INTERNET POLICY REVIEW
Journal on internet regulation

Volume 6 | Issue 3

Accountability challenges confronting cyberspace governance

Jacqueline Eggenschwiler
Centre for Doctoral Training in Cyber Security, University of Oxford, United Kingdom

Published on 20 Sep 2017 | DOI: 10.14763/2017.3.712

Abstract: Traditional, linear conceptions of account rendering bear little relevance in the realm of cyberspace governance, where accountability structures are often decentred. Building on existing accountability scholarship, this paper identifies key accountability challenges confronting cyberspace governance, including the problem of many hands, the profusion of issue areas, as well as the hybridity and malleability of institutional arrangements, and presents a set of policy recommendations geared towards addressing the latter. This paper holds that in order to address and mitigate the challenges identified, accountability relationships need to be consciously reframed and discursively constructed.

Keywords: Cyber security, Governance, Policy challenges

Article information

Received: 25 Jan 2017 **Reviewed:** 04 Jun 2017 **Published:** 20 Sep 2017

Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/accountability-challenges-confronting-cyberspace-governance

Citation: Eggenschwiler, J. (2017). Accountability challenges confronting cyberspace governance. *Internet Policy Review*, *6*(3). https://doi.org/10.14763/2017.3.712

INTRODUCTION

What a little more than forty years ago started as a government-sponsored network research project has evolved into a "global [...] substrate that [...] underpins the world's critical socio-economic systems" (Demchak & Dombrowski, 2013, p. 29; Weber, 2013). Cyberspace has become a key domain of power execution and a core issue of global politics (Nye, 2010). Initially construed as a space free from regulation and intervention (Barlow, 1996; Johnson & Post, 1996), the rising tide of threats to the stability and future development of cyberspace has spurred calls for more expansive governance.

Over the course of the past two decades, the term governance has enjoyed widespread use across

a great number of discourses (Enderlein, Wälti, & Zürn, 2010). In the context of cyberspace, governance has come to refer to the sum of regulatory efforts put forward with regard to addressing and guiding the future development and evolution of cyberspace (Baldwin, Cave, & Lodge, 2010, p. 525). Cyberspace governance is characterised by a large quantity of actors, issue areas, and fora involved in processes of steering. Accountability structures are often incoherent in settings of this nature and questions such as who is accountable to whom for what by which standards and why remain opaque, and warrant closer examination (Bovens, Goodin, & Schillemans, 2014). For purposes of illustration, it is worth considering the following: while critically important to the workings of the digital realm, the activities of some of the largest cyberspace governance entities, including among others the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Governance Forum (IGF), or the Internet Engineering Taskforce (IETF) are not based on or mandated by international legal instruments. Furthermore, "there are no clear [or only few] existing structures such as courts, legislative committees, national auditors, ombudsmen, and so on, to which recourse can be made to render [these cyberspace governance institutions] accountable" (Black, 2008, p. 138).

Taking note of the complexities related to processes of account rendering in the context of cyberspace governance, this paper asks the following interrelated research questions:

- Conceptually, what are the key accountability challenges confronting cyberspace governance?
- How can these accountability challenges be addressed?

Attaining a better understanding of how accountability structures play out in cyberspace governance is key for increasing transparency, assessing processes of legitimisation, and scrutinising impending models of regulation.

This paper is structured along four sections: Section I reviews relevant background information and concepts, and lays out the methodology. Section II highlights key accountability challenges confronting cyberspace governance. Section III stipulates a set of policy recommendations geared towards addressing the accountability challenges identified as part of Section II. Section IV summarises the findings of this paper and offers some concluding remarks.

CONCEPTUAL FRAME AND METHODOLOGY

In order to grasp the accountability challenges confronting cyberspace governance, it is necessary to establish a common point of departure and lay out key concepts, i.e. cyberspace and accountability.

CYBERSPACE

Termed by William Gibson in the mid-1980s (Ottis & Lorents, 2010), cyberspace is the most elemental concept with regard to cyberspace governance (Kello, 2013, p. 17). It lays out the domain within which cyberspace governance can be construed. Even though cyberspace has become deeply embedded in everyday life, there is little clarity on what it comprises (Murray, 2007). The understanding of cyberspace is still nascent and the concept riddled with terminological ambiguity. The number of definitional accounts pertaining to cyberspace is bewilderingly large, ranging from technological to socio-political and economic descriptions (NATO Cooperative Cyber Defence Centre of Excellence, 2017).

Cyberspace is often equated with the World Wide Web but the two are not the same. Cyberspace can be thought of as a complex, highly distributed network infrastructure (Clarke & Knake,

2012). In contrast, the World Wide Web denotes a collection of resources (e.g. webpages) identifiable by means of global Uniform Resource Identifiers (URI), and accessible via cyberspace (World Wide Web Consortium, 2004).

The view of cyberspace adopted in this a paper is consistent with Chris Demchak's and Peter Dombrowski's understanding of cyberspace as a "global [...] substrate that [...] underpins the world's critical socio-economic systems" (Demchak & Dombrowski, 2013, p. 29). Their definition underscores the economic, social, and political importance of the network infrastructure, and alludes to the multitude of docking points for governance and policy interventions, as well as stakeholder concerns.

ACCOUNTABILITY

In terms of conceptual coherence, accountability struggles with similar definitional ambiguity to that of cyberspace. Over the past decade, accountability has become something of a catchword, and has been assigned various meanings by scholars of different disciplines, impairing consistent and comprehensive terminological application and research (Bovens et al., 2014). Although scholars seem to agree on the concept's overall importance, they appear to be less unified apropos its constitutive elements.

Consciously abstaining from advancing yet another definition or reconceptualisation of accountability, and increasing the term's elusiveness, this paper relies on what Bovens, Goodin and Schillemans call the minimal conceptual consensus:

"The minimal conceptual consensus entails, first of all, that accountability is about providing answers; is about answerability towards others with a legitimate claim to demand an account. Accountability is then a relational concept, linking those who owe an account and those to whom it is owed. Accountability is a relational concept in another sense as well, linking agents and others for whom they perform tasks or who are affected by the tasks they perform" (Bovens et al., 2014, p. 6).

Emphasising the concept's socio-relational core, i.e. the onus of an actor or body to give reasons for or defend conduct to another set of actors, the minimal definitional consensus is concise, yet broad enough to ascertain empirical validity and operationalisation in complex analytical environments, such as cyberspace governance (Bovens, 2007, p. 13).

Far from a coherent system, cyberspace governance resembles a jungle of different, at times competing, regulatory endeavours. Such endeavours can take many forms: they can be hierarchical with clear sanctions attached, e.g. legal rules and ordinances, international and national contracts and agreements, or softer, e.g. voluntary technical standards and protocols, and informal codes of conduct (Levi-Faur, 2011, p. xvi). In order to counter tendencies of disintegration and ensure continuous openness and stability of the digital environment, tangible accountability structures are of critical importance (Scholte, 2008, p. 15; Weber, 2014, p. 78).

METHODS

From a methodological point of view, this paper employs qualitative means of data collection and analysis. It is grounded in a review of policy documents and secondary academic literature on accountability, cyberspace governance, and international relations. Data was collected by means of online desk research. Databases queried included among others: Taylor & Francis Online, EBSCOhost, Elsevier Science Direct, Google Scholar, Google Books, as well as Search Oxford Libraries Online (SOLO). The sources identified were grouped and examined by means of content analysis.

Building on existing accountability scholarship and engaging in further theorisation, this paper serves as a steppingstone for thinking more rigorously about accountability in the context of cyberspace governance. Its goal is to contribute to current scholarly debates, and formulate relevant policy recommendations.

The findings of this paper are contextually and temporally specific and need to be understood as such. Much of the topic under investigation is still very much in flux. Conceptually, the governance of cyberspace is a field that is likely to remain under construction for the foreseeable future (Dutton & Peltu, 2007).

KEY CHALLENGES

Cyberspace governance involves a great number of different constituencies, spans across various issue areas, and exhibits a high degree of institutional malleability (Kleinwächter, 2011; Mueller, Mathiason, & Klein, 2007, p. 237; Raymond & DeNardis, 2015, p. 41). Cumulatively, these factors contribute to a rise in complexity apropos basic structures of accountability.

A juxtaposition of the concepts of cyberspace and accountability reveals the following accountability challenges with regard to the governance of the virtual domain: the problem of many hands, the profusion of issue areas, and the hybridity and malleability of institutional arrangements.

The problem of many hands refers to a condition of accountability obfuscation caused by a great number of actors engaged in concurring regulatory ventures (Bovens, 2007; Papadopoulos, 2003). "Because many different officials contribute in many ways□to decisions and policies [...] it is difficult even in principle to identify who is morally responsible for political [and technical] outcomes" (Thompson, 1980, p. 905). In the context of cyberspace governance, the number of stakeholders contributing to policy outcomes and regulatory deliberations is immense. To illustrate, questions such as "*who is accountable for the current and future development of the virtual realm*" may yield any of the following answers: the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), the Internet Governance Forum (IGF), the International Telecommunications Union (ITU), large Internet Service Providers (ISPs) such as AT&T, powerful nation states or departments, such as the US Department of Commerce or the US National Security Agency, influential software companies, as well as civil society groups and individual experts who take part in and contribute to the operations of organisations, such as ICANN or the IETF (DeNardis, 2014; Scholte, 2008, p. 19). While the abundance of actors involved in cyberspace governance does not (necessarily) imply an absence of accountability mechanisms, it does mean higher degrees of complexity.

The heterogeneity of stakeholder configurations can aggravate questions of agency and contribution. Accountability structures are more difficult to determine because actors co-produce outcomes and contribute to the end-product in hybrid constellations. Accountability structures can further be complicated by the conflation of stakeholder-specific traditions, standards, and expectations (Koppell, 2005, p. 94). Not only is the variety of actors contributing to governance ventures and their goals larger, making the identification of accountability objects more difficult (i.e. for which goals should accountability be rendered?), but their expectations can diverge and complicate the emergence of clear lines of responsibility or accountability (Bovens et al., 2014; Carr, 2016, p. 43). Indeed, environments characterised by multiple

stakeholders tend to provide opportunities for blame-shifting (Papadopoulos, 2010, p. 1039).

The problem of many hands represents but one accountability challenge in the context of cyberspace governance. The profusion of issue areas, spanning across technical, socio-political, and economic spheres, constitutes another conundrum. In the context of cyberspace governance, the excess and coming together of technical and non-technical issue areas can severely complicate accountability structures. Seemingly unrelated issue areas may suddenly converge. Examples of such convergence can, among others, be found in areas related to intellectual property rights protection and address naming and numbering:

"The names and numbers given to Internet entities, such as domain names used in Internet addresses, may seem to be a [solely technical] issue to be managed by the Internet Corporation for Assigned Names and Numbers (ICANN). But, the registration of a well-known trademark as a domain name with the intention of selling it back to the owner, called 'cyber-squatting', has led to governance issues that are also the concern of international organisations, like the World Intellectual Property Organisation (WIPO), and national and international legislation and regulations which also cover more traditional trademark and related concerns" (Dutton & Peltu, 2007, p. 8).

The confluence of issue areas can lead to "tangled web[s] of relationships" (Dubnick & Frederickson, 2014, p. xxi). Left untangled, these intertwined webs of relationships can have fatal consequences for accountability structures. For one thing, they can result in the erosion of (pre-existing) accountability structures and cause accountability deficits. For another thing, they can lead to dysfunctional amalgamations of accountability arrangements and bring about situations of accountability overcrowding (Bovens, 2007, p. 462).

The hybridity of institutional arrangements pertaining to cyberspace governance poses yet another accountability challenge. Cyberspace governance is characterised by the absence of a coherent regime or organisation in charge of enacting globally consistent and comprehensive norms and policies. A considerable number of institutions involved in cyberspace governance exhibit characteristics of fluidity and ad-hocism. Accountability structures tend to suffer from the dispersion of topics across different organisational settings and related institutional volatility. They are further aggravated by the fact that stakeholders can take on different roles across different fora of interaction.

The propensity for role-shifting means that certain actors may be involved in the production of outcomes in one forum (be accountors) but may play the part of accountees in other institutional settings. For example, an academic research group may contribute substantially to the development of new security protocols, e.g. in the context of IETF meetings, but may hold private sector companies accountable for faulty implementation/commercialisation of said security protocols, e.g. in circumstances of dispute resolution (Dickinson, 2014). "Insofar as accountability mechanisms are present, [...] mechanisms [can] become mixed. The [jumble] of accountability mechanisms that results from this [can give] rise to uncertainty, confusion, or shrinking" (Bovens et al., 2014, p. 250).

The hybridity of institutional setups also makes developments hard to track and procedural access for some stakeholders, including civil society, uneven, thereby undermining processes of public account giving (Jayawardane, Larik, & Jackson, 2015, p. 7). Civil society organisations have voiced concerns re unequal participation and the fact that decisions of sensitive, yet far-reaching nature are made behind closed doors across several I* organisations, including, for example, the Internet Society (ISOC), IETF, ICANN, W3C, the Internet Architecture Board

(IAB), as well as the regional Internet registries (RIRs), and country code domain name registries (APNIC, 2017).

POLICY RECOMMENDATIONS

In the context of cyberspace governance, the heterogeneity of stakeholders, the profusion of issue areas, as well as the malleability and distribution of institutional arrangements generate deep-rooted accountability tensions that are not easy to resolve. However, these tensions should not discourage researchers and policymakers from thinking about potential solutions and devising relevant strategies (Black, 2012). The subsequent paragraphs offer a set of policy recommendations geared towards addressing the three challenges identified above.

HETEROGENEITY OF STAKEHOLDERS

Cyberspace governance is not a unitary undertaking but exhibits characteristics of post-sovereignty. Processes of steering are "institutionally diffuse and lack a single locus of supreme, absolute, and comprehensive authority" (Scholte, 2008, p. 18). Given the complexity of the realm and the absence of a final arbiter, policy prescriptions centring on hierarchical command and control mechanisms appear ill-suited to resolve the tensions identified. Accountability structures should be reflective of the diversity of stakeholders, and be established on a collective basis. In view of the dominance of sovereigntist (hierarchical) accountability artefacts, the implementation of shared accountability structures may entail a deliberate rehashing of account rendering functions and processes. While the call for collective accountability structures does not imply the participation of the entirety of stakeholders, it does mean the enfranchisement of all relevant parties (Malcolm, 2015, p. 2). The enlistment of stakeholders essential to the resolution of specific cyberspace governance problems presents an important first step with regard to streamlining collective accountability structures and identifying corresponding responsibilities.

In terms of accountability enforcement, the institutionalisation of multistakeholder-oriented checks and balances is key. Independent, constitutionally inspired oversight mechanisms, such as ombudsmen or multistakeholder-versed third-party supervisory and review authorities, and clear standards provide useful instruments in this regard. The latter support the introduction of meaningful benchmarks of expected behaviour and set criteria against which conduct can be assessed (Weber, 2009, p. 159). Given the heterogeneity of stakeholders, relevant standards need to be flexible, yet specific enough to take effect in the respective cyberspace governance arenas.

The adoption of constitutionally inspired enforcement mechanisms has proven fruitful in various cases. In the context of ICANN, for example, the appointment of an ombudsman has helped clarify otherwise murky accountability structures, and provided community members with a useful mechanism of recourse. The ICANN ombudsman evaluates complaints about the organisation (including staff, board, supporting organisations, and advisory committees) lodged by community members, and promotes understanding of pertinent community issues (Davidson, 2009, p. 137).

PROFUSION OF ISSUE AREAS

The intertwining of political, technical, economic, and cultural dimensions, requires a conscious re-calibration of cyberspace governance debates. Given the scale and scope of the cyberspace governance landscape, accountability arrangements cannot meaningfully be established based

on broadly framed, overarching legal instruments, e.g. global treaties or covenants. Rather, discussions of accountability should be organised around specific, manageable issue areas, and include stakeholders from different backgrounds, which are capable of flagging areas of intersection and convergence. The identification of relevant issue areas around which procedures and actor expectations can converge is critical for the emergence of tangible accountability structures (Krasner, 1985, p. 2). Issue specificity helps to reduce ambiguity apropos actor relations, incentives, and goals, and allows for the strategic construction and connection of different cyberspace governance debates, as well as for the attribution of stakeholder responsibilities (Slack, 2016, p. 76).

In the absence of clearly defined processes of account rendering, issue-specific policy networks can offer a useful corrective. In the context of the IGF, for example, so-called Dynamic Coalitions have served as critical means for creating accountability-related anchor points. Dynamic Coalitions are informal, issue-oriented groups of stakeholders working on specific cyberspace governance topics, e.g. freedom of expression and freedom of the media on the internet, network neutrality, or the internet of thing. To be recognised, they have to "produce a written statement which [outlines] the need for the coalition, an action plan, a mailing list, the contact person(s), [as well as] a list of representatives from at least three stakeholder groups" (Internet Governance Forum, 2016). Such thematic groupings go some way in creating a collective identity and sense of responsibility among stakeholders (Harlow & Rawlings, 2007, p. 560).

MALLEABILITY AND DISTRIBUTION OF INSTITUTIONAL ARRANGEMENTS

To avoid forum-related accountability confusion, institutions and stakeholders involved in processes of cyberspace governance are well advised to clearly specify their mission and openly communicate their role (Malcolm, 2015, p. 4). Well-defined mission statements and mandates help to create longer-term commitment and guidance, and reduce the risk of ad-hocism and agenda shifting brought about by changing stakeholder configurations.

Institutional inaccessibility and discrimination should be addressed through proactive engagement and resourcing, as well as through flexible institutional set-ups. Cyberspace governance bodies need to be procedurally and structurally open to admit the participation of all stakeholders who are significantly affected by specific policy problems, or interested in the deliberation and resolution of cyberspace governance issues (Malcolm, 2015). "Proactive dissemination of pertinent, appropriate and quality information [...] at the right time, in the right format, and through the right channels increases the likelihood of uptake by [relevant stakeholders and decreases the possibility of defection and exclusion]" (World Health Organisation, 2015, p. 10). Organisational transparency and certainty, as well as meaningful stakeholder inclusion structured around specific issue areas are of critical importance for the creation of clear accountability structures and the assurance of continuous stakeholder buy-in.

CONCLUSION

In as complex and dispersed an environment as cyberspace, the examination and institutionalisation of accountability structures is not a straightforward undertaking. Researchers and policymakers are confronted with tangled webs of accountability relationships of different texture and design. Untangling these webs, requires conscious and concerted efforts at process and institutional levels (Bovens et al., 2014, p. 251).

This paper has argued that accountability structures are contested by the very elements that are constitutive of cyberspace governance, namely, the number of stakeholders contributing to regulatory ventures, the multiplicity of issue areas concerned, and the hybridity and distribution of institutional arrangements involved. Taken together, these factors bring about the following accountability challenges: the problem of many hands, the profusion of issue areas, as well as the malleability of institutional arrangements.

With a view to addressing the challenges identified, this paper has reasoned that in accordance with the distributed nature of the realm, accountability needs to be exercised and structured in a collective fashion. Given the polycentric nature of cyberspace governance, one-dimensional, sovereigntist conceptions of accountability that intend to attach ultimate responsibility to a unitary source of authority are misplaced. In the absence of a single locus of authority, accountability structures need to be consciously reframed, involving all relevant stakeholders. "All nodes in a given [cyberspace governance venture] must play their part in delivering transparency, consultation, evaluation, and correction" (Scholte, 2008, p. 20). Clear communication of and clarity about institutional and stakeholder-related roles, goals, and expectations are key success factors for establishing accountability structures in complex governance settings. Greater organisational transparency, proactive stakeholder engagement, and procedural openness are key prerequisites for tackling institutional malleability and elusiveness.

No claim is made that the recommendations stipulated by this paper will resolve all accountability challenges pertaining to the governance of the digital realm. On the contrary, this paper recognises that much of what has been discussed is still very much *terra incognita* and requires continuing research. Establishing accountability structures in polycentric governance environments is a demanding and difficult enterprise which requires concerted and sustained efforts by scholars and practitioners alike.

REFERENCES

APNIC. (2017). I* organizations – APNIC. Retrieved May 31, 2017, from https://www.apnic.net/community/ecosystem/iorgs/

Baldwin, R., Cave, M., & Lodge, M. (2010). *The Oxford Handbook of Regulation*. (R. Baldwin, M. Cave, & M. Lodge, Eds.). Oxford University Press. doi:10.1093/oxfordhb/9780199560219.001.0001

Barlow, J. P. (1996). *A Declaration of the Independence of Cyberspace*. Retrieved from https://projects.eff.org/~barlow/Declaration-Final.html

Black, J. (2008). Constructing and contesting legitimacy and accountability in polycentric regulatory regimes. *Regulation & Governance*, *2*(2), 137–164. doi:10.1111/j.1748-5991.2008.00034.x

Black, J. (2012). Calling Regulators to Account: Challenges, Capacities and Prospects. *SSRN Electronic Journal*. doi:10.2139/ssrn.2160220

Bovens, M. (2007). Analysing and assessing accountability: a conceptual framework. *European Law Journal*, *13*(4), 447–468. doi:10.1111/j.1468-0386.2007.00378.x

Bovens, M., Goodin, R. E., & Schillemans, T. (2014). *The Oxford Handbook Public Accountability*. (M. Bovens, R. E. Goodin, & T. Schillemans, Eds.). Oxford University Press. Retrieved from http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199641253.001.0001/oxfordhb-9780199641253

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43–62. doi:10.1111/1468-2346.12504

Clarke, R. A., & Knake, R. K. (2012). *Cyber War: The Next Threat to National Security and What To Do About It*. *Terrorism and Political Violence*. HarperCollins. doi:10.1080/09546553.2011.533082

Davidson, A. (2009). *The Law of Electronic Commerce*. Cambridge University Press. Retrieved from https://books.google.co.uk/books?id=VfIfAwAAQBAJ

Demchak, C., & Dombrowski, P. (2013). *Cyber Westphalia: Asserting State Prerogatives in Cyberspace*. *Georgetown Journal of International Affairs*. Retrieved from http://www.jstor.org/stable/43134320

DeNardis, L. (2014). *The Global War for Internet Governance*. New York, New York, USA: Yale University Press. doi:10.12987/yale/9780300181357.001.0001

Dickinson, S. (2014). *Background Paper* (IGF 2014 Workshop 96: Accountability challenges facing Internet governance today). Retrieved from http://www.intgovforum.org/cms/wks2014/uploads/proposal_background_paper/internet-governance-accountability-challenges-background-paper.pdf

Dubnick, M. J., & Frederickson, H. G. (2014). *Accountable Governance: Problems and Promises*. M.E. Sharpe. Retrieved from https://books.google.co.uk/books?id=M32XUtMBSh4C

Dutton, W. H., & Peltu, M. (2007). The emerging Internet governance mosaic: connecting the pieces. *Information Polity*, *12*(1–2), 63–81. Retrieved from https://www.oii.ox.ac.uk/archive/downloads/publications/FD5.pdf

Enderlein, H., Wälti, S., & Zürn, M. (2010). *Handbook on Multi-Level Governance*. Edward Elgar Publishing Limited. Retrieved from https://books.google.ch/books?id=YlmoCs207UAC

Harlow, C., & Rawlings, R. (2007). Promoting Accountability in Multilevel Governance: A Network Approach. *European Law Journal*, *13*(4), 542–562. doi:10.1111/j.1468-0386.2007.00383.x

Internet Governance Forum. (2016). Dynamic Coalitions. Retrieved September 14, 2017, from http://www.intgovforum.org/cms/dynamiccoalitions

Jayawardane, S., Larik, J., & Jackson, E. (2015). *Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance*. Retrieved from http://www.thehagueinstituteforglobaljustice.org/information-for-policy-makers/policy-brief/cyber-governance-challenges-solutions-and-lessons-for-effective-global-governance/

Johnson, D. R., & Post, D. (1996). Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review*, *48*(5), 1367. doi:10.2307/1229390

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*, *38*(2), 7–40. doi:10.1162/ISEC_a_00138

Kleinwächter, W. (2011). A new Generation of Regulatory Frameworks: The Multistakeholder Internet Governance Model. In *Kommunikation: Festschrift für Rolf H. Weber zum 60. Geburtstag* (pp. 559–580). Stämpfli Verlag.

Koppell, J. G. S. (2005). Pathologies of accountability: ICANN and the challenge of "Multiple Accountabilities Disorder." *Public Administration Review*, *65*(1), 94–108. doi:10.1111/j.1540-6210.2005.00434.x

Krasner, S. D. (1985). *International regimes* (Vol. 3a). Cornell University Press. Retrieved from https://books.google.de/books?id=WIYKBNM5zagC

Levi-Faur, D. (2011). *Handbook on the Politics of Regulation*. (D. Levi-Faur, Ed.). Cheltenham: Edward Elgar Publishing. doi:10.4337/9780857936110

Malcolm, J. (2015). Criteria of meaningful stakeholder inclusion in internet governance. doi:10.14763/2015.4.391

Mueller, M., Mathiason, J., & Klein, H. (2007). The Internet and Global Governance: Principles and Norms for a New Regime. *Global Governance*, *13*, 237–254.

Murray, A. (2007). *The Regulation of Cyberspace*. Taylor & Francis. doi:10.4324/9780203945407

NATO Cooperative Cyber Defence Centre of Excellence. (2017). Cyber Definitions. Retrieved May 31, 2017, from https://ccdcoe.org/cyber-definitions.html

Nye, J. S. (2010). Cyber Power. *Belfer Center for Science and International Affairs*, (May), 1–31. Retrieved from http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf

Ottis, R., & Lorents, P. (2010). Cyberspace: Definition and Implications. In *Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April* (pp. 267–270).

Papadopoulos, Y. (2003). Cooperative forms of governance: Problems of democratic accountability in complex environments. *European Journal of Political Research*, *42*(4), 473–501. doi:10.1111/1475-6765.00093

Papadopoulos, Y. (2010). Accountability and Multi-level Governance: More Accountability, Less Democracy? *West European Politics*, *33*(5), 1030–1049. doi:10.1080/01402382.2010.486126

Raymond, M., & DeNardis, L. (2015). Multistakeholderism: anatomy of an inchoate global institution. *International Theory*, *7*(3), 572–616. doi:10.1017/S1752971915000081

Scholte, J. A. (2008). *Global governance, accountability and civil society*. doi:10.1017/CBO9780511921476

Slack, C. (2016). Wired yet Disconnected: The Governance of International Cyber Relations. *Global Policy*, *7*(1), 69–78. doi:10.1111/1758-5899.12268

Thompson, D. F. (1980). Moral Responsibility of Public Officials: The Problem of Many Hands. *American Political Science Review*, *74*(4), 905–916. doi:10.2307/1954312

Weber, R. H. (2009). Accountability in Internet Governance. *International Journal of Communications Law and Policy*, *13*, 152–167.

Weber, R. H. (2013). The legitimacy and accountability of the internet's governing institutions. In *Research Handbook on Governance of the Internet* (pp. 99–120). Edward Elgar Publishing Limited.

Weber, R. H. (2014). *Realizing a New Global Cyberspace Framework: Normative Foundations and Guiding Principles*. Springer. Retrieved from https://books.google.co.uk/books?id=YemZBAAAQBAJ

World Health Organisation. (2015). *WHO Accountability Framework*. Retrieved from http://www.who.int/about/who_reform/managerial/accountability-framework.pdf

World Wide Web Consortium. (2004). *Architecture of the World Wide Web*. (I. Jacobs & N. Walsh, Eds.). W3C. Retrieved from https://www.w3.org/TR/webarch/