: Multistakeholderism in Internet Governance

Multistakeholderism is a model of Internet governance that involves the participation of multiple stakeholders, including governments, private sector entities, non-governmental organisations, and individual Internet users. This model emerged from the belief that Internet governance should reflect the diversity of the Internet community and the wide range of interests and perspectives it encompasses.

While the multistakeholder model is generally recognised as the most inclusive and democratic approach to Internet governance, implementing it in practice can be challenging. Key issues include ensuring meaningful and balanced participation from all stakeholder groups, ensuring that parties can’t deliberately stall progress by manipulating consensus processes, managing conflicts of interest, and addressing power imbalances. Moreover, the complexity and technical nature of many Internet governance issues can create barriers to participation, particularly for individuals and organisations with limited resources or expertise.

Despite these challenges, the multistakeholder model has had a significant impact on the evolution of the Internet. It has enabled a broad range of voices to contribute to policy discussions, facilitated the development of innovative solutions to complex issues, and helped to maintain the open and decentralised nature of the Internet. Moreover, it has provided a framework for addressing contentious issues in a collaborative and consensus-oriented manner.

Various multistakeholder initiatives have been implemented to improve the effectiveness of this model. For example, the IGF has implemented capacity-building programs to enhance the ability of underrepresented stakeholders to participate in Internet governance discussions. Meanwhile, entities like ICANN have developed mechanisms to ensure that policy decisions are made through a bottom-up, consensus-based process.

These initiatives highlight the potential of Multistakeholderism to foster an inclusive and democratic approach to Internet governance. However, they also underscore the need for ongoing efforts to strengthen the model and address its limitations. This includes enhancing transparency, improving representativeness, and developing resources and support to facilitate wider and more meaningful participation.

The case study of Multistakeholderism in Internet governance underscores the importance of cooperation and dialogue in managing the Internet's complex ecosystem. It reaffirms the value of inclusivity and diversity in decision-making processes and highlights the need for continuous efforts to ensure that the benefits of the Internet are shared equitably.

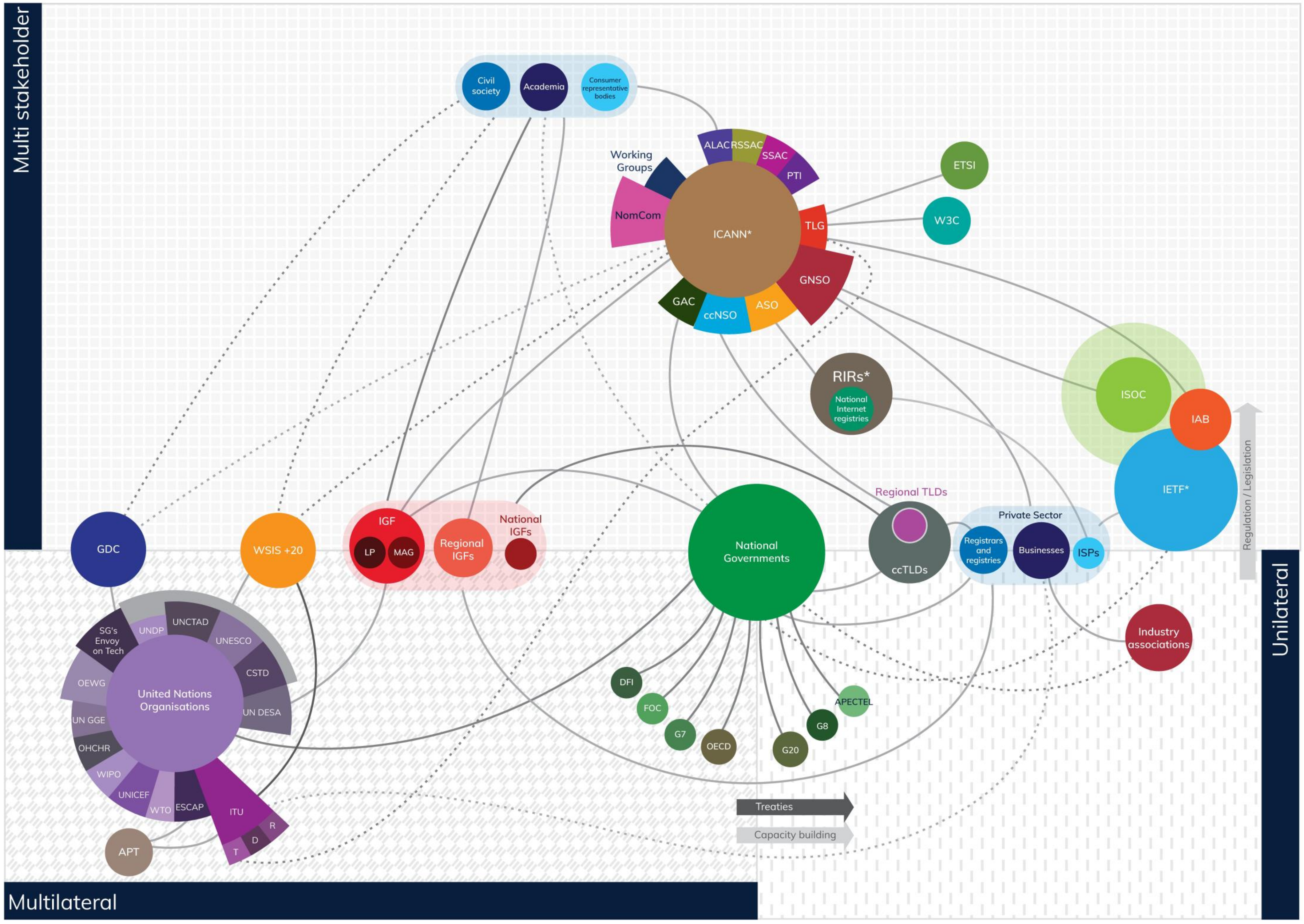
Figure 1: Overview of the Internet Governance Landscape (updated further to stakeholder feedback)

ALAC	At-Large Advisory Committee
APT	Asia-Pacific Telecommunity
ASO	Address Supporting Organization
ccNSO	Country Code Names Supporting Organization
ccTLDs	Country Code Top Level Domains
CSTD	Commission on Science and Technology for Development
DFI	Declaration for the Future of the Internet
ESCAP	Economic and Social Commission for Asia and the Pacific
ETSI	European Telecommunications Standards Institute
FOC	Freedom Online Coalition
G7	Group of Seven
GAC	Governmental Advisory Committee
GDC	Global Digital Compact
GNSO	Generic Names Supporting Organization
IAB	Internet Architecture Board
ICANN	Internet Corporation for Assigned Names and Numbers
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
ISOC	Internet Society
ISPs	Internet service providers
ITU	International Telecommunication Union
ITU-D	ITU Telecommunication Development Sector
ITU-R	ITU Radiocommunication Sector
ITU-T	ITU Telecommunication Standardization Sector
LP	Leadership Panel
MAG	Multistakeholder Advisory Group
NomCom	Nominating Committee
NRO	Number Resource Organisation
OECD	Organisation for Economic Co-operation and Development
OEWG	Open-Ended Working Group
OHCHR	Office of the United Nations High Commissioner for Human Rights
RIRs	Regional Internet Registries
RSSAC	Root Server System Advisory Committee
SSAC	Security and Stability Advisory Committee
SG	United Nations Secretary-General
TLDs	Top Level Domains
TLG	Technical Liaison Group
UNCTAD	United Nations Conference on Trade and Development
UNDESA	United Nations Department of Economic and Social Affairs
UNDP	United Nations Development Programme
UNESCO	United Nations Educational, Scientific and Cultural Organization
UN GGE	United Nations Group of Governmental Experts
UNICEF	United Nations Children's Fund
W3C	World Wide Web Consortium
WSIS	World Summit on the Information Society
WTO	World Trade Organization

In the multistakeholder model all stakeholders that have an interest in the Internet contribute to how the Internet is governed. Stakeholders include users, academia, businesses, non-profit organisations, internet organisations and governments.

Australian Government
Department of Infrastructure, Transport,
Regional Development, Communications and the Arts

Overview of the Internet Governance Landscape

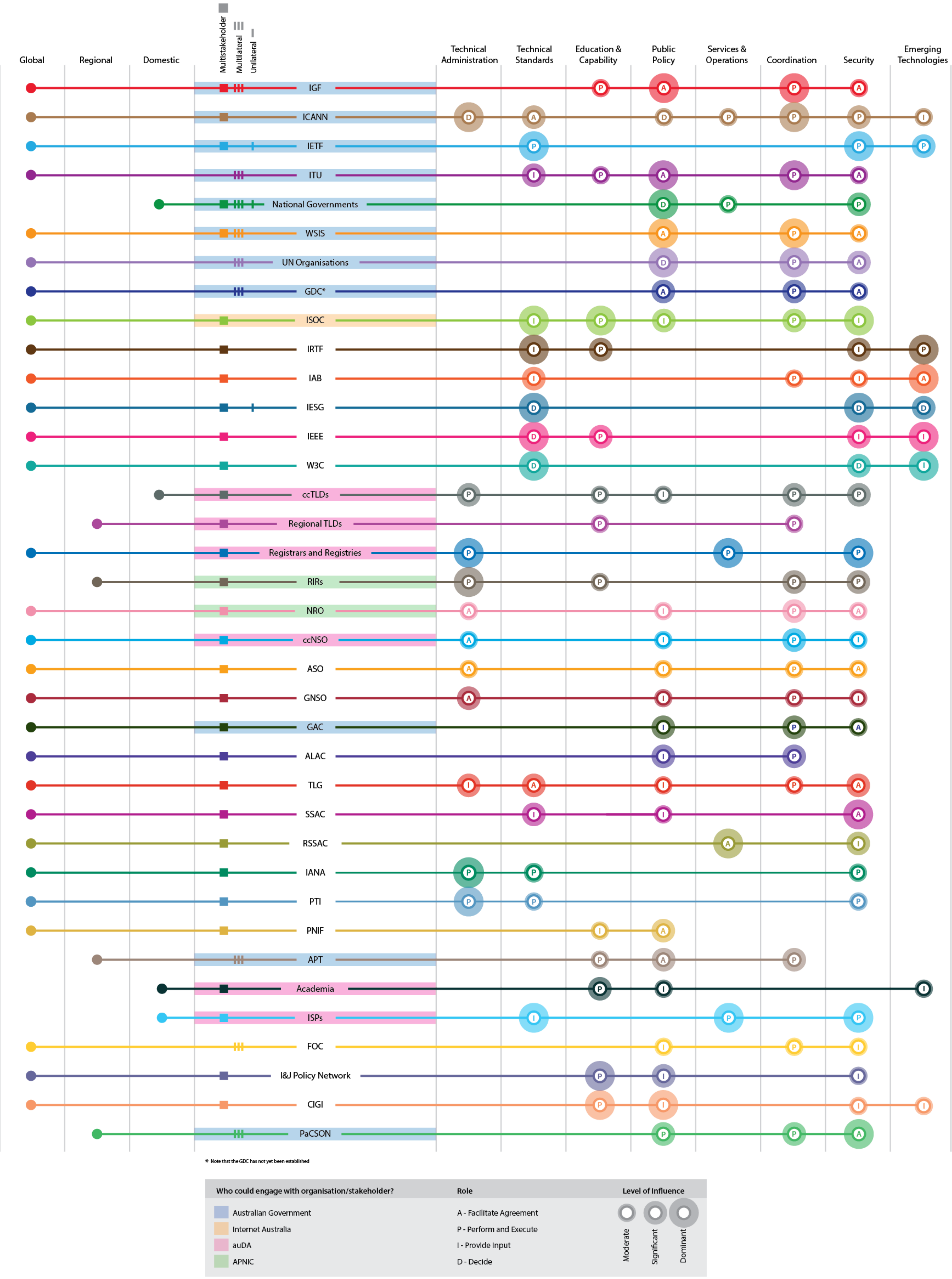


Size: level of influence on the landscape **Position:** preference or ability for means of influence (multistakeholder/ multilateral/ unilateral) — significant relationships between entities .... moderate relationship between entities
*Technical associations taking on coordindation of the technical transport layers of the internet

29th of September 2023

Figure 2: Stakeholders/fora by topic

Stakeholder/Fora by Topic



Global	Regional	Domestic	Multistakeholder	Multilateral	Unilateral		Technical Administration	Technical Standards	Education & Capability	Public Policy	Services & Operations	Coordination	Security	Emerging Technologies
●			■	III		IGF			P	A		P	A	
●			■			ICANN	D	A		D	P	P	P	I
●			■		I	IETF		P					P	P
●				III		ITU		I	P	A		P	A	
		●	■	III	I	National Governments				D	P		P	
●			■	III		WSIS				A		P	A	
●				III		UN Organisations				D		P	A	
●				III		GDC*				A		P	A	
●			■			ISOC		I	P	I		P	I	
●			■			IRTF		I	P				I	P
●			■			IAB		I				P	I	A
●			■		I	IESG		D					D	D
●			■			IEEE		D	P				I	I
●			■			W3C		D					D	I
		●	■			ccTLDs	P		P	I		P	P	
	●		■			Regional TLDs			P			P		
●			■			Registrars and Registries	P				P		P	
	●		■			RIRs	P		P			P	P	
●			■			NRO	A			I		P	A	
●			■			ccNSO	A			I		P	I	
●			■			ASO	A			I		P	A	
●			■			GNSO	A			I		P	I	
●			■			GAC				I		P	A	
●			■			ALAC				I		P		
●			■			TLG	I	A		I		P	A	
●			■			SSAC		I		I			A	
●			■			RSSAC					A		I	
●			■			IANA	P	P					P	
●			■			PTI	P	P					P	
●			■			PNIF			I	A				
	●			III		APT			P	A		P		
		●	■			Academia			P	I				I
		●	■			ISPs		I			P		P	
●				III		FOC				I		P	I	
●			■			I&J Policy Network			P	I			I	
●			■			CIGI			P	I			I	I
	●			III		PaCSON				P		P	A	

* Note that the GDC has not yet been established

Who could engage with organisation/stakeholder?	Role	Level of Influence
🟦 Australian Government	A - Facilitate Agreement	○ Moderate
🟧 Internet Australia	P - Perform and Execute	○ Significant
▨ auDA	I - Provide Input	○ Dominant
🟩 APNIC	D - Decide	

Table 3: List of acronyms used in Figures 1 and 2

Acronym	Name
ALAC	At-Large Advisory Committee
APT	Asia-Pacific Telecommunity
ASO	Address Supporting Organization
ccNSO	country code Names Supporting Organization
ccTLDs	country code Top Level Domains
CIGI	Centre for International Governance Innovation
CSTD	Commission on Science and Technology for Development
DFI	Declaration for the Future of the Internet
ESCAP	Economic and Social Commission for Asia and the Pacific
ETSI	European Telecommunications Standards Institute
FOC	Freedom Online Coalition
G7	Group of Seven
GAC	Governmental Advisory Committee
GDC	Global Digital Compact
GNSO	Generic Names Supporting Organization
I&J Policy Network	Internet & Jurisdiction Policy Network
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IEEE	Institute of Electrical and Electronics Engineers
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IRTF	Internet Research Task Force
ISOC	Internet Society
ISPs	Internet service providers
ITU	International Telecommunication Union
ITU-D	ITU Telecommunication Development Sector
ITU-R	ITU Radiocommunication Sector
ITU-T	ITU Telecommunication Standardization Sector
LP	Leadership Panel
MAG	Multistakeholder Advisory Group
NomCom	Nominating Committee
NRO	Number Resource Organisation
OECD	Organisation for Economic Co-operation and Development
OEWG	Open-Ended Working Group
OHCHR	Office of the United Nations High Commissioner for Human Rights
PaCSON	Pacific Cyber Security Operational Network
PNIF	Policy Network on Internet Fragmentation
PTI	Public Technical Identifiers
Regional TLDs	Regional Top Level Domains
RIRs	Regional Internet Registries
RSSAC	Root Server System Advisory Committee
SG	United Nations Secretary-General
SSAC	Security and Stability Advisory Committee
TLDs	Top Level Domains
TLG	Technical Liaison Group
UN GGE	United Nations Group of Governmental Experts
UN Organisations	United Nations Organisations
UNCTAD	United Nations Conference on Trade and Development
UNDESA	United Nations Department of Economic and Social Affairs
UNDP	United Nations Development Programme
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNICEF	United Nations Children's Fund
W3C	World Wide Web Consortium
WSIS	World Summit on the Information Society
WTO	World Trade Organization

Key parts of the Internet governance landscape

The Internet governance landscape at the logical layer is comprised of various parts that need to be governed:

- IP addresses
- domain names
- shared services such as root servers, Internet exchange points and network operations
- technical standards and protocols
- policy and regulation.

Even though content is excluded from this list, often issues related to content trigger changes to policy and regulation that have flow-on effects on other parts of the landscape (e.g., personal names and trademarks used within domain names). An example of this can be seen in the case study below.

Case Study: The Impact of GDPR on Internet Governance

BACKGROUND

The General Data Protection Regulation (GDPR) is a comprehensive privacy law adopted by the European Union (EU) on 14 April 2016 and took effect on 25 May 2018. The law aims to protect the personal data of EU citizens and residents and regulate how businesses handle such data. While GDPR is a regional regulation, its global reach has significant implications for Internet governance due to the borderless nature of the Internet.

THE CHALLENGE

Before GDPR, the WHOIS system, managed by the Internet Corporation for Assigned Names and Numbers (ICANN), publicly displayed the contact information of domain name registrants, including names, addresses, and email addresses. This transparency was vital for many stakeholders, including law enforcement agencies, intellectual property rights holders, and cybersecurity researchers, to track malicious activity and enforce laws on the Internet.

However, GDPR's stringent rules on personal data protection posed a challenge to this system. The open display of registrant information was deemed non-compliant with GDPR, leading to a conflict between regional privacy law and global Internet governance standards. The implementation of GDPR forced ICANN to redact personal information from WHOIS data, significantly affecting how different stakeholders interacted with the system.

ACTIONS TAKEN AND LESSONS LEARNED

In response to the challenges posed by GDPR, ICANN adopted a Temporary Specification in May 2018 to modify the existing requirements in the Registrar Accreditation and Registry Agreements in order to comply with GDPR. The Temporary Specification maintains robust collection of registration data but restricts most personal data to layered/tiered access. Users with a legitimate and proportionate purpose for accessing the non-public Personal Data will be able to request such access through Registrars and Registry Operators. The Temporary Specification has resulted in Registrars and Registry Operators devising their own approaches.

In May 2018 ICANN filed injunction proceedings against a German-based registrar who informed ICANN that it would no longer collect administrative and technical contact information. The registrar believes collection of that particular data would violate the GDPR. ICANN’s contract with the registrar requires that information to be collected. Through filing the injunction, ICANN asked the German legal system to interpret the legality of the WHOIS system with regards to GDPR. The court refused to issue an injunction – a decision that stands unchanged despite two appeals by ICANN.

The Temporary Specification expired in May 2019. In July 2018 ICANN initiated an expedited policy development process (EPDP) to determine if the Temporary Specification should become an ICANN Consensus Policy as is or with modifications. In February 2020 the EPDP team published its initial report for public comment which proposed a new system, known as the System for Standardized Access/Disclosure (SSAD). The SSAD aims to provide accredited users with access to non-public WHOIS data, balancing the need for data access with GDPR's privacy mandates. In January 2022 ICANN published its SSAD Operational Design Assessment where is estimates that the development and implementation will take 5-6 years. The process of implementing the proposed SSAD system is still ongoing.

Throughout this process, ICANN sought input from EU authorities and its constituents. Such cooperation sought to address the needs of various stakeholders, however the inability to resolve this issue in a timely manner is often cited as an example of the slowness inherent in a multistakeholder model and the need for the model to evolve to be more responsive.

GDPR is an example of how governments can take unilateral action to influence the Internet governance landscape. As governments face increasing pressure from their citizens to regulate the Internet, they pass laws that may have global implications on how the Internet works. This underscores the complex interplay between regional laws and global Internet governance standards, highlighting the challenges of accommodating diverse legal frameworks in a borderless digital realm.

The GDPR and WHOIS case serves as a potent reminder that Internet governance is not solely a technical issue. It is deeply intertwined with broader societal values and norms, such as privacy and data protection. This calls for a holistic approach to Internet governance that considers not only the technical and operational aspects but also legal, economic, and societal factors.

Key players, influence and relationships

The high-level overview of the Internet governance landscape in Figure 1 shows the key players in the landscape. These players often collaborate and engage with each other through various fora, creating a complex web of relationships that shape the global Internet governance landscape.

The relative influence on the landscape is indicated by the size of the circles representing each stakeholder. In the current landscape, multistakeholder Internet organisations like ICANN and IETF have a large influence on the landscape. Multilateral organisations such as the UN have a slightly lesser influence on Internet governance now. Governments also have a big influence when they implement unilateral regulation and legislation. The driver for governments exerting influence unilaterally is demonstrated by the lesser level of influence they possess as part of ICANN's Government Advisory Committee (GAC) and attempts at multilateral influence through the ITU, EU and other UN organisations.

The relationships between stakeholders and fora are indicated by the lines between stakeholders in Figure 1 to demonstrate pathways of influence for various stakeholder groups. These lines show the interface points for stakeholders from various parts of the landscape. This means that organisations, whether they operate regionally like RIRs, or domestically like country code Top Level Domain organisations (ccTLDs), can influence and shape global Internet governance by providing their unique perspectives and insights.

Key stakeholders and fora by topic

The roles performed by various stakeholders are summarised in Figure 2. Many organisations perform several roles to varying degrees. The figure indicates the primary roles performed, noting that some stakeholders also perform secondary roles that are not reflected in the diagram.

The roles performed by stakeholders in the landscape can be categorised by the following topics:

- **Registration Services:** administers IP addresses and the domain name system.

- **Technical Standards:** develops or maintains the protocols and standards that determine how data is routed through the Internet.
- **Education & Capability:** performs research, training and upskilling activities related to Internet governance.
- **Public Policy:** develops, discusses or implements norms, policies, regulations, and legislation related to Internet governance.
- **Services & Operations:** provides shared services required for the Internet to operate, such as root servers, internet exchange points, networks and services that allow users to connect and participate in the Internet.
- **Coordination:** facilitates the coordination of stakeholders to perform tasks and create opportunities for stakeholders to discuss topics relevant to Internet governance.
- **Security:** has influence in the standards, policies, norms or regulations that keep the Internet secure and safe.
- **Emerging Technologies:** has influence or capability to develop new technology that could impact the Internet governance landscape.

Figure 2 aims to identify the relevant stakeholders and fora that have influence or a strong interest in the topics above. Knowing which stakeholders or fora to engage with on a particular issue is an important factor for stakeholders who want to contribute to Internet governance.

> The mechanism for influencing the landscape depends on the domain that is impacted.
>
> Subject Matter Expert Research Participant

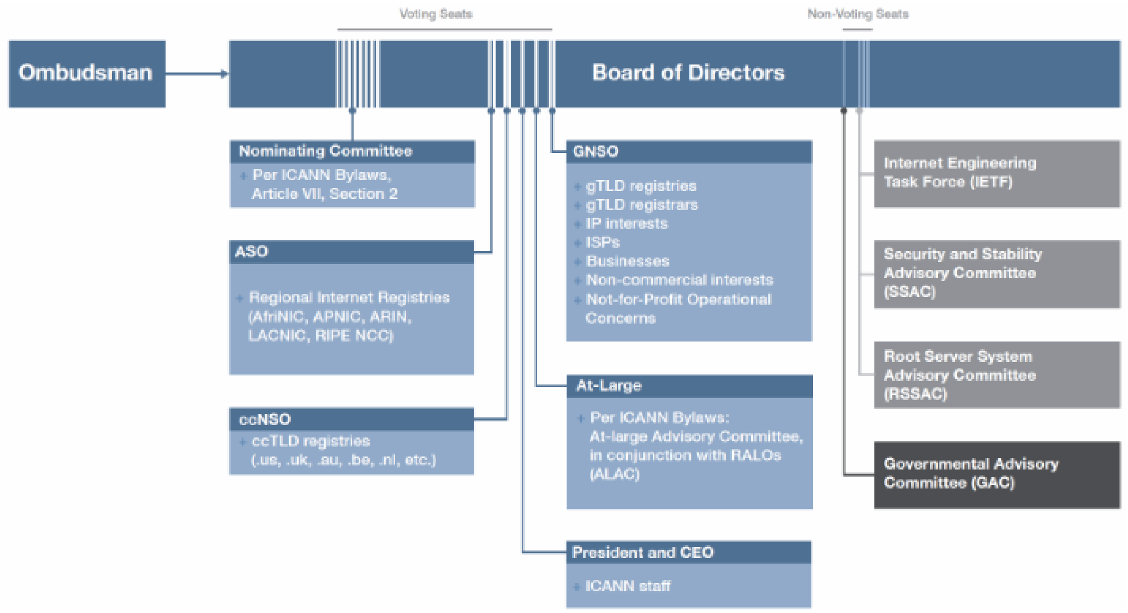
ICANN

ICANN (Internet Corporation for Assigned Names and Numbers) plays a crucial role in the Technical Administration, Coordination, and Security of the Internet. As a non-profit organization, ICANN is responsible for coordinating the maintenance and procedures of various databases that manage the namespaces and numerical spaces of the Internet. This coordination ensures the stable and secure operation of the network.

To make policy decisions related to the Internet's unique names and numbers, ICANN follows a multistakeholder approach. It establishes supporting organisations and groups that allow stakeholders from diverse backgrounds to contribute to policy development. The composition of ICANN's Board of Directors reflects this diversity and represents the multitude of stakeholders coordinated by ICANN.

The composition of ICANN's Board of Directors in Figure 3 reflects the diverse range of stakeholders that are coordinated by ICANN.

Figure 3: The multistakeholder representation of ICANN's board of directors[5]


Voting Seats
Non-Voting Seats
Ombudsman
Board of Directors
Nominating Committee
Per ICANN Bylaws, Article VII, Section 2
ASO
Regional Internet Registries (AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC)
ccNSO
ccTLD registries (.us, .uk, .au, .be, .nl, etc.)
GNSO
gTLD registries
gTLD registrars
IP interests
ISPs
Businesses
Non-commercial interests
Not-for-Profit Operational Concerns
At-Large
Per ICANN Bylaws: At-large Advisory Committee, in conjunction with RALOs (ALAC)
President and CEO
ICANN staff
Internet Engineering Task Force (IETF)
Security and Stability Advisory Committee (SSAC)
Root Server System Advisory Committee (RSSAC)
Governmental Advisory Committee (GAC)

While ICANN sets broad policies, it recognizes the need for RIRs, ccTLDs managers, registries, and registrars to apply additional policies based on the specific requirements of their jurisdictions, such as government legislation and regulation. Sometimes ICANN must update its policies to comply with national governments' legislation and regulations, as seen in the GDPR case study on page 26.

In terms of Technical Administration, ICANN is responsible for the operation of DNS root servers and the technical management of unique names and numbers. The IANA functions, which include the administration of unique numbers, are performed by Public Technical Identifiers (PTI) as an ICANN affiliate. The coordination of unique names involves collaboration with ccTLD managers, registries, and registrars.

ICANN engages in the multilateral landscape through participation in forums like the Internet Governance Forum (IGF). Additionally, ICANN's Technical Liaison Group (TLG) ensures representation and cooperation with the International Telecommunication Union's Telecommunication Standardization Sector (ITU-T). These interactions further promote coordination and collaboration across different organisations and initiatives in the Internet governance landscape.

ICANN Supporting Organisations

ICANN has several Supporting Organisations that play integral roles in its operations and decision-making processes:

Address Supporting Organization (ASO): Reviews and develops recommendations on IP address policy and advises the ICANN Board on policy issues related to the operation, assignment, and management of IP addresses. The ASO represents the Regional Internet Registries (RIRs) and contributes their expertise in shaping IP address policies.

[5] From: ICANN, 'Groups', accessed 23 June 2023. https://www.icann.org/resources/pages/groups-2012-02-06-en

Country Code Names Supporting Organization (ccNSO): Created for and by country code Top-Level Domain (ccTLD) managers, the ccNSO provides a platform for consensus-building, technical cooperation, and the development of voluntary best practices among ccTLDs. It fosters collaboration among ccTLD managers to effectively manage and govern their respective country code domains.

Generic Names Supporting Organization (GNSO): Develops policies related to generic Top-Level Domains (gTLDs) to ensure fair and orderly operation across the global Internet. The GNSO aims to promote innovation and competition while maintaining a balanced and inclusive approach to gTLD management.

These Supporting Organisations within ICANN, in conjunction with the ICANN Groups, Affiliates, and Departments, collectively contribute to Technical Administration, Public Policy, Coordination, and Security aspects of the Internet. Their collaborative efforts and expertise are essential in achieving the stable and secure operation of the global Internet ecosystem.

ICANN Groups

ICANN has various groups that contribute to its mission in different capacities:

At-Large Advisory Committee (ALAC): Represents the interests of end-users and advises on ICANN activities and policies. ALAC includes members from Regional At-Large Organisations (RALOs) worldwide. RALOs include 251 At-Large Structures (e.g., Internet Society Chapters, national consumer groups) across 104 countries and territories, allowing diverse participation from Internet-related consumer rights groups, academic organisations, and individual members. This inclusive community ensures a broad range of perspectives in Internet governance.

Governmental Advisory Committee (GAC): The GAC constitutes the voice of Governments and Intergovernmental Organizations (IGOs) in ICANN's multistakeholder structure. Created under the ICANN Bylaws, the GAC is an advisory committee to the ICANN Board. The GAC's key role is to provide advice to ICANN on issues of public policy, and especially where there may be an interaction between ICANN's activities or policies and national laws or international agreements.

Some member states with large populations who do not yet have access to the Internet find little benefit in contributing to Internet policies that have no impact on their citizens. Some member states who were excluded from the development of the Internet at its inception still feel disenfranchised when concerns raised via the GAC are dismissed by stakeholders who 'know better'. This is exacerbated by some other stakeholders in ICANN who are resistant and even hostile to government input[6]. However, if GAC member states do not feel heard or respected by ICANN stakeholders, it motivates these member states to pursue other avenues to influence Internet governance through top-down multilateral or unilateral approaches.

Nomination Committee (NomCom): An independent group within ICANN responsible for selecting members of the ICANN Board of Directors and other key leadership positions. The

[6] This view is best captured in the John Perry Barlow's Declaration of the Independence of Cyberspace outlining a vision of the Internet where governments have no sovereignty or say in internet governance.

NomCom plays a vital role in ensuring a capable and diverse leadership that can effectively address the organization's goals.

Root Server System Advisory Committee (RSSAC): Advises the ICANN Board and community on matters concerning the operation, administration, security, and integrity of the Root Server System. RSSAC's insights contribute to maintaining the stability and security of this critical infrastructure.

Security and Stability Advisory Committee (SSAC): Provides advice to the ICANN community and Board on matters related to the security and integrity of the Internet's naming and address allocation systems. SSAC's expertise contributes to the overall security and stability of the Internet ecosystem.

Technical Liaison Group (TLG): Offers technical advice to the ICANN Board on specific matters relevant to ICANN's activities. The TLG consists of representatives from renowned organisations such as the **European Telecommunications Standards Institute (ETSI)**, **Internet Architecture Board (IAB)**, **ITU-T**, and **World Wide Web Consortium (W3C)**. Their technical insights assist ICANN in making informed decisions.

Working Groups: ICANN has several working groups focused on specific activities aligned with its initiatives. These groups collaborate to address various aspects of Internet governance, policy development, and operational matters.

Affiliates and Departments

ICANN's affiliates and departments are instrumental in fulfilling its responsibilities:

IANA (Internet Assigned Numbers Authority): As a department of ICANN, IANA coordinates essential elements that contribute to the smooth functioning of the Internet. This includes the allocation of IP addresses and the management of the Domain Name System (DNS).

PTI (Public Technical Identifiers): As an affiliate of ICANN, PTI performs the IANA functions on behalf of ICANN. PTI ensures the operational coordination and maintenance of the Internet's unique identifiers in a responsible, unbiased, and effective manner.

These ICANN groups, affiliates, and departments collectively contribute to the Technical Administration, Public Policy, Coordination, and Security aspects of the Internet. Their expertise and efforts are crucial for ensuring the stable and secure operation of the global Internet ecosystem.

Regional Internet Registries

Regional Internet Registries (RIRs) play a crucial role in the Technical Administration of the internet. These organisations are responsible for overseeing the allocation and registration of Internet number resources in specific regions across the globe. There are five recognized RIRs: the African Network Information Centre (AFRINIC), the American Registry for Internet Numbers (ARIN), the Asia-Pacific Network Information Centre (APNIC), the Latin America and Caribbean Network Information Centre (LACNIC), and the Réseaux IP Européens Network Coordination Centre (RIPE NCC). It is worth noting that most RIRs were established before the Internet Corporation for Assigned Names and Numbers (ICANN).

Each RIR operates with independent communities and develops policies through independent processes. These policies are created using a bottom-up approach, driven by the community itself. However, it is important to acknowledge that the contribution to policy development is often limited to network engineers, mainly due to the knowledge barrier. Following the transition of the Internet Assigned Numbers Authority (IANA) to ICANN, ICANN now supports RIRs through a Service Level Agreement for IANA numbering functions. Under this agreement, ICANN assigns blocks of IP addresses to each RIR, which are then further allocated by the respective RIRs to Internet Service Providers (ISPs) and organisations with substantial networks. This collaborative effort, guided by a multistakeholder approach, ensures the efficient distribution and management of IP address resources in the technical administration of the internet.

In the realm of Security, RIRs play a critical role in ensuring the stability and security of Internet number resources. As organisations responsible for allocating and registering IP addresses, RIRs implement robust security measures and policies to prevent misuse and unauthorized access to these valuable resources. They collaborate with network operators, ISPs, and other stakeholders to promote secure practices and address security-related concerns. By facilitating a secure and reliable allocation system, RIRs contribute to the overall security posture of the internet, safeguarding its infrastructure and the smooth functioning of online services.

NRO (Number Resource Organization): plays a pivotal role in the coordination of Internet number resources, specifically IP addresses. As a coordinating body, the NRO brings together the five Regional Internet Registries (RIRs) to ensure a cohesive and globally synchronized approach. By fostering collaboration among the RIRs, the NRO facilitates efficient management and distribution of these vital resources.

The primary responsibility of the NRO is to represent the collective interests of the RIRs within the ICANN Address Supporting Organization (ASO). This representation ensures that the RIRs' voices are heard in matters concerning policy development and decision-making related to Internet number resources. By advocating for the needs and concerns of the RIRs, the NRO contributes to the creation of a harmonized and consistent framework for the allocation and administration of IP addresses on a global scale. Through this coordination, the NRO plays a crucial role in maintaining the stability and effectiveness of the Internet's addressing system.

Top Level Domain (TLD) Organisations

ccTLD Registries play a significant role in the Technical Administration of the internet. These registries are responsible for the technical management and operation of country-specific TLDs consisting of two letters, representing a particular country, sovereign state, or autonomous territory. For example, the ccTLD registry, .au Domain Administration (auDA), is responsible for Australia's (.au) TLD. ccTLDs ensure that these domains are effectively administered to serve the needs of their respective communities. In addition to adhering to ICANN's policies, ccTLDs often implement additional policies to comply with local legislation and cater to the specific requirements of their jurisdictions.

Regional TLDs, on the other hand, serve as essential entities in facilitating Services and Operations related to domain name registries within a specific region. These non-profit associations provide a platform for ccTLD organisations to exchange valuable information and insights concerning technological and operational aspects. By fostering collaboration and knowledge sharing, regional TLDs such as the Asia Pacific Top-Level Domain Association and the Council of European National Top-Level Domain Registries enable member organisations to enhance their domain name registry services, address common challenges, and promote best practices for efficient operations.

Commercial stakeholders

Registries and registrars, play a significant role in the Technical Administration of the internet. Registries are responsible for managing TLDs, including creating domain name extensions and establishing rules for those domains. They work closely with registrars to sell domain names to the public. Accredited through ICANN and operating under contracts developed through multistakeholder inputs, registries and registrars contribute to the Internet governance landscape by engaging in ICANN's Generic Names Supporting Organization (GNSO). They also apply additional policies to comply with legislation and regulations in their respective jurisdictions. While they may lobby governments directly, registries and registrars generally prefer the influence they can exert through multistakeholder mechanisms rather than multilateral approaches.

Businesses, including prominent technology companies, have a role in Technical Standards and Services and Operations within the Internet governance landscape. They engage in ICANN’s GNSO and participate in local Internet Governance Forums (IGFs). Subject to government legislation and regulation, big tech companies can influence the Internet governance landscape through unilateral actions that impact Internet governance or by directly lobbying governments to shape legislation and regulations. While businesses participate in multistakeholder forums, their direct influence through this mechanism is relatively lower compared to other approaches.

ISPs (Internet Service Provider) primarily focus on the hardware infrastructure of the Internet and contribute inputs to ICANN through the GNSO and local IGFs. As they are subject to government legislation and regulation, ISPs often choose to lobby governments directly due to their significant impact on critical infrastructure. While ISPs are crucial enablers of the Internet, their influence in the Internet governance landscape is relatively limited compared to other stakeholders.

Technical Standards

Internet Society (ISOC)

ISOC is a global non-profit organization dedicated to promoting the open development, evolution, and use of the Internet for the benefit of all people worldwide. ISOC plays a significant role in Technical Standards through its participation in ICANN’s GNSO and TLG. It also acts as an informal coordinator among various Internet organisations and supports policy makers in understanding the impacts of policies on Internet governance. ISOC has a strong influence within the technical Internet community and serves as the corporate home for the Internet Architecture Board (IAB), Internet Engineering Task Force (IETF), and Internet Research Task Force (IRTF). While ISOC is the corporate home, IETF and IRTF operate independently.

Internet Architecture Board (IAB) provides long-term technical direction for Internet development, ensuring that the Internet continues to grow and evolve as a platform for global communication and innovation. As an advisory body of the Internet Society, the IAB oversees the technical activities of the IETF and IRTF. It plays a crucial role in shaping Technical Standards by providing guidance and expertise on Internet protocols and standards.

Internet Engineering Task Force (IETF) is an open standards organization responsible for developing and promoting voluntary Internet standards, particularly the standards that comprise the Internet protocol suite (TCP/IP). With a rich history dating back to the inception of the Internet, the IETF works collaboratively with industry stakeholders to create interoperable standards that drive the Internet's technical standards. IETF is the primary organisation that performs the role of developing technical standards for the Internet. It also contributes to the security of the internet by developing specifications and standards for secure routing such as DNSSEC and RPKI. The IETF performs a role in developing emerging technologies to support the internet, however it takes a shorter-term view than the IRTF.

Anyone can participate in the development of IETF standards by authoring documents, engaging via mailing list discussion, or attending meetings. The IETF operates under the oversight of the Internet Architecture Board (IAB) and works in parallel with the Internet Research Task Force (IRTF).

IESG (Internet Engineering Steering Group): The group within the IETF which is responsible for the technical management of IETF activities and the Internet standards process. It is directly responsible for the actions associated with entry into and movement along the Internet "standards track," including final approval of specifications as Internet standards. Internet standards are developed in an open, bottom-up approach by the IETF, but the IESG decides which standards are created and approved.

Internet Research Task Force (IRTF) is a non-profit technology research organization focused on long-term technical topics related to Internet protocols, applications, architecture, and technology. Like the IETF, the IRTF operates under the oversight of the Internet Architecture Board (IAB). It conducts research and explores emerging areas of Internet technology, contributing to the development of Technical Standards that shape the future of the Internet.

European Telecommunications Standards Institute (ETSI)

ETSI is one of the three European Standards Organisations responsible for telecommunications, broadcasting, and electronic communications networks and services. ETSI plays a vital role in Technical Standards by defining regional standards and promoting the interoperability of telecommunications systems within Europe.

Institute of Electrical and Electronics Engineers (IEEE)

IEEE is a leading developer of industry standards in a wide range of technologies. IEEE's work in Technical Standards drives the functionality, capabilities, safety, and interoperability of products and services, making a significant impact on how people live, work, and communicate globally. For example, Wi-Fi and Ethernet connections rely on IEEE standards.

World Wide Web Consortium (W3C)

W3C is an international community where member organisations, staff, and the public collaborate to develop Web standards that enable users to access the Internet. Established in 1994, W3C was created to foster a consistent architecture to accommodate the rapid pace of progress in web standards for building websites, browsers, and devices. W3C's contributions to Technical Standards have played a pivotal role in shaping the web as we know it today.

These organisations, such as ISOC, IAB, IETF, IRTF, ETSI, IEEE, and W3C, are key players in Technical Standards. Their contributions and collaborations drive the development, evolution, and interoperability of technologies, protocols, and standards that form the foundation of the Internet.

United Nations Organisations

Many UN organisations are actively involved in various aspects of Internet governance due to the Internet's role in enabling economic and social benefits aligned with the UN's Sustainable Development Goals. While some UN organisations have a more direct influence on Internet governance, others address related topics that can impact Internet governance in intended or unintended ways.

ITU (International Telecommunication Union)

A specialised agency of the United Nations that is responsible for issues that concern information and communication technologies, including the development of technical standards. It is the oldest global international organisation.

The ITU is most commonly cited as the UN organisation that would lead Internet governance processes in a multilateral model. The ITU is also where some countries are trying to exert multilateral influence on the Internet governance landscape (see the New IP case study on page 13)

The ITU consists of the following three sectors, of which the ITU-T sector is most important for Internet governance:

- **ITU-T (ITU Telecommunication Standardization Sector):** Develops international standards for global infrastructure of telecommunications and information and communication technologies. Standards are critical to the interoperability of these technologies by ensuring that countries' networks and devices are speaking the same language. Historically, the standards developed by the ITU-T are less technical than the highly technical standards developed by standard organisations such as IETF, IEEE and W3C. ITU-T is not deemed to produce technical standards but works with standard development organisations. Representatives from the ITU-T are part of ICANN's TLG which advises ICANN on technical standards and ITU-T collaborates with other standard organisations as required (see New IP case study on page 13).
- **ITU-D (ITU Telecommunication Development Sector):** Works to close the digital divide and drive digital transformation for economic prosperity, job creation, digital skills development, gender equality, diversity, a sustainable and circular economy, and for saving lives.
- **ITU-R (ITU Radiocommunication Sector):** Ensures the rational, equitable, efficient and economical use of the radio-frequency spectrum by all radiocommunication services.

Technical Administration

As a specialized agency of the UN, the ITU is responsible for addressing telecommunications-related and information and communication technology issues and developing technical standards. It engages directly with ICANN, as well as other technical standard organisations like the IETF and IEEE, when necessary. The ITU's Telecommunication Standardization Sector (ITU-T) plays a crucial role in developing international standards that ensure interoperability among countries' networks and devices.

Technical Standards

The ITU-T sector within the ITU is primarily responsible for developing international standards for telecommunications-related and information and communication technologies. While historically, ITU-T standards have seen less adoption by industry compared to other standard organisations like the IETF, IEEE, and W3C, the ITU-T collaborates with these organisations as needed.

Coordination

The ITU serves as a platform for collaboration between national governments, offering multilateral processes that allow for coordination on Internet governance issues. Some countries may advocate for a more multilateral approach to Internet governance through the ITU (see New IP case study on page 13).

Security

The ITU addresses security concerns related to telecommunications and information and communication technologies, playing a role in ensuring the security and integrity of global communication systems.

UN Fora Supporting Internet Governance

IGF (Internet Governance Forum): A multistakeholder forum for policy dialogue on issues of Internet governance. It brings together all stakeholders in the Internet governance debate, including governments, the private sector, civil society, academia and the technical community. It allows for a bottom-up approach by creating a structure of regional and national IGFs organised by each respective community where inputs can be fed up to the global IGF. **The IGF is often cited as the most influential forum for Internet governance**, however, the IGF's influence is limited by its lack of decision-making powers and its lack of direct control of any parts of the Internet governance landscape. The influence of the IGF rests on its role in bridging the three models as it is driven by UN processes but includes all the stakeholders who are typically excluded from multilateral fora. The IGF has a precedent of letting participants organise specialised workshops which gives them the ability to informally set the agenda to allow discussion on a wide range of topics that are not covered in other Internet governance fora. The IGF is beneficial in discussing policy and creating a shared understanding, but it has no binding decision-making authority. Issues related to Internet governance that falls outside of the purview of Internet organisations such as ICANN do not currently have a forum for resolution. The IGF is supported by the following UN organisations:

- **MAG (Multistakeholder Advisory Group):** Prepares the programme and schedule of the annual IGF meeting. Advises the Secretary-General of the UN on the programme and schedule of the IGF meetings. The MAG is comprised of 55 members from governments, the private sector and civil society, including representatives from the academic and technical communities.
- **UNDESA (United Nations Department of Economic and Social Affairs):** Responsible for facilitating major global conferences and summits in the economic, social and environmental fields to assist countries as they find common ground, set norms, and take decisive steps forward towards sustainable development for all. Provides substantive and administrative support to the IGF Secretariat.

WSIS (World Summit on the Information Society): Co-organized by UN organisations such as UNCTAD, UNDP, and UNESCO, the WSIS is an UN-sponsored summit focused on information, communication, and the broader information society. It promotes discussions and actions to bridge the digital divide and foster digital transformation for sustainable development.

GDC (Global Digital Compact): The term "Global Digital Compact" refers to international efforts to collaborate on digital matters. The UN Tech Envoy, a position established by the UN Secretary-General, leads the establishment of the GDC, enhancing coordination and capacity for digital cooperation within the UN. The GDC is not yet established. Its implementation could have significant implications on the level of influence multilateral stakeholders have on Internet governance.

APT (Asia-Pacific Telecommunity): The APT operates as an intergovernmental organization in conjunction with telecom service providers, manufacturers of communications equipment, and research organisations. While not having a major influence on Internet governance, the APT provides a platform for discussions and alignment on Internet governance topics within the Asia-Pacific region. The APT was co-founded by ESCAP and ITU.

UN Organisations with Indirect Interests in Internet Governance

While the following UN organisations do not directly focus on Internet governance, the topics discussed within their fora often relate to the Internet and may have consequences for Internet governance:

- **CSTD (Commission on Science and Technology for Development):** Provides the General Assembly and Economic and Social Council with advice on relevant science and technology issues.
- **UN GGE (United Nations Group of Governmental Experts):** Established to study different aspects of information security. Their reports form a key part of the discussion at the United Nations on norms of responsible state behaviour in cyberspace.
- **UN OEWG (United Nations Open-Ended Working Group):** Discussed developments in the field of information and telecommunications in the context of international security.
- **UHCHR (Office of the High Commissioner for Human Rights):** Works to promote and protect the human rights.
- **UNICEF (United Nations International Children's Emergency Fund):** Responsible for providing humanitarian and developmental aid to children worldwide.
- **WIPO (World Intellectual Property Organization):** Leads the development of a balanced and effective international intellectual property system that enables innovation and creativity for the benefit of all.
- **WTO (World Trade Organization):** Deals with the global rules of trade between nations. Its main function is to ensure that trade flows as smoothly, predictably, and freely as possible.

These UN organisations contribute to global discussions, policy development, and cooperation on various aspects that intersect with Internet governance, ensuring a comprehensive and inclusive approach to addressing the challenges and opportunities of the digital age.

Other Fora

In addition to the previously mentioned stakeholders, there are several other fora that can play a role in Internet governance, addressing various aspects related to technical administration, technical standards, coordination, and security. While these fora are not exhaustive, they provide insight into the diverse landscape where Internet governance issues can arise.

Public Policy

OECD (Organisation for Economic Co-operation and Development): The OECD is an international organization focused on developing policies for better lives, aiming to shape policies that promote prosperity, equality, opportunity, and well-being. While Internet governance is not its primary focus, discussions and decisions within OECD fora can have an impact on Internet governance. Some view the OECD processes as more outcome-oriented compared to UN processes, and topics discussed in OECD fora can sometimes foreshadow issues that later emerge in UN processes. However, the OECD's limited inclusion of countries restricts its effectiveness as an inclusive forum for Internet governance.

Coordination and Security

FOC (Freedom Online Coalition): The FOC is a coalition of 37 governments working together to support Internet freedom and protect fundamental human rights, such as free expression, association, assembly, and online privacy worldwide. While the FOC does not currently hold significant influence in the Internet governance landscape, its existence demonstrates the presence of numerous fora that have the potential to impact Internet governance.

These additional fora reflect the diverse range of stakeholders and organizations involved in discussions and decisions concerning Internet governance. While their impact may vary, they contribute to the complex landscape of Internet governance and highlight the need for collaboration and coordination among various entities to address the challenges and opportunities of the digital era.

Research

In the realm of research, several organizations contribute to the understanding and advancement of Internet governance, particularly in the areas of technical administration, technical standards, coordination, and security.

Academia

Academia has historically played a significant role in shaping the development of the Internet. Through ongoing research and engagement in Internet governance processes, academia continues to contribute valuable insights and expertise. Participation in forums such as ICANN's At-Large Advisory Committee (ALAC) and local, regional, and global Internet Governance Forums (IGFs) allows academia to contribute to policy discussions and shape the future of Internet governance.

Policy and Governance Think Tanks

Internet & Jurisdiction Policy Network (I&J Policy Network): This multistakeholder organization addresses the complex tension between the cross-border nature of the Internet and national jurisdictions. By facilitating a global policy process involving governments, major internet companies, technical operators, civil society groups, academia, and international organizations from over 70 countries, the I&J Policy Network aims to develop innovative policy frameworks that reconcile these competing interests.

Centre for International Governance Innovation (CIGI): CIGI is an independent, non-partisan think tank dedicated to conducting world-leading research and analysis to offer innovative policy solutions for the digital era. With a focus on the intersection of technology and international governance, CIGI addresses critical global issues related to the Internet. Through its research efforts, CIGI contributes to shaping effective policies that promote a secure, inclusive, and well-governed digital environment.

These research-focused organizations, through their academic pursuits and policy analysis, provide valuable insights and recommendations that inform discussions and decision-making processes in the field of Internet governance. Their contributions contribute to the overall understanding and improvement of technical administration, technical standards, coordination, and security within the global Internet ecosystem.

Challenges to effective Internet governance

In an era marked by increasing digitisation, the governance of the Internet presents numerous challenges that must be addressed effectively to ensure its continued growth and utility. These challenges range from technical issues to legal and socio-political dilemmas, including the fragmentation of the Internet, unilateral action, the digital divide, the role of Big Tech companies, cybersecurity threats, and ethical concerns. This section delves into each of these challenges, shedding light on their implications and the urgency of addressing them in the evolving landscape of Internet governance.

Fragmentation of the Internet

Fragmentation is the idea that the Internet may be in danger of splitting into a series of cyberspace segments, thus endangering its global connectivity. The risk of the Internet splitting into several networks that are not interoperable with each other is a major concern for all stakeholders because the greatest utility of the Internet comes from its global, interoperable nature.

Fragmentation of the Internet does not have a widely agreed definition yet, but the following definitions may be helpful:

- **Technical fragmentation**: fragmentation that challenges the interoperability of the global core of the Internet
- **Fragmentation of the user experience**: fragmentation that results in a different user experience of the Internet, depending on where one is accessing from.

Fragmentation of the user experience typically occurs in the content layer of the internet and is often the result of government or business policies, actions or practices that constrain or prevent certain uses of the Internet to create, distribute, or access information resources. Fragmentation of the user experience can be desirable (e.g., parental control to restrict children's access to inappropriate content or geo-blocking certain content on streaming services to uphold licensing agreements). Governments have a sovereign right to implement policies and actions that may constrain or prevent certain uses of the Internet to align to their legislation and their citizens' culture, religions and social norms. These points of difference are often not considered fragmentation even though they do result in a fragmentation of the user experience. Fragmentation of the user experience has an impact on human rights and social freedoms (e.g., it may constrain your right to access information or your right of free speech or it may make it difficult to assert your right to defend yourself against defamatory content that you cannot see within your jurisdiction). However, fragmentation of the user experience does not put the core of the Internet at risk (unless a continued disruption of free flow of data leads to the creation of alternative applications or services that are not interoperable with the Internet).

Technical fragmentation occurs when the underlying infrastructure no longer allows systems to be fully interoperable and exchange data packets and function consistently at all end points. Technical fragmentation is a threat to the core of the Internet.

Technical fragmentation can stem from many causes, including the non-exhaustive list below:

- Technical issues:

  - IPv4 to IPv6 transition: IPv4 is the fourth version of the Internet Protocol which has ~4.3 billion IP addresses. The explosive growth of the Internet has meant that IPv4 does not have sufficient IP addresses to support the future growth of the Internet. IPv6 was created to solve this problem by allowing for 3.4×10^{38} IP addresses. IPv4 and IPv6 are not interoperable and an unsuccessful transition from IPv4 to IPv6 could lead to technical fragmentation. This risk has been mitigated by implementing dual stacking where networking devices are configured with both IPv4 and IPv6 capabilities.
  - Duplication or competition between standards: if standards bodies like IETF and ETSI publicly duplicate standards that result in competing alternative protocols it could cause fragmentation of the technical layer of the Internet. (See New IP case study on page 13)
  - Internationalized Domain Name (IDN) technical errors: Depending on the software used, there can be variations and failures to successfully look up domain names in the IDN format. Efforts continue to implement this processing in a uniform fashion to minimize unintended fragmentation of the DNS.
- Unilateral action:
  - Governments' creating national Internets within geographical borders: Governments that want to avoid the free flow of data through their geographical borders may decide to create distinct national networks that are not interoperable with the Internet. There is also a potential link between fragmentation of the user experience and technical fragmentation when a continued disruption of the access to the free flow of data (e.g., because of blocking or filtering) leads to creation of alternative and separate applications and services that constitute separate ecosystems not interoperable with the Internet.
  - Big Tech creating private infrastructure: Big Tech companies have the resources to create their own global networks. They could route Internet traffic through this private infrastructure instead of through the interconnected networks of the Internet.
  - Government legislation or policy: The rise of national and regional Internet policies and regulations that diverge significantly can lead to the fragmentation of the Internet. This is especially true when legislation related to the Internet impacts the technical layer of the Internet, intended or unintended. This is an ongoing risk because policymakers can lack the technical expertise to identify any unintended consequences of policy or legislation on the technical layer of the Internet.

Technical fragmentation of the Internet is the most common and most undesirable outcome that could result from many of the challenges identified related to Internet governance.

> *Poor Internet governance will result in the technical fragmentation of the Internet.*

Unilateral action

Stakeholders such as governments and Big Tech can take unilateral action that may impact the Internet governance landscape. Governments, whose responsibility is to safeguard the interests of their citizens, are increasingly passing legislation to regulate the Internet, which may have unintended consequences on how the Internet is governed (see the GDPR case study on page 26). Countries or regions (e.g., EU) often enact regulations based on national or regional considerations, which may conflict with global norms or the regulations of other countries. For example, data localisation laws require companies to store data within national borders, raising issues for businesses operating internationally. Similarly, the regulation of online content and speech varies widely among countries, creating complexities for platforms with global user bases. As the regulation of the Internet increases, it will become difficult for Internet governance to adapt to complex legislation which may not be interoperable between countries.

Maturity of governance arrangements

Internet organisations are responsible for and have direct control over key parts of the Internet governance landscape (e.g., IP addresses, domain names, root servers, technical standards and protocols). This means that these organisations could take unilateral action in how the Internet is governed. These organisations are operationally independent with no formal oversight which allows them to set their own policies.

These organisations are fierce proponents of the multistakeholder model and act in accordance with its principles. However, there is a risk of capture of these key organisations by self-interested parties with commercial or ideological aims. If such parties can take control of these organisations through inadequate governance arrangements, then these organisations can take unilateral action that impacts how the Internet operates.

In addition, poor governance in these organisations can lead to fraud which undermines the trust that is placed on these organisations to perform their critical role in the operation of the Internet.

Case Study: The Need for Maturing Governance

Over the last few years RIRs have been embroiled in several issues that stem from poor governance.

AFRINIC

- In 2019 a founding employee of AFRINIC resigned after allegations that he stole and sold blocks of IP addresses worth an estimated $50 million. These allegations are still pending an internal investigation.
- In 2021 AFRINIC reclaimed IP addresses from Cloud Innovation in an unusually strong response to violation of an AFRINIC policy. This led to several court cases with unexpected outcomes, including a temporary bank freeze which threatened the day-to-day operations of AFRINIC and almost led to its dissolution.
- In 2022, the Mauritius Supreme Court ruled that AFRINIC's board of directors had been constituted unlawfully, thus voiding its resolutions and causing the suspension of the organisation's CEO.

APNIC

In APNIC's 2023 Executive Council Election, a number of candidates stood who were connected to a single commercial entity with an intent to reform the governance of APNIC to replace its bottom-up multistakeholder approach with a more corporate-style structure. These candidates were also linked to an individual directly involved in the court cases between AFRINIC and Cloud Innovation. APNIC was made aware of nine instances of inappropriate conduct by election nominees (offering money or gifts for votes and abusing APNIC WHOIS data for the purpose of sending unsolicited (spam) emails to Members). None of the nominees were elected but, in response to these events, APNIC intends to adopt a stricter code of conduct for nominees and update its due diligence procedures for evaluating nominees. It is also reviewing its governance, structure and by-laws.

Digital divide

The digital divide – the gap between those who have access to the Internet and digital technologies and those who do not, continues to be a significant challenge. Despite rapid growth in global Internet access, substantial disparities persist, particularly between developed and developing countries, and urban and rural areas. This divide extends to quality of access, digital literacy, and the ability to leverage digital technologies for social and economic benefits. Good Internet governance reduces the digital divide because it ensures the Internet is free and open (less barriers to entry). The digital divide is of significant interest to countries whose populations do not have widespread access to the internet. These countries are increasingly looking towards multilateral fora to discuss their concerns because these concerns are not currently addressed by existing multistakeholder mechanisms.

Role of Big Tech

The growing power of Big Tech companies in the digital economy has implications for Internet governance. These companies control significant aspects of the Internet infrastructure, influence technical standards, and shape the online experiences of billions through their platforms. Their policies and practices can have a far-reaching impact on issues such as privacy, freedom of expression, and competition. Balancing the role of these private entities with the public interest and ensuring accountability and transparency in their operations is a key challenge in the governance of the Internet.

Case Study: The Role of Big Tech in Internet Governance

‘Big Tech’ refers to the largest and most dominant companies in the information technology industry, such as Google, Amazon, Facebook, Apple, and Microsoft. These companies have significantly influenced the development of the Internet, offering platforms and services that have become integral parts of daily life for billions of people worldwide.

While these companies have contributed to the Internet's rapid growth and evolution, their size, power, and influence have raised serious concerns about their role in Internet governance. Concerns include market dominance, data privacy, misinformation, and the potential stifling of competition. Their influence over the Internet's technical infrastructure and digital economy has led to calls for increased regulation and oversight.

Their vast resources and control over major platforms give them a significant say in shaping Internet policies and norms. Their decisions about content moderation, search algorithms, and data usage can influence public discourse, affect businesses worldwide, and impact individual privacy and digital rights. On the other hand, these companies also drive innovation, create services that billions of people rely on, and contribute to economic growth.

In recent years, there has been growing pressure from governments, regulators, and civil society for greater transparency and accountability from Big Tech companies. In response, some of these companies have made efforts to improve their policies and practices, including more transparency around content moderation decisions and investments in initiatives to combat misinformation.

However, there is an ongoing debate about what further actions are needed, including potential regulatory measures, to ensure that ‘Big Tech’ supports the public good. This may involve strengthening antitrust laws, implementing more stringent data protection regulations, or developing new governance models that allow for greater public participation.

Another consideration in regulating Big Tech is that more stringent regulations can create barriers to entry for new players who have less resources to comply to increasingly complex legal and regulatory requirements across jurisdictions. Thus, regulation can often enable additional dominance in these already dominant companies.

This case study underscores the importance of balancing private sector innovation with the need for accountability, transparency, and respect for user rights. It also highlights the need for multistakeholder dialogue and cooperation to address the challenges posed by the increasing concentration of power in the digital realm.

Cybersecurity threats

With increasing reliance on the Internet for critical services and infrastructure, the potential impact of cyber threats such as data breaches, cybercrime, and cyber warfare, has grown dramatically. Developing effective and coordinated responses to these threats while preserving the open nature of the Internet is a complex task. It requires cooperation among a wide range of actors including governments, private sector entities, and technical communities.

Case Study: Cybersecurity Threats in the Digital Age

In response to the growing cybersecurity challenges, various measures have been implemented. These include the development of advanced encryption technologies, security protocols, and robust system architectures. The Internet Engineering Task Force (IETF) is a key contributor to this by creating specifications and standards for secure routing such as Domain Name System Security Extensions (DNSSEC) and Resource Public Key Infrastructure (RPKI).

DNSSEC authenticates domain name queries to ensure that Domain Name System (DNS) queries return the correct IP address. The DNS by itself is not secure. It was designed at a time when security was not a primary consideration. It is possible for malicious attackers to forge (spoof) the source IP address of a DNS query. This means that malicious attackers can redirect users to a potentially malicious site without the user realising. DNSSEC reduces this risk by adding additional authentication for DNS queries.

RPKI authenticates IP address queries through a digital signature mechanism. Route leaks occur when a network on the Internet tells other networks to route traffic through it even though traffic should not normally pass through this network. For example, in June 2019 a small Internet Service Provider in Pennsylvania advertised routes for part of the Internet that incorrectly routed traffic to the network causing congestion and unreachable network errors for end users. While some route leaks are innocuous, malicious attackers can purposefully cause route leaks to direct traffic to their network to steal data or issue certificates to impersonate domains. RPKI secures routing to avoid route leaks.

Regional Internet Registries (RIRs), registry operators and registrars support the implementation of these standards. In addition, the Internet Society (ISOC) works with operators, enterprises, and policymakers to implement crucial fixes needed to reduce the most common routing threats through a global initiative called Mutually Agreed Norms for Routing Security (MANRS).

In addition to routing security, private sector entities, particularly those in the technology sector, have invested in sophisticated cybersecurity tools and capabilities. There's also a growing emphasis on training and awareness to ensure that all Internet users understand basic cybersecurity practices.

The lessons learned from dealing with cybersecurity threats underscore the importance of a proactive and comprehensive approach to digital security that involves not only technological solutions but also policy frameworks, human resource development, and international cooperation.

Ethical concerns

The rise of technologies such as AI and the Internet of Things (IoT)[7] has brought ethical concerns to the forefront of Internet governance. These include issues related to privacy, surveillance, bias in algorithms, and the societal impact of automation. Moreover, the growth of data-driven business models and practices raises questions about consent, data ownership, and the commodification of personal information. Navigating these ethical considerations while fostering innovation and growth is a key challenge in the governance of the digital future.

[7] Internet of Things (IoT): This refers to the network of physical devices, vehicles, appliances, and other items embedded with sensors, software, and network connectivity, which enables these objects to connect and exchange data over the Internet. These devices, often referred to as "smart" devices, can be remotely monitored and controlled, and can interact with each other autonomously to some degree. The IoT has applications across various sectors, including consumer, industrial, agricultural, and medical contexts, among others.

Opportunities for enhanced Internet governance

Despite the challenges, the dynamic nature of the Internet and its governance also presents ample opportunities for enhancement and innovation. The advent of emerging technologies, the increasing focus on digital inclusion, the necessity of strengthening cybersecurity, and the scope for improved collaboration and dialogue among stakeholders all contribute to a broad spectrum of opportunities. In this section, we explore these potential areas of advancement and how they could contribute to more robust, inclusive, and effective Internet governance.

Emerging technologies and their potential role

Emerging technologies such as Web3[8] (underpinned by blockchain[9], smart contracts and decentralised autonomous organisations), artificial intelligence (AI)[10], and the IoT have the potential to significantly impact and reshape Internet governance. Web3's decentralised and transparent nature could offer novel solutions for digital identity, data integrity, transactional trust, and democratised decision-making. AI and machine learning can help manage and analyse large datasets, aid in cybersecurity, and enhance the efficiency of Internet operations. However, their use also requires careful governance to ensure ethical and fair use. Thus, embracing these technologies in governance structures offers both opportunities and challenges.

Promoting digital inclusion and universal accessibility

Promoting digital inclusion and universal accessibility is both a challenge and an opportunity for enhanced Internet governance. This involves not only expanding Internet access to currently underserved communities but also ensuring they have the necessary skills and resources to leverage digital technologies.

A vital aspect of this is the implementation of Internationalised Domain Names (IDNs), which allow domain names to be represented in local languages and scripts. By making domain names

[8] Web3: This term refers to the proposed third generation of the Internet, which would be built on blockchain technology. The vision of Web3 is a decentralised online environment where users have control over their own data and interactions, rather than these being controlled by centralized entities such as tech companies. This vision is underpinned using technologies such as blockchain, smart contracts, and decentralized autonomous organisations (DAOs).

[9] Blockchain: A blockchain is a type of distributed ledger technology, where transactions or records are grouped together in 'blocks' and then linked together in a 'chain'. This technology is decentralized, meaning that it doesn't rely on a central point of control. Instead, multiple copies of the blockchain are kept on different computers, and these copies are constantly checked and updated against each other. The technology is known for its transparency, security, and ability to resist tampering.

[10] Artificial Intelligence (AI): AI refers to the simulation of human intelligence processes by machines, especially computer systems. These processes include learning (the acquisition of information and rules for using the information), reasoning (using rules to reach approximate or definite conclusions), and self-correction. Applications of AI include expert systems, natural language processing, speech recognition, and machine vision. AI can be used to analyse large datasets, aid in cybersecurity, enhance the efficiency of Internet operations and many other applications.

more accessible and meaningful to non-English speakers, IDNs can help bring a more diverse group of people online and enable them to engage more fully in the digital world.

Additionally, initiatives to promote digital literacy, develop locally relevant content, foster digital entrepreneurship, and ensure universal design principles are integrated into digital services can contribute to economic and social development. These efforts are crucial to addressing the 'digital divide' and ensuring that everyone, regardless of their background or abilities, can access and use the Internet effectively.

Moreover, digital inclusion fosters diversity and representation in digital spaces, which in turn enriches the discourse and decision-making in Internet governance. The Internet's global nature necessitates a multi-faceted approach to inclusion and accessibility, ensuring it truly serves as a tool for global communication, collaboration, and development.

Strengthening cybersecurity

The Internet, now an integral part of society, necessitates a strong emphasis on cybersecurity to ensure its safety and reliability. Strengthening cybersecurity contributes to the resilience of the global Internet in several key ways:

- **Development and implementation of robust security standards and practices:** This involves creating and enforcing stringent rules and methods to protect networks, systems, and data. These standards and practices act as a frontline defence against potential cyber threats, making it harder for malicious actors to exploit vulnerabilities.
- **Promoting a 'security by design' approach in digital products and services:** This concept implies integrating security measures into the initial design of products and systems, rather than adding them later. By considering security from the outset, potential vulnerabilities can be minimized, making digital products and services inherently more secure.
- **Fostering cooperation and information sharing among different stakeholders:** Collaboration and transparency among governments, private sector entities, and other stakeholders can facilitate the swift identification, mitigation, and prevention of cyber threats. Shared knowledge and resources can lead to more effective responses and proactive measures against emerging threats.
- **Building capacity and awareness in cybersecurity, especially in developing countries:** Education and training in cybersecurity can equip individuals and organisations with the knowledge and skills to protect their digital assets. This is particularly important in developing countries, where a lack of resources and expertise can make them more vulnerable to cyberattacks.

By bolstering cybersecurity in these ways, the resilience of the global Internet can be significantly enhanced, reducing potential disruptions, and ensuring its safe and reliable operation.

Encouraging collaboration and dialogue among stakeholders

The multistakeholder model of Internet governance hinges on the active participation and collaboration of various stakeholders, including governments, the private sector, civil society, academia, and technical communities. Encouraging greater dialogue and cooperation among these stakeholders can lead to more inclusive and balanced governance outcomes. This includes improving mechanisms for stakeholder engagement, fostering a culture of consensus and compromise, and ensuring that diverse voices, particularly those from underrepresented or marginalised groups, are heard in decision-making processes. Such collaborative efforts can contribute to the legitimacy, effectiveness, and sustainability of Internet governance.

Improving coordination and robustness of governance

Opportunities exist to improve Internet governance by improving coordination between stakeholders and robustness of governance processes.

There is a need to improve communication between the multilateral world and the multistakeholder world (instead of seeing these models as being in conflict). The IGF or other internet governance organisation can act as this bridge if it is enabled to do so by multilateral and multistakeholder parties.

The organisations that operate in a bottom-up multistakeholder approach need to address the challenge of the significantly increased participation by stakeholders as the importance of the Internet continues to grow. New mechanisms need to be explored to drive discussions towards consensus amongst a large number of stakeholders in a timely manner.

The internal governance processes and formal oversight, accountability and transparency of organisations that contribute to the Internet governance landscape need to continue to improve. This will reinforce the trust that is placed in these organisations and mitigate against the risk of interested parties taking control of these organisations.

Emerging technology trends and their impact on Internet governance

Technology trends

Emerging Technologies and Internet Governance

Emerging technologies such as artificial intelligence (AI), blockchain, and the Internet of Things (IoT) are reshaping the Internet and introducing new challenges and opportunities for Internet governance. These technologies all require a stable and secure Internet to be successful.

AI and Internet governance

As technology continues to evolve at an unprecedented pace, it is reshaping the landscape of Internet governance. AI is creating new challenges and opportunities. These technologies are disrupting traditional models of governance, necessitating new regulatory frameworks and policies.

IoT and Internet governance

IoT is another technology that's significantly impacting Internet governance. It poses new challenges related to data privacy, device security, and interoperability among different IoT systems.

Blockchain and Internet governance

Blockchain technology, underpinning the idea of decentralised information, is also creating fresh challenges and opportunities in the landscape of Internet governance.

Cybersecurity and Internet governance

Cybersecurity threats are becoming increasingly sophisticated, with state and non-state actors posing significant risks to the integrity and security of the Internet. This has prompted a greater focus on cybersecurity in Internet governance discussions.

Big Tech companies and their influence

The growing influence of Big Tech companies like Apple, Google, Facebook, and Amazon in Internet governance is a significant trend. Their role has sparked debates about monopolistic behaviour, privacy rights, and the need for greater regulation.

Web3 and its implications for Internet governance

Web3, or the third iteration of the Internet, is a concept that envisions a decentralised online environment powered by blockchain technology and cryptocurrencies. Some argue this new iteration of the Internet could enable peer-to-peer interactions, reduce the control of Big Tech over the online world, and increase individual privacy and control over data.

The Metaverse and Internet governance

The Metaverse is a virtual reality space where users can interact with a computer-generated environment and other users. The governance of the Metaverse presents a unique set of challenges and opportunities for the future of Internet governance.

Socio-political Trends

Regional perspectives on Internet governance

The Global South[11] is becoming increasingly central to Internet governance discussions as Internet penetration in these regions continues to grow. There are concerns about digital divide, censorship, and the need to ensure that the voices of these countries are heard in global Internet governance forums.

Data sovereignty and Internet governance

Data sovereignty and localization are becoming prominent issues in Internet governance, driven by concerns about privacy, security, and economic competitiveness.

Regulatory challenges and policy

As the impact of the Internet on society becomes more profound, the need for effective regulation and policy becomes more pressing. This includes regulations around data privacy, content moderation, and antitrust laws.

Trends in Internet fragmentation

The trend towards increasing fragmentation, or the so-called ‘"splinternet’", is a major concern for the future of Internet governance.

Digital Rights, inclusion, and sustainability

Digital rights and inclusion are increasingly at the forefront of Internet governance discussions. Additionally, the environmental impact of the Internet and digital technologies is becoming a more prominent issue in Internet governance.

Economic Trends

The role of data in economy

Data-driven business models are becoming increasingly influential in the global economy. The regulation and governance of these models, and the vast amount of data they generate, is a key issue in Internet governance.

Cryptocurrencies and Internet governance

The rise of cryptocurrencies, powered by blockchain technology, has introduced new economic paradigms and challenges in Internet governance. The decentralised and often anonymous nature of these digital currencies raises issues related to financial regulation, fraud, and criminal activity.

[11] Global South: The term "Global South" is often used to refer to low and middle-income countries located primarily in the Southern Hemisphere. This includes countries in Latin America, Africa, Asia, and the Pacific Islands. It is important to note that the term is not strictly geographical but is more indicative of socio-economic and developmental contexts.

Future of Internet governance

As we look towards the future, several anticipated changes and trends in Internet governance between now and 2030 include:

1. **Increasing role of non-state actors:** The influence of private companies that operate across national boundaries, civil society organisations, and other non-state actors in Internet governance will likely grow, further emphasising the need for a multistakeholder approach.
2. **Increasing role of state actors:** governments and supranational organisations are increasingly exerting influence on the Internet landscape through unilateral action (legislation and regulation) and multilateral mechanisms (e.g., raising Internet governance topics like New IP into ITU discussion (see case study on page 13)).
3. **Global policy convergence and divergence:** As the Internet becomes more intertwined with everyday life, we may see both convergence and divergence in global policy approaches, with some countries adopting similar policies to address common challenges, while others adopt more restrictive or nationalistic approaches.
4. **Technological advancements:** Rapid advancements in technology will continue to shape the Internet governance landscape, as emerging technologies such as artificial intelligence, the Internet of Things, the metaverse[12] and blockchain present new opportunities and challenges for policymakers and regulators.
5. **Evolving cybersecurity threats:** As the digital landscape becomes more complex, cybersecurity threats will continue to evolve, necessitating greater collaboration and coordination among stakeholders to address these challenges.

Opportunities and challenges for stakeholders

As the Internet continues to evolve, stakeholders within the Internet governance ecosystem must adapt to changing circumstances and shifting priorities. This section will explore the opportunities and challenges that different stakeholders may face as they navigate the complex landscape of Internet governance. By understanding these potential hurdles and prospects, stakeholders can better position themselves to drive positive change and influence the future of Internet governance.

As the future of Internet governance unfolds, different stakeholders will face distinct opportunities and challenges:

- **Governments:** Governments will need to strike a balance between promoting innovation and economic growth while also ensuring the security and privacy of their citizens. They must navigate the increasingly complex landscape of international norms and regulations while fostering a multistakeholder approach to Internet governance.
- **Private sector:** Companies, particularly those in the technology sector that operate globally, will play an increasingly crucial role in shaping the future of Internet governance. They will

[12] Metaverse: a vision of what many in the computer industry believe is the next iteration of the Internet: a single, shared, immersive, persistent, 3D virtual space where humans experience life in ways they could not in the physical world.

need to collaborate with governments, civil society, and other stakeholders to address challenges like privacy, cybersecurity, and the digital divide while promoting innovation and economic growth.

- **Civil society:** Civil society organisations will continue to advocate for their interest in how the Internet should be governed. They will need to work collaboratively with other stakeholders to provide input on Internet governance policies and practices that impact their interests.
- **International organisations:** As the Internet continues to evolve, international organisations will need to adapt their roles and responsibilities to address new and emerging challenges. This may include developing new norms, standards, and regulations that reflect the changing landscape of Internet governance.
- **Academia and research Institutions:** Academia and research institutions will play an important role in informing policy decisions and driving innovation in Internet governance. They will need to continue to explore and analyse the implications of emerging technologies and trends and provide evidence-based recommendations to policymakers.
- **Individuals and communities:** Individuals and communities will continue to shape the future of Internet governance through their use of and engagement with digital technologies. They will need to be informed about their rights and responsibilities online and work together to ensure that the Internet remains a safe, inclusive, and equitable space for all.

Overall, the future of Internet governance will require collaboration and cooperation among diverse stakeholders to address the complex challenges and opportunities presented by emerging technologies and the changing digital landscape. A multistakeholder approach that recognizes the roles and responsibilities of governments, the private sector, civil society, international organisations, academia, and individuals will be crucial to achieving a more open, secure, and inclusive Internet for all.

Scenarios of the future

The following two scenarios explore what the future could look like if Internet governance was to depart from the status quo. The intent of these scenarios is to demonstrate potential consequences of actions (or inactions) to change the status quo.

Multilateral model replaces the multistakeholder model

Governments become increasingly frustrated with their participation in ICANN's GAC. They feel like their concerns and inputs are not taken seriously by other stakeholders at ICANN. The topics that concern them are not relevant to discuss at ICANN, so they focus more efforts on engaging at the IGF. However, the IGF does not deliver any tangible outcomes. Many of these governments do not have the influence of supranational organisations like the EU to influence the Internet governance landscape unilaterally through legislation. They have no forum to resolve their concerns and they are frustrated. These governments form coalitions to advocate for the ITU to take over the role currently performed by ICANN and the IETF. The ITU becomes the central forum for Internet governance. The ITU still collaborates with stakeholders in the technical community, but decisions are made in a top-down approach by governments.

A government representative once told me: "the multistakeholder model exists because the multilateral model allows it to."
Interview Participant

Technical expert stakeholders such as registries and IETF have less influence and need to compete with giant technology companies to lobby their governments to act for the good of the Internet at the ITU. With technical experts further removed from decision-making, the decisions made by governments at the ITU have unintended technical consequences that threaten the stability of the Internet's infrastructure. The world starts to see more DNS service disruptions.

When countries or Big Tech companies commit human right violations, ITU resolutions are passed to sanction these actors by removing domain names or ccTLDs from the DNS. Denying access to the Internet is used as a geopolitical tool. Governments and Big Tech that rely on the Internet for their economic survival start to invest in their own networks that they have direct control over. These networks are not interoperable and have limited utility to users. Companies charge users a subscription fee to access these networks. Less users can access these networks but users in developed countries can afford the technologies required to switch between using the various networks required to access services or information.

The multistakeholder model evolves

The Internet organisations that currently administer the Internet continue to improve their transparency and accountability. They adapt to better meet the needs of disenfranchised governments. Multistakeholder processes are adapted to be more responsive while still receiving broad input from all stakeholders. Outcome-based fora are created to discuss and resolve broader Internet governance issues that are of concern to stakeholders. All governments recognise and support the legitimacy of the established Internet governance mechanisms. Stakeholders stop forum shopping when they do not get their way because they know that there is no alternative pathway that will be supported by other stakeholders. The Internet continues to operate outside of the control of commercial and geopolitical forces. Technical experts continue to support the Internet to be open, secure and interoperable. Governments have more influence to advocate for the needs of their citizens. Access to the Internet remains free and the Internet continues to grow to support emerging technologies and services which relies on the Internet for success.

Australia's Internet governance landscape

This section describes Australia's Internet governance landscape and explains the need for a thriving domestic ecosystem. In addition to informing Australian stakeholders of the Australian landscape, this section aims to provide a use study for stakeholders in other countries who want to contribute to Internet governance more meaningfully.

The need for a thriving domestic ecosystem

A thriving domestic Internet governance ecosystem is important for Australia to be able to participate in the regional and global forums in a meaningful way. Investing in a thriving domestic ecosystem addresses the challenges below that undermine stakeholders' ability to Influence the global Internet governance landscape:

- there are too many forums to be able to attend them all
- the forums are attended by many people which makes it difficult to have a say
- even though formal mechanisms of influence exist, the level of influence is based on personal relationships
- domestic misalignment and lack of technical understanding undermines credibility.

Internet governance is global and occurs at fora across the world. Participating at these fora requires travelling to various locations or attending virtually online, often at inconvenient times due to time zone differences. Many domestic stakeholders may not have the budget or capacity to participate in these fora. And even if they do participate, these fora are attended by hundreds or thousands of people which makes it difficult to engage in productive dialogue.

Domestic fora, such as local and regional IGFs, provide an opportunity for domestic stakeholders who are unable to attend or meaningfully participate in the global fora to have their voice heard. Domestic and regional fora allow stakeholders with overlapping interests to coordinate their approaches so that these interests can be represented at global fora. This is particularly important due to the impact of personal relationships on the level of influence that can be exerted. By coordinating domestically, existing relationships with global stakeholders can be more effectively leveraged. Some stakeholders in the civil society and government sectors have a responsibility to represent the views of their constituents, even if there is not agreement on those views by all stakeholders. Meaningful domestic participation is important to understand the views of constituents and to coordinate ways to present those views in global fora.

The Internet is ubiquitous in people's everyday life, which means that issues related to the Internet are discussed in a wide range of fora. These issues can often have direct or indirect impacts on Internet governance. It is difficult for stakeholders to keep track of the issues that come up in the various fora (for example, there are at least 15 UN organisations where Internet-related topics can be discussed). By engaging widely with various stakeholder groups in the domestic ecosystem, some of these issues can be identified early. In this way, a thriving domestic ecosystem can act as an 'early-warning system' so that stakeholders can provide early input on these issues at the relevant global or regional fora. An example of this can be seen in the ' Trademark Disputes in Domain Names and Internet Governance' case study.

Case Study: Trademark Disputes in Domain Names and Internet Governance

BACKGROUND

The Internet's global nature has allowed individuals and businesses from all corners of the world to interact and conduct business on a scale never seen before. A key element of this is the DNS, which enables users to navigate the Internet using understandable names instead of numerical IP addresses. With the proliferation of businesses and brands online, there has been an increasing number of disputes over domain names, particularly regarding trademark infringement.

THE CHALLENGE

In the late 1990s and early 2000s, as the Internet started to become a significant commercial force, companies began to see the value of owning domain names that matched their trademarks. However, this led to a rush of 'cybersquatting' – the practice of registering, trafficking in, or using a domain name with bad-faith intent to profit from a trademark belonging to someone else.

One famous example is the case of Madonna Ciccone, known as Madonna, the singer, and the domain name Madonna.com. The domain was originally registered by a man named Dan Parisi, who used it for a pornography site. Madonna Ciccone filed a complaint under the ICANN's Uniform Domain Name Dispute Resolution Policy (UDRP) and won the right to the domain.

These trademark disputes over domain names presented a significant challenge to Internet governance. They involved multiple jurisdictions, differing national laws, and the need for a system that could deliver fast and cost-effective resolution to disputes.

THE IMPACT

These challenges led to growing concerns about the potential for abuse of the DNS system, which could undermine trust in the Internet and the DNS. It also risked marginalizing smaller businesses and individuals who lacked the resources to fight expensive legal battles over domain names.

ACTIONS TAKEN AND LESSONS LEARNED

In response to these challenges, ICANN, a non-profit organization responsible for coordinating the Internet's naming systems, established the Uniform Domain Name Dispute Resolution Policy (UDRP) in 1999. The UDRP provides a streamlined, cost-effective mechanism for resolving domain name disputes without the need for court litigation. It's administered by various dispute resolution service providers, including the World Intellectual Property Organization (WIPO).

The UDRP has helped to resolve thousands of domain name disputes and has been instrumental in curbing the practice of cybersquatting. It has shown the importance of coordinated, multilateral action in Internet governance, demonstrating that unilateral decisions often lead to confusion and conflict.

The case of domain name disputes also underlines the need for balance in Internet governance – between protecting the rights of trademark owners and ensuring a fair and accessible system for all Internet users. It illustrates that in the complex, multi-jurisdictional space of the Internet, flexible and adaptive governance mechanisms are essential.

It has also highlighted the need for ongoing vigilance and adaptability in Internet governance. New challenges continue to emerge, such as the advent of new generic top-level domains (gTLDs) like .app, .blog, etc., and the potential for new forms of cybersquatting and trademark disputes. Internet governance structures must continue to evolve and adapt to these changing circumstances to ensure a fair and stable online environment.

Understanding the views of domestic stakeholders allows stakeholders who participate in global fora to be more influential. When stakeholders' understanding of issues are informed by a wide range of perspectives domestically, they are seen as more credible when they contribute at a regional or global level.

It is important for Australian Government departments to be aligned in their policy positions. As demonstrated in Figure 4, governments consist of several departments and agencies which have the potential to impact Internet governance (often inadvertently) when discussing policy and implementing regulations. When the government implements regulations domestically that contradict their international policy positions, the government loses credibility in global fora.

More importantly, these regulations have the potential to inadvertently fragment the Internet when domestic regulation is not interoperable with existing policies or standards that underpin the operation of the Internet. An example of this can be seen in the 'The Impact of GDPR on Internet Governance' case study on page 26.

Overall, a thriving domestic ecosystem depends on a high level of trust between stakeholders. Since each stakeholder cannot participate in all fora, there is a need to trust other domestic stakeholders to accurately represent views of others in the fora where they participate. The need for trust also highlights the importance of a whole-of-government coordinated approach, since when the government implements regulations that contradict policy positions, it undermines the trust stakeholders have in the government.

> *"We need trust on steroids."*
> Subject Matter Expert Research Participant

Key stakeholders

Australia's domestic Internet governance landscape includes stakeholders from government, Internet organisations, civil society, industry and the At-Large community (representing users and consumer groups). Figure 4 shows the relationships between these stakeholders and the fora where they interface. The size of the circles in the diagram indicates the relative level of influence each stakeholder has on the landscape. The vertical position of the stakeholders on the diagram shows the extent to which they engage in either multistakeholder or multilateral/bilateral fora internationally. The distance stakeholders are from the centre of the domestic fora circle indicates the extent that stakeholders engage internationally in Internet governance fora.

The key stakeholders in the Australian ecosystem include:

- .au Domain Administration (auDA): the administrator of Australia's .au top-level domain (i.e., Australia's ccTLD). auDA also performs a critical coordinating role in the domestic ecosystem by engaging widely with domestic stakeholders.
- Asia-Pacific Network Information Centre (APNIC): the Regional Internet Registry administering IP addresses for the Asia Pacific region.
- Australian Government: develops and implements public policy and regulation that impacts the Internet governance landscape. Also plays an important role in representing domestic stakeholder views at regional and global fora.

Some domestic stakeholders, especially in government departments, might not be aware of the influence they have on the landscape. Regulatory changes related to privacy, critical infrastructure, cybercrime, intellectual property, etc., could have implications on the Internet governance landscape that may not have been considered. This is why mapping out the landscape is critical for a cohesive approach to policy making.

The following stakeholders are currently under-represented in the domestic landscape:

- Academia: currently does not have a major presence, especially when compared to the role of academia in other countries. Investing in domestic academic study, research and collaboration related to Internet governance will help inform domestic stakeholders and open new avenues of influence through international research collaborations and discussions.
- Government: current interest and resourcing for the government to engage in the landscape is not proportionate to the importance the Internet has on the nation's economy.
- Industry (such as Internet service providers and content platforms): these companies tend to lobby the government directly to influence policy rather than engaging in multistakeholder forums.

Key Fora

The NetThing is Australia's local IGF. The IGF is the most important forum for the domestic ecosystem because it is where all domestic stakeholders can participate. Some domestic stakeholders have suggested that the NetThing can be improved through increased funding support to allow more stakeholders to participate. This includes increasing the frequency of meetings, hosting meetings at more diverse locations to include more stakeholders and removing barriers for participation such as attendees needed to pay for travel costs.

In addition to domestic fora, the following regional fora are relevant to Australia:

- **Asia Pacific Regional Internet Governance Forum (APrIGF):** an important multistakeholder forum where Internet governance topics of interest to the Asia Pacific region can be discussed. Provides an opportunity for regional stakeholders to align on issues that can be raised at the global IGF.
- **Asia Pacific Regional Internet Conference on Operational Technologies (APRICOT):** important technical forum but utility is limited by the number of people who attend, and the knowledge barrier required to meaningfully engage.
- **APNIC conferences/meetings:** key fora to provide input on how IP addresses and related protocols are governed in the Asia Pacific region. The utility of these fora is limited by the knowledge barrier required to meaningfully engage.
- **Asia Pacific Top Level Domain Association (APTLD) meetings**: this forum helps the coordination and capacity building of ccTLD registries in Asia Pacific region.
- **Asia-Pacific Telecommunity (APT)**: does not have a major influence on Internet governance, but it provides an opportunity for Asia Pacific members to discuss and align on Internet governance topics that are relevant to the region.
- **Asia-Pacific Economic Cooperation (APEC):** APEC has no concrete outcomes engaging in telecommunication working group allows Internet governance issues to be socialised with other governments in the region. They provide an opportunity to highlight and discuss projects and ideas in a safe space.

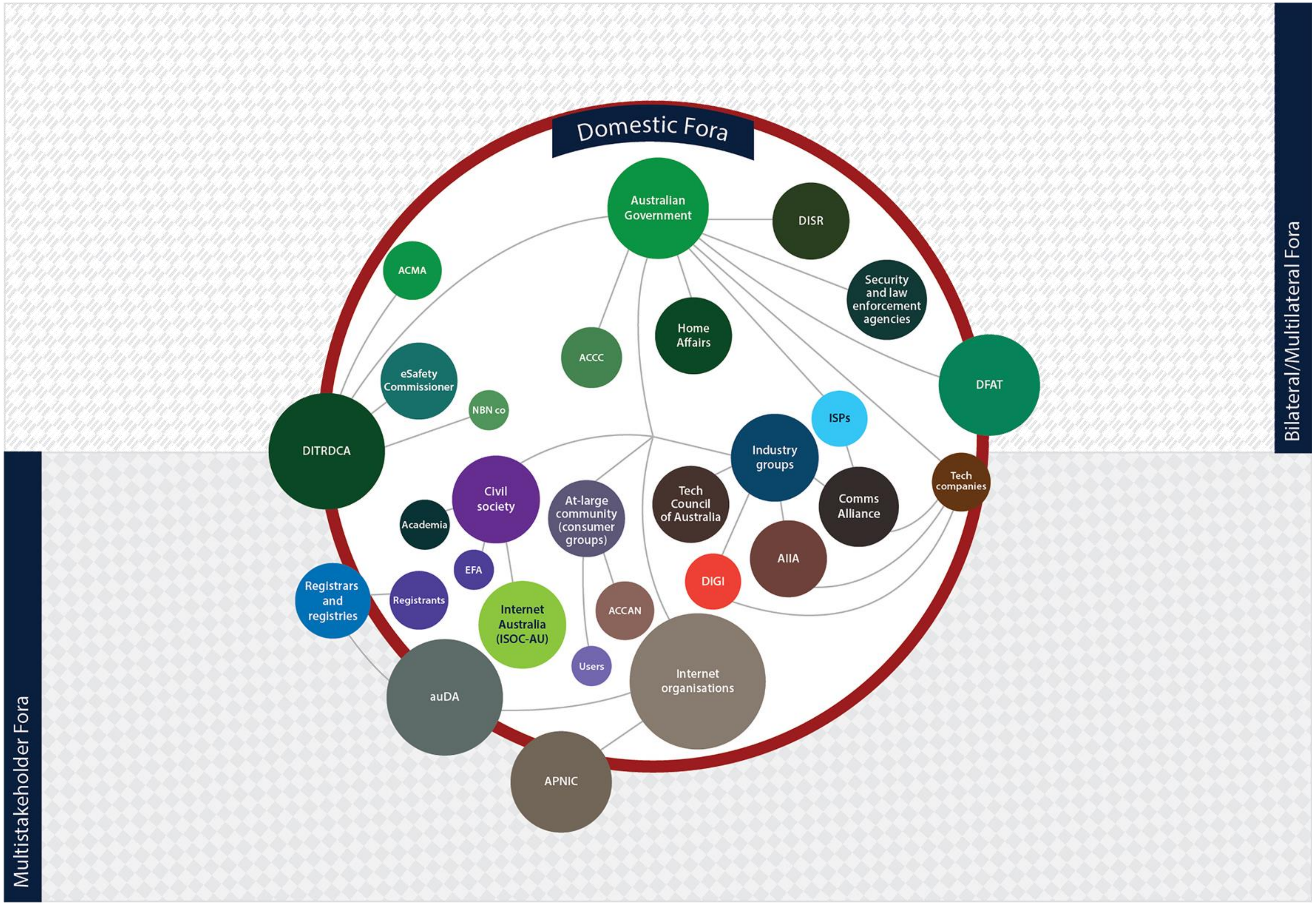
- **OECD:** useful forum for practical outcomes but excludes countries that already feel disenfranchised.
- **PaCSON (Pacific Cyber Security Operational Network):** an operational cyber security network, consisting of regional working-level cyber security experts and technical experts from eligible governments across the Pacific working to improve cybersecurity capabilities and readiness across the Pacific. While not a significant influence on the overall Internet governance landscape, this is an important forum for the Pacific region to build capability.

Some of these fora (such as APRICOT, APNIC meetings) require technical understanding to meaningfully participate. Other fora, such as APT, are multilateral fora which are not open to all stakeholder groups. These barriers to participation in regional fora underscore the importance of local fora like NetThing to ensure that a wide range of stakeholder views are represented at regional (and global) fora.

Table 4: List of acronyms used in Figure 4

Acronym	Name
ACCAN	Australian Communications Consumer Action Network
ACCC	Australian Competition and Consumer Commission
ACMA	Australian Communications and Media
AIIA	Australian Information Industry Association
APNIC	Asia-Pacific Network Information Centre
auDA	.au Domain Administration
Comms Alliance	Communications Alliance
DFAT	Department of Foreign Affairs and Trade
DIGI	Digital Industry Group
DISR	Department of Industry, Science and Resources
DITRCDA	Department of Infrastructure, Transport, Regional Development, Communications and the Arts
EFA	Electronic Frontiers Australia
ISPs	Internet service providers

Figure 4: The Australian Internet Governance Landscape



Size: level of influence on the landscape **Lines:** relationships between entities **Vertical position:** involvement in multistakeholder or multilateral/bilateral fora **Distance from centre:** extent of international engagement

Findings and implications

This section of the report presents the principal findings derived from the comprehensive analysis of Internet governance. It succinctly summarises the key points, distilling complex facets into understandable insights. Additionally, it outlines the implications of these findings, offering context and potential directions for future actions. The objective is to provide a clear understanding of Internet governance, enabling stakeholders to make informed decisions for a safer, equitable, and more efficient Internet ecosystem.

Throughout the report, we have examined the various aspects of Internet governance, from its historical origins to the ongoing debates surrounding its future direction. The following are some of the most significant findings of our analysis and the implications of these findings:

The multistakeholder model

The multistakeholder model has been a key driver of the Internet's success, fostering innovation and enabling a broad range of voices to participate in the governance process. As the Internet continues to evolve, maintaining this inclusive approach to governance will be crucial to ensuring that the benefits of connectivity are shared widely and equitably.

Implication: Policymakers, industry stakeholders, and civil society should work together by engaging in multistakeholder processes to preserve and strengthen the multistakeholder model, as it is essential for the Internet's continued growth and development.

Fragmentation and unilateral regulation

These challenges pose significant risks to the future of Internet governance, as they threaten to undermine the open, interconnected nature of the Internet. In an increasingly digital world, it is essential to address these issues to prevent the Internet from becoming a patchwork of disconnected networks, each governed by its own set of rules.

Implication: Governments, including the Australian Government, should work together with stakeholders in bilateral discussions as well as in multistakeholder and multilateral fora to develop a coordinated, global approach to Internet governance that respects national sovereignty while preserving the open, interconnected nature of the Internet.

The role of governments

In shaping the future of Internet governance, the role of governments is critical, both in terms of protecting national interests and ensuring that the Internet remains a global public good. As the Internet continues to play an increasingly important role in the global economy, governments must strike a delicate balance between regulation and innovation, ensuring that the benefits of the digital revolution are widely shared while mitigating the risks associated with an increasingly interconnected world.

Implication: The Australian Government and other national governments should actively engage with other stakeholders in the Internet governance ecosystem, collaborating to address common challenges and capitalise on shared opportunities. This will require ongoing

dialogue, cooperation, contribution of technical expertise, and trust-building among a diverse range of actors, both within and across national borders.

Security and privacy

As the Internet continues to grow in scale and complexity, ensuring the security and privacy of users is becoming an increasingly important challenge. Cyber threats, data breaches, and concerns over mass surveillance have all highlighted the need for robust and effective governance mechanisms that can protect the rights and interests of users while maintaining the resilience and integrity of the Internet.

Implication: The Australian Government, along with other stakeholders, must prioritise efforts to strengthen the security and privacy of the Internet, working collaboratively to develop and implement best practices, standards, and policies that can effectively address emerging threats and protect user rights.

Digital inclusion and capacity building

As the Internet continues to expand its reach, it is crucial to address the digital divide and ensure that all individuals and communities can participate in and benefit from the digital economy. This will require concerted efforts to promote digital inclusion, build capacity, and empower individuals and communities to harness the potential of the Internet for social and economic development.

Implication: The Australian Government should work with other stakeholders to support initiatives aimed at fostering digital inclusion and capacity building, both domestically and internationally. By investing in education, training, and infrastructure development, policymakers can help ensure that the benefits of the digital revolution are shared widely and equitably.

In conclusion, the Internet governance landscape is a complex and dynamic ecosystem, characterised by a diverse range of actors, interests, and challenges. As the Internet continues to play an increasingly important role in our daily lives and the global economy, understanding the governance structures and potential future developments is essential for policymakers, industry stakeholders, and civil society alike. By addressing the key findings and implications outlined in this report, we can work together to ensure that the Internet remains a powerful force for innovation, collaboration, and positive change in the years to come.

Implications for policymakers, industry stakeholders and civil society

The findings of this report have notable implications for various stakeholders in the Internet governance landscape. The following discussion aims to elucidate these in the context of policymakers, industry stakeholders, and civil society.

For **policymakers**, the importance of active engagement in Internet governance, both domestically and internationally, cannot be overstated. Policymakers must strive to strike a balance between regulation and innovation, considering the global nature of the Internet and the importance of preserving its open and interconnected structure. Policymakers should work collaboratively with other stakeholders to address shared challenges, including fragmentation, unilateral regulation, and cybersecurity threats. The focus should be on fostering a coordinated, global approach to Internet governance that respects national sovereignty while preserving the Internet's fundamental characteristics.

Industry stakeholders also have a significant role to play in Internet governance. With their technical expertise and practical experience, they are well positioned to contribute to the development of standards, best practices, and policies that can enhance the security, stability, and functionality of the Internet. Industry stakeholders should collaborate with other actors in the Internet governance ecosystem, including governments and civil society, to promote innovation, competition, and consumer protection. They should also take a proactive role in addressing ethical concerns, promoting digital inclusion, and bridging the digital divide.

For **civil society**, the findings highlight the importance of active and meaningful participation in Internet governance processes. Civil society groups play a crucial role in representing the interests of Internet users, advocating for digital rights, and promoting transparency and accountability in Internet governance. They should continue to engage in dialogue with other stakeholders, raise awareness about Internet governance issues, and work towards a more inclusive and equitable Internet ecosystem.

In conclusion, the findings of this report underscore the complex and interconnected nature of Internet governance and the need for cooperation and dialogue among all stakeholders. By understanding and addressing the implications of these findings, policymakers, industry stakeholders, and civil society can work together to shape a more secure, stable, and inclusive digital future.

Conclusion

The Internet, as we know it today, is the result of decades of collaborative effort by numerous stakeholders worldwide. The governance of this global resource has also evolved in response to the technological advancements and the expanding user base. As new technologies continue to reshape the Internet, the need for effective Internet governance has never been more critical.

Concluding insights from the report

Reflecting on the discussions and findings presented in this report, several significant points come to the forefront. The Internet's governance is an intricate, multifaceted, and dynamic process that involves multiple stakeholders. The multistakeholder model, despite facing some challenges, remains a cornerstone of the Internet's success, fostering innovation and inclusivity. However, challenges such as fragmentation, unilateral regulation, and the increasing influence of Big Tech necessitate continuous attention and collaborative efforts from all stakeholders. Additionally, the role of governments and private sectors in Internet governance is of paramount importance, requiring a delicate balance between regulation and innovation. Furthermore, the report highlighted the necessity of bridging the digital divide and ensuring that security and privacy considerations are at the forefront of Internet governance discussions.

Moving forward: A collaborative approach to Internet governance

The complexities of Internet governance require a collective approach to address ongoing challenges and harness opportunities for progress. Policymakers, industry stakeholders, civil society, and other actors in the Internet governance landscape should view this report's findings as a call to action. The need to strengthen the multistakeholder model, address the issues of fragmentation and unilateral regulation, bridge the digital divide, and tackle cybersecurity threats should be prioritised.

Governments, including the Australian Government, are encouraged to play an active role in shaping the Internet governance landscape, protecting national interests, and ensuring the Internet remains a global public good. Industry stakeholders should take a proactive role in setting standards and best practices, promoting innovation, competition, and consumer protection. Civil society groups should continue to advocate for digital rights and promote transparency and accountability in Internet governance.

The future of the Internet is in our hands. Together, we can shape an Internet governance framework that is secure, inclusive, and conducive to innovation and growth. The time to act is now.

Annex A: Methodology

This section outlines the methodology used in this report to analyse the Internet governance landscape, including the information collection process, problem analysis approach, and design principles applied throughout the report.

Problem analysis

A problem analysis workshop was conducted with government stakeholders which guided the direction of this report. The overall problem statement ('The Internet governance landscape is complex and opportunities for intervention may not be well understood across the Australian Government or by relevant domestic stakeholders') was analysed by identifying related causes and effects. This allowed the key needs for this report to be identified.

Information collection process

To ensure the comprehensiveness and accuracy of the information presented in this report, a systematic approach to data collection was employed. Multiple sources were utilised to gather information about the various stakeholders, organisations, processes, and challenges in the field of Internet governance. The information collection process involved:

1. **Literature review:** A thorough review of existing literature, including academic articles, policy documents, and reports from international organisations, was conducted to gather insights into the Internet governance landscape, its evolution, and the key issues currently being addressed.

2. **Stakeholder interviews:** In-depth interviews with experts and stakeholders from various sectors, such as government, private sector, civil society, and academia, were conducted to gain first-hand perspectives on Internet governance and its implications for different actors.

3. **Online research:** A comprehensive online search was performed to gather additional information about the organisations, initiatives, and forums involved in Internet governance, as well as to identify recent developments and trends in the field.

4. **Data analysis and synthesis:** The collected information was analysed, compared, and synthesised to identify key themes, patterns, and relationships within the Internet governance landscape.

Development process

The approach used to develop this report aimed to provide a structured and systematic understanding of the Internet governance landscape. This approach involved:

1. **Identifying key components:** The various stakeholders, organisations, processes, and challenges involved in Internet governance were identified and categorised to provide a comprehensive overview of the landscape.

2. **Analysing relationships:** The relationships between the different components of the Internet governance landscape were examined, highlighting the connections, dependencies, and potential points of conflict or collaboration.

3. **Assessing dynamics:** The dynamics of the Internet governance landscape were analysed, taking into consideration the evolving nature of the Internet, the roles of different stakeholders, and the emerging challenges and opportunities in the field.
4. **Identifying opportunities for intervention:** Based on the analysis of the Internet governance landscape, potential areas for intervention by the Australian Government and the broader Internet community were identified, considering the interests, resources, and capabilities of various stakeholders.

Design principles applied in the report

Throughout the report, several design principles were applied to ensure the clarity, coherence, and effectiveness of the information presented. These design principles include:

1. **Relevance to research questions:** Ensure that the report addresses the specific research questions for the report:
    a. What are all the various ‘parts' to the Internet governance landscape? How do each of the parts operate, and how do they differ?
    b. Which are the main countries or organisations attached to each ‘part'?
    c. How are all the ‘parts' connected? Do they overlap or intersect? Do they conflict?
    d. How might the Internet governance landscape evolve between now and 2025?
    e. Where are the opportunities for intervention? For governments and for the Australian multistakeholder Internet community (i.e., industry and civil society)?
2. **Audience-centric:** Tailor the report to the needs and interests of the identified audience groups, including the Department of Infrastructure Transport Regional Development, Communication and the Arts (DITRCDA) (the Internet Governance Team and senior leaders in the department), Australian Government departments, government representatives in other countries, the public, and domestic, regional, and global Internet communities. Clearly communicate key messages that meet their needs.
3. **Comprehensive and concise:** Provide a thorough overview of the Internet governance landscape while maintaining brevity and avoiding unnecessary detail. Ensure that the report strikes a balance between being comprehensive and easy to digest for the target audiences.
4. **Focused on opportunities:** Highlight potential opportunities for future work and position Noetic as a suitable partner for such engagements. This includes subtle messaging within the report, as well as tailoring the approach to the engagement to build rapport with the client.
5. **Structure and organisation:** The report is structured to provide a logical flow of information, guiding readers from the introduction and context of Internet governance to the in-depth analysis of the landscape and the identification of opportunities for intervention.
6. **Visual representations:** Visual elements, such as diagrams, charts, and tables, are used throughout the report to illustrate complex concepts, relationships, and trends, making the information more accessible and engaging for readers.

By employing a rigorous methodology, structured problem analysis, and thoughtful design principles, this report offers a comprehensive, accurate, and accessible analysis of the Internet governance landscape, providing valuable insights for policymakers, industry leaders, and the wider Internet community.

Design principles for the Systems Map

1. **Standalone Systems Map:** Design the systems map to be a self-sufficient visual representation of the Internet governance landscape, allowing for independent understanding and retention. The report should complement the systems map, enhancing the overall comprehension of the subject matter.

2. **Versatility and adaptability:** Create a stand-alone infographic that can be used as a versatile communication tool for a wide audience and can be easily updated to reflect changes in the Internet governance landscape over time.

3. **Integration of anticipated changes:** Incorporate the ability to visualize how the Internet governance landscape may evolve over the next two years through overlayed infographics, using a timeline slide bar or other interactive elements to show changes from the current state to the future state.

4. **Focus on key players and relationships:** Clearly depict the main countries, organisations, and stakeholders involved in the Internet governance landscape, as well as their roles, relationships, and areas of intersection or conflict.

5. **Specific design principles catering to audience needs:** Tailor the design of the systems maps to incorporate specific principles, such as "Simple/approachable" for the public, that address the needs of various audience groups identified in the Deliverable Design Template. This ensures that the visualisations effectively communicate key messages and insights relevant to each group.

6. **Simple:** the systems map needs to be able to be understood by a wide audience that has no prior knowledge.

7. **Comprehensive:** All encompassing: needs to provide a big-picture view that encompasses the entire landscape, not just a particular model within the landscape.

8. **Layers of detail:** the detailed view of the landscape are provided in lower layers of the system map that flesh out the simple high-level view.

By following these design principles, the report and systems map will provide a coherent, comprehensive, and visually compelling overview of the Internet governance landscape, tailored to the specific needs and interests of the identified audience groups.

Annex B: Bibliography

ANU Tech Policy Design Centre (2019), 'New kit to deliver better tech policy', accessed 7 March 2023. https://techpolicydesign.au/news/new-kit-to-deliver-better-tech-policy

APNIC, ' APNIC in the Internet ecosystem', APNIC, accessed 12 May 2023. https://www.apnic.net/community/ecosystem/

Attrill N & Fritz A (2021), 'China's cyber vision: how the Cyberspace Administration of China is building a new consensus on global Internet governance', Australian Strategic Policy Institute, accessed 12 May 2023. https://www.aspi.org.au/report/chinas-cyber-vision-how-cyberspace-administration-china-building-new-consensus-global

Barlow JP (1996), ' A Declaration of the Independence of Cyberspace', Electronic Frontiers Foundation, accesses 12 May 2023. https://www.eff.org/cyberspace-independence

Commonwealth of Australia, Department of Foreign Affairs and Trade (2021), 'Australia's International Cyber and Critical Technology Engagement Strategy, accessed 12 May 2023. https://www.internationalcybertech.gov.au/strategy

Council of Europe (2021), 'Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence', Council of Europe, accessed 12 May 2023. https://www.coe.int/en/web/cybercrime/second-additional-protocol

de Bossey C (2005) 'Report of the Working Group on Internet Governance. Geneva: World Summit on the Information Society', accessed 7 March 2023. https://www.wgig.org/docs/WGIGREPORT.pdf

Drake WJ, Cerf VG, Kleinwächter W (2016), 'Future of the Internet Initiative White Paper: Internet Fragmentation: An Overview', World Economic Forum, accessed 23 June 2023, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

Groch S & Bonyhady N (2023), 'The secret service agents had a message: take down the app or go to jail. How is the Internet splintering', The Sydney Morning Herald, accessed 30 April 2023. https://www.smh.com.au/technology/the-secret-service-agents-had-a-message-take-down-the-app-or-go-to-jail-how-is-the-internet-splintering-20230327-p5cvl2.html.

Hoxtell W & Nonhoff D (2019), 'Internet governance: Past, present and future', Global Public Policy Institute, accessed 7 March 2023. https://www.gppi.net/media/Internet-Governance-Past-Present-and-Future.pdf

Internet Corporation for Assigned Names and Numbers (ICANN) (2019), 'Access Domain Names in Your Language', accessed 11 May 2023. https://www.icann.org/resources/pages/idn-2012-02-25-en

'IGF 2022 MAG Statement: Ensuring a Multistakeholder Approach to the Global Digital Compact', Internet Governance Forum, 2022, accessed 7 March 2023. https://intgovforum.org/en/filedepot_download/24/23090

IGF 2022 Policy Network on Internet Fragmentation (2023), 'Output document', Internet Governance Forum, accessed 23 June 2023. https://www.intgovforum.org/en/filedepot_download/256/24127

Internet Society (2022),' Huawei's New IP Proposal: Frequently Asked Questions', Internet Society, accessed 23 June 2023. https://www.internetsociety.org/resources/doc/2022/huaweis-new-ip-proposal-faq/

Internet Society (2022), 'The internet ecosystem', Internet Society, accessed 11 May 2023. https://www.internetsociety.org/wp-content/uploads/2022/07/2022-Internet-Ecosystem-EN.pdf

Internet Society (2016), 'Internet Governance: Why the Multistakeholder Approach Works', Internet Society, accessed 12 May 2023. https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/

Internet Society (2016), 'The history of IANA: And extended timeline with citations and commentary', accessed on 12 May 2023. https://www.internetsociety.org/ianatimeline/

Kleinwachter, W. (2018), 'Framing the Internet governance debate: The long road to WSIS+20 (2025)', CircleID, accessed 7 March 2023. https://circleid.com/posts/20210304-framing-the-internet-governance-debate-long-road-to-wsis-2025

Lee TB (2014), ' 40 maps that explain the Internet', Vox, accessed 12 May 2023. https://www.vox.com/a/internet-maps

Lee TB (2015), ' The internet, explained', Vox, accessed 29 August 2023. https://www.vox.com/2014/6/16/18076282/the-internet

Leiner BM, Cerf VG, Clark DD, Kahn RE, Kleinrock L, Lynch DC, Postel J, Roberts LG & Wolff S (1997), 'Brief History of the Internet', Internet Society, accessed 11 May 2023. https://www.internetsociety.org/resources/doc/2017/brief-history-internet/

McKinght G, & Calderon A (2017) 'Virtual School of Internet Governance Series: Overview', Internet Society, accessed 7 March 2023. https://www.slideshare.net/gmcknight/virtual-school-of-internet-governance

National Science and Media Museum (2020), 'A short History of the Internet', accessed 11 May 2023. https://www.scienceandmediamuseum.org.uk/objects-and-stories/short-history-internet

Pigatto JT, Datysgeld MW & da Silva LGP (2021), 'Internet governance is what global stakeholders make of it: a tripolar approach', Revista Brasileira de Politica Internacional, 64(2), e011.

ANU Tech Policy Design Centre (n.d), 'Tech Policy Process', ANU Tech Policy Design Centre, accessed 7 March 2023. https://techpolicydesign.au/tech-policy-process

The Senate (2021), 'Select Committee on Foreign Interference through Social Media: First Interim Report', accessed: 11 May 2023.

https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Interference_through_Social_Media/ForeignInterference/Interim_Report [Accessed: 11 May 2023]

The Working Group on Internet Governance (2005), 'Background Report'.

Tucows (n.d.), 'Making the Internet better', Tucows, accessed 11 May 2023. https://tucowsdomains.com/making-the-internet-better/

U.S. Department of State (2022), 'Declaration for the Future of the Internet', U.S. Department of State, accessed 12 May 2023. https://www.state.gov/declaration-for-the-future-of-the-internet

UN Secretary-General's High-level Panel on Digital Cooperation (2019), 'The Age of Digital Interdependence', United Nations, accessed 12 May 2023. https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf

United Nations (2020), 'Report of the Secretary-General: Roadmap for Digital Cooperation', United Nations, accessed 12 May 2023. https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf

Annex C: Glossary

Throughout this report, numerous terms and acronyms related to Internet governance have been used. For ease of understanding and reference, this glossary provides definitions and explanations of these terms.

AI (Artificial Intelligence): The development of computer systems that can perform tasks typically requiring human intelligence, such as visual perception, speech recognition, decision-making, and language translation.

ACCAN (Australian Communications Consumer Action Network): Australia's peak communications consumer organisation representing individuals, small businesses and not-for-profit groups as consumers of communications products and services. More Info

ACCC (Australian Competition and Consumer Commission): Australia's national competition, consumer, fair trading and product safety regulator. More Info

ACMA (Australian Communications and Media Authority): Regulates communications and media to contribute to maximising the economic and social benefits of communications infrastructure, services and content for Australia. More Info

AIIA (Australian Information Industry Association): Australia's peak representative body and advocacy group for those in the digital ecosystem. A not-for-profit organisation that pursues activities to stimulate and grow the digital ecosystem, to create a favourable business environment for our members and to contribute to Australia's economic prosperity. More Info

ALAC (At-Large Advisory Committee): The ICANN committee that advocates for the interests of end-users. It advises on the activities of ICANN, including Internet policies developed by ICANN's Supporting Organisations and participates in ICANN's outreach and engagement programs. One At-Large member is selected to serve on ICANN's Board of Directors. More Info

APNIC (Asia Pacific Network Information Centre): An open, member-based, not-for-profit organisation, whose primary role is to distribute and manage Internet number resources (IPv4, IPv6 and AS Numbers) in the Asia Pacific region's 56 economies. More Info

APT (Asia-Pacific Telecommunity): An intergovernmental organisation that operates in conjunction with telecom service providers, manufacturers of communications equipment, and research and development organisations active in the field of communication, information, and innovation technologies. More Info

APTLD (Asia Pacific Top Level Domain Association): An organisation for ccTLD (Country Code Top Level Domain) registries in Asia Pacific region. More Info

ASO (Address Supporting Organization): One of ICANN's three supporting organisations. ASO reviews and develops recommendations on IP address policy and advises the ICANN Board on policy issues relating to the operation, assignment, and management of IP addresses. More Info

auDA (.au Domain Administration Limited): The policy authority and industry self-regulatory body for the .au domain space. More Info

Big Tech: Refers to the largest and most dominant companies in the information technology industry, such as Google, Amazon, Facebook, Apple, and Microsoft. These companies have significantly influenced the development of the Internet, offering platforms and services that have become integral parts of daily life for billions of people worldwide.

Blockchain: A blockchain is a type of distributed ledger technology, where transactions or records are grouped together in 'blocks' and then linked together in a 'chain'. This technology is decentralized, meaning that it doesn't rely on a central point of control. Instead, multiple copies of the blockchain are kept on different computers, and these copies are constantly checked and updated against each other. The technology is known for its transparency, security, and ability to resist tampering.

ccNSO (country code Names Supporting Organization): A body within the ICANN structure created for and by ccTLD managers. The ccNSO provides a platform to nurture consensus, technical cooperation and skill building among ccTLDs and facilitates the development of voluntary best practices for ccTLD managers. More Info

ccTLDs (country code Top-Level Domains): Two-letter Internet top-level domains (TLDs) specifically designated for a particular country, sovereign state, or autonomous territory for use to service their community. More Info

Censorship: The suppression or prohibition of any parts of the Internet, including websites, content, or communication, considered politically unacceptable, harmful, or otherwise objectionable.

CIGI (Centre for International Governance Innovation): An independent, non-partisan think tank conducting world-leading research and analysis to offer innovative policy solutions for the digital era. Addresses significant global issues at the intersection of technology and international governance. More Info

Comms Alliance (Communications Alliance): Provides a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services. offers a forum for the industry to make coherent and constructive contributions to policy development and debate. More Info

Critical Infrastructure: Physical and virtual systems and assets that are essential to the functioning of a society and its economy, including the Internet and its underlying infrastructure.

CSTD (Commission on Science and Technology for Development): A subsidiary body of the Economic and Social Council (ECOSOC), one of the six main organs of the United Nations. It provides the General Assembly and ECOSOC with high-level advice on relevant science and technology issues. More Info

Cybersecurity: The practice of protecting Internet-connected systems, including hardware, software, and data, from digital attacks, damage, or unauthorised access.

Data Privacy: The protection of personal information from unauthorised access, disclosure, or misuse, including the right to control how one's data is collected, used, and shared.

Decentralized Autonomous Organisations (DAOs): An emerging form of legal structure that has no central governing body and whose members share a common goal to act in the best interest of the entity. Popularized through cryptocurrency enthusiasts and blockchain technology, DAOs are used to make decisions in a bottom-up management approach. More Info

DFAT (Department of Foreign Affairs and Trade): Promotes and protects Australia's international interests to support our security and prosperity. Works with international partners and other countries to tackle global challenges, increase trade and investment opportunities, protect international rules, keep our region stable and help Australians overseas. More Info

DIGI (Digital Industry Group): A not for profit industry association advocating for the digital industry in Australia. DIGI is the industry association for companies that invest in online safety, privacy, cyber security and a thriving Australian digital economy. Brings together global, Australian, large and scale-up technology companies together on issues of shared public policy interest. More Info

Digital Divide: The gap between individuals, households, businesses, and geographic areas at different socio-economic levels concerning their opportunities to access information and communication technologies (ICTs) and their use of the Internet.

Digital Rights: The human rights and legal rights that apply to the digital environment, including privacy, freedom of expression, and access to information.

DISR (Department of Industry, Science and Resources): The Australian department for industry, science and resources, supports Australia's critical technology industries and capabilities. Additionally, it has a whole of government coordination function on standards for critical technologies. More Info

DITRDCA (Department of Infrastructure, Transport, Regional Development, Communications and the Arts): Provides strategic policy advice, administer fit-for-purpose regulation and deliver programs and services in the Australian communications sector. Represents the Australian Government in multistakeholder Internet governance fora and represents the Australian Government at the ITU. More Info

Domain Name System (DNS): A system used to translate human-friendly domain names (e.g., www.example.com) into the IP addresses that computers use to identify each other on the network.

DNS abuse: Malicious behaviour aimed at disrupting DNS infrastructure or operations. DNS abuse is classified into five categories; malware (such as ransomware), botnets, phishing, pharming and spam (where it facilitates one of the other four categories of abuse. More Info

DNSSEC (Domain Name System Security Extensions): A suite of extensions to DNS that provides additional security measures, such as cryptographic signatures, to protect against DNS-related security threats.

EFA (Electronic Frontiers Australia): An Australian non-profit organisation promoting and protecting online civil liberties. Advocates for free speech and unfettered access to information. More Info

ESCAP (Economic and Social Commission for Asia and the Pacific): One of the five regional commissions of the United Nations. Promotes cooperation among its member States in the Asia-Pacific region in pursuit of solutions to sustainable development challenges. More Info

ETSI (European Telecommunications Standards Institute): One of the three European Standards Organisations. ETSI is the recognized regional standards body dealing with telecommunications, broadcasting and other electronic communications networks and services. More Info

European Union (EU): A political and economic union of 27 member states that are located primarily in Europe. More Info

FOC (Freedom Online Coalition): Coalition of 37 governments working together to advance internet freedom so that human rights and fundamental freedoms are protected online. More Info

Fragmentation of the Internet: The idea that the Internet may be in danger of splitting into a series of cyberspace segments, thus endangering its connectivity. More Info

GAC (Governmental Advisory Committee): The GAC constitutes the voice of Governments and Intergovernmental Organizations (IGOs) in ICANN's multistakeholder structure. Created under the ICANN Bylaws, the GAC is an advisory committee to the ICANN Board. The GAC's key role is to provide advice to ICANN on issues of public policy, and especially where there may be an interaction between ICANN's activities or policies and national laws or international agreements. More Info

GDC (Global Digital Compact): A term used to describe international efforts to work together on digital matters. It is often associated with the UN Secretary-General's Roadmap for Digital Cooperation, which outlines eight key areas for action. More Info

GDPR (General Data Protection Regulation - EU): A regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas. More Info

Geopolitical Risks: The potential impact of political, economic, and social events on the stability and security of the Internet and its governance.

Global Commission on Internet Governance: An initiative launched in 2014, aimed at promoting good governance and enhancing economic development. More Info

GNSO (Generic Names Supporting Organization): One of ICANN's three supporting organisations. Develops policies related to gTLDs. The GNSO strives to keep gTLDs operating in a fair, orderly fashion across one global Internet, while promoting innovation and competition. More Info

gTLD (Generic Top-Level Domain): A top-level domain not tied to a specific country or territory, typically used for broad categories (e.g., .com, .org, .edu).

I&J Policy Network (Internet & Jurisdiction Policy Network): The multistakeholder organization addressing the tension between the cross-border Internet and national jurisdictions. Its Secretariat facilitates a global policy process engaging over 400 key entities from governments, the world’s largest internet companies, technical operators, civil society groups, academia and international organisations from over 70 countries. More Info

IAB (Internet Architecture Board): Provides long-range technical direction for Internet development, ensuring the Internet continues to grow and evolve as a platform for global communication and innovation. The IAB oversees the IETF and IRTF and is an advisory body of the Internet Society. More Info

IANA (Internet Assigned Numbers Authority): A department of ICANN responsible for coordinating some of the key elements that keep the Internet running smoothly, such as the allocation of IP addresses and the management of the DNS.

ICANN (Internet Corporation for Assigned Names and Numbers): A non-profit organisation that is responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet, ensuring the network's stable and secure operation. More Info

IEEE (Institute of Electrical and Electronics Engineers): Nurtures, develops, and advances the building of global technologies. As a leading developer of industry standards in a broad range of technologies, IEEE drives the functionality, capabilities, safety, and interoperability of products and services, transforming how people live, work, and communicate. More Info

IESG (Internet Engineering Steering Group): The group within the IETF which is responsible for technical management of IETF activities and the Internet standards process. It is directly responsible for the actions associated with entry into and movement along the Internet "standards track," including final approval of specifications as Internet standards. More Info

IETF (Internet Engineering Task Force): An open standards organisation, which develops and promotes voluntary Internet standards, in particular the standards that comprise the Internet protocol suite (TCP/IP). Overseen by the IAB and works in parallel with the IRTF. More Info

IGF (Internet Governance Forum): A multistakeholder forum for policy dialogue on issues of Internet governance. It brings together all stakeholders in the Internet governance debate, whether they represent governments, the private sector or civil society, including the technical and academic community, on an equal basis and through an open and inclusive process. More Info

Internet Governance: The development and application of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet.

Interoperability: The ability of diverse systems, devices, and applications to work together and exchange information efficiently and effectively.

IoT (Internet of Things): A network of physical objects embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems over the Internet.

IP Address (Internet Protocol Address): A unique numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.

IPv4 (Internet Protocol version 4): The fourth version of the Internet Protocol, widely used to identify devices on a network through an addressing system.

IPv6 (Internet Protocol version 6): The most recent version of the Internet Protocol, which expands the number of available IP addresses and introduces several improvements to IPv4.

IRTF (Internet Research Task Force): A non-profit technology research organisation focused on long-term technical topics related to internet protocols, applications, architecture and technology. Overseen by the IAB and works in parallel with the IETF. More Info

ISOC (Internet Society): A global non-profit organisation dedicated to promoting the open development, evolution, and use of the Internet for the benefit of all people throughout the world. The corporate home for the IAB, IETF and IRTF. More Info

ISP (Internet Service Provider): A company that provides access to the Internet for customers, typically through wired or wireless connections.

ITU (International Telecommunication Union): A specialised agency of the United Nations that is responsible for issues that concern information and communication technologies, including the development of technical standards. It is the oldest global international organisation. More Info

ITU-D (ITU Telecommunication Development Sector): Works to close the digital divide and drive digital transformation to leverage the power of ICTs for economic prosperity, job creation, digital skills development, gender equality, diversity, a sustainable and circular economy, and for saving lives. More Info

ITU-R (ITU Radiocommunication Sector): Ensures the rational, equitable, efficient and economical use of the radio-frequency spectrum by all radiocommunication services, including those using satellite orbits, and to carry out studies and approve recommendations on radiocommunication matters. More Info

ITU-T (ITU Telecommunication Standardization Sector): Develops international standards which act as defining elements in the global infrastructure of information and communication technologies. Standards are critical to the interoperability of these technologies by ensuring that countries' networks and devices are speaking the same language. More Info

MAG (Multistakeholder Advisory Group): Prepares the programme and schedule of the annual IGF meeting. Advises the Secretary-General of the UN on the programme and schedule of the IGF meetings. The MAG is comprised of 55 members from governments, the private sector and civil society, including representatives from the academic and technical communities. More Info

Metaverse: a vision of what many in the computer industry believe is the next iteration of the Internet: a single, shared, immersive, persistent, 3D virtual space where humans experience life in ways they could not in the physical world. More Info

Multistakeholder Model: A governance framework that includes multiple stakeholders, such as governments, the private sector, civil society, academia, and technical communities, in the decision-making process.

Net Neutrality: The principle that Internet service providers must treat all data on the Internet the same, without discriminating or charging differently by user, content, website, platform, or application.

NetThing: An Australian Internet Governance Forum, a platform for anyone interested in Australian Internet policy to contribute to the discussion. More Info

NIST (National Institute of Standards and Technology): A U.S. federal agency that develops and promotes measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

NGO (Non-Government Organisation): A voluntary group of individuals or organisations, usually not affiliated with any government, that is formed to provide services or to advocate a public policy. Although some NGOs are for-profit corporations, the vast majority are non-profit organisations.

NomCom (Nomination Committee): An independent group within ICANN tasked with selecting members of the ICANN Board of Directors and other key ICANN leadership positions. More Info

NRO (Number Resource Organization): A coordinating body for the five Regional Internet Registries (RIRs) that manage the distribution of Internet number resources, such as IP addresses. It ensures that each RIR can function in a globally coordinated manner. More Info

OECD (Organisation for Economic Co-operation and Development): An international organisation that works to build better policies for better lives. Its goal is to shape policies that foster prosperity, equality, opportunity, and well-being for all. More Info

UOHCHR (Office of the High Commissioner for Human Rights): A department of the Secretariat of the United Nations that works to promote and protect the human rights that are guaranteed under international law and stipulated in the Universal Declaration of Human Rights of 1948. More Info

Open Standards: Technical standards that are publicly available and developed through a collaborative, consensus-driven process, enabling multiple stakeholders to create compatible products and services.

PaCSON (Pacific Cyber Security Operational Network): An operational cyber security network, consisting of regional working-level cyber security experts and technical experts from eligible governments across the Pacific working to improve cyber security capabilities and readiness across the Pacific. More Info

PNIF (Policy Network on Internet Fragmentation): An IGF intersessional activity born out of a community initiative by a multistakeholder coalition of civil society, business and technical community organisations to raise awareness of the technical, policy, legal and regulatory measures and actions that pose a risk to the open, interconnected and interoperable Internet. More Info

PTI (Public Technical Identifiers): An affiliate of ICANN performing the IANA functions on behalf of ICANN. Responsible for the operational aspects of coordinating the Internet's unique identifiers and maintaining the trust of the community to provide these services in an unbiased, responsible and effective manner. More Info

Regional TLDs (Regional Top-Level Domain associations): Non-profit entities that provide a forum for ccTLD organisations to exchange information regarding technological and operational issues of domain name registries in the region (e.g., Asia Pacific Top Level Domain Association, Council of European National Top-Level Domain Registries, etc).

RFC (Request for Comments): A publication from the technology community. It can come from many bodies including from the Internet Engineering Task Force (IETF). An RFC can be nearly any type of document, e.g., a standard, a protocol, a procedure, or a report. More Info

Registrant: An individual or company that owns a domain name.

Registrar: An organization that has the authority to issue a domain name license to a registrant.

Registry: An organization that manages top-level domain names (TLDs). They create domain name extensions, set the rules for that domain name, and work with registrars to sell domain names to the public.

RIRs (Regional Internet Registries): RIRs are organisations that oversee the allocation and registration of Internet number resources within a particular region of the world. There are five RIRs, namely: African Network Information Centre (AFRINIC), American Registry for Internet Numbers (ARIN), Asia-Pacific Network Information Centre (APNIC), Latin America and Caribbean Network Information Centre (LACNIC), and Réseaux IP Européens Network Coordination Centre (RIPE NCC). More Info

Roadmap for Digital Cooperation: A report issued by the UN Secretary-General in 2020, outlining a set of recommendations on how to improve global digital cooperation. More Info

RPKI (Resource Public Key Infrastructure): A security framework that helps prevent malicious IP resource hijacks, which can result in critical outages or fraudulent traffic manipulation. More Info

RSSAC (Root Server System Advisory Committee): Advises the ICANN Board and community on matters relating to the operation, administration, security, and integrity of the Root Server System. More Info

SSAC (Security and Stability Advisory Committee): Advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. More Info

System for Standardized Access/Disclosure (SSAD): Aims to provide accredited users with access to non-public WHOIS data, balancing the need for data access with GDPR's privacy mandates.

Technical Community: In the context of Internet governance, the "technical community" typically refers to a diverse group of individuals and organisations that contribute to the development, deployment, and maintenance of the Internet's technical infrastructure. This includes but is not limited to software developers, engineers, researchers, network operators, and institutions such as the IETF, ICANN, and W3C, which set standards and protocols to ensure the interoperability and functionality of the Internet.

TLD (Top Level Domain): The last segment of a domain name, or the part that follows immediately after the "dot" symbol. TLDs are mainly classified into two categories: generic TLDs and country specific TLDs. Examples include .com, .org, .net, .gov, .biz and .edu, and country specific TLDs such as .us, .au, .in, and .uk. More Info

TLG (Technical Liaison Group): Provides technical advice to the ICANN Board on specific matters pertinent to ICANN's activities. Members consist of representatives from ETSI, IAB, ITU-T and W3C. More Info

UN GGE (United Nations Group of Governmental Experts): UN Groups of Governmental Experts have been established several times to study different aspects of information security. Their reports form a key part of the discussion at the United Nations on norms of responsible state behaviour in cyberspace. More Info

UN OEWG (United Nations Open-Ended Working Group): An initiative established by the United Nations to discuss developments in the field of information and telecommunications in the context of international security. More Info

UN Tech Envoy (United Nations Technology Envoy): A position established by the United Nations Secretary-General to enhance the world body's coordination and capacity to advance digital cooperation and to help address the growing impact of digital technology on our world and on the UN. Its responsibilities include working towards the Global Digital Compact. More Info

UNCTAD (United Nations Conference on Trade and Development): A permanent intergovernmental body established by the United Nations General Assembly, responsible for dealing with development issues, particularly international trade – the main driver of development. Co-organises the WSIS. More Info

UNDESA (United Nations Department of Economic and Social Affairs): Part of the UN Secretariat responsible for facilitating major global conferences and summits in the economic, social and environmental fields to assist countries as they find common ground, set norms, and take decisive steps forward towards sustainable development for all. Provides substantive and administrative support to the IGF Secretariat. More Info

UNDP (United Nations Development Programme): The United Nations' global development network. It promotes technical and investment cooperation among nations and advocates for change and connects countries to knowledge, experience, and resources to help people build a better life for themselves. Co-organises the WSIS. More Info

UNESCO (United Nations Educational, Scientific and Cultural Organization): A specialised agency of the United Nations aimed at promoting world peace and security through international cooperation in education, the sciences, and culture. Co-organises the WSIS. More Info

UNICEF (United Nations International Children's Emergency Fund): A United Nations agency responsible for providing humanitarian and developmental aid to children worldwide. More Info

United Nations: An international organisation founded in 1945. It is currently made up of 193 Member States. The mission and work of the United Nations are guided by the purposes and principles contained in its founding charter. More Info

W3C (World Wide Web Consortium): An international community where member organisations, a full-time staff, and the public work together to develop Web standards led by Web inventor and Director Tim Berners-Lee and CEO Jeffrey Jaffe. More Info

Web3: This term refers to the proposed third generation of the Internet, which would be built on blockchain technology. The vision of Web3 is a decentralised online environment where users have control over their own data and interactions, rather than these being controlled by centralized entities such as tech companies. This vision is underpinned using technologies such as blockchain, smart contracts, and decentralized autonomous organisations (DAOs).

WHOIS: A system, managed by ICANN, that publicly displays the contact information of domain name registrants, including names, addresses, and email addresses.

WIC (World Internet Conference): An annual conference organised by Chinese government agencies for global discussions and exchanges on global Internet issues and trends. More Info

WIPO (World Intellectual Property Organization): A specialised agency of the United Nations that leads the development of a balanced and effective international intellectual property (IP) system that enables innovation and creativity for the benefit of all. More Info

WSIS (World Summit on the Information Society): A two-phase United Nations-sponsored summit on information, communication and, in broad terms, the information society that took place in 2003 in Geneva and in 2005 in Tunis. More Info

WSIS+10: Refers to the ten-year review of the World Summit on the Information Society (WSIS) process, which was held in 2015. More Info

WTO (World Trade Organization): An organisation that deals with the global rules of trade between nations. Its main function is to ensure that trade flows as smoothly, predictably, and freely as possible. More Info

Noetic by atturra

PO Box 4177
Kingston ACT 2604

Level 4, 42 Macquarie Street
Barton ACT 2600 Australia

T +61 2 6234 7777

noeticgroup.com