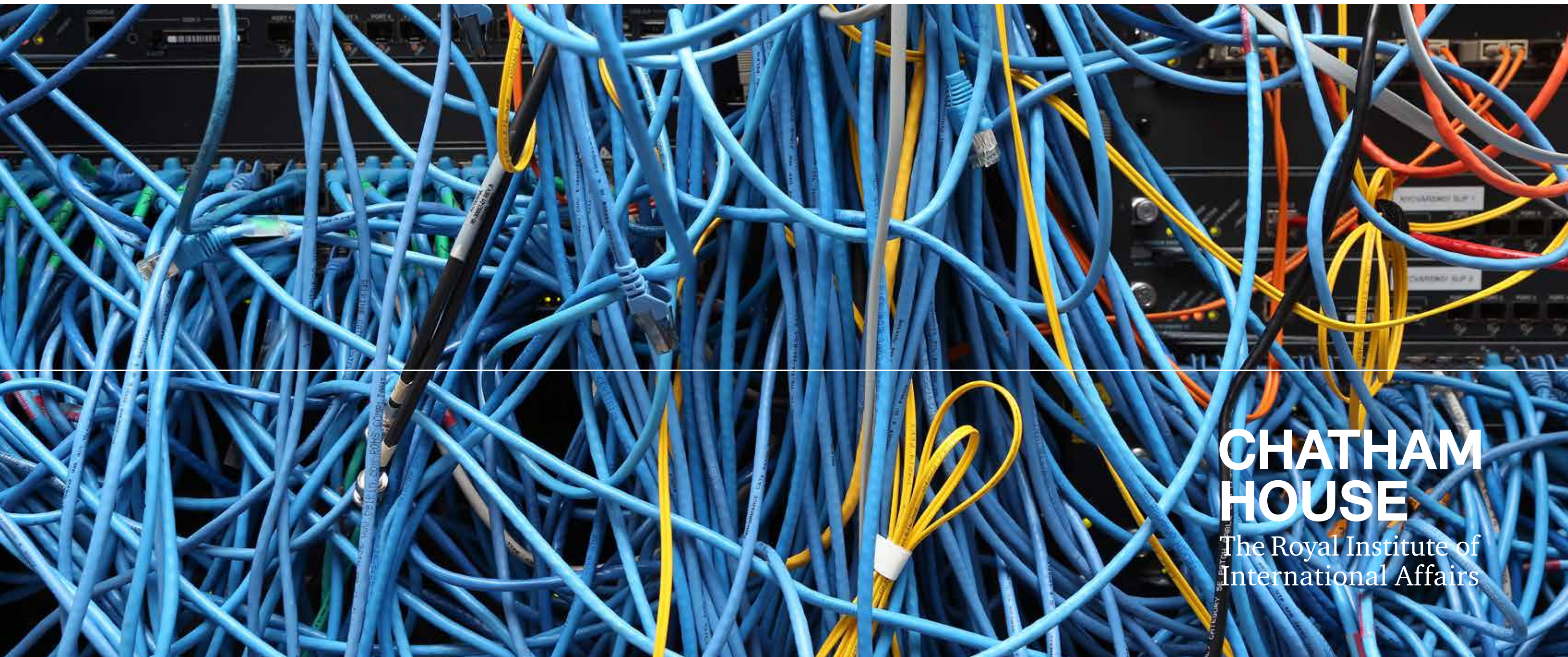
Research Paper

Emily Taylor and Stacie Hoffmann
International Security Department | November 2019

EU–US Relations on Internet Governance



CHATHAM HOUSE
The Royal Institute of International Affairs

Contents

Summary

- As internet governance issues emerge in the wake of innovations such as the Internet of Things (IoT) and advanced artificial intelligence (AI) there is an urgent need for the EU and US to establish a common, positive multi-stakeholder vision for regulating and governing the internet.

- Political, economic, sociological and technological factors are poised to challenge EU and US ideological positions on internet governance, which will make it difficult to find consensus and common ground in the years to come.

- The EU and US share core values and perspectives relating to internet governance, such as openness, freedom and interoperability, as well as a human rights framework for cybersecurity. There have been many examples of successful multi-stakeholder cooperation between the EU and US, including the Internet Assigned Numbers Authority (IANA) transition and the European Dialogue on Internet Governance (EuroDIG).

- There are also subtle differences between the EU and US, and each has different reasons to support multi-stakeholderism. Cases that highlight growing tensions in EU–US coordination on internet governance include the controversies surrounding the EU General Data Protection Regulation (GDPR), the WHOIS system that governs domain name registration data, and the board of the Internet Corporation for Assigned Names and Numbers (ICANN), which undermined an independent cybersecurity review.

- Internet governance is becoming more complex, with a multiplicity of actors and no obvious authority for important emerging issues. Additionally, the rise of China and its authoritarian vision for the future of the internet is a threat to the current internet governance institutions that have been shaped by and reflect Western values.

- To bridge ideological gaps the EU and US should build capacity between likeminded stakeholders, create a taskforce on effective multi-stakeholder internet governance, and work through non-governmental stakeholders to improve participation.

1. Introduction

This research paper is part of a series commissioned by the EU Delegation to the US. The purpose of this paper is to provide new perspectives and proposals to improve the effectiveness of EU–US relations on internet governance. It explores converging and diverging ideological positions, highlights common interests, and makes recommendations to enhance cooperation. The primary audience of this paper is the EU Delegation, to whom the recommendations are addressed.

The EU Delegation was closely involved in shaping the scope and structure of the paper and provided detailed feedback on early drafts. With the agreement of the EU Delegation, the paper does not attempt to provide a comprehensive background on the current landscape. Instead, it is operational in character and provides a focus on issues that illustrate successful actions or areas of tension, which provide the motivation for recommendations that are addressed to the EU Delegation.

The paper begins with a working definition of internet governance and 'multi-stakeholderism', an analysis of drivers for change from the external environment, and reviews major players and processes in internet governance. It goes on to analyse areas where the EU–US relationship is working effectively, identifies the barriers to effectiveness – each illustrated with case studies – and looks ahead to the future of internet governance. The paper makes five recommendations, including the establishment of a taskforce to measure and improve the effectiveness of internet governance processes.

Any discussion of internet governance tends to be jargon-laden and acronym-heavy. This paper is no exception as its primary audience is expert in the field and its purpose is to provide strategic and operational advice. For newcomers to the subject area, the authors have provided a list of abbreviations and acronyms to explain their use in the paper.

Methodology

The research draws on a variety of primary and secondary sources including interviews and documents. Interviews were conducted with individuals who are current or former officials in the US and EU administrations, and senior staff members at the Internet Corporation for Assigned Names and Numbers (ICANN). The individuals agreed to speak on a non-attribution basis, and their input informs the paper's analysis and recommendations. Desk research included resources from internet governance organizations, output documents, reports and articles regarding internet governance and international relations. The authors applied qualitative analysis techniques to determine points of convergence and divergence between the EU and US, elucidate nuances in internet governance between actors, and develop recommendations for both the EU Delegation and broader EU institutions.

2. Context

What is meant by internet governance?

Internet governance is associated with ‘a vital but relatively narrow set of policy issues related to the global coordination of internet domain names and addresses’.[1] These are managed by ICANN through the Internet Assigned Numbers Authority (IANA) function. ICANN’s bylaws expressly limit its areas of responsibility and prevent it from engaging in issues outside its scope, such as content issues, or the impact of artificial intelligence on societies. Additionally, the internet’s landscape evolves in response to new technologies and innovations throughout the ecosystem, which limits the effectiveness of a narrow governance approach.

In 2005, the Working Group on Internet Governance defined internet governance more broadly, as ‘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’.[2] The Internet Governance Forum (IGF), created by the World Summit on the Information Society,[3] has adopted an inclusive attitude towards internet governance topics, and this flexible approach has enabled the evolving dialogue to reflect emerging issues.[4]

Domain names and Internet Protocol (IP) addresses are fundamental to the internet’s core architecture, giving each device connected to the web an identifier that is globally unique and universally accepted.[5] Both domain names and IP addresses enable this and have remained relevant in the face of remarkable technological change over the past 20 years. That said, there are signs of a shift taking place. Since 2005, the number of domains per 100 internet users has declined from a highpoint of 12 (2008) to 9 (2018).[6] The past decade has seen several substitutes for domain names gaining market share, notably social media accounts for individuals and businesses and apps

[1] Mueller, M. (2010), *Networks and States*, Cambridge, MA, MIT Press, p. 9.

[2] Working Group on Internet Governance (2005), ‘Report of the Working Group on Internet Governance’, p. 4, http://www.wgig.org/docs/WGIGREPORT.pdf (accessed 4 Oct. 2019).

[3] International Telecommunications Union (ITU) (2005), *Tunis Agenda for the Information Society,* 18 November 2005, para 72, https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html (accessed 4 Oct. 2019).

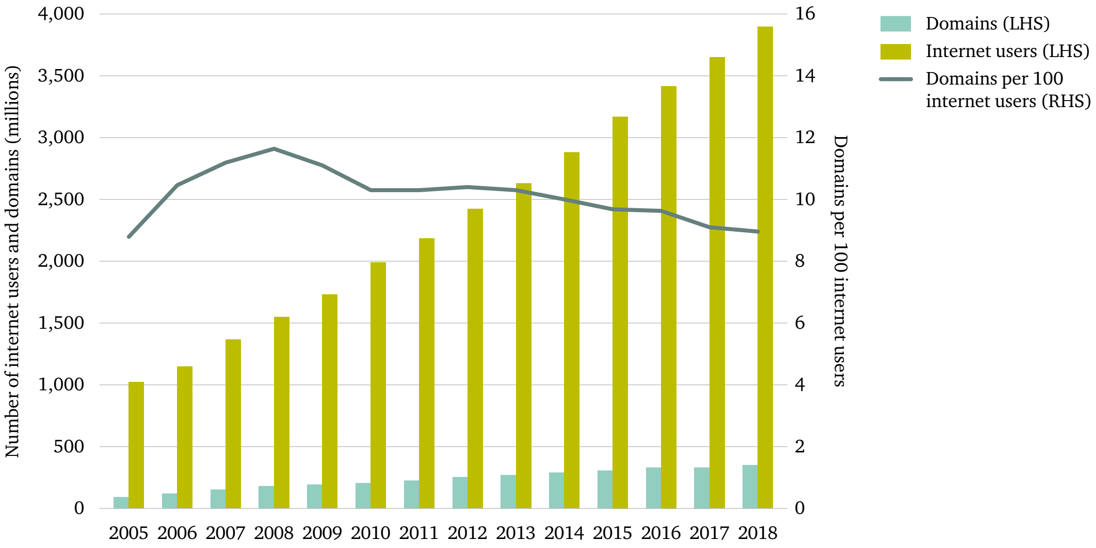
[4] At the first IGF meeting in 2006, the main session topics were openness, access, security, diversity and emerging issues, see Doria, A. and Kleinwachter, W. (eds) (2008), *Internet Governance Forum: The First Two Years*, Internet Governance Forum, http://www.intgovforum.org/multilingual/filedepot_download/3367/5 (accessed 14 Oct. 2019). By 2018, the core topic of the IGF meeting was ‘The Internet of Trust’ and the main sessions were on cybersecurity, trust and privacy; the evolution of internet governance; development, innovation & economic issues; and human rights, gender and youth, see IGF (2018), ‘The Internet of Trust’, conference schedule, https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/6785/1342 (accessed 14 Oct. 2019).

[5] O’Hara, K. and Hall, W. (2018), ‘Four Internets: The Geopolitics of Digital Governance’, CIGI Papers No. 206, December 2018, https://www.cigionline.org/publications/four-internets-geopolitics-digital-governance (accessed 4 Oct. 2019).

[6] Authors’ analysis based on the following sources: Verisign (n.d.), ‘Verisign Domain Name Industry Brief Archive (2009–2018)’, https://www.verisign.com/en_US/domain-names/dnib/domain-name-industry-brief-reports/index.xhtml#2019 (accessed 4 Oct. 2019); ITU (2018), ‘Key ICT indicators for developed and developing countries and the world (totals and penetration rates)’, https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2018/ITU_Key_2005-2018_ICT_data_with%20LDCs_rev27Nov2018.xls (accessed 4 Oct. 2019).

for the mobile market, particularly in emerging economies.[7] New internet protocols that support basic operations of the internet, like domain name system (DNS) over HTTPS (DoH) released by the Internet Engineering Task Force (IETF), risk splitting the internet's DNS root zone. It also remains unclear what role, if any, domains and IP addresses will play as the Internet of Things (IoT) develops into a globally interoperable network. Meanwhile, slow adoption of IPv6[8] and increased use of network address translation[9] continue to risk fragmentation of the IP address space. As of September 2019, only 24 per cent of the world's internet traffic was IPv6 preferred.[10]

Figure 1: Domains per internet user 2005–18



Source: Compiled by the authors from Verisign Domain Name Industry Brief and ITU Key 2005-2018 ICT data.

Whether or not domain names and IP addresses have as much relevance in the future, an essential component of any internet governance strategy is the continuing focus on the system's unique identifiers. But this narrow focus is insufficient to tackle widely recognized urgent internet governance issues, which currently have no internationally agreed upon multi-stakeholder home. These issues include AI, big data, IoT and its applicable technical standards, oversight of new recursive resolvers (i.e. using DoH), as well as privacy, cybersecurity and the role of states in cyberspace.

[7] Oxford Information Labs, EURid, Emily Taylor Consultancy and Abu-Ghazeleh Intellectual Property (2016), *Middle East and Adjoining Countries DNS Marketplace Study*, ICANN 2016, https://www.icann.org/en/system/files/files/meac-dns-study-26feb16-en.pdf (accessed 4 Oct. 2019); Oxford Information Labs, LACTLD, EURid and InterConnect Communications (2017), *Latin American and Caribbean DNS Marketplace Study*, ICANN, 13 March 2017, https://www.icann.org/en/system/files/files/lac-dns-marketplace-study-13mar17-en.pdf (accessed 4 Oct. 2019).

[8] See, for example, InterConnect Communications (2012), *MC/111 Internet Protocol Version 6 Deployment Study*, Ofcom, https://www.ofcom.org.uk/__data/assets/pdf_file/0028/55891/internet-protocol.pdf (accessed 4 Oct. 2019).

[9] See, for example, InterConnect Communications (2013), *MC/159 Report on the Implications of Carrier Grade Network Address Translators*, Ofcom, https://www.ofcom.org.uk/__data/assets/pdf_file/0020/37802/cgnat.pdf (accessed 4 Oct. 2019).

[10] Asia-Pacific Network Information Centre (APNIC) (n.d.), 'IPv6 Capable Rate by country (%)', https://stats.labs.apnic.net/ipv6 (accessed 4 Oct. 2019).

The changing nature of internet governance and strategic risks

O'Hara and Hall's 'Four Internets' paper, describes four competing visions for the future of internet governance: the 'open internet' favoured by the US; the 'bourgeois' internet of the EU 'where trolling and bad behavior are minimized and privacy protected, possibly at the cost of innovation'; China's 'authoritarian' model; and the 'spoiler' internet for states such as Russia and North Korea, which exploit its open standards for strategic gain.[11] All four approaches have differences that could characterize the future shape of the internet, or even fragment it. However, there are greater commonalities between the EU and US versus Chinese and Russian approaches – accentuating a potential East–West divide.

> As the field of internet governance necessarily evolves to meet the challenges of technological and societal change, ideological fault lines between the EU and US are likely to emerge.

The relevance of the four internets model to this paper is that while internet naming and addressing (the traditional core of internet governance) have not to date posed major ideological differences between the EU and US, continued agreement cannot be taken for granted. As the field of internet governance necessarily evolves to meet the challenges of technological and societal change, ideological fault lines between the EU and US are likely to emerge. The future of a free, open internet in which human rights and the rule of law are respected is not guaranteed.[12] There is a strategic imperative for the EU and US to emphasize areas of common ground in order to prevail against the emergence of an internet whose fundamental values differ from those upon which the network was founded. It is, therefore, important for the EU and US to work together to encourage participation of moderate, like-minded stakeholders in internet governance processes. The authors recommend that the EU Delegation seek to establish a taskforce for this purpose.

The term multi-stakeholder has become ubiquitous when discussing internet governance processes over the past 20 years, particularly those originating from the US. What does multi-stakeholder mean, and why has it become a charged term in the context of the four competing visions for the future of internet governance?

What does multi-stakeholder mean?

The term 'multi-stakeholder' was first coined in the 1990s as a way of extending the types of actors involved in policy and corporate decision-making. The starting point is a 'complex, controversial issue on an international scale',[13] not unlike climate change.

[11] O'Hara, K. and Hall, W. (2018), *Four Internets: The Geopolitics of Digital Governance*, CIGI Papers No. 206, December 2018, https://www.cigionline.org/publications/four-internets-geopolitics-digital-governance (accessed 4 Oct. 2019).

[12] Ibid.; Global Commission on Internet Governance (2016), 'One Internet', https://www.cigionline.org/sites/default/files/gcig_final_report_-_with_cover.pdf (accessed 15 Oct. 2019); Hoffmann, S., Bradshaw, S., and Taylor, E. (forthcoming 2019), 'Networks and geopolitics: how great power rivalries infected 5G', CIGI.

[13] Hofmann, J. (2016), 'Multi-stakeholderism in Internet governance: putting a fiction into practice', *Journal of Cyber Policy*, 1(1), pp. 29–49, https://doi.org/10.1080/23738871.2016.1158303.

In theory, multi-stakeholder governance decentralizes and democratizes decision-making. In internet policy, it is usually associated with 'bottom-up', 'rough consensus' policies developed by all stakeholders on an equal footing. For the majority of Western commentators this is viewed as the appropriate model for governing the internet,[14] on the basis that involving diverse stakeholders leads to better policy outcomes.[15] Multi-stakeholder is viewed as an alternative approach to intergovernmental, multilateral processes (typified by the International Telecommunication Union (ITU) and favoured by authoritarian regimes such as Russia, China and Iran). In this sense both have become charged expressions that import their advocates' contrasting visions for the future of the internet – divided along the East–West or 'four internets' axis.

ICANN is above all the poster child of multi-stakeholder internet governance. Unfortunately, gaps between theory and ICANN's practice threaten to become a strategic risk for both the EU and US visions for the future of internet governance. As practised within ICANN, multi-stakeholder governance gives equivalency to all voices, no matter how radical or self-interested, and there are underdeveloped mechanisms for breaking a deadlock or asserting the public interest.

The role of governments remains a contentious point, illustrating that, behind EU and US support for multi-stakeholder governance, there may not be a consistent, shared understanding of what 'multi-stakeholder' actually means. The structure of ICANN illustrates how these divergent views can impede closer cooperation in practice.

From ICANN's inception in 1998, it was intended by the US government that the 'private sector… take leadership for domain name system (DNS) management'.[16] A foundational principle for ICANN – and what marks it out as different from the multilateral ITU – is that it is not government-led. This was originally articulated as 'private-sector led'[17] and, following the conclusion of the World Summit on the Information Society 2003–2015 (WSIS), morphed into 'a bottom-up consensus-based multi-stakeholder process'.[18] The ICANN structure has two types of stakeholder groups: the 'supporting organizations' – the Generic Names Supporting Organization (GNSO), the Address Supporting Organization (ASO) and the country code Names Supporting Organization (ccNSO) – which are focused on making policy for domain names and IP addresses; and the 'advisory committees' – the Governmental Advisory Committee (GAC), the Security and Stability Advisory Committee (SSAC), the Root Server System Advisory Committee (RSSAC), and the At Large Advisory Committee (ALAC) – which provide advice to the ICANN board. The

[14] For example, OECD (2014), 'Principles for Internet Policy Making', http://www.oecd.org/internet/ieconomy/oecd-principles-for-internet-policy-making.pdf (accessed 15 Oct. 2019); Global Commission on Internet Governance (2016), 'One Internet'.

[15] Wentworth, S. (2017), 'Internet multi-stakeholder governance', *Journal of Cyber Policy*, 2(3), pp. 318–322, https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1400574 (accessed 15 Oct. 2019).

[16] United States Department of Commerce (1998), 'White Paper on the Management of Internet Names and Addresses', https://www.icann.org/resources/unthemed-pages/white-paper-2012-02-25-en (accessed 4 Oct. 2019).

[17] National Telecommunications and Information Administration (NTIA) (1998), 'Statement of Policy on the Management of Internet Names and Addresses, https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses (accessed 4 Oct. 2019).

[18] The term 'multi-stakeholder' first appeared in ICANN's bylaws in October 2016, following extensive revisions associated with the IANA transition. At the time of the WSIS, ICANN's core values included 'While remaining rooted in the private sector'; compare ICANN (2005), 'Bylaws for Internet Corporation for Assigned Names and Numbers', https://www.icann.org/resources/pages/bylaws-2005-04-08-en (accessed 4 Oct. 2019); and ICANN (2016), 'Bylaws for Internet Corporation for Assigned Names and Numbers', https://www.icann.org/resources/pages/bylaws-2016-09-30-en (accessed 4 Oct. 2019).

advice of governments and other advisory committees is not binding on the ICANN directors, but over time the bylaws have strengthened the board's obligations to provide reasons for not following GAC advice.[19]

Throughout ICANN's numerous transitional periods, the US government has increasingly tried to stay at arms-length from ICANN to ensure its independence from government oversight. A respected advisory committee role within the community and acknowledgment of government's role in internet governance suited this aim. Additionally, the US is traditionally a free market-driven economy with a light regulatory touch and decentralized governance, which is both an alternative structure compared to the EU and provides private industry a strong position in internet governance. With respect to multi-stakeholderism, the US vocally supports inclusion of all stakeholders, such as academia and civil society, but the US style of multi-stakeholderism can seem from the outside to be market-led.[20]

> The US is traditionally a free market-driven economy with a light regulatory touch and decentralized governance, which is both an alternative structure compared to the EU and provides private industry a strong position in internet governance.

European policymakers would likely have set up ICANN in a different manner, for example, possibly including more accountability to the public to counterbalance corporate interests.[21] To European policymakers, and representatives of other governments (especially authoritarian governments such as China, which would favour a multilateral solution to internet governance[22]), it is conceptually troubling to have sovereign states in a capacity that may be perceived as lesser than or secondary to the directors of a private corporation. In reality, the board's powers to reject the policy recommendations of supporting organizations have always been limited.[23]

However, differences in status of the various stakeholder groups and advisory committees within ICANN are, for the most part, more problematic in concept than in practice. Over time, the powers and influence of 'advisory committees' has grown (for example, the SSAC is one of the most influential organs of the ICANN community), and successive changes to the bylaws have gradually strengthened the role of governments within ICANN.

[19] Compare Section 3(a) of the original 1998 bylaws, which requires the board to 'consider' government advice, to the most recent bylaws (section 12.2(a)(x)), which adopt a 'comply or explain' formula, and sets a minimum threshold of 60 per cent vote of the board to reject GAC consensus advice, ICANN (1998), 'Bylaws for Internet Corporation for Assigned Names and Numbers, https://www.icann.org/resources/unthemed-pages/bylaws-1998-11-23-en (accessed 4 Oct. 2019); and ICANN (2018), 'Bylaws for Internet Corporation for Assigned Names and Numbers', https://www.icann.org/resources/pages/governance/bylaws-en (accessed 4 Oct. 2019).

[20] O'Hara and Hall (2018), *Four Internets: The Geopolitics of Digital Governance*; Global Commission on Internet Governance (2016), 'One Internet'.

[21] Anonymous interviews for this paper, November 2018; O'Hara and Hall (2018), *Four Internets: The Geopolitics of Digital Governance*

[22] Ibid.

[23] See, for example, ICANN's original bylaws, section 1(c) 'The Board shall accept the recommendations of a Supporting Organization if the Board finds that the recommended action, policy or procedure (1) complies with the Articles and Bylaws, (2) was arrived at through fair and open processes (including permitting participation by representatives of other Supporting Organizations if requested), (3) is not reasonably opposed by any of the other Supporting Organizations, and (4) furthers the purposes of, and is in the best interest of, the Corporation', ICANN (1998), 'Bylaws for Internet Corporation for Assigned Names and Numbers, https://www.icann.org/resources/unthemed-pages/bylaws-1998-11-06-en#VI (accessed 15 Oct. 2019).

A more practical way of thinking about multi-stakeholder processes is to adopt a flexible, results-orientated approach, driven by considerations of required expertise, which caters to those who are currently not being heard.[24]

What are the key internet governance institutions?

An exhaustive review of the institutions involved in internet governance is outside the scope of this paper. Table 1 summarizes the characteristics of key institutions active in the internet governance landscape. There are others, such as technical standards bodies, the regional and national domain name registries, registrars, and the organizations that manage the distribution of IP addresses. The intention is to focus on areas of interest and possible influence for the EU Delegation.

Table 1 shows the institution's characteristics, openness (how easy it is for stakeholder groups to participate), what the forum's decision-making process is (if there is one), whether government plays a formal role, primary participating stakeholders, the oversight body or convener of the forum, and the type of formal and informal outputs by the forum.

Table 1: Internet governance forums

Characteristics	IGF	National/Regional IGF (NRIs)	IETF	ITU	UN GGE
Openness[25]	Open	Open	Open	Closed	Closed
Decision-making process	n/a	n/a	Rough consensus	Consensus among member states	Consensus within the group
Formal government role	No	No	No	Yes	Yes
Participation[26]	• Civil Society • Gov't • Academia • Industry	• Civil Society • Gov't • Academia • Industry	• Industry • Civil Society • Academia • Gov't	• Gov't • Industry • Academia (very minor)	• Gov't
Oversight/ Convener	UN	National & regional bodies	Internet Society (ISOC)	Members (states, industry, some academia)	UN
Outputs	• Multi-stakeholder dialogue • Published Proceedings	• Multi-stakeholder dialogue • Reports published by the IGF	• Technical specifications	• Development aid • Radio standards • Telecoms standards	• Report published by the UN

Source: Compiled by the authors.

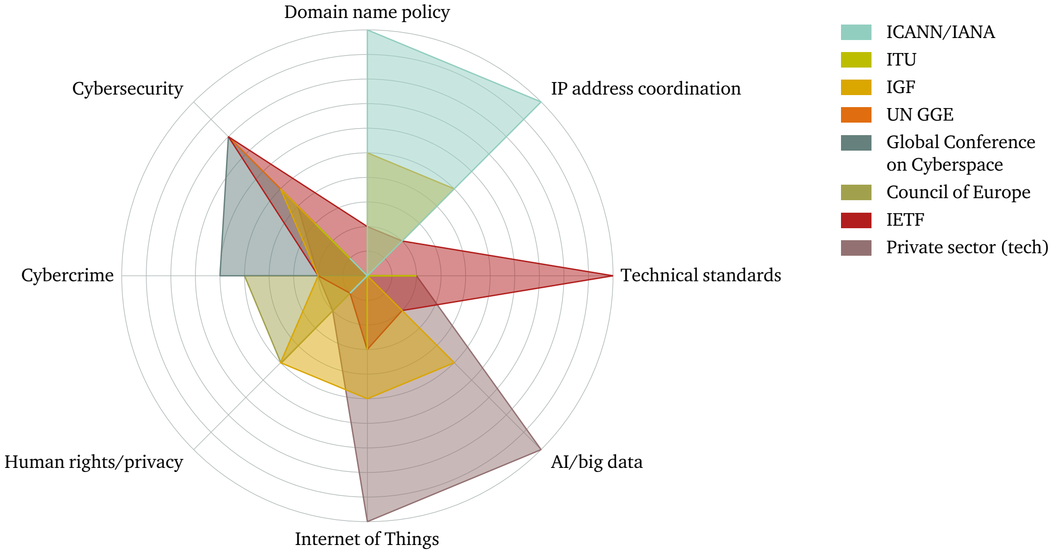
[24] Wentworth, S. (2017), 'Internet multi-stakeholder governance'.

[25] Openness is assessed on the ease with which stakeholders can engage meaningfully in the forum. This may include attendance, ability to observe processes, participation in discussions and output creation, participation in decision-making processes, access to meeting notes or summaries, financial barriers to participation, etc.

[26] Multi-stakeholders were divided into four groups (government, academia, civil society, and industry). Other groups, such as technical experts, could be included in any of these four groups. The order of the groups is intended to describe the relative importance of that group to the forum but is not definitive.

To identify potential gaps in the thematic coverage of internet governance institutions, Figure 2 summarizes the institutions involved in the internet governance space and their areas of activity. The numbers assigned for each activity are an estimate of the intensity of each institution's involvement in different areas. The analysis focuses on international processes and omits several institutions, which play important roles in shaping policy and standards at the national or regional levels, such as courts, sector regulation and laws, regional internet registries, and national and regional standards bodies such as the US National Institute for Science and Technology (NIST) and the European Technical Standards Institute (ETSI).

Figure 2: The internet governance radar



Source: Compiled by the authors.
Note: The intensity of activity and selection of organizations reflect the authors' view and may not reflect the views of the relevant institutions or processes.

Viewed through a thematic lens, the analysis reveals gaps in the international coordination of policy issues that have a major societal impact. For example, much of the policy on AI and big data is being handled de facto by a small number of private platforms as part of product development. Likewise, the IoT lacks an international policy space and key aspects of the technical standards are also occurring within technical companies or opaquely through the ITU.

Environmental analysis (far environment)

The far environment

To analyse drivers in the far environment, which may affect the EU–US relationship, this paper uses the familiar 'PEST' environmental scanning framework to review Political, Economic, Sociological and Technological factors relevant to internet governance. This analysis does not attempt to be exhaustive. Instead, the tool is used to give a high-level view of the drivers of change in the far environment that are likely to have an impact on internet governance processes.

Political

- China's rise as a global superpower and its increasing influence in intergovernmental organizations such as the UN;
- Resurgence of Russia and the 'Axis of Incivility';[27]
- 'Swing states' (e.g. in the Gulf and in Africa) attracted by authoritarian and state-control solutions for communications technology;
- Loss of influence (US);
- Isolationist policies pursued by the current US administration are straining international cooperation;[28] and
- Loss of confidence in democratic processes in liberal democracies and the rise of populism.

These drivers may undermine international support for multi-stakeholder internet governance, which is characterized by its critics as being favoured and dominated by US interests.

Economic

- Increased influence and coordination of the rest of the world, notably by China and Russia, whose visions for internet governance are incompatible with those of the EU and US;
- China and Russia are now competing in terms of investment and know-how with the US, in ways that were inconceivable a short time ago;
- Russia's new 'sovereign internet' law and reported ability to 'disconnect' from the global internet';[29]
- China has developed home-grown internet and technology giants (such as Alibaba and Huawei) that are competing internationally;[30] and
- China's Belt and Road Initiative, which so far spans 70 countries[31] and aims to support technical infrastructure development in sub-Saharan Africa for decades.[32]

[27] O'Hara and Hall (2018), 'Four Internets: The Geopolitics of Digital Governance'.

[28] Volcovici, V. (2017), 'U.S. submits formal notice of withdrawal from Paris climate pact', Reuters, 4 August 2017, https://www.reuters.com/article/us-un-climate-usa-paris/u-s-submits-formal-notice-of-withdrawal-from-paris-climate-pact-idUSKBN1AK2FM (accessed 16 Oct. 2019); BBC News (2018), 'EU tariffs on US goods come into force', https://www.bbc.co.uk/news/business-44567636 (accessed 16 Oct. 2019); Lockie, A. (2018), 'Trump torches allies, threatens NATO pullout after tense WWI memorial trip to Paris', Business Insider, http://uk.businessinsider.com/trump-slams-allies-threatens-nato-pullout-after-wwi-paris-trip-2018-11?r=US&IR=T (accessed 16 Oct. 2019).

[29] Jee, C. (2019), 'Russia wants to cut itself off from the global internet. Here's what that really means', *MIT Technology Review*, 21 Mar 2019, https://www.technologyreview.com/s/613138/russia-wants-to-cut-itself-off-from-the-global-internet-heres-what-that-really-means/ (accessed 4 Oct. 2019).

[30] See, for example, Mourdoukoutas, P. (2017), 'Alibaba beats Amazon', *Forbes*, 22 August 2017, https://www.forbes.com/sites/panosmourdoukoutas/2017/08/22/alibaba-beats-amazon/#488706773f97 (accessed 16 Oct. 2019).

[31] Hillman, J. E. (2018), 'China's Belt and Road Initiative: Five Years Later', Center for Strategic and International Studies, https://www.csis.org/analysis/chinas-belt-and-road-initiative-five-years-later-0 (accessed 4 Oct. 2019).

[32] See, for example, World Bank (2008), 'Building Bridges', https://siteresources.worldbank.org/INTAFRICA/Resources/Building_Bridges_Master_Version_wo-Embg_with_cover.pdf (accessed 16 Oct. 2019); The Infrastructure Consortium for Africa (2015), 'Africa's ICT sector and China', https://www.icafrica.org/en/topics-programmes/ict/africa%E2%80%99s-ict-sector-and-china/ (accessed 16 Oct. 2019).

The impact on internet governance is seen through the growth in support from 'swing states' (states that are undecided on the future direction of internet governance) for the ITU, a government-led standardization body, to have a role in internet governance – an approach favoured by authoritarian states such as China.

Sociological

- The future of work,[33] combined with ageing[34] and declining populations in the developed world,[35] will result in decreasing tax revenues;
- While several emerging economies (e.g. China, Russia and Brazil) have below replacement-level fertility, India and many African countries have large youth populations;[36] and
- Decisions over how new technologies like 5G and protocols like DoH are adopted at the national and regional levels are likely to deepen the digital divides, as are the handling of other policy issues such as data protection, surveillance, access to services, and the right to disconnect.

These factors will inhibit the ability of developed world governments (especially the US and EU) to effect change or sustain a multi-stakeholder vision for internet governance without the support of other stakeholders.

Technological

- Forces for a 'splinternet' are strengthening[37] – not only risking alternative DNS roots, but other technological splits (e.g. in 5G with a Chinese Huawei internet vs a Western internet);
- The future of the internet will not be web- or email-based; and
- China has emerged as a global leader in technology development and deployment. How far will Chinese technologies embed an alternative, authoritarian, approach to governance, human rights (e.g. privacy), and surveillance.

With the roll-out of smart cities, the IoT and advances in artificial intelligence, governing tomorrow's internet will be more complex than coordinating domain names and IP addresses, and will involve politically, ethically and culturally challenging issues.

[33] World Development Report 2016 (2016), 'Digital Dividends', Figure O.17, p. 22 https://openknowledge.worldbank.org/bitstream/handle/10986/23347/9781464806711.pdf (accessed 16 Oct. 2019).

[34] World Population Prospects: the 2017 Revision indicates that the number of older persons aged 60 or over is expected to double by 2050 and to more than triple by 2100, United Nations (n.d.), 'Ageing', http://www.un.org/en/sections/issues-depth/ageing/ (accessed 16 Oct. 2019).

[35] See United Nations (2015), 'World Fertility Patterns 2015', p. 3, http://www.un.org/en/development/desa/population/publications/pdf/fertility/world-fertility-patterns-2015.pdf (accessed 4 Oct. 2019).

[36] See, for example, UN (2017), 'World Population Prospects, The 2017 Revision: Key Findings and Advance Tables', https://population.un.org/wpp/Publications/Files/WPP2017_KeyFindings.pdf (accessed 4 Oct. 2019).

[37] Global Commission on Internet Governance (2016), 'One Internet'.

3. How is the EU–US Relationship on Internet Governance Working?

Shared values and concerns

At a high level, the EU and US share core values in relation to the internet's development, particularly when contrasted with the ambitions of authoritarian and non-democratic regimes. There is significant goodwill and willingness to work together to promote an open and free internet.

With few exceptions, a non-interventionist, private-sector led, free market approach to internet governance has had support on both sides of the Atlantic. The US approach has remained relatively consistent and has sustained bipartisan support for the past 20 years. The main topic of contention and differing approaches has been in relation to the historical US government role in the development of the DNS root (the IANA). The George W. Bush administration announced during the WSIS process that it was unwilling to give up its control over the IANA;[38] the Obama administration triggered the process that led to the transition of the IANA to the ICANN community.[39] The IANA transition took place prior to the US presidential election in 2016. The current US administration has indicated hostility to the IANA transition[40] but has not attempted to reverse it so far.

The EU Council Conclusions on Internet Governance of 2014[41] provide positive examples of the common interests and values of the EU and US, including:

- An open, neutral environment in which freedom of expression and innovation can thrive, with an assumption that the network's distributed architecture would mitigate against concentrations of economic or political power.
- Support for multi-stakeholder solutions for governing the internet's core resources, including the transition of the IANA function to the global multi-stakeholder community.
- Support for the Internet Governance Forum.
- Avoiding fragmentation of the internet and strengthening cybersecurity within the context of a free and open internet.

[38] NTIA (2005), 'U.S. Principles on the Internet's Domain Name and Addressing System', https://www.ntia.doc.gov/other-publication/2005/us-principles-internets-domain-name-and-addressing-system (accessed 4 Oct. 2019).
[39] NTIA (2014), 'NTIA Announces Intent to Transition Key Internet Domain Name Functions', https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions (accessed 4 Oct. 2019).
[40] Masnick, M. (2016), 'Donald Trump Doubles Down On Ted Cruz's Blatantly Confused And Backwards Argument Over Internet Governance', *techdirt*, 22 September 2016, https://www.techdirt.com/articles/20160921/16292135589/donald-trump-doubles-down-ted-cruzs-blatantly-confused-backwards-argument-over-internet-governance.shtml (accessed 4 Oct. 2019).
[41] Council of the European Union (2014), 'Council conclusions on Internet Governance', http://italia2014.eu/media/3769/council-conclusions-on-internet-governance.pdf (accessed 4 Oct. 2019).

The EU and US share objectives and values in core issues relating to cybersecurity. These include the prevention of cybercrime, responsible state behaviour in cyberspace, improving the resilience of critical infrastructure to withstand cyberattacks, all within a robust human rights framework. When discussing issues relating to cybersecurity, the EU tends to focus on specific topical areas of concern, such as cybercrime, disinformation or data protection. The US, on the other hand tends to talk in terms of technical cybersecurity located further down the internet stack – closer to the networks and protocols as opposed to the applications and services – using language such as interoperability, resilience, standards and security. This may in part reflect differing regulatory approaches between the EU and US. Developing common language and terminology presents an opportunity for closer cooperation between the EU and US in promoting enhanced cybersecurity within a free and open internet.

Both the EU and US have shared, defensive interests in preventing the rise of China and its authoritarian vision for the future of internet governance, which threatens to undermine the future of the single, free and open internet.

Both the EU and US are active in improving cybersecurity at numerous levels, including efforts to promote greater cooperation through the G7,[42] strengthening the EU Agency for Cybersecurity (ENISA), implementing the Network Information Security (NIS) Directive, membership of the UN Group of Governmental Experts (GGE), engagement in national, regional, and industry-led standards bodies (e.g. NIST, ETSI and 3GPP), and opposing the ambitions of authoritarian states to implement a cybersecurity treaty.[43] In October 2018, a group of NATO allies coordinated a series of public statements denouncing Russian activities in cyberspace,[44] a show of strength and resolve by calling out irresponsible behaviour. One area where EU–US coordination on cybersecurity could be strengthened is the ICANN process, particularly as a number of forward-looking security initiatives are under way.

Furthermore, both the EU and US have shared, defensive interests in preventing the rise of China and its authoritarian vision for the future of internet governance, which threatens to undermine the future of the single, free and open internet. Both the EU and US have resisted calls for a UN ‘solution’ to internet governance.

While both the US and EU have struggled for resources since the global financial crisis, they also have strong institutions, a track record of rules-based governance, strong civil society organizations and – most important – the ideals and values on which both were founded.

[42] See, for example, G7 (2019), ‘Dinard declaration on the cyber norm initiative’, https://www.elysee.fr/admin/upload/default/0001/04/d37b5326306c7513b58c79d26938f678d95cb2ff.pdf (accessed 16 Oct. 2019).

[43] United Nations (2018), ‘First Committee Approves 27 Texts, Including 2 Proposing New Groups to Develop Rules for States on Responsible Cyberspace Conduct’, https://www.un.org/press/en/2018/gadis3619.doc.htm (accessed 16 Oct. 2019).

[44] Reals, T. (2018), ‘Netherlands says Russia tried cyberattack on global chemical weapons agency’, CBS News, 4 October 2018, https://www.cbsnews.com/news/russia-gru-cyberattack-operation-targeting-opcw-chemical-weapons-netherlands-2018-10-04/ (accessed 16 Oct. 2019).

Areas where the EU and US have worked effectively

The following section examines two case studies that illustrate examples of effective cooperation between the EU and US on internet governance issues. The examples are not intended to be exhaustive but illustrate activity across strategically important institutions and processes.

IANA transition

Shortly after the US National Telecommunications and Information Administration (NTIA) announced its intent to transition oversight of the IANA function to the global multi-stakeholder community, the EU Council endorsed the US decision. EU stakeholders, including the EU institutions, actively engaged in the two-year process within ICANN to define a multi-stakeholder future. Eventually, all segments of the ICANN community, including the GAC, unanimously endorsed the outcomes[45] of the Cross-Community Working Group (CWG). Europeans comprised the second largest group of the 155 members and participants of the CWG (26 per cent, compared with 23 per cent from North America, and 33 per cent from Asia).[46] European participants were drawn from multiple stakeholder groups and were among the most active attendees, including a European co-chair.[47]

The IANA transition showed that multi-stakeholder processes can be effective at solving complex problems quickly. The process also harnessed the capabilities of EU stakeholders (who tend to be most active in ccNSO and GAC, less so in GNSO) and brought them into cross-community working. However, the discussions were tightly scoped by the original NTIA announcement, which specifically tasked ICANN with finding a solution (rather than throwing the challenge open to the then imminent NETmundial meeting) and stipulated a multi-stakeholder outcome (thus vetoing an ITU solution).[48]

The European Dialogue on Internet Governance – an example of successful EU multi-stakeholderism

The European Dialogue on Internet Governance (EuroDIG) has become one of the most effective and best-known of the regional and national IGF projects. While EuroDIG is not particularly an example of successful EU–US coordination, it does demonstrate what can be achieved if the European institutions wholeheartedly participate in multi-stakeholder processes. European institutions have provided positive engagement and support for EuroDIG throughout its lifetime, which lends legitimacy and guarantees the participation of high-level speakers from all stakeholder groups

[45] ICANN (2015), 'Letter from Thomas Schneider to Lise Fuhr and Jonathan Robinson', Governmental Advisory Committee, https://community.icann.org/display/gnsocwgdtstwrdshp/GAC+Approval?preview=/53782164/54003923/GAC%20Letter%20to%20CWG%20re%20Final%20ProposalFinal.docx (accessed 4 Oct. 2019).
[46] ICANN (2016), 'CWG Statistics and Diversity', https://community.icann.org/pages/viewpage.action?pageId=49362655 (accessed 4 Oct. 2019).
[47] ICANN (2016), 'Attendance Log CWG-Stewards', https://community.icann.org/display/gnsocwgdtstwrdshp/Attendance+Log+CWG-Stewardship (accessed 4 Oct. 2019).
[48] NTIA (2014), 'NTIA Announces Intent to Transition Key Internet Domain Name Functions', 14 March 2014, https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions (accessed 4 Oct. 2019).

(including from the European Commission and parliamentarians). These institutions have helped to sustain momentum through their participation in the bottom-up programme planning process, without 'taking over' or undermining EuroDIG's distinctly multi-stakeholder character.

The European institutions have continued to support EuroDIG and the global IGF alongside other stakeholders, by contributing to the bottom-up programme planning process and being heavily involved in the event, for example by providing speakers both at EuroDIG[49] and the IGF (the commissioner spoke at the 2017 and 2018 IGFs), and a delegation of MEPs to the global IGF.[50]

Some stakeholders question the effectiveness of the IGF, as high-level government and industry participation decreases while civil society participation increases. Additionally, the IGF has always struggled to achieve sustainable funding and requires the host country to foot the bill of IGF meetings; the IGF has been held in Europe at least three years in a row, which shows a downturn of wider commitment and resources for the forum. It is also important to note that the internet governance landscape – in terms of quantity and variety of internet forums – is profoundly different to what it was in 2006 when the IGF was founded. Stakeholders now acknowledge that it is time to modernize the forum in order to keep it relevant.

At the time of writing, the IGF Multistakeholder Advisory Group (MAG) is taking stock of IGF 2018 and setting expectations for 2019 following an open consultation. This moment affords those who value the IGF's open, multi-stakeholder dialogue forum, such as the EU and US, opportunities to shape its future impact on internet governance. A joined-up European and American perspective and approach to updating the IGF to keep it current would provide a strong future vision for the forum that reflects shared values. Topics for cooperation include funding models, how the National and Regional Initiatives (NRIs) and wider-spectrum stakeholders interact with the international forum, identifying key focus areas, effectively attracting all relevant stakeholders to the table, and promoting wider international support (e.g. hosting).

Barriers to effectiveness

Despite a close alignment on the principles of multi-stakeholder internet governance, there are several factors that pose challenges to the effectiveness of EU–US cooperation on internet governance.

Different reasons to support multi-stakeholderism

Once discussions of the issues move beyond broad principles, differences of approach begin to emerge between the US and the EU. The following examples illustrate the EU and US's differing interpretations of what multi-stakeholder internet governance comprises.

[49] See EuroDIG (2018), 'Consolidated Programme 2018', https://eurodigwiki.org/wiki/Consolidated_programme_2018 (accessed 16 Oct. 2019).
[50] European Internet Forum (2018), '#EIFasks – Internet Governance Forum (IGF) preparatory meeting', https://www.internetforum.eu/news/365-igf-preparatory-meeting.html (accessed 16 Oct. 2019).

From the US perspective, there appears to be a genuine belief that multi-stakeholder processes are more effective and legitimate than the available alternatives for governing the internet. In the US, it is quite normal and natural for individuals to move between public and private sectors throughout their career,[51] subject to rules on conflict of interest. While the same may be true in Northern Europe, it is more unusual in Southern Europe, or even in the European Institutions. This relatively trivial example of a difference in approach can be interpreted as one of self-interest from an EU perspective, which may assume that the actions of US officials are at risk of being influenced by the hope of gaining a lucrative private-sector role after leaving office. This has strengthened suspicion by some in the EU that multi-stakeholder processes favour the interests of corporations or lobbyists.

The EU publicly supports multi-stakeholder internet governance,[52] and pays substantial financial contributions to the IGF, EuroDIG and the ICANN GAC secretariat. On 5 December 2018, a revised regulatory framework for the .eu top-level domain (TLD) was published. Changes to the framework bring it in line with international best practices on internet governance.[53] The new regulatory framework will create a multi-stakeholder council, which will have a limited scope of 'informing and advising the European Commission' rather than adopting a pure multi-stakeholder policymaking process.

> An EU perspective may assume that the actions of US officials are at risk of being influenced by the hope of gaining a lucrative private-sector role after leaving office. This has strengthened suspicion by some in the EU that multi-stakeholder processes favour the interests of corporations or lobbyists.

Internet governance gains from engagement with the diverse stakeholders that help to govern, provide and benefit from the global internet. Fostering participation of like-minded stakeholders in processes will result in better multi-stakeholder participation, and more robust internet governance.

Perceived lack of international influence/priority on IG (EU)

Interviewees for this paper all mentioned the high staff turnover at both the Commission and EU member state level on the internet governance portfolio. From the Commission's perspective, the staff turnover reflects the Commission's reorganization of responsibilities for internet governance bringing it closer to technical competence and line management. The Commission has also pushed through the .eu REFIT with the intention of opening up and modernizing internet governance policies across Europe.

[51] Examples of former government staff now working in the private sector include Asst Secretary of Commerce Lawrence Strickling; Amy Pope, former US deputy homeland security adviser; Ambassador David Gross, who led the US delegation to the UN during the WSIS; Julie Brill, former FTC Commissioner; Andrew McLaughlin who has held roles at ICANN, Tumblr, Google, and the White House.

[52] Council of the European Union (2014), 'Council conclusions on Internet Governance', http://italia2014.eu/media/3769/council-conclusions-on-internet-governance.pdf (accessed 4 Oct. 2019).

[53] See European Commission (2018), 'Why .eu top level domain', https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/doteu_infographic_20180419_6-page-001.jpg (accessed 17 Oct. 2019).

However, the steep learning curve for this technical, complex policy area means that it takes at least a year for a new participant to become effective. Since the successful transition of the IANA function from US government oversight in 2016, there has been a sense that the EU has afforded a lower priority to internet governance.[54] High staff turnover leads to a loss of continuity and institutional effectiveness and may contribute to a perception on the part of some stakeholders that internet governance is a low priority for the EU. Meanwhile, core staff at the US NTIA has remained consistent for the past 20 years. Whether the longevity of staff should be a source of concern or not, there is no doubt that at present (particularly within the introspective and conservative internet governance communities) US officials have more extensive experience and contacts, and that these contribute to greater institutional memory.

From some perspectives (including those interviewed for this paper), the practical impact, both at institutional and member-state level, is a difficulty in getting high-level input from the EU on internet governance issues. 'The EU bubble can be very self-absorbed, and it is difficult to get a Commissioner to pay attention to things that don't have obvious relevance to Commission priorities, such as the Digital Single Market'.[55] The institutional structures, and dividing lines between the roles and responsibilities of institutions versus member states, require so much coordination that the 'EU ends up with the lowest common denominator negotiating positions, which leave the Commission with no mandate to manoeuvre or be flexible'.[56] At the member-state level, officials are not adequately supported either, with the result that they depend on Brussels for guidance and expertise.

> High staff turnover leads to a loss of continuity and institutional effectiveness and may contribute to a perception on the part of some stakeholders that internet governance is a low priority for the EU.

Unlike the US and the Five Eyes, the EU does not engage in dedicated coordination across subject-matter boundaries. The US and Five Eyes bring together security professionals to discuss internet governance and sent representatives from their security communities to the ITU Plenipotentiary 2018, whereas EU attendees were mainly from trade or communications portfolios.

Outside the EU institutions, the participation of EU stakeholders in ICANN can be patchy, particularly in the GNSO. 'Even if you have the numbers, the ones who are active and vocal are Americans'.[57] Experience of trying to stimulate broader EU stakeholder participation in ICANN and IGF has also been disappointing, 'European chambers of commerce don't care'.[58]

These views are not shared from inside the Commission. The commissioner was at IGF Geneva and Paris, demonstrating a strong commitment to internet governance. The importance of internet governance is in her mission letter and has been stressed in several public statements (e.g. the EuroDIG message). Over the last two years the High Level group on Internet

[54] Author interviews, November 2018.
[55] Interviewee #3, November 2018.
[56] Interviewee #1, November 2018.
[57] Interviewee #3, November 2018.
[58] Interviewee #3, November 2018.

Governance (HLIG) process has been rejuvenated, with more frequent and rapid interactions and less committee-style meetings. The Commission more regularly coordinates in Council, as demonstrated by different EU lines, including NETmundial[59] or more recently of WHOIS.[60] From the EU institutional perspective, far from having no mandate to negotiate or be flexible, the Commission negotiates well within the GAC (e.g. on the WHOIS).

These differing perspectives reveal a communication gap, which if addressed could strengthen mutual trust and confidence between the EU and US. This could be particularly useful in addressing problematic issues or those that require a careful balance between stakeholder interests, such as WHOIS and GDPR.

Institutional weaknesses (ICANN/IGF)

ICANN's multi-stakeholder community has been criticized for lacking in transparency and accountability, being US-centric, having high costs of participation, and being unable to reach timely conclusions on well understood policy issues (such as WHOIS: privacy issues and lawful access to data).[61] For most stakeholders, there are low incentives to participate in long drawn-out policy processes, the outcomes of which have only tangential relevance to their lives or work.[62]

There are warnings since coming under the remit of the IANA, the ICANN community may not be robust enough to hold the board to account, as demonstrated by the board's suspension of one of the specific reviews (on security, stability and resiliency) mandated by the post-IANA transition settlement.[63] The ability of a single individual – the serving CEO – to flip the organization's direction and strategy (contrast Fadi Chehadé's expansionism, with Göran Marby's conservatism) is also a sign that internal planning processes, checks and balances may be weak.

The IGF was designed as a forum for dialogue, rather than a decision-making body, and was deliberately kept separate from the UN bureaucratic machinery,[64] as a consequence it has always struggled financially. While the IGF's mandate was extended for a further 10 years in 2015,[65] criticisms persist – it has not yet achieved the hoped-for policy influence and its MAG is sometimes criticized as inward-looking and self-absorbed.

[59] European Commission (2014), 'Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions: Internet Policy and Governance, Europe's role in shaping the future of Internet Governance', https://ec.europa.eu/digital-single-market/en/news/communication-internet-policy-and-governance (accessed 4 Oct. 2019).

[60] See Council of the European Union (2018), 'EU Lines to Take on WHOIS policy reform', http://data.consilium.europa.eu/doc/document/ST-13443-2018-INIT/en/pdf.

[61] Taylor, E. (2015), 'ICANN, Bridging the Trust Gap', Global Commission on Internet Governance, https://www.cigionline.org/sites/default/files/gcig_paper_no9.pdf (accessed 4 Oct. 2019).

[62] InterConnect Communications Ltd. (2013), *ATRT2 GNSO PDP Evaluation Study*, https://www.icann.org/en/system/files/files/gnso-evaluation-21nov13-en.pdf (accessed 4 Oct. 2019).

[63] ICANN (2017), 'Letter from Asst Secretary of Commerce Redl to Cherine Chalaby', https://www.icann.org/en/system/files/correspondence/redl-to-chalaby-12dec17-en.pdf (accessed 4 Oct. 2019).

[64] ITU (2005), *Tunis Agenda for the Information Society,* para 72, https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html (accessed 4 Oct. 2019).

[65] United Nations General Assembly (2016), 'UN General Assembly resolution 70/125', para 63, http://workspace.unpan.org/sites/Internet/Documents/UNPAN96078.pdf (accessed 4 Oct. 2019).

The role of civil society

Both the US and EU approaches to multi-stakeholder internet governance lack consistent, constructive engagement with civil society. Where there is engagement with non-governmental stakeholders, industry is often viewed as a more natural partner. This is a missed opportunity. ICANN may not be the most productive environment in which to build such dialogue, due to the narrow range of issues and entrenched positioning from some civil society actors. However, there are civil society organizations that are more practical and willing to have a dialogue with governments and industry, for example, Article 19 and Access Now (including the #keepiton initiative to prevent internet shutdowns), which are both active in the standards and technology environment, including the ITU.

Complexity of the internet governance space

The internet governance space is becoming more confusing and complex as the definition of internet governance broadens and issues emerge that require urgent international coordination. For example, a perception that there was insufficient international attention on cybersecurity led to the creation of the Global Conference on Cyberspace (GCCS) in 2011 – drawing on the same small pool of global internet governance participants. Although designed as a forum for multi-stakeholder dialogue, only 5 per cent of participants at the 2017 GCCS meeting came from academia and civil society.[66]

The Internet Governance Forum 2018 was scheduled at the same time as the ITU Plenipotentiary. Both meetings are held under the UN umbrella, and there is a high degree of overlap in attendees – particularly from governments and the technology sector – so the scheduling conflict syphoned off already stretched government resources.

Cases highlighting tensions or failures in coordination

EU General Data Protection Regulation and WHOIS

The General Data Protection Regulation 2016 (GDPR), its long-arm jurisdiction, and its impact on WHOIS have exposed divisions between the EU and US.[67] Domain name registration data, available through the public WHOIS service, has been widely relied upon by law enforcement and intellectual property owners to investigate and combat online crime and abuse. Despite the EU raising concerns and written advice relating to privacy aspects of WHOIS over a 14-year period,[68] the US and the ICANN community failed to predict and prepare for the impact of GDPR on WHOIS, or to safeguard legitimate third-party interests.

[66] Kaspar, L. (2017), 'GCCS 2017: a cyberspace free, open and secure (but mostly secure)', *Global Partners Digital*, 29 November 2017, https://www.gp-digital.org/gccs2017-a-cyberspace-free-open-and-secure-but-mostly-secure/ (accessed 4 Oct. 2019).

[67] O'Hara and Hall (2018), *Four Internets: The Geopolitics of Digital Governance*.

[68] ICANN (2007), 'Article 29 Working Party to ICANN' https://www.icann.org/en/system/files/files/schaar-to-cerf-12mar07-en.pdf (accessed 4 Oct. 2019).

Alarmed by the GDPR's turnover-based fines, ICANN's board imposed a Temporary Specification on gTLD Registration Data,[69] which according to ICANN rules was required to expire on 25 May 2019. ICANN then set up an Expedited Policy Development Process (EPDP), tasked with crafting a permanent policy and defining access to WHOIS data.[70] The EPDP completed its first phase in February 2019 and the ICANN community approved its work by establishing an Interim Registration Data Policy for gTLDs.[71] The Interim Registration policy continues with the approach taken in the Temporary Specification and will remain in place until the EPDP has completed the second phase of its work. The Temporary Specification provides an overly conservative interpretation of GDPR by redacting key registration data, not just for natural persons, but for legal persons as well. The public WHOIS lost registrant names, addresses, email addresses and phone and fax numbers as a result of GDPR.[72] This was not the result that the EU had pushed for.

In contrast, the European ccTLDs, including .eu, have worked successfully with European data protection authorities over a period of 20 years, to retain key aspects of the WHOIS output while also respecting individual rights to privacy.

> WHOIS could become a trade issue between the EU and US if a workable solution that safeguards law enforcement access to data cannot be found.

The positions of the EU and US have evolved since the issue first came to light. The stakes are high. WHOIS could become a trade issue between the EU and US if a workable solution that safeguards law enforcement access to data cannot be found,[73] and the EU may find itself blamed if its long-arm law (GDPR) results in the loss of tools for law enforcement.[74] Initially, both the EU and US were defensive and staunch in their positions; now there is constructive dialogue aimed at resolving the issue. A Commission official is a member of the EPDP team, and the EU, US and ICANN are reported[75] to be working effectively together to try to reach a workable outcome.

Improving cybersecurity within ICANN

Despite 'security and stability' being at the heart of ICANN's mission, cybersecurity has played a relatively minor role in discussions in the ICANN community. Two processes – the second Security and Stability Review Team Review (SSR2) and the Security and Stability Advisory Committee (SSAC) – deserve greater attention.

[69] ICANN (2018), 'Temporary Specification on gTLD Registration Data', https://www.icann.org/resources/pages/gtld-registration-data-specs-en (accessed 4 Oct. 2019).

[70] ICANN (2018), 'EPDP Charter', https://gnso.icann.org/sites/default/files/file/field-file-attach/temp-spec-gtld-rd-epdp-19jul18-en.pdf (accessed 4 Oct. 2019).

[71] ICANN (2018), 'Interim Registration Data Policy for gTLDs', https://www.icann.org/resources/pages/interim-registration-data-policy-en (accessed 4 Oct. 2019).

[72] For more on the EPDP see Taylor, E. (2018), 'Why the public directory of domain names is about to vanish', Chatham House Expert Comment, 18 October 2018, https://www.chathamhouse.org/expert/comment/why-public-directory-domain-names-about-vanish (accessed 4 Oct. 2019).

[73] Ross, W. (2018), 'EU data privacy laws are likely to create barriers to trade', *Financial Times*, 30 May 2018, https://www.ft.com/content/9d261f44-6255-11e8-bdd1-cc0534df682c (accessed 4 Oct. 2019).

[74] Interviewee #3, November 2019.

[75] Interviewees #1, #3, #4, November 2019.

SSR2

Key discussions on the security, stability and resilience of the DNS are currently taking place in the ICANN SSR2 review,[76] one of the specific reviews on which the IANA transition was contingent.[77] In a surprise move, the ICANN Board – the target of the independent review – suspended the SSR2 in October 2017 for a period of more than six months, for reasons which were not fully articulated. While Assistant Secretary David Redl placed on record the US concerns regarding the board's action,[78] reactions from the EU and the ICANN community were limited. There are three representatives from Europe currently on the SSR2 team[79] (none from China), and the group's fact-finding work continues. However, the suspension of a key review raises questions about ICANN's accountability and commitment to cybersecurity.

SSAC

Within ICANN, the Security and Stability Advisory Committee (SSAC) is a key venue for discussions regarding cybersecurity. SSAC is a highly influential body within the ICANN ecosystem. SSAC's advisory notes have been used by the ICANN board as the basis to make controversial decisions.[80] The key actors participating in ICANN's SSAC are from the US and Europe. Although the CEO of CNNIC (the Chinese ccTLD registry) is a member of SSAC.[81] Unlike other ICANN bodies, membership of the SSAC is by invitation only, and many of its discussions take place behind closed doors. A recent independent review of SSAC recommended that the group take a more active role within the ICANN community, so that security concerns can be raised at an early stage.[82]

[76] ICANN (2019), 'SSR2 Review', https://community.icann.org/display/SSR/SSR2+Review (accessed 4 Oct. 2019).

[77] ICANN (2018), 'Article 4.6(c), ICANN Bylaws 2018', https://www.icann.org/resources/pages/governance/bylaws-en/#article4.6 (accessed 4 Oct. 2019).

[78] ICANN (2017), 'Letter from Asst Secretary of Commerce Redl to Cherine Chalaby'.

[79] Žarko Kecić, Boban Krsic and Laurin Weissinger. For a full list of members: https://community.icann.org/display/SSR/Composition+of+Review+Team.

[80] See Hershkop, S. et al. (2018), *Independent Review of the ICANN Security and Stability Advisory Committee: Draft Final Report*, pp. 43–45, https://www.icann.org/en/system/files/files/ssac-independent-review-draft-final-15oct18-en.pdf (accessed 4 Oct. 2019).

[81] ICANN (2013), 'Appointment of Xiaodong Lee and Carlos Martinez to the SSAC', https://www.icann.org/en/system/files/bm/briefing-materials-2-23oct13-en.pdf (accessed 4 Oct. 2019).

[82] Hershkop, S. et al. (2018), *Independent Review of the ICANN Security and Stability Advisory Committee: Draft Final Report*.

4. Looking Ahead: The Future of Internet Governance

The nature of discussion on internet governance has shifted over the years. ICANN is no longer central to internet governance conversations, and future issues may not involve ICANN. Diverse players are involved in internet governance relating to cybersecurity, IoT, AI, big data, search markets, social media, mobile operators and human rights. The landscape is more complex and more structurally difficult. There is no single venue in which to explore issues relating to internet governance writ large.[83]

China with its ambitions to become a technological superpower has been active within the UN more broadly[84] and the ITU specifically to shape technical standards, which would support its authoritarian vision for internet governance. An example of this is the Chinese-led work related to IMT-2020 (International Mobile Telecommunications 2020), the ITU's version of 5G technology, such as machine learning and edge computing. Russia is also using the ITU to advance its own technological vision, a prime example being the Digital Object Architecture (DOA) that could support Russia's 'sovereign internet' aims and, if adopted, could destroy the internet as we know it.[85] More recently, a group of countries tried unsuccessfully to pass a resolution at the ITU Plenipotentiary Conference 2018 in Dubai to task an intergovernmental institution to start developing policy and regulatory guidelines for AI. The same week in New York, the UN First Committee put forward two conflicting resolutions on responsible state behaviour in cyberspace, one was the Open Ended Working Group proposed by Russia the other was proposed by the US and like-minded countries to reinstate the GGE; both are going ahead. These developments are a warning sign that a multi-stakeholder future for internet governance is not inevitable.

If EU and US governments do not start coordinating with a positive, multi-stakeholder vision and effective processes for future internet governance challenges, the governance of future communications technologies could drift towards authoritarian regimes, such as China, or an unaccountable private sector. Neither would be a good outcome. EU–US coordination can take place at the national or regional levels, or in groups of like-minded countries.

[83] Interviewee #2, November 2019.
[84] Okano-Heijmans, M. and van der Putten, F-P. (2018), 'A United Nations with Chinese characteristics?', *Clingendael*, https://www.clingendael.org/sites/default/files/2018-12/China_in_the_UN_1.pdf (accessed 4 Oct. 2019).
[85] For a critique of DOA, see Internet Society (2016), 'Overview of the Digital Object Architecture (DOA)', https://www.internetsociety.org/resources/doc/2016/overview-of-the-digital-object-architecture-doa/.

5. Conclusion

A multi-stakeholder future for internet governance is not guaranteed.[86] Authoritarian states such as China are patiently working through existing multilateral processes, capitalizing on the waning attention and resources of EU institutions, to undermine the open, free internet that Western countries have taken for granted. While the EU is unlikely to change the approaches of authoritarian regimes simply by engaging or investing more, the real risk is that by failing to engage, Western allies will be leaving the field to states that have a radically different vision of what the internet should be – and that a less free, or even fragmented internet will follow. By working together more effectively, with an emphasis on commonalities rather than differences, the EU and US can reduce risks of internet fragmentation, and aim to preserve a single, free and open internet.

As the meaning of internet governance expands beyond naming and addressing, it is essential that the EU and US build on positive foundations, learn lessons from failures in coordination, to enhance the effectiveness of existing multi-stakeholder processes, and proactively plan to ensure that future developments (AI, IoT, search markets, social media, mobile carriers, cybersecurity and responsible state behaviour in cyberspace) have multi-stakeholder homes.

[86] See extensive discussions on this issue in Global Commission on Internet Governance (2016), 'One Internet'.

6. Recommendations

> In times of difficulty, [the best way forward is to] find easy common ground and build on that. Post-transition, it is much easier to build on the common ground, i.e. that governments should not play a single determining role in internet governance.[87]

The following recommendations are directed to EU institutions in general as different bodies within the EU institutions lead on particular aspects of internet governance. However, the EU Delegation to the US is uniquely placed to work closely with US colleagues and EU institutions, to build consensus – particularly in relation to the sensitive issue of the proposed taskforce.

Build on common ground

1. Build capacity by encouraging the participation of moderate, European and likeminded stakeholders in internet governance.

This approach should improve the quality of decision-making by identifying what perspectives and voices are missing from current debates, and fill gaps on a case-by-case basis. Internally, the EU should ensure that its coordination on internet governance cuts across different functions and responsibilities (e.g. security, human rights, innovation, competition and the Digital Single Market) to raise awareness, build internal capacity and engagement. This will foster a higher level and more critical engagement with US counterparts.

2. Create, in partnership with like-minded stakeholders, a taskforce on effective, multi-stakeholder internet governance

The US and EU, in partnership with likeminded states, stakeholders and organizations should establish a taskforce that brings together a diverse group of stakeholders, who would eventually self-manage according to principles of inclusion, transparency and balance. The US and EU should be prepared to take a sustained, proactive role in shaping the taskforce's terms of reference, protecting against capture and fostering effective, collegial working methods. The taskforce at an early stage should establish meaningful dialogue with China about the future of internet governance.

The taskforce is not intended to compete with, or replace, existing processes, but to work within them to monitor their effectiveness, and identify policy gaps. To minimize suspicion, and secure buy-in from the notoriously prickly multi-stakeholder communities, the EU Delegation should

[87] Interviewee #2, November 2019.

seek to build consensus with US colleagues and key stakeholders on how best to move forward with this proposal. Possibilities for constructive beginnings to the project could:

- Start the conversations informally before making any public announcements.
- Work closely with existing institutions – the Internet Society for example may be a potential collaborator – and seek out influencers within the ICANN and IGF communities.
- Persuade like-minded community leaders – across all stakeholder groups – from those environments to chair and play proactive roles.
- The EU and US should be prepared to make commitments to participate proactively, and to provide co-funding in partnership with other stakeholders but should not be perceived as ‘owning' the process. Successful examples include the Global Commission on Internet Governance, which was established by Chatham House and CIGI, or the Global Commission on the Stability of Cyberspace, which is funded in part by the Dutch government, and has an independent secretariat comprising two think-tanks.[88]

The tasks ahead will have the following focus:

- Evolving the **principles and practices** of multi-stakeholder internet governance in consultation with all stakeholders and ensuring that it remains fit for purpose in the relevant forums.
- **Map cybersecurity policy development** in the US and EU jurisdictions to make sure they align or at least support the same values, to support the free flow of goods and services across borders.
- Publish an **annual scorecard** to monitor the effectiveness and accountability of multi-stakeholder governance across the institutions and processes active in internet governance, based on robust, meaningful key performance indicators. The taskforce can make comparisons between multi-stakeholder organizations and multilateral processes such as ITU. It is expected that the multi-stakeholder organizations will show better accountability, transparency and regular review.
- Identify emerging issues and gaps in the existing policy landscape, bringing together appropriate stakeholders to resolve complex, and contentious problems affecting the internet space.
- Engage in **capacity-building and training** to cultivate the active participation of individuals from across the range of stakeholder groups who are capable of adopting a wider viewpoint (as opposed to pursuit of short-term, narrow self-interest), which is compatible consensus-building within the multi-stakeholder model and the furtherance of shared EU–US values within the ICANN environment.

[88] Taylor, E. (2015), ‘ICANN, Bridging the Trust Gap', *Global Commission on Internet Governance,* https://www.cigionline.org/sites/default/files/gcig_paper_no9.pdf (accessed 4 Oct. 2019).

- Cultivate **cross-cutting dialogues** that bring together individuals and organizations working in disjointed silos (e.g. cybersecurity, internet governance, human rights, tech platforms).
- Establish **annual awards** that identify good practice, and recognize individuals' commitments to furthering inclusive, moderate, multi-stakeholder policies.

Immediate, targeted interventions for the EU institutions

3. Work through non-governmental, like-minded stakeholders to achieve stronger multi-stakeholder participation.

Engage in regular coordination of European (and like-minded) participants prior to key events (ICANN, IGF, EuroDIG). This could be started informally through calls, face-to-face meetings, or a social event at each meeting. Coordination would enable the Commission to understand the range of topics in which European participants are engaged – where gaps and opportunities for influence exist. Conducted in a sustained way, such coordination could embed a culture of working through non-governmental stakeholders to support the ICANN model.

4. Foster a balanced outcome on WHOIS and GDPR

In addition to the work the Commission does in ICANN via the EU GAC representative, it should contribute more proactively to the work of the EPDP on gTLD Registration Data primarily – but not exclusively – through the EU GAC representative on the team, and dialogue with European EPDP members. The Delegation of the European Union to the Council of Europe (EUDEL) may have the ability to coordinate closely with US counterparts on key topics and prior to meetings, and feed this information to relevant Commission offices and the Directorate-General for Justice and Consumers (DGJUST) and Directorate-General for Communications Networks, Content and Technology (DG CONNECT). Additionally, the Commission could coordinate a briefing or joint written advice from across law enforcement, business and data protection representatives (e.g. from DG Home, Justice, Connect and EDPB and possibly EUROPOL) to provide moderate implementation advice for the contracted parties, and make the point that GDPR sits within the general legal framework and supports the objectives of law enforcement, subject to necessity, proportionality and in accordance with the law.

5. Strengthen cybersecurity awareness and input throughout the ICANN process

The SSAC is an influential body within ICANN, which is struggling for capacity to proactively participate in community policymaking. The Commission should work with relevant stakeholders to strengthen SSAC's membership – helping to identify suitably qualified women, European and like-minded individuals (from any region) who have the requisite skills and who are capable of influencing a moderate, security conscious policy debate throughout ICANN.

Abbreviations and Acronyms

3GPP	3rd Generation Partnership Project
ALAC	At Large Advisory Committee to ICANN
ASO	Address Supporting Organization to ICANN
ccNSO	country code Name Supporting Organisation to ICANN
ccTLD	country code top-level domain, such as .eu, .uk, .de, .cn
CIGI	Center for International Governance Innovation
CNNIC	China Internet Network Information Center (the Chinese ccTLD registry)
CWG	Cross-community Working Group (an ICANN working group related to the IANA transition)
DNS	domain name system
DOA	Digital Object Architecture, an alternative vision for the internet's system of unique identifiers, designed by Bob Kahn (one of the inventors of a key internet protocol TCP/IP) and championed through the ITU.
DoH	DNS over HTTPS
ENISA	European Union Agency for Cybersecurity
EPDP	Expedited Policy Development Process, established by the ICANN community to resolve issues relating to the GDPR and WHOIS.
ETSI	European Telecommunications Standards Institute
EU	European Union
EuroDIG	European Dialogue on Internet Governance
GAC	Government Advisory Committee to ICANN
GCCS	Global Conference on Cyber Space
GDPR	General Data Protection Regulation, 2016
GGE	Group of Governmental Experts, established through the United Nations in 1999, under the auspices of UNIDIR (the United Nations Institute for Disarmament Research).
GNSO	Generic Names Supporting Organisation to ICANN
gTLD	generic top-level domain, such as .com, .net, .org and the 'new' gTLDs established in 2012 such as .xyz and others. ICANN provides policy coordination for gTLDs through the global multi-stakeholder ICANN community.
HLIG	High Level Group on Internet Governance
HTTPS	Hyper Text Transport Protocol Secure
IANA	Internet Assigned Numbers Authority, responsible for management of the DNS root database. Operated through ICANN in the post IANA transition arrangements.
ICANN	Internet Corporation for Assigned Names and Numbers, a California non-profit company established in 1998 for the global coordination of the internet's unique identifiers (naming and numbering).

IETF	Internet Engineering Task Force. A non-governmental, multi-stakeholder process responsible for establishing technical standards for the internet through consensus processes. Its outputs are called 'Requests for Comment' or RFCs.
IGF	Internet Governance Forum, a process for non-binding multi-stakeholder dialogue relating to internet governance, established by the United Nations through the Tunis Agenda 2005 (an outcome of the World Summit on the Information Society).
IMT-2020	International Mobile Telecommunications 2020
IP	Internet Protocol, the numbering system that identifies each device connected to the internet. Key protocols in use today are IP version 4 (IPv4) and IP version 6 (IPv6).
ITU	International Telecommunication Union, a multilateral UN agency established in 1865.
MAG	Multistakeholder Advisory Group to the Internet Governance Forum
MEP	Member of European Parliament
NIS Directive	the EU Network on security of network and information systems, 2016. To be transposed into member states national laws by 9 May 2018.
NIST	United National Institute of Standards and Technology
NRI	National and Regional Initiatives, establishing national and regional IGFs, such as EuroDIG for Europe, or the US IGF in the United States.
NTIA	National Telecommunications and Information Administration, a division of the United States Department of Commerce. Historically responsible for oversight of changes to the IANA database.
REFIT	the European Union's Regulatory Fitness Programme (described in the Commission Communication to the Parliament: Better Regulation for Better Results 2015[89]).
RSSAC	Root Server System Advisory Committee to ICANN
SSAC	Security and Stability Advisory Committee to ICANN
SSR2	second Security and Stability Review, one of the Specific Reviews established by section 4.6 of the ICANN Bylaws (as amended in relation to the IANA transition in 2016). The Specific Reviews are key instruments of ICANN's accountability to its community.
TLD	top-level domain (such as a ccTLD or gTLD), which form distinct namespaces within the DNS.
UN	United Nations
US	United States
WHOIS	tool used to find information on domain name registrants
WSIS	World Summit on Internet Society, 2003–2005

[89] European Commission (2015), 'The need for better regulation', https://ec.europa.eu/smart-regulation/better_regulation/documents/com_2015_215_en.pdf (accessed 4 Oct. 2019).

About the Authors

Emily Taylor is an associate fellow with the International Security Department at Chatham House and is the editor of the *Journal of Cyber Policy*. She is CEO of Oxford Information Labs. She is the author of several research papers and is a frequent panellist and moderator at conferences and events around the world. Previous roles have included chair of ICANN WHOIS Review Team, Internet Governance Forum Multistakeholder Advisory Group, Global Commission on Internet Governance research network, and director of Legal and Policy for Nominet. She has written for the *Guardian*, *Wired*, *Ars Technica*, the *New Statesman* and *Slate*, and has appeared on the BBC Now Show and the BBC Radio 4 'Long View'. Emily is a graduate of Cambridge University, qualified as a solicitor in England and Wales, and has an MBA from the Open University.

Stacie Hoffmann is an internet policy and cybersecurity consultant at Oxford Information Labs. Stacie is an experienced researcher, data analyst, writer, presenter and project manager, focusing primarily on the internet addressing (DNS) ecosystem, IoT, AI, Over-the-Top (OTT) services, and cybersecurity. Stacie is a CESG certified Cyber Security/Information Assurance Auditor Practitioner and holds a certificate in ISO/IEC 27001 Information Security Management Principles. In 2015, Stacie was an ICANN NextGen participant.

Acknowledgments

This publication has been produced with the assistance of the European Union. The contents of this publication are the sole responsibility of the authors, and can in no way be taken to reflect the views of the European Union.

Chatham House is part of a consortium, coordinated by B&S Europe, implementing the EU Policy & Outreach Partnership in the United States.

The authors would like to thank the anonymous interviewees who provided invaluable insights, the International Security Department at Chatham House and the Delegation of the European Union to the United States for their assistance in the writing of this paper, and the two anonymous peer reviewers for their comments on the draft. Remaining errors and omissions are the authors' own.

Independent thinking since 1920

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies build a sustainably secure, prosperous and just world.

Chatham House does not express opinions of its own. The opinions expressed in this publication are the responsibility of the author(s).

Cover image: Server room network cables in New York City, November 2014.

Photo credit: Copyright © Michael Bocchieri/Staff/Getty

ISBN 978 1 78413 377 1

This publication is printed on FSC-certified paper.

FSC

Typeset by Soapbox, www.soapbox.co.uk

The Royal Institute of International Affairs
Chatham House
10 St James’s Square, London SW1Y 4LE
T +44 (0)20 7957 5700 F +44 (0)20 7957 5710
contact@chathamhouse.org www.chathamhouse.org

Charity Registration Number: 208223