European Commission

FORESIGHT

Trust at Risk:

Implications for EU Policies and Institutions

Research and Innovation

EUROPEAN COMMISSION

Directorate-General for Research and Innovation
Directorate A — Policy Development and Coordination
Unit A.3 — Horizon 2020 Policy

Contact: Heiko Prange-Gstöhl

E-mail: Heiko.Prange-Gstoehl@ec.europa.eu
RTD-PUBLICATIONS@ec.europa.eu

European Commission
B-1049 Brussels

EUROPEAN COMMISSION

Trust at Risk:

Implications for EU Policies and Institutions

Report of the Expert Group

"Trust at Risk? Foresight on the Medium-Term Implications for European Research and Innovation Policies (TRUSTFORESIGHT)"

2017 Directorate-General for Research and Innovation EN

EUROPE DIRECT is a service to help you find answers to your questions about the European Union

Freephone number (*):
00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you)

LEGAL NOTICE

Luxembourg: Publications Office of the European Union, 2017.

PDF ISBN 978-92-79-65517-3 doi: 10.2777/364327 KI-04-17-105-EN-N

Table of contents

Contributors

Members of the Expert Group

Boda, Zsolt, is Head of Department, Institute of Political Science, at the Hungarian Academy of Sciences, Budapest, Hungary.

Flyverbom, Mikkel, is an Associate Professor at the Department of Intercultural Communication and Management, Copenhagen Business School, Denmark.

Hermerén, Göran, is a Professor of Medical Ethics at the Faculty of Medicine, Lund University, Sweden, and Chair of the ALLEA Permanent Working Group for Science and Ethics.

Hiltunen, Elina, is a Futurist and Founder of What's Next Consulting Oy, Finland.

Hofmann, Jeanette, is Head of the Project Group 'The Internet Policy Field' at the Berlin Social Science Center, and Director of the Alexander von Humboldt Institute for Internet and Society, Germany.

Lancee, Bram, is an Assistant Professor of Sociology at the University of Amsterdam, The Netherlands.

Morales, Laura, is a Professor of Political Science in the Department of Politics and International Relations at the University of Leicester, United Kingdom.

Pitlik, Hans, is an Extraordinary Professor and Research Group Coordinator at the Austrian Institute of Economic Research, Vienna, Austria.

Van de Walle, Steven, is Research Professor at the Public Governance Institute, Katholieke Universiteit Leuven, Belgium.

Wright, David, is the founder and Director of Trilateral Research Ltd, London, United Kingdom.

Guest contributors

Hosking, Geoffrey, is Emeritus Professor of Russian History, University College London, United Kingdom.

Prange-Gstöhl, Heiko, is a Senior Policy Officer for Policy Development and Foresight in the European Commission's Directorate-General for Research and Innovation, Brussels, Belgium.

CHAPTER 5

Constellations of trust and distrust in internet governance

Jeanette Hofmann

1. Trust and distrust: inseparable companions

In a general sense, trust can be defined as a 'hypothesis of future conduct, which is sure enough to become the basis of practical action' and resides as a 'condition between knowing and not knowing another person' (Simmel 1906, p. 450). We do not need to trust in situations of complete information, and we cannot trust under conditions absent of any information. Hence, trust is a mechanism allowing us to act in situations of uncertainty by transforming past experiences into assumptions about the future. While Simmel's 'hypothesis of future conduct' focused on people, other authors extended it to events, systems, organisations or abstract principles (Giddens 1990, p. 34).

Trust is commonly understood as a facilitator of social relationships. Trust enables sociability and cooperation, mutual responsiveness and what Emile Durkheim called 'moral density' (Durkheim 1997; Sztompka 1998, p. 22); it enables cooperation, political participation and reduces transaction costs. Distrust, on the other hand, is usually considered a negative phenomenon that enhances uncertainty, lowers cooperation and, thus, increases transaction costs.

This chapter challenges the view that trust is conducive to the general well-being of Europe and its citizens and distrust seems to forebode crises. Instead, I argue that an overall, unqualified bias towards trust risks missing the productive and thus positive aspects of distrust and, likewise, potential downsides of unfounded, disproportionate degrees of trust. Reflecting on the desirability of trust and distrust is not just a theoretical exercise, however. 'Weak signals' for a decline of trust or other indicators thereof can only be adequately interpreted against the background of an unbiased multi-dimensional concept.

A multi-dimensional concept of trust assumes that trust and distrust are not opposite occurrences on a single spectrum but separate ones closely interlinked (Lewicky et al. 1998, p. 339). Treating trust and distrust as separate dimensions means that they can co-occur and interact with each other. Instead of an 'either-or' relationship, trust and distrust may be analysed as dynamic components of multi-faceted social relationships, through which they form evolving constellations. Lewicky et al. (1998, p. 447) come to the conclusion that in the twenty-first century 'distrust is much more prevalent than students of trust in organizations have been willing to admit'. In fact, well-established relationships between organisations can be expected to display both, high levels of trust and distrust. Trust, according to Lewicky et al. (1998, p. 443) develops from sketchy impressions to evidence-based experience that allows all actors involved to be increasingly specific about people, promises and performances they trust and those they distrust. Hence, the relationship between trust and distrust is likely to change over time, based on practical experiences individuals and organisations make with each other.

Referring to Luhmann (1979)[1], the authors reason that 'trust cannot exist apart from distrust' and that 'social structures appear most stable where there is a healthy dose of both trust and distrust' (Lewicky et al. 1998, p. 450). Too much trust or distrust without their respective counterparts is identified as potential sources of dysfunctionality. Considering that distrust is commonly regarded

[1] Luhmann's approach to trust as a (necessary) way of reducing complexity is well known. Less known is his notion of distrust as a functional equivalent. According to Luhmann (1979), both trust and distrust reduce complexity and uncertainty, just by opposite cognitive operations: Like trust, distrust is also based on simplifications that reinforce existing expectations at the cost of a more comprehensive yet less coherent picture of social reality. The area of Internet governance offers many examples of generalized distrust as a form of reducing complexity. One that comes to mind would be the common negative attitude towards intergovernmental organizations.

as something bad in need of being allayed, one may ask how trust and distrust actually interact and how the latter is able to unfold its positive effects. A key to an answer can be found in Sztompka's (1998) observations of the 'paradox of democracy'. Sztompka's work is of particular relevance to this report because it focuses on social and organisational rather than individual forms of trust and links the notions of trust and distrust to the political sphere of public discourse and rule-making.

The democratic order, Sztompka (1998, p. 25) contends, is a 'significant trust-generating force' precisely because it has managed to institutionalise distrust. Democracy creates 'generalised trust'[2] by transforming the ubiquitous distrust towards the exercise of political power into a set of rules, procedures and institutions that aim to lower the risk of its abuse. Sztompka's paradox of democracy states that the institutionalisation of distrust enables the unfolding of a culture of trust (Sztompka 1998, p. 26; see also Schaal 2004).

The observation that distrust has a productive role to play in creating cultures of trust is highly pertinent for the field of Internet governance, as I will show in the next section of this chapter. However, before I outline the interplay between trust and distrust in Internet governance, it is useful to dig a bit deeper into the conditions understood to generalise trust and to consider how democratic orders consolidate those conditions.

In the search for structural elements conducive to the unfolding of cultures of trust (and distrust respectively), Sztompka (1998, p. 23ff) identifies several conditions. In a nutshell these conditions are 1. normative certainty and stability of social order, 2. transparency of social organization, 3. accountability of power, 4. enactment of rights and obligations including the safeguarding of dignity, integrity and autonomy, and 5. enforcement of duties and responsibilities.[3] Sztompka argues that democratic orders help to produce these conditions by providing reliable safeguards against their violation. These safeguards, among them the division of power, the rule of law, independent courts, constitutionalism, legitimacy and elections, etc., in turn, reflect a profound and persistent distrust towards the exercise of power. Hence, distrust may entail the protective effect of preventing damage. It may obviate the risk of trusting a bogus email, a business deal or even the public assertions of a national secret service. Democratic constitutions are supposed to translate traditional national attitudes towards trust and distrust into an institutional apparatus of both enabling and constraining political authority (Schaal 2004, p. 36).

The reference to national constitutions as trust-generating expressions of distrust indicates how close but also ambiguous the ties are between trust and distrust. Moreover, the case of constitutions demonstrates why the mere appearance of distrust should not be interpreted as a 'weak signal' denoting an erosion of trust. Changing relations of trust and distrust may precede a crisis but they may as well reflect an ongoing learning process about the trustworthiness of organisations interacting with each other (see Schaal 2004). In practice, it is very hard, if not impossible, to distinguish a healthy from a crisis-prone constellation of trust and distrust. Yet, it should be possible to narrow down the signs for a crisis of confidence. For this purpose, it is useful to turn to Albert Hirschman's (1970) contribution on 'exit and voice'.

Hirschman identifies exit and voice as the two basic choices that we face in cases of disappointment with the performance of an organisation or individual. The political sphere is more likely to create 'voice-prone situations' (Hirschman 1980, p. 438) characterised by acts of protest or opposition while the competition-based commercial sphere lends itself to exit behaviour. To give a practical example: disappointment with the quality of service of an Internet access provider might lead to ending the contract and switching to a competitor while discontent with the political course of Internet governance organizations could result in voicing one's criticism. Hirschman offers a beautiful explanation of why 'the use of voice' may be an option even if it is costly and its

[2] As a collective trait, trustfulness represents a 'typical orientation' that increases Durkheim's 'moral density' (Sztompka 1998).

[3] Cultures of distrust are caused by the opposing conditions such as normative chaos, instable social orders, etc.

outcome fundamentally uncertain. 'It is in the nature of the 'public good'', notes Hirschman (1980, p. 433), 'that striving for it cannot be neatly separated from possessing it'. Throughout the process of political engagement for a public good such as the preservation of the open Internet or the overcoming of the digital divide, the means may turn into ends and thereby become 'the next best thing to having that policy' (Hirschman 1980, p. 433). Internet governance, a 'regulatory space' (Hancher/Moran 1989) populated to a high degree or even predominantly by volunteers, is a good example of this transformation of means into ends. Although political progress is rarely achieved in Internet governance, the loyalty of stakeholders has been high and the number of NGOs and volunteers in this area seems to be growing over the years. Yet, as research on transnational governance arrangements confirms, the foundation of global policy-making outside of intergovernmental structures tends to be fragile (Tamm Hallström/Boström 2010) and 'exit' always remains an option. Exit interpreted in the context of trust-distrust constellations would mean an erosion of loyalty and a stricter separation of means and ends, costs and benefits. A significant number of participants may lose confidence that discontent eventually leads to change and that distrust expressed will be institutionalized in the form of rules that effectively lessen the chances for an abuse of power. A noticeable decline in participation in Internet governance processes could thus be interpreted as a (weak) signal indicating an emerging crisis of the governance model. Luhmann's (1979, p. 73) reference to thresholds and turning points seems particularly relevant in this context.[4] The next section offers a brief overview of Internet governance and simultaneously contextualizes the dynamics of trust and distrust within this field.

2. Internet governance: private authority in the making

Internet governance is a 'difficult horse to catch', as Ziewitz and Pentzold (2013, p. 1) rightly observe. The field is neither well-defined nor stable or coherent. In the second half of the 1990s when the term gained currency (for an early contribution see Kahin/Keller 1997), it referred to the coordination of the technical resources that enable the Internet to be a network of autonomous networks. For the first ten years, Internet governance used to designate rule-making or policies for Internet addresses, the Domain Name System and a few other parameters, all of which have in common that uniform rules across the Internet are necessary to allow for a coherent communication space.[5] Examples for such rules refer to the allocation of Internet addresses or the assignment of Top Level Domains such as '.eu'. For the Internet to function, both 'names' and 'numbers', also referred to as Critical Internet Resources, have to be unique and therefore demand a global management process.[6] In the early 2000s, the common understanding of Internet governance began to broaden. During the UN World Summit on the Information Society (WSIS) (2002-2005), the first intergovernmental process, which systematically addressed political aspects of Internet governance such as the oversight authority over global infrastructure resources, a distinction emerged between a narrow and a broad understanding of the term. The latter included a growing number of non-technical issues such as the digital divide, copyright regulation, cybercrime prevention and cyber security, net neutrality, human rights and, particularly, freedom of speech and data protection. The most widespread definition of Internet governance which emerged out of WSIS reflects this broad notion of the term:

---

[4] Thresholds are defined as an 'artificial discontinuity which levels out the area of expertise before and after the threshold, and thus makes a simplification'. The idea of turning points suggests that 'small steps can bring great changes' in the constellation between trust and distrust. If distrust gains the upper hand, it turns into a destructive force, according to Luhmann. A practical example would be precautions against the abuse of power, which increase the transaction costs in consensus building to a degree that bottom-up policy making in Internet governance becomes more or less impossible. As a result, voluntary participation, an essential source of the multi-stakeholder approach, would noticeably decline.

[5] The same is true for the international postal and telephone networks, both of which require standardized addresses, transmission techniques and procedures, etc. to allow for cross-border communication.

[6] At a minimum, Critical Internet Resources comprise the address space (IP addresses), the Domain Names System including the root servers and specific protocol parameters (protocol parameters comprise, for example, the numbering of standards, autonomous systems, TCP port numbers, etc.). Some experts add exchange points, peering arrangements and other forms of Internet service provision to the list of Critical Internet Resources.

> 'Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet' (WGIG 2005).

This rather broad definition of Internet governance goes beyond the original, strictly technical, understanding and covers norm-setting processes which, while directly affecting the Internet, its applications, services and communication processes, are not necessarily part of its established institutional landscape, now commonly referred to as the 'Internet governance eco system'. A striking feature of Internet governance is its polycentric, fragmented structure. It is quite telling that there is neither a text nor a chart available on the Internet that seeks to encompass all relevant organisations, treaties and regulatory processes that correspond to the definition of Internet governance quoted above. One of the scenarios described further below expects that, as part of a gradual process of constitutionalisation, more formal ties may emerge among organizations whose activities explicitly or implicitly contribute to Internet governance. However, for the time being, it is important to keep in mind that there is incongruence between narrow and broad understandings of the field and that, depending on the context, different definitions are in use.

Internet governance has been a contested policy area from early on. The core controversial question revolves around authority: who and what should govern the Internet, a multilateral body with corresponding treaties, a public-private or a private contract-based regime? Unlike previous communication infrastructures such as the postal and the telephone system, the Internet is not managed under the auspices of a special UN agency. The institutional evolution of Internet governance has, in fact, been shaped by a deep-rooted distrust of both intergovernmental processes and national public authorities (see Epstein 2013; Mueller 2002). One could even argue that the distrust held by key actors in the early days of Internet governance against multilateral institutions and public administrations formed a productive force driving the development of the Internet's organisational architecture.

The first battleground over the future shape of a global data network emerged in the 1970s between various standard setting communities who disagreed on the design of the network architecture. As Abbate (2000) and DeNardis (2009) convincingly showed, standards are political artifacts that aim to inscribe into technology the future location and division of control over the technical object. While the national telephone operators traditionally built centrally controlled public communication architectures and firmly distrusted the distributed, de-centralised model of network architecture envisioned by the computer engineers, the latter expressed distrust towards centrally operated networks.[7]

A similar constellation between public and private regulatory models emerged in the course of the debate over rights in and rules for the Domain Name System in the mid-1990s. One of the central issues concerned the management and expansion of this new resource that quickly gained commercial value following the privatisation of the Internet. Some observers saw the Domain Names System as a public resource 'subject to public trust' (cited in Mueller 2002, p. 144) that should therefore be co-managed by intergovernmental bodies such as the International Telecommunication Union (ITU) and the World Intellectual Property Organization (WIPO). Others argued for a market-driven solution with competition and consumer choice as the basic cornerstones. Due to the intervention of the US government, the latter approach prevailed. The US government argued that 'private-sector action' was preferable to government control and that neither governments nor intergovernmental organisations should be involved in the management

[7] Since the original funding for the development of the Internet came from US military research, the scenario used by the computer engineers concerned a hostile attack on the US communication infrastructure. A distributed network architecture, they argued, would be able to survive such an attack while a central architecture would not (see Hofmann 2007).

of the Internet infrastructure. Subsequently, in 1998, the US government founded the Internet Corporation of Assigned Names and Numbers (ICANN), an 'industry-led' organisation.[8]

With the founding of ICANN, a non-multilateral path became established that has structured the organisational but also the political development of Internet governance ever since. All operational functions that keep the global digital infrastructure running are governed by private entities.[9] There are only two noticeable exceptions to this rule. The first concerns the role of the US government. In the course of founding ICANN, the US government created a unilateral oversight position for itself, which amounts to a sort of universal stewardship role hovering over major parts of the coordination of the Internet's technical infrastructure. The second exception pertains to the Internet Governance Forum (IGF). A hybrid between a multi-lateral and a multi-stakeholder organization, the IGF is formally convened by the United Nations but practically shaped by the contributions of civil society, the private sector, the technical community and governments. Over the nearly ten years of its existence, the IGF has used its dialogue-centered mandate to help establish a transnational public for Internet governance issues.[10]

While the strong preference for private self-regulation structures can be interpreted as the result of widespread distrust among the (at that time predominantly North American) Internet community towards intergovernmental organisations, the non-governmental approach to the management of the Internet infrastructure has provoked a lot of distrust itself over the last nearly 20 years. Key reasons for this distrust are the unilateral oversight executed by the US government and the informal, partly experimental character of Internet governance organisations. Given the strong anti-multilateral impetus in this area, the evolution of the organisational landscape could not draw on internationally well-established precedents. Institutional frameworks for private authority are still new and somewhat provisional in the transnational sphere. This is particularly true for multi-actor arrangements that seek to gain legitimacy by including many different stakeholder groups. More importantly, Internet governance is not constitutionalised to a degree that could serve as a source for a culture of trust. To date, Internet governance still lacks normative certainty, robust mechanisms to hold authorities to account and a reliable enactment of rights and enforcement of duties and responsibilities.[11] Thus, Internet governance has to generate itself the specific conditions that are expected to enable a culture of trust.

In light of Schaal's (2004, p. 36) observation that constitutions reflect national discourses on political trust and distrust, one might interpret the ongoing debate about appropriate forms of Internet governance as a meandering process of transnational constitution building. Recent works

---

[8] Governments have always been involved in ICANN, however. This is particularly true for the US Government. Although the National Telecommunication and Information Administration (NTIA) of the US Department of Commerce had planned to supervise the evolution of ICANN only for a limited time of approximately two years, the contractual relationship between NTIA and ICANN has only narrowed down, but as yet not disappeared. In spring 2014, the US government announced that it may relinquish its oversight role over ICANN (NTIA 2014).

[9] This includes the technical development in the form of technical standard setting, the regulation of the domain name system, the allocation of Internet addresses through regional Internet registries (RIRs), the operation of the physical infrastructure and that of Internet exchange points that allows Internet service providers to exchange data traffic.

[10] The IGF emerged out of the UN World Summit on the Information Society. The civil society groups involved in the summit had argued that Internet governance lacks a global space, which would allow interested groups to come together to discuss pertinent issues in this policy domain (Drake 2005). The WSIS declaration (Tunis Agenda 2005, para 67-79) defines the mandate of the IGF. Noteworthy about this mandate are the restrictions imposed on the activities of the IGF. The forum neither produces formal outcomes nor does it have any decision-making capacity. The IGF is designed to facilitate a dialogue in the form of a multi-stakeholder process (Epstein 2012; Mueller 2010).

[11] See Beck (2008, p. 798) who once described the need of legitimacy for large transnational corporations in these terms: 'But nowadays corporations as quasi-states also have to make political decisions, and they are at the same time fundamentally dependent on negotiation and trust, and thus thoroughly dependent on legitimation. Furthermore, they become legitimation-dependent players without being able to draw on democratic sources of legitimation.'

on global constitutionalism support such a view. This new research field pivots on 'institutional arrangements in the non-constitutional realm' assumed to have taken on a 'constitutional quality' (Wiener 2012, p. 5). Constitution in this context is not meant to be understood literally as 'public law text emanating from state authority and sitting at the pinnacle of a pyramid of legal normativity" (Zumbansen 2012, p. 50). Rather, constitutionalism represents a non-territorial frame of reference or 'vocabulary' for assessing, i.e., 'contesting or justifying' the exercise of power in terms of its legitimacy (Kumm 2014, p. 1). The legitimacy of authority, in turn, results from its commitment to constitutional norms incorporated in or expressed in the form of declarations of human rights, democracy, procedural fairness and the rule of law (Kumm 2014; Wiener et al. 2012; Zumbansen 2012).[12] Research on global constitutionalism and on global governance share the premise that transnational processes and organisations require new constitutional architectures (Wiener et al. 2012). Thus, constitutionalism has a double meaning; it denotes a frame of reference but also assumes an observable process of evolutionary norm development in a heterarchic trans-border world (Zumbansen 2012, p. 50).

The multi-stakeholder approach can be regarded as one attempt of transposing national democratic norms of participation into a transnational setting. The term multi-stakeholder in the context of Internet governance means that governments, the private sector, civil society and the technical community recognise each other as relevant actors who, to varying degrees, depend on reciprocal collaboration. Before this idea gained traction in Internet governance in the early years of the new millennium, the multi-stakeholder approach had already been put into practice in various other transnational policy contexts (Boström/Tamm Hallström 2013). Multi-stakeholder initiatives typically emerge around regulatory gaps and aim to produce voluntary, non-binding rules that cannot be enforced. Today, they are understood to 'represent a key element in the emerging global regulatory order that has been characterized as private governance' (Mena/Palazzo 2012, p. 528; also Sloan/Oliver 2013).

The outcome documents of the UN World Summit on Information Society, particularly its definition of Internet governance, 'ratified' the role of non-state actors in this domain (Mueller 2010, p. 9). Following WSIS, the multi-stakeholder approach has become associated with inclusiveness, participation, diversity of opinions and expertise. Over the last ten years, it has advanced as a common hallmark, which confers legitimacy to Internet governance processes and bodies. Various organisations, among them ICANN or the Internet Society, an influential US non-profit organization, now portray themselves as multi-stakeholder bodies. The IGF, whose programme and meeting format are supposed to reflect the collaboration of the stakeholder groups, is considered the epitome of this approach. Yet, to some extent, the reference to multi-stakeholder principles has already become ceremonial; and not all organisations and processes live up to its standard of eye-level collaboration (DeNardis/Raymond 2013, p. 16). Critics of this approach stress the power asymmetry between the participating stakeholder groups and deem it to be mere window dressing.

To conclude, a lack of trust towards the assumed opacity, exclusiveness and bureaucratic heavy-handedness of UN organisations has motivated, and legitimised, the development of innovative governance structures. The institutional evolution of Internet governance is also driven by the belief that the intergovernmental regime with its anchoring in the territorial nation state is the wrong approach to governing the non-territorial architecture of the Internet. Hence, unlike traditional communication infrastructures, trust in Internet governance is not generated through intergovernmental agencies and processes. A dominant group of Internet stakeholders[13] has managed to turn their distrust of multilateral organisations into a productive source of institution-building and thereby generate a unique, unparalleled model of transnational regulation. In this context, the multi-stakeholder concept has advanced as an experimental process of transnational coordination that nowadays strives to present itself as a counter-model to multilateral regimes. However, under the popular multi-stakeholder umbrella many different ways of going about

[12] This abstract understanding of constitutionalisation differs from that of Sztompka (1998) who refers to the traditional notion of a national legal document.

[13] There are a significant number of governments and NGOs who regard a multilateral, UN-based approach to Internet governance as the preferable, more democratic solution. The governing set of values in this field marginalises such arguments.

participation, representation and diversity can be identified, not all of them as accountable, open and transparent as the discourse on Internet governance would suggest and its participants might wish for. Echoing Sztompka (1998) once more, Internet governance can be characterised as a policy space without the basic structural and normative ingredients for the paradox of democracy to unfold its specific version of generalised trust. Internet governance lacks the safeguards that national democratic orders provide to produce and protect these conditions. As yet, there is no division of power, no independent court system, no election procedure or transnational equivalents thereof that would reduce the likelihood of abuses of power. Recalling Lewicky et al.'s (1998) observation that we can expect simultaneously high levels of trust and distrust in most contemporary organisations, one may assume in the Internet governance domain more frequent, tempestuous and perhaps also less predictable swings between expressions of trust and distrust than on the national level.

An actual example of this fragility will be presented in the next part. The impact of Edward Snowden's revelations on public mass surveillance programs forms the empirical background for two ideal-type scenarios, which sketch out opposite developments of Internet governance for the coming 15 years. The scenarios are inspired by Hirschman's 'exit and voice' concept; that is they are based on the assumption that a possible long-term loss of trust in the Internet caused by publicly organised mass surveillance and espionage may reinforce two trends or combinations thereof: the 'voice' option leading to a constitutionalisation and a gradual expansion of the scope of Internet governance, and the 'exit' option, which increasingly undermines the interoperability and cohesion of the network or networks. A mixture of these two options would mean the emergence of both, islands of constitutionalisation accompanied by growing evidence of fragmentation. The astute reader will realise that both scenarios involve different actors, actions and venues.[14] If processes of constitutionalisation and fragmentation are likely to take place in different governance arrangements, i.e. technical standard setting and transnational rule making, can one then still speak of a choice between 'exit' and 'voice'? I will address this question in more detail in the following section.

3. Two scenarios of Internet governance: constitutionalisation and fragmentation[15]

Starting in summer 2013, the revelations of Edward Snowden initiated a cascade of distrust in Internet governance, the impact of which could be felt both on the global and the national level.

The extensive national surveillance programmes and the cooperation across countries, public and private sectors they require have shaken the constellation of trust and distrust not only in the Internet and its communication services but also, to some degree, in the ability of governments to protect their citizens against the violation of human rights (CIGI/Ipsos 2014)[16]. Interestingly, this loss of trust has evoked two almost polar responses that can be interpreted in terms of Hirschman's 'voice' and 'exit'. By and large, the voice strategy consists in moves towards a more binding regulatory framework for the Internet and its use. The exit strategy amounts to reconsidering the merits of a globally distributed network architecture to regionalise specific functions and regulations at the risk of causing fragmentation of the Internet. There is enough empirical evidence to assume that both paths are being actively pursued by different groups of actors, which are nonetheless aware of each other.

[14] I thank Benjamin Bergemann for pointing out this potential inconsistency of the two scenarios.

[15] In spring 2015, shortly before I completed this text, the fellows of the Global Governance Futures Program released a document with two scenarios about Internet governance, the 'Cyber Davos' and the 'Google Shock' predicting collaboration or the collapse of the status quo respectively. While centered more on economic aspects, the scenarios share some assumptions with those presented below.

[16] http://www.cigionline.org/internet-survey.

3.1. Scenario 1: Voice - constitutionalisation of internet governance

As a consequence of the Snowden revelations, in spring 2014 the US government announced its intent to withdraw from its oversight role and transition it to the 'global multi-stakeholder community' (NTIA 2014). As part of the transition process, the NTIA asked ICANN, the present contractor of the IANA functions, to 'convene the multi-stakeholder process' to develop a consensual model (transition proposal) that would replace the supervisory role held by the USG.[17]

The withdrawal of the US government from its supervisory role would end the remaining public control over the critical Internet resources and thus eliminate the perceived 'backstop with regard to ICANN's organization-wide accountability' (ICANN 2014).[18] The 'shadow of hierarchy' against which the development of Internet governance has taken place would weaken, which is why ICANN now faces the challenge of generating, by its own means, the trust that has so far rested in the contractual relationship with the US Government. Considering the overall importance of the Internet infrastructure, this step towards full privatisation has caused nothing less than a mid-size earthquake in the Internet governance world. Following the announcement of the US government, the participants of ICANN's various constituencies have started working on procedures to replace the role of an external supervisor and simultaneously make the organisation more accountable. Looking at these activities from outside, the Snowden revelations have evoked a period of intense constitutionalisation of the management of the Domain Names System. The intended withdrawal of the US government and its effect on the accountability provisions of ICANN is just one example of how the crisis of confidence caused by mass surveillance has set in motion a process towards addressing the legitimacy of regulatory structures in Internet governance and thereby significantly changing its organisational framework.

Another initiative towards constitutionalising Internet governance goes back to Brazil's president Dilma Rousseff who, in a passionate speech to the UN General Assembly in September 2013, addressed the 'grave violation of human rights and of civil liberties' caused by pervasive surveillance. She declared that the 'time is ripe to create the conditions to prevent cyberspace from being used as a weapon of war' and announced Brazil's intention to work on a 'civilian multilateral framework for the governance and use of the Internet [...] to ensure the effective protection of data that travels through the web' (Rousseff 2013). Following that statement at the UN, governments, private sector, civil society and the technical community initiated the development of a policy framework and a roadmap for the future evolution of Internet governance, to be agreed upon at the NetMundial conference in spring 2014 in Sao Paulo. For the first time governments, private sector, the technical community and civil society co-authored a declaration, the 'NETmundial Multistakeholder Statement'.[19] While its normative substance does not go beyond agreed language of existing multilateral declarations, the collaborative process of organizing the conference and its outcome clearly set new procedural standards in Internet governance. Although none of these events come close to constitute what research on global constitutionalism defines as legitimate authority, the activities in the aftermath of the revelations by Snowden indicate a trend towards constitutionalising the sphere of Internet governance. Crises of trust may form a driver of such developments.

The constitutionalisation scenario assumes that in the coming 15 years we will witness an increasing density of the governance network. New organisations will emerge and existing organisations are likely to expand with the goal to fill the perceived gaps in the 'Internet governance ecosystem'. This may concern the implementation or enforcement of policies and standards or the strengthening of ties and collaboration between various bodies in, as well as outside, this field. Other conceivable voids to be addressed pertain to cross-arbitration, redress,

---

[17] One of the conditions set by the US Government is that neither a government-led nor an inter-governmental organisation can take over the coordination of the IANA function (NTIA 2014).

[18] https://www.icann.org/stewardship-accountability.

[19] http://netmundial.br/netmundial-multistakeholder-statement. The author of this article actively contributed to the conference and its outcome document.

capacity building and consultancy. The growing density of the governance structures will be accompanied, and perhaps even driven, by the formation of a transnational public, which will, through various means, monitor and assess the performance of policy making, attempt to keep the key players in check but probably also call for an expansion of the regulatory scope.

As stated above, the scope and boundaries of Internet governance have been in flux throughout the last decade. The revelations about mass surveillance indicate a growing incongruence between policies squarely affecting the Internet on the one hand, and organisations involved in Internet governance processes so that their policies can be challenged and influenced on the other. To state the obvious, security agencies rarely participate in multi-stakeholder processes and are unlikely to voluntarily subject their strategies to public scrutiny. Yet, at the same time they do intervene in substantive ways in standard setting and technology development, the operation and use of the Internet. The constitutionalisation scenario predicts a growing public pressure towards the integration of all policy actors and policies into the Internet governance domain that are assumed to substantially affect the future development of the Internet. It further predicts that the common distinction between nationals and foreigners in state surveillance legislation will come under pressure and eventually be abandoned in order to sustain cross-border communication and trade. This process of constitutionalisation will be fueled by both civil society and the Internet industry even if for different motives. While the first stakeholder group fights for the recognition of civil rights and the rule of law in the digital sphere, the latter seeks to protect its business model and market share. Seen from a constitutionalisation perspective, the concept of legitimate authority and its underlying norms, particularly human rights, democratic participation and the rule of law, would become the generally accepted frame of reference against which principally all policies and standards affecting the Internet can be challenged or justified (Kumm et al. 2014, p. 1).

The process of constitutionalisation does not come without its downsides, however. As a response to criticism from its membership, we can expect the relevant Internet governance bodies to undergo progressive bureaucratisation. In order to improve transparency, inclusiveness, fairness of process and the overall accountability, governance activities will become increasingly burdened with procedural obligations which, in turn, will exclude a growing number of volunteers from participating in the policy making. As an unintended consequence, the constitutionalisation of Internet governance will cause a push of professionalisation and, correspondingly, a decline of voluntary participation (see also Tamm Hallström/Boström 2010, p. 167f for this phenomenon).

Paradoxically, the drive towards formally constituted legitimate authority is likely to lead to an adaptation of the Internet governance regime to the very multilateral system against which it once emerged and set itself apart from. With increasing relevance, the performance and legitimacy of Internet governance organisations will be judged against standards common for public or intergovernmental organisations and thus gradually be forced to adopt them in one form or another (Botzem/Hofmann 2010). The evolution of policy making in ICANN over the last years may illustrate such trends towards bureaucratization. Other transnational multi-stakeholder processes also seem to confirm them:

> 'We have seen a need to establish mechanisms and structures that resemble state structures (…) They refer to input, procedures, output, forms for representation, representativeness, and division of power: dividing, standard setting, accreditation, and certification, for instance. The increasing complexity of these governance arrangements relates, at least partially, to legitimacy aspirations - to aspirations to achieve various democratic ideals around deliberation, participation, and representation in the eyes of a plurality of stakeholders' (Tamm Hallström/Boström 2010, p. 168).

Thus the constitutionalisation scenario predicts that in order to respond to expressions of distrust and to conform to expectations of legitimacy, the institutional framework of Internet governance will indeed become increasingly constitutionalised; yet to the effect that the differences to intergovernmental bodies, which are highly relevant for the identity of its core organisations might gradually disappear. This process of adaptation will transform the institutional repertoire available to respond to crises of confidence but not eliminate such crises per se.

3.2. Scenario 2: Exit - fragmentation of the internet

Another widespread response to the Snowden revelations consists in a decline of trust in and support for the concept of a global, cross-border communication space. Instead of strengthening the normative basis for transnational information flows and instead of improving the security of transmitting, processing and storing data across the globe, relevant actors increasingly consider national or regional data services and suggest keeping data as much as possible in the respective country. Ideas such as 'Schengen routing', the 'Euro cloud' or nationally certified email services are enjoying growing popularity. European Internet providers, for instance, are offering special cloud services that guarantee to keep data on European ground, compliant with European data protection standards. Such new forms of territorial consciousness also affect digital hardware. The discovery of so-called backdoors, both in Chinese and American hardware products, has encouraged national efforts to strengthen the domestic Internet industry (for Brazil, see Woodcock 2013; see Chander/Le 2015 for further examples).

Recent efforts at data localisation are causing concerns over an imminent 'fragmentation of the Internet'. Referring to Berners-Lee, Hill (2012, p. 12) defines fragmentation as a state 'where the experience of one Internet user is radically different from another's. (…) A website should look the same to a person in China as it does to a person in Chile. In other words, the experience of every Internet user should be the same regardless of geographic location, computer type, or any other distinguishing characteristic of the user' (Hill 2012, p. 12). Such a broad understanding of fragmentation does not zero in on China's great firewall or Iran's plans to build a discrete national information network that can be cut off from the global Internet but covers all sorts of public and private forms of data regulation. And it implies that today's Internet is already fragmented to an alarming degree. Common examples for content-based fragmentation are censorship, mundane techniques of personalising content (Hosanagar et al. 2014), but also violations of neutrality such as the new trend towards zero rating contracts (Gillmor 2014). Other sources of fragmentation include differing privacy laws, copyright provisions and territorial licensing schemes, but also competing technical standards (Hill 2012, p. 5f).

These examples show that practices of fragmenting the Internet are by no means new. Neither are the concerns over a 'splinternet' that would break along geographic, technical and content-based boundaries. As Kuner (2015, p. 2092) argues, national frontiers on the Internet have emerged due to the 'widespread unease with the breakdown of national regulatory borders'. A case in point is the EU data protection legislation and its safe harbor provisions designed to enforce these rules also for data flows between Europe and the US. Yet, surveillance activities have doubtlessly increased existing fears for 'informational sovereignty' (Kuner (2015, p. 2091). 'The era of a global Internet may be passing', state Chander and Le (2015, p. 679) and warn against a future of 'data nationalisation'.

Given the increasing trends towards fragmenting data flows, the second scenario assumes that decreasing trust in the Internet infrastructure will manifest itself in stable and long-term forms of territorial and application-based compartmentalisation. The lack of constitutional rights in the transnational sphere will accelerate the fragmentation of the Internet. Rather than fighting for enforceable (human) rights, relevant actors will back off and begin re-orienting their activities towards local platforms and services. The regionalization of commercial, political and private online activities will be accompanied by a profound shift in values. The previous vision of a seamless global communication space able to accommodate everyone and everything will lose its progressive, emancipatory connotation and be gradually replaced by the esteem for secure communication. The more everyday objects and activities become part of digital networks, the more security concerns will outweigh those over freedom of communication and information.

The Internet industry will respond to this long-term transformation of the hierarchy of societal values and norms by shifting investment, standard setting and technology development from the open Internet architecture towards more specialised digital networks optimised for specific applications and users. In retrospect, the Internet of things will be identified as one of the crucial innovations that sealed the fate of the Internet and promoted the development of competing network architectures. Within a decade, consumers, who won't like to be called users anymore because the latter term is not recognised in national law, will have forgotten the technical features that once accounted for the open Internet.

Simultaneously, global platforms and services will be gradually abandoned in favor of more tailor-cut solutions emphasizing security, reliability, central control and homogeneity over diversity, openness and otherness. The 'Google Shock' scenario developed by Khan et al. (2015, p. 14) predicts that, following the disclosure that collaborations between intelligence agencies and Internet industry was much closer than previously reported, investors and users will 'leave Facebook in droves' leaving 'the company reeling' and ultimately going bankrupt. Inevitably, 'Facebook clones' will surface splintering the original social network along regional and national lines (Khan et al. 2015, p. 15). As a result, we can expect the innovation dynamics, the quality and reliability of cross-border services to drop. In 15 years, most of the global services and platforms will be a thing of the past, vaguely remembered as that strange fashion style of the early decades of the two-thousands. Facing cumbersome security provisions, broken links, slow connections and deserted networking sites filled with dubious content, people will find it difficult to comprehend what the dream of the global, open and decentralised Internet once was about.

Summing up, it should be highlighted that these scenarios are not fabricated but rather extrapolate present developments. This implies that they are not mutually exclusive but may well evolve simultaneously. It is indeed conceivable that we will see islands of constitutionalisation emerging around key Internet resources and functions such as the management of the Domain Name System, the allocation of Internet addresses, the development of routing policies or peering arrangements and the development of technical standards without which the Internet would cease to exist. Distrust repeatedly voiced by stakeholders including governments would bring about a system of rules and procedures for critical Internet resources more or less on a par with national regulatory regimes bound by the rule of law. Notwithstanding islands of constitutionalisation, safety on the Internet would generally become associated with services regulated by domestic law and protected by national borders. Pioneered by critical infrastructure services and security relevant industries, a growing number of digital networks independent of and in competition with the Internet will emerge and be in high demand by consumers and companies alike. The crucial factor determining the relative significance or impact of voice and exit moves is likely to be public pressure. So, even if the stakeholders pursuing these voice and exit strategies are different, the public sphere links them together and turns them into options for people to choose.

4. R&I policy recommendations

4.1. Constitutionalising the transnational sphere

The Internet constitutes a cross-border sphere of global scope. However, constitutions predominantly regulate the exercise of power on the national level. As the mass surveillance of Internet traffic shows, citizens are not sufficiently protected when they use the Internet. Considering growing trends towards transnational and international policy making, questions regarding the structural conditions for and modes of constitutionalised, legitimate authority beyond the nation state are likely to become more pertinent. Global constitutionalism is a new interdisciplinary research field able to address these issues. Constitutions, as Sztompka (1998) observes, are a crucial source of generalised trust. It would be most relevant to study whether constitutional frameworks for private authority on the transnational level have similar effects. Empirical research is needed to study indicators for processes of constitutionalisation, their drivers and obstacles as well as their actors and resources. Empirical analysis should also cover the potential role of technology in constitutionalising the transnational sphere. Even if code is not law, digital technology plays an important role in regulating the behaviour of users and data flows on the Internet, as initiatives such as 'privacy by design' show.

4.2. Potential, limits and conditions of success of multi-stakeholder arrangements

Although the multi-stakeholder approach has been in use for more than a decade in the Internet governance domain, there has yet to be a systematic analysis of its capacity, its strengths and weaknesses. Could multi-stakeholder processes that integrate governments, private sector and civil society form a basis for constitutionalising Internet governance? Critics of this approach claim that multi-stakeholder approaches unduly increase the influence of the stakeholder groups with most resources at their disposal and thus generally suffer from asymmetric power relations. It is an open question whether such imbalances of power are an inherent quality of multi-stakeholder

processes or if this model can be designed in ways to create relevant opportunities for social participation and increase the democratic quality of transnational policy making. A related question concerns the long term performance of multi-stakeholder processes. To what extent can the findings of Tamm Hallström and Boström (2010) on the increasing bureaucratisation of multi-stakeholder standard setting be generalized and is it possible to prevent such developments? A last aspect refers to the relationship between multilateral and multi-stakeholder processes. In Internet governance there is some evidence suggesting that the interplay of multilateral and multi-stakeholder processes has positive effects for the quality of the policy discourse and its potential outcome. However, a comparative perspective would be needed to confirm or qualify this impression. Although multi-stakeholder processes have gained relevance in the transnational sphere, they still form a genuine research gap.

4.3 Evolution towards a cohesive policy domain

The scenario of a gradual constitutionalisation assumes that the policy scope of Internet governance will expand over time. Comparable to the development of environmental policy in the 1970s, which integrated a number of discrete measures and tasks previously addressed by separate bodies, Internet governance, too, may come to encompass a growing array of international policies and treaties such as free trade agreements, foreign and security policies, data protection or copyright reform with significant impact on digital communication. Integrating relevant policy issues into Internet governance would allow assessing, challenging or supporting them against constitutional norms relevant to the preservation of the global Internet and, as a side effect, improve the conditions for a culture of trust. However, little research has so far been done on the modalities and mechanisms of assembling heterogeneous policy issues into a cohesive policy domain. Comparative empirical studies may help to understand how transnational governance networks emerge, agree on a policy scope and acquire regulatory authority for it.

REFERENCES

Abbate, Janet (2000), Inventing the Internet. Cambridge: MIT Press.

Beck, Ulrich (2008), 'Reframing Power in the Globalized World', in: Organization Studies, 29(5), 793-804.

Boström, Magnus/Tamm Hallström, Kristina (2013), 'Global multi-stakeholder standard setters: how fragile are they?', in: Journal of Global Ethics, 9(1), 93-110.

Botzem, Sebastian/Hofmann, Jeanette (2010), 'Transnational governance spirals: the transformation of rule-making authority in Internet regulation and corporate financial reporting', in: Critical Policy Studies, 4(1), 18-37.

CIGI [Centre for International Governance Innovation]/Ipsos (2014), Global Survey on Internet Security and Trust (https://www.cigionline.org/internet-survey).

Chander, Anupam/Lê, Uyê P. (2015), 'Data Nationalism', in: Emory Law Journal, 64(3), 677-739.

DeNardis, Laura (2009), Protocol Politics: The Globalization of Internet Governance. Cambridge, MIT Press.

DeNardis, Laura/Raymond, Mark (2013), Thinking Clearly about Multistakeholder Internet Governance. Paper Presented at Eighth Annual GigaNet Symposium, Bali, Indonesia, October 21, 2013.

Drake, William J. (editor) (2005). Reforming Internet Governance: Perspectives from the Working Group on Internet Governance. ICT Task Force Series, United Nations Information and Communication Task Force.

Durkheim, Emile (1997 [1893]), The Division of Labor in Society. New York, Free Press.

Epstein, Dmitry (2012), The duality of information policy debates: the case of the Internet Governance Forum. Dissertation presented to the Faculty of the Graduate School of Cornell University. Cornell University.

Epstein, Dmitry (2013), 'The making of institutions of information governance: the case of the Internet Governance Forum', in: Journal of Information Technology, 28(2), 137-149.

Giddens, Anthony (1990), The Consequences of Modernity. Cambridge: Polity Press.

Gillmor, Dan (2014), A government ruled for net neutrality. Too bad it wasn't your government. The Guardian, 6 June 2014.

Hancher, Leigh/Moran, Michael J. (1989), Organizing regulatory space, in: Hancher, Leigh, Moran, Michael J. eds.), Capitalism, Culture, and Economic Regulation. New York: Clarendon Press of Oxford University Press, pp. 271-300.