V. Development of a "Global Cyberspace Framework" (GCF)

A. Introductory Remarks

The first four chapters have evidenced that the classical forms of rule-making can hardly cope with the challenges of cyberspace and that many new approaches of norm-setting have been developed without, however, establishing a systematic framework which could govern cyberspace. Obviously, such new regime is difficult to design and implement in view of the manifold requirements to be met in order to come to stable and reliable normative terms. Therefore, this concluding chapter does not promote specific rules to be adopted by legislators on a global or a national level but envisages drafting general principles suitable for application in a changing technological and social environment.

Without any doubt it is difficult to forecast the future as experience has shown for centuries. Prognostications and definitive statements are always risky in times of uncertainty. This assessment is true for social and natural sciences notwithstanding the fact that technical developments have been subject to anticipations that were quite correct as the following examples show:[619]

- Already in the fifteenth century Leonardo da Vinci who was not only a famous painter and thinker, but also a visionary, was sketching parachutes, helicopters, hang gliders, and even airplanes.[620] When engineers started to build the respective machines based on Leonardo's sketches some twenty to thirty years ago it became apparent that in fact the constructed machines did function as expected.
- The famous French novelist Jules Verne published a prophetic book in the year 1863, called "Paris in the Twentieth Century";[621] in this ambitious project Verne described new inventions that seemed to be unthinkable at the time of publication. In fact, the manuscript was lost for almost 130 years and was only published in 1994. At the time of its re-discovery, the surprised public was astonished to see that Verne predicted that Paris would have glass skyscrapers, air conditioning, television equipment, elevators, etc. within the following hundred years. Shortly after the mentioned book, Verne published two other

619 For an overview see also Weber, 2012b, 1/2.

620 For further details see Fritjof Capra, The Science of Leonardo: Inside the Mind of the Genius of the Renaissance, New York 2007.

621 Jules G. Verne, Paris au XXe siècle, Paris 1863, only published in 1994.

Co-Publication with Schulthess Juristische Medien AG

Published by Springer-Verlag GmbH Berlin Heidelberg 2015
R.H. Weber, *Realizing a New Global Cyberspace Framework*,
DOI 10.1007/978-3-662-44677-5_5

novels, namely "From the Earth to the Moon" (1865)[622] and "Around the Moon" (1870)[623], outlining numerous details of the missions of the US astronauts to the moon some hundred years later (1969). Verne predicted the size of the space capsule, the duration of the voyage and the weightlessness of the astronauts.[624] Notwithstanding the fact that Verne was not a scientist, he amassed a vast archive encompassing the great scientific discoveries of his time.

- In the year 1949 George Orwell gave a quite accurate forecast on the expected technological environment in the year 1984.[625] Particularly after Snowden's numerous revelations since June 2013 that made transparent the vast collection of data by secret services' entities and supervisory authorities, most individuals now do have the impression that "big brother is watching you".

Obviously, technologies are quickly changing the environment, thereby confronting mankind with partly unexpected challenges. To ensure that the legal framework for cyberspace is based on reliable technological foundations the following developments have to appropriately be taken into account:[626]

- Information technologies including cloud computing and big data analytics will increasingly become utilities ("mass technologies"). As for electricity or telecommunications, utilities are required in case of need; in principle, users do not care about the provider. Nevertheless, it should not be underestimated (mainly by natural science experts) that technological equipment', in particular robots, will not be able to perform certain human activities, at the forefront pattern recognition and exercise of common sense.[627] These human abilities enable and require the creation of multiple models that are more easily apt to meet the diverse forthcoming developments and to approximate future events.
- Fast technological developments are responsible for the acknowledgment of the so-called Moore's law saying that the number of components in integrated circuits doubles every year (later corrected to two years). However, queries have been raised regarding the viability of Moore's law in the long run. Gordon Moore himself, when asked about a possible collapse of the celebrated law named after him, predicted in the year 2005 that it would end in ten to

622 Jules G. Verne, De la Terre à la Lune, Paris 1865.
623 Jules G. Verne, Autour de la Lune, Paris 1870.
624 Kaku, 2011, 5.
625 George Orwell, Nineteen Eighty-Four, London 1949.
626 See also Weber, 2012b, 2/3
627 Kaku, 2011, 83; to the risk for humans of being (partly) replaced by machines see Lanier, 2013, 5/6.

twenty years.[628] Some futurists (Ray Kurzweil, Bruce Sterling, Vernor Vinge) who are of the opinion that this law will ultimately lead to a technological singularity expressed more fundamental concerns; in other words, the period in which progress in technology occurs becomes almost instant.[629] In addition, technology on its own is neither the cause of, nor a solution to a particular constellation of problems.[630]

- Looking from a general perspective of human development it can be argued that individuals seem to be in a transition phase from being passive observers of law to becoming the choreographers of nature and finally conservators of nature. As a consequence, human beings will have to be able to control objects of the environment and the technical equipment would need to have the ability to decipher an individual's wishes in order to subsequently carry them out.[631]

Another important aspect concerns the likelihood of a fundamental political influence exercised by new technologies. Science in general, if developed in a future-oriented way, can question political structures by causing an unsettling effect:[632] (i) A good historical example is the controversy between Galileo Galilei presenting the idea of a round world (thereby questioning religious assumptions) and the Catholic Church represented by the pope; in the year 1633 an inquisition ban on reprinting Galileo's work was released by the pope which was only lifted in 1718.[633] (ii) Recently, representatives of several social sciences' disciplines have expressed the opinion that the "Arab spring movements/revolutions" could not have happened without the available information technology instruments such as mobile phones and social networks.[634]

Drawing a preliminary conclusion from these observations it must be acknowledged that technology is also a social endeavor. Internet technologies in particular (as well as their legal implementation) are to be understood through the lens of social interpretation since they have an identifiable socio-legal effect beyond their direct contribution to the fabric of society.[635] As a consequence, this (last) chapter exploits the legal settlements that design the cyberspace environment.

---

628 See Manek Dubash, Interview, Techworld 2005, retrieved from http://news.techworld.com/operating-systems/3477/moores-law-is-dead-says-gordon-moore/.

629 See Ray Kurzweil, The Singularity is Near: When Humans Transcend Biology, New York 2005.

630 Franklin, 2013, 94.

631 See Kaku, 2011, 58.

632 Weber, 2012b, 3.

633 See John L. Heilbron, Censorship of Astronomy in Italy after Galileo, in: Ernan McMullin (ed.), The Church and Galileo, Notre Dame 2005, 279–304.

634 See the special issue of the International Journal of Communication, Vol. 5, 2011, 1435 et seq. with the title "The Arab Spring and the Role of ICTs".

635 Weber, 2012b, 3; Murray, 2007, 37–42.

B. Policy parameters for cyberspace rule-making

Discussions so far have shown that legal instruments are exposed to challenges in cyberspace and that the implementation of legal means must be executed with great care and prudence in order to avoid undesired effects. Before the basic parameters and the guiding principles of an international cyberspace framework will be analyzed it seems justified to assess the political visions of rule-making as well as their inherent scope and limits.

1. Political visions of rule-making

Looking at the experience of the last few years it seems obvious that the success of an appropriate legal framework governing the future of cyberspace depends on the ability of the policymakers to embrace new approaches using different tools from the still dominant and traditional model of command-and-control regulation.[636] Furthermore, the identification of underlying structures and the basic shortcomings as well as the assessment of the international legal order's rational potential merit greater attention.[637]

Usually, two visions of political power exist, namely (i) the dominance of State power and (ii) the power distribution.[638] State power is founded on the sovereignty concept; power distribution relies on a variety of stakeholders. Questions in assessing possible political systems refer to the structure of the international rule-making agenda, the extent and form of supra-state institutions and the role of sovereign States.[639]

Political forces have always intended to get involved in the organization and administration of cyberspace, irrespective of the fact that scientific communities and private actors were responsible for the main developments. The attempt of States to regain power became particularly obvious prior to and mainly during the World Conference on International Telecommunications (WCIT) in Dubai (December 2012); the advocates of a "cyber-sovereignty" approach raised their voices louder, expressing the opinion that for public interest and security reasons control

636 Weber, 2012b, 3; Weiser, 2009, 538/39 refers to a "multiparty contracting problem".

637 This theoretical discussion cannot be deepened hereinafter; for a recent overview see Altwicker/Diggelmann, 2014, 69 et seq.; to the constellations of regulatory instruments in global governance see Michèle Rioux/Nicolas Adam/Biel Company Pérez, Competing Institutional Trajectories for Global Regulation — Internet in a Fragmented World, in: Roxana Radu/Jean-Marie Chenou/Rolf. H. Weber (eds.), The Evolution of Global Internet Governance. Principles and Policies in the Making, Zürich 2013, 37, 49–54.

638 Klimburg, 2013, 1.

639 Weber, 2013, 95.

over the Internet should remain in the competence of national governments including the right to regulate the activities occurring in the Internet as far as accessible by the domestic population.[640] The negotiations in Dubai showed that some countries such as Russia, China or Saudi Arabia are attempting to subordinate the management of the Internet to governmental control, mainly by referring to security and public order interests, even if such a development would lead to a (national) fragmentation of the Internet. Quantitatively, the promoters of cyber-sovereignty had a slight majority amongst the ITU members in Dubai, thus also making it difficult to develop a moderate approach by introducing more flexibility in the decision-making processes.

At first, the differentiation between (i) the proponents of a liberal structuring of cyberspace, having confidence in a private-economic fulfillment of tasks with as little State interventions as possible and (ii) the representatives of a concept featuring national control interests, may appear rather insignificant.[641] However, this distinction points into the direction of different regulatory approaches, namely one in which the political power is increasingly distributed and includes non-state actors, and one in which State power is dominant.[642] After the WCIT, a binary global scene seems to have emerged, most of the developing world (with the exception of India) sided with the cyber-sovereignty advocates. The WCIT morphed into a "battle", partly (and problematically) even called a "digital cold war" of the liberal West against the rest of the world.[643]

The process of international regime formation was already confronted with diverging opinions in the past; insofar, the discussions at the WCIT did not come as novelty. Usually the globalists pleading for international legal harmonization are confronted with the objections of the skeptics; the respective general arguments are summarized in the following diagram *(Table 17)*:[644]

640 For further details see Weber, 2013, 98.

641 Weber, 2013, 101.

642 Klimburg, 2013, 1; see also Katherine Maher, The New Westphalian Web, Foreign Policy, February 25, 2013.

643 Weber, 2013, 101; for a detailed discussion of the political initiatives prior to and during the WCIT see Hill, 2013, 79 et seq.

644 See Antonova, 2008, 67/68, and Weber, 2009, 93.

	Globalists	*Skeptics*
Concepts	— One world, shaped by extensive, intensive and rapid flow of goods/ services/ data	— Internationalization, not globalization — Regionalization
Power	— Rise of multilateralism — Decline of Nation State — Erosion of State sovereignty, autonomy and legitimacy	— Nation State rules — Intergovernmentalism
Culture	— Emergence of global popular culture	— Resurgence of nationalism and national identity
Economy	— Transnational economy — Global informational capitalism	— Development of regional blocs — New imperialism
Inequality	— Growing inequality within and across societies — Erosion of old hierarchies	— Growing North-South divide — Irreconcilable conflicts of interests
Order	— Global civil society — Multilayered global governance — Cosmopolitanism	— International society of States — Political conflicts among States — Communitarianism

Obviously, the above diagram cannot be directly mirrored in cyberspace but it contains valuable elements. In addition, there is clearly no easy way forward to overcome the emerging tensions between the cyber-sovereignty and the civil society-inclusive approaches. Moreover, different routes exist and the choice of the way forward depends on the specific environment.[645] Generally, it can be said that the traditional understanding of political structures as command must be reflected by a new understanding which allocates to the rule-makers the incentive of inducing civil society to execute certain actions in the sense that people think about what to choose and what to do in a decentralized system.[646] Guiding principles for humanity do have a global nature, even if influenced by smaller entities; in other words, the absence of hierarchical structures and the fact that new issues are com-

645 Weber, 2013, 105.
646 Reed, 2012, 248 et seq.

plex must be acknowledged; flat structures on different appropriate levels facilitate decision-making by including the relevant persons and organizations at the actual point of their concern.[647]

The current challenges in the context of cyberspace regulation by nature require a broader and more collective decision-making than in a traditional State. As already Fukuyama mentioned, the normative order was established to limit discretion of exclusive State power.[648] Therefore, the movement towards global governance is unavoidable and the structure of international law will need some adaptions.[649] Global governance refers to a new order encompassing States, non-state actors, and new geographic and/or functional entities in a power-sharing framework.[650] The crucial point concerns the appropriate balance of power between sovereign States' governance and non-territorial and privatized mechanisms.[651]

Therefore, global governance must encompass collective efforts enabling the concerned persons to identify, understand, and address worldwide problems that go beyond the capacity of individual States to solve.[652] The respective efforts must acknowledge that changes with regard to the separation of the traditional power model (Montesquieu) seem unavoidable.[653] As a further insight it must be recognized that the failures attributed to the multilaterism approach cannot easily be remedied by a minilaterism concept, at least not in the – globally oriented – cyberspace field.[654] Consequently, different levels at which political theory may operate are to be taken into account: (i) A global framework needs to be combined with domestic political theory, i.e. it must be assessed to what extent notions of domestic importance are to be adapted at the global level, and if so, how it should be done. (ii) A global political theory must be able to provide guidance as to what principles should be adopted and which institutions should be put into practice. (iii) Finally, the question is to be tackled how general principles should be applied to specific issues.[655]

647 Weber, 2013. 106.
648 Fukuyama, 2004, 98/99.
649 To the discussion about the structure of international law see Altwicker/Diggelmann, 2014, 78–81.
650 Winchester, 2009, 22.
651 See also DeNardis, 2014, 23.
652 Weber, 2010a, 15.
653 For more details see Burkert, 2012, 100–109.
654 Brummer, 2014, 165 et seq. proposes a minilaterism approach in the fields of international finance and international trade.
655 Caney, 2006, 2/3.

In order to cope with the globalization of (inter-)governmental relations and governance, the political theorists are referring to the notion of "cosmopolitanism" which embraces three elements, namely individualism, universality, and generality.[656] A broad understanding of "cosmopolitanism" in decision-making procedures reflects and even extends the Kantian framework highlighting global distributive justice besides launching civil and political rights.[657] Future democratic iterations will make interconnectedness and interdependence deeper and wider; this development does not undermine democracy but shows the emergence of new political configurations.[658] In order to overcome the existing gap in the regulatory perceptions for cyberspace, it is necessary to strengthen the efforts (i) to establish appropriate structures and organizational elements for the implementation of decentralized decision-making procedures involving a variety of stakeholders and (ii) to implement adequate fora for debates and discussions.[659]

2. Scope and limits of rule-making approaches

The analysis of the different regulatory models, which can lead to a new legal order,[660] has shown that fresh approaches are needed in order to build an appropriate legal framework for cyberspace. If a regulatory need is recognized in cyberspace, the concerned members of civil society as well as businesses may not be satisfied with national legal provisions and may not be willing to wait for multilateral treaties. Consequently, as experience evidenced over the last two decades, soft law has spread out with the objective to fill the gaps emerging in traditional legal regimes; later, the vagueness of the soft law notion has led to the concept of informal law-making. However, even if these (new) models will play an important role in practice, such assessment does not suffice to build an appropriate legal framework as long as the models are not embedded into the international legal regime.[661]

Therefore, the identification of scope and limits of rule-making approaches and particularly the establishment of reliable pillars in a future cyberspace environment gain importance. In view of the reliability issue, light should be shed on different debated ideas:

656 Pogge, 1994, 89/90.
657 Lane, 2013, 22; see also Koskenniemi, 2005, 611.
658 See Benhabib, 2006, 74.
659 Weber, 2013, 113.
660 See above Chapter IV.A.-E.
661 Weber, 2012b, 7.

(i) As mentioned, any legal order has social impacts.[662] Therefore, the setting of a legal framework for cyberspace should consider realizing optimal conditions for a perfect society. Such an approach does have a long standing tradition: Almost five hundred years ago, in 1516, Sir Thomas Morus published the novel "Utopia", envisioning a paradise on a fictional island in the Atlantic Ocean.[663] Again in the nineteenth century, many social movements in Europe searched for various forms of utopia or utopian environments.[664]

During the last fifty years scholars have tried to better incorporate a utopian environment into the structure of legislative (national and international) frameworks. Forty years ago, autonomous cultural arrangements were qualified as "framework of utopia", thereby giving a structure to the utopian environment itself.[665] More recently, the eminent scholar Martti Koskenniemi assessed the structure of international legal reasoning through the lens "From Apology to Utopia", outlining the descriptive and normative concerns of the international legal order. Koskenniemi argues that in respect of the relevant issues grammar has not changed extensively, but new topics such as human rights and environment emerged.[666] Nevertheless, even with a higher degree of concretization, "utopia" is not an ideal concept for the design of an appropriate cyberspace framework since it is difficult to identify sufficiently clear contours in this concept and since it seems quite impossible to draw structural elements, possibly aiming at future developments, from this concept.[667]

(ii) Nearly half a century ago, Louis Henkin phrased the often cited sentence that "almost all nations observe almost all principles of international law and almost all of their obligations all of the time".[668] This assertion does not seem very convincing anymore.[669] Compliance is not only doubtful in the military and political arena (for example in view of interventions into the sovereignty of other countries) but also in the cyberspace field; more and more States undermine the globality of the Internet by interfering into the free cross-border information flow, thereby jeopardizing the freedom of expression through a national fragmentation of the Internet, or by applying wide-spread communication surveillance mechanisms, thereby violating the right of privacy, both fundamental human rights

662 See above III.C.1.
663 Thomas Morus, The Utopia, 2002, retrieved from http://www.idph.com.br/conteudos/ebooks/Utopia.pdf.
664 For further details see Herbert George Wells, A Modern Utopia, Leipzig 1905.
665 Robert Nozick, Anarchy, State and Utopia, Oxford 1974.
666 Koskenniemi, 2009, 562–573.
667 Weber, 2012b, 7; see also MacKinnon, 2012, 232–236.
668 Henkin, 1979, 47.
669 Weber, 2012b, 8.

being guaranteed by international and regional legal instruments (for example the UN Convention on Human Rights).[670]

Moreover, it cannot be overlooked that the increasingly dense framework of rules with different legal qualities rather leads to uncertainties than clear acknowledgments in respect of compliance with (international) rules by States.[671] At best it can be said that the international legal framework provides instruments for reconciling conflicting interests and settling disputes.[672] In addition, it should not be overlooked that narrowly designed and oriented rules usually are not apt to comply with the challenges of rapidly changing technologies;[673] as a consequence, a polycentric regulatory approach should be chosen.[674]

Other models are based on specific compliance aspects: For example, Chayes/Handler express the opinion that States obey international rules not because they are threatened, but because they are persuaded by the dynamic created in form of treaty regimes to which they belong.[675] Instead of persuasion (or reputation) the substantive fairness of international rules can also be considered as decisive element; particularly Franck relies more on fairness concepts than on managerial processes in the international domain.[676]

Both approaches, however, underestimate procedural elements, i.e. the complex processes of institutional interactions in a transnational legal setting as well as the processes of internalization of global norms.[677] Apart from procedural objections, structural reasons also do not support the ideas of persuasion and fairness.[678] Furthermore, from a historical perspective, Hobbes' famous concept, outlined in his Leviathan,[679] based on the assumption that law is to be defined in political terms, which means in terms of power, does not fit the structures of cyberspace anymore since the regulatory environment is linked to the multistakeholder participation (and the civil society's involvement in the decision-making processes).[680]

670 Jørgensen, 2013, 37–41.
671 Weber, 2012b, 8.
672 Kaufmann, 2011, 1199; Howse/Teitel, 2010, 127 et seq.
673 See above III.C.1.
674 See above IV.E.2 and Senn, 2011, 186 et seq.
675 Chayes/Handler Chayes, 1998.
676 Franck, 1995, 1 et seq.
677 See Weber, 2012b, 8; Shaffer, 2010, 10 et seq.; Koh, 1997, 2599, 2602, 2645/46, 2655/56.
678 See Howse/Treitel, 2010, 128–130.
679 Hobbes, 1651.
680 Weber, 2012b, 8; Frydman, 2004, 231; to the multistakeholder approach in particular see below V.C.3.

3. Structured rule-making processes (multi-layer governance)

The design of a legal framework must be based on the acknowledgement that its principles are to be embedded into the global governance debate. This concept is described as new "order, characterized in part by porous borders and power sharing amongst States, non-state actors, and new geographic and functional entities".[681]

a) Principles of a multi-layer approach

Notwithstanding the manifold facets of global governance the widely accepted statement might be made that "there is no such thing as" a sole global governance.[682] Moreover, global governance has to be looked at from a multi-layer (multi-level) perspective,[683] i.e. different layers (levels) are to be taken into account depending on the actors involved, the topics at stake and the problems to be solved.

Multi-layer governance requires the development of common foundations applicable to all relevant layers, while at the same time it must respect diversity and pluralism in order to be commensurate with the respective level of integration.[684] An important aspect of this movement is the acknowledgment of the need for increased cooperation when trying to achieve a multi-layer consistency.[685] Therefore, multi-layer governance addresses normative guidance as to how relations between different layers of governance should be framed in a coherent and not fragmented manner, encompassing both analytical and prospective issues in building upon observations of legal phenomena.[686] The definition of the proper interaction of the different levels has a direct impact on an ideally coherent regulatory architecture of multi-layer governance, i.e. multi-layer governance "proposes a process and direction".[687] If common legal rights and obligations can be identified, the ensuing legal framework enjoys special legitimacy, which is essential for the operation and effectiveness of law.[688]

---

681 See Winchester, 2009, 22.
682 Weber, 2012b, 7.
683 For a general overview see Weber, 2010c, 689/90.
684 Cottier, 2009, 656/57.
685 See Breining-Kaufmann, 2005, 118.
686 Weber, 2010c, 689.
687 Cottier, 2009, 656.
688 Weber, 2010c, 690; Cottier, 2009, 659/60.

Since regulatory frameworks evolve within a given societal and political context,[689] private regimes are part of the overall legal design, particularly if their weaknesses can be eliminated or at least diminished;[690] these regimes have a certain place in a multi-layer structure, if developed with the objective of establishing an appropriate institutionalization, based on broad initiation and wide building support.[691] Other elements are the significance of the institutional environments, the dynamics of relationships, and how non-sovereign bodies respond to multiple legitimacy claims in complex and dynamic regulatory situations.[692] In relation to non-state or private networks and organizations, the governance emphasis should not be based on normative validity; moreover, the trend towards efficiency and public value maximization also needs to be supported.[693]

b) Development of normative multi-layer governance principles

Multi-layer governance is a topic, which is discussed in many fields outside cyberspace regulation, particularly in the field of financial markets.[694] The inclusion of several layers into the regulatory considerations is a consequence of the acknowledgment that State law is not solely capable of designing an appropriate legal framework anymore and that private and semi-autonomous rule-making can make valuable contributions to the implementation of a reasonable normative order. However, the multi-layer structure should not be understood as a hierarchical order but as a polycentric network of participating entities.

Notwithstanding the fact that some elements, which define multi-layer governance in a global context, seem diffuse, important core themes can be distilled:[695]

- Future regulatory problems by their nature will require broader and more collective decision-making than applied in traditional regimes; global interactions necessitate the establishment of a multistakeholder regime.[696]
- Responses to new problems are complex on the global level and flat structures on different sub-levels facilitate decision-making by including the relevant persons and organizations in the process at the actual point of their respective concern.

---

689 Following Weber, 2012b, 7.
690 To the weaknesses of private regimes see above II.C.4 and the examples given by Tambini/Leonardi/Marsden, 2013, 296/7.
691 Bernstein/Cashore, 2007, 347–371.
692 Black, 2008, 137–164.
693 Senn, 2011, 228 and 259.
694 See Weber, 2010c, 689/90.
695 Waters, 2009, 33; Weber, 2010c, 692.
696 See below V.C.3.

- The ongoing processes of globalization and integration necessarily lead to an altered perception and notion of State sovereignty and ask for new elements of legitimacy in this respect.

Furthermore, globalization is not a clearly defined term. Commercial globalization reflects the fact of having increased transnational businesses and economic activities. Cultural globalization addresses the issues related to the manifold social policies. Legal globalization looks at the harmonization of the States' normative orders or the implementation of cross-border legal rules.

In this context, the new dimensions of global administrative law merit further attention since this concept looks at institutional differentiations and elaborated procedural techniques.[697] Assessing the dichotomy of regulatory sources and the emergence of new regimes introduced by civil society, adapted transnational concepts need to be developed in the administrative law field.[698] Institutions can lead States to a more cooperative behavior than they otherwise might have, building mutual connections from peripheral points, in federative or associate forms.[699]

Hand in hand with the development of global administrative law the regulatory system and design has increasingly accepted the importance of public notice and consent procedures.[700] Recently the fruition of these ideas was mainly seen in connection with the execution of functions by the G-20 in respect of financial regulation.[701] However, lessons from the respective experiences can also be drawn for other segments of society.[702]

c) Macro-legal and micro-legal level approach as alternative

Another theoretical approach does not differentiate between a multiple of layers, but between the macro-legal and the micro-legal level. The foundation of this approach is based on the assessment that the legal character of different objects might not be identical. Some scholars have coined the term of "yet unidentified legal objects" in the context of the attempt to develop a global law, encompassing the objects, which have a "doubtful" or "controversial" legal character.[703] Such objects require the acceptance of a certain degree of normativity since they are pragmatically implemented (in practice).[704] Departing from the well-known dis-

697 Kingsbury/Casini, 2009, 319 et seq.
698 See also Senn, 2011, 71.
699 See also Cassese, 2005, 674; Senn, 2011, 215/16.
700 Barr/Miller, 2006, 41.
701 Wouters/Ramopoulos, 2012, 12 et seq.
702 Weber, 2012b, 7.
703 Frydman, 2012, 17, 20.
704 Duss, 2012, 21.

tinction between «objective law» and "subjective rights" the approach differentiates between the macro-legal and the micro-legal level;[705] thereby, the model provides for the possibility to assume a micro-legal concept of normativity without the need to implement a macro-legal framework.[706]

This approach has been hardly tested in cyberspace reality but it appears possible that the respective ideas can be made fruitful in connection with the implementation of appropriate organizational rules in social communities. On the one hand, for example, moral norms falling under the notion of "netiquette"[707] are relevant for online macro-communities.[708] On the other hand, communities built around email and discussion lists or bulletin board systems could be seen as micro-communities, however, such narrow understanding hardly corresponds to the perceptions of the users themselves.[709] Even if the classification of online micro-communities causes major difficulties, a certain taxonomy can be done, for example by distinguishing commercial communities, online/offline communities, gaming communities, cafe communities, knowledge communities, and creative communities[710], allocating to each class a primary purpose. However, from a regulatory perspective this taxonomy does not provide for major substantive insights.

4. Legitimacy of cyberspace rule-making

The multi-layer concept and the hereinafter discussed multistakeholder participation approach challenge the traditional legal and political understanding of legitimacy as a notion primarily relevant to sovereign States as subjects of the international legal order according to the prevailing doctrine. As a consequence, several questions arise:[711] Who can be a legitimate stakeholder in a multi-layer framework (for which layer)? Do the same criteria for legitimacy apply in a multi-layer regime as in the traditional regime? What importance does legitimacy have in a multi-layer environment? Is not the inclusion of many stakeholders legitimizing enough?

Legitimacy can be perceived as a justification of authority giving the governed the feeling that their own values are represented in a decision-making context;[712] an

705 See also Weber, 2012b, 7.
706 Frydman, 2012, 21.
707 For examples see above II.C.5.
708 See Murray, 2007, 141–144.
709 For a detailed description of the various studies done in this field see Murray, 2007, 145–148.
710 This is the approach of Murray, 2007, 148.
711 See also Weber, 2009, 105/06.
712 Weber, 2002, 46/47.

authority's "right to rule" is to be traced back to a translation of the Latin word "legitimus" as meaning "lawful, according to law".

In the sociological perspective of Max Weber three models *("Idealtypen")* of governance exist, the rational or legal, the traditional and the charismatic authority; legitimacy in a wider sense also encompasses an ethical-philosophical dimension, which heaves legitimacy above positive law.[713] Some scholars differentiate between "normative theories" on legitimacy, which set out general criteria for evaluating the right to rule, and "empirical theories", which focus on belief systems of those subject to government.[714] As a result, legitimacy can either be justified by formal ideas as the rule of law rationale (legality) or by substantive value rationality based on morality and justice.[715]

According to a source-oriented perception of legitimacy, an authority may be qualified as legitimate when referring to democratic States, which base their authority on the "demos", the public.[716] In reality, procedural aspects within the different governing entities may enhance the legitimacy of policy-making decisions in cyberspace.[717] This comprehension of legitimacy can be traced back to Luhmann who argued that legitimization could be effected through adequate procedures.[718] Franck described legitimacy as "the aspect of governance that validates institutional decisions as emanating from a right process. What constitutes right process is described in a society's adjectival constitution or rules of order, or is pedigreed by tradition and historic custom".[719]

The procedural approach[720] may be complemented by a result-oriented type of legitimacy, i.e. a substantive conception which looks at the outcome of the legitimizing procedures; this result-oriented approach depends on the values deemed as "right" by the stakeholders concerned, thus in part justifying them as legitimizing sources.[721] But such an approach reveals a particular difficulty, because it relies on subjective perceptions of legitimate values, which are related to cultural and societal differences and evolve over time.[722] For such reasons, Habermas tried to link the procedural aspects with specific notions of contents ("discourse princi-

713 For a detailed discussion of Max Weber's concept see Weber, 2009, 110.
714 Clark, 2005, 18.
715 Clark, 2005, 19.
716 Habermas, 1992, 117.
717 Weber, 2009, 110.
718 Luhmann, 1975, 9–53.
719 Franck, 1995, 1.
720 To the elements of the procedural legitimacy (transparent and accountable operations) see also Brownsword, 2012, 257/58.
721 Weber, 2009, 110/11.
722 Clark, 2005, 13.

ple"), assuming that just those norms can claim validity that receive the approval of all potentially effected people, insofar as they participate in a free and rational discourse.[723] The problem with the discourse principle, however, consists in the fact that it is challenged by particular aspects of fair processes of consensus-building.

Legitimacy must also be measured in light of constitutional values and principles. Such a constitutional approach to cyberspace regulation, based on particular architectural principles, could provide important inputs. Clark specifies "three cognate concepts — legality, morality, and constitutionality", which are set to "mark out the terrain within which the practice of legitimacy tends to take place".[724] Legitimacy is thereby perceived as a reconciling norm, enabling consensus on how these three elements can be accommodated amongst each other.[725] In addition, legitimacy should be assessed from the perspective of regulatory purposes and standards, regulatory instruments, regulatory effectiveness, and regulatory connection.[726]

Such perceptions of legitimacy emphasize the origins of the concept in political sciences, which – in contrast to cyberspace governance – does not specifically focus on States. As a "virtual province", cyberspace is mainly "managed" through a bottom-up approach with a large number of stakeholders; apart from this fact, with international law gaining importance, legitimacy questions are becoming weightier not only for the international society in general, but also for the stability of the international order.[727]

723 Habermas, 1992, 161.
724 Clark, 2005, 19.
725 Clark, 2005, 20.
726 For more details see Brownsword, 2012, 258–264.
727 Weber, 2009, 111; Clark, 2005, 12–17.

C. Guiding principles of a Global Cyberspace Framework

1. Formal/procedural principles of a Global Cyberspace Framework

a) Need for a dynamic and flexible approach

The fast technological developments make it necessary to apply a dynamic and flexible approach in the regulatory design of a global cyberspace framework. The traditional way of norm-setting does not meet the requirements of a fast moving environment anymore. State legislators often do not have sufficient "technical" knowledge of the matter to be regulated and are therefore exposed to industry lobbyists. Furthermore, the legislative democratic process is usually long and the risk exists that legal norms will be enacted and implemented only at a time when technology has already changed (so-called regulatory lag).[728]

User dynamism can also be seen in a competitive market environment: As experience in the online world has shown, network platforms with interactive users resemble (dynamic) communities rather than two-sided versions of perfectly competitive markets.[729] User dynamism within a community is beneficial in terms of generating content, creativity, and quality accounts for a larger share of value on these platforms.[730]

A dynamic and flexible approach should lead to a taxonomy, which allocates functional areas and tasks to specific institutional actors being most apt to deal with the respective issues. DeNardis/Raymond recently developed such taxonomy for the specific area of Internet governance; this taxonomy may serve as example how relevant issues of cyberspace and the corresponding institutional actors can be structured *(Table 18)*.[731]

728 Weber, 2002, 59.
729 Mehra, 2011, 905.
730 Mehra, 2011, 905/06 and 952.
731 DeNardis/Raymond, 2013, 4/5.

Functional Area	*Tasks*	*Primary Institutional Actor*
I. Control of "Critical Internet Resources"	Central Oversight of Names and Numbers	ICANN, lANA, US DoC
	Technical Design of IP Addresses	IETF
	New Top-Level Domain Approval	ICANN
	Domain Name Assignment	Internet Registrars
	Oversight of Root Zone File	US DoC/NTIA
	IP Address Distribution (allocation/assignment)	lANA, RIR, LIR, NIR, ISP
	Management of Root Zone File	lANA
	Autonomous System Number Distribution	lANA, Regional Internet Registries
	Operating Internet Root Servers	VeriSign, Cogent, others
	Resolving DNS Queries (Billions per Day)	Registry Operators (VeriSign, others)
II. Setting Internet Standards	Protocol Number Assignment	lANA
	Designing Core Internet Standards	IETF
	Designing Core Web Standards	W3C
	Establishing Other Communication Standards	ITU, IEEE, MPEG, JPEG, ISO, others
III. Access and Interconnection Coordination	Facilitating Multilateral Network Interconnection	Internet Exchange Point Operators
	Peering and Transit Agreements to Interconnect	Private Network Operators, Content Networks, CDN
	Setting Standards for Interconnection	IETF
	Network Management (Quality of Service)	Private Network Operators
	Setting End User Access and Usage Policies	Private Network Operators
	Regulating Access (e.g. Net Neutrality)	National Governments/ Agencies

Functional Area	*Tasks*	*Primary Institutional Actor*
IV. Cybersecurity Governance	Securing Network Infrastructure	ISP, Network Operators, Private End User Networks
	Designing Encryption Standards	Standards-Setting Organizations
	Cybersecurity Regulation/ Enforcement	National Statutes/Multilateral Agreements
	Correcting Software Security Vulnerabilities	Software Companies
	Software Patch Management	Private End Users
	Securing Routing, Addressing, DNS	Network Operators, IETF, Registries
	Responding to Security Problems	CERT/CSIRT
	Trust Intermediaries Authenticating Web Sites	Certificate Authorities (CA)
V. Information Intermediation	Commercial Transaction Facilitation	E-Commerce Sites, Financial Intermediaries
	Mediating (of) Government Content Removal Requests (Discretionary Censorship)	Search Engines, Social Media Companies, Content Aggregation Sites
	App Mediation (Guidelines, Enforcement)	Smartphone Providers (e.g. Apple)
	Establishing Privacy Policies (via End User Agreements and Contracts)	Social Media, Advertising Intermediaries, Email Providers, Network Operators
	Responding to Cyberbullying and Defamation	Content Intermediaries
	Regulating Privacy, Reputation, Speech	Statutory and Constitutional Law
	Mediating Govt. Requests for Personal Data	Content Intermediaries, Network Operators

Functional Area	*Tasks*	*Primary Institutional Actor*
VI. Architecture-Based Intellectual Property Rights Enforcement	Domain Name Trademark Dispute Resolution	ICANN UDRP, Registrars, Accredited Dispute Resolution Providers
	Removal of Copyright Infringing Content	Content Intermediaries
	Algorithmic Enforcement (e.g. Search Rankings)	Search Engine Companies
	Blocking Access to Infringing Users	Network Operators/ISP
	Domain Name System IPR Enforcement	Registries/Registrars
	Regulating Online IPR Enforcement	National Statutes, International Treaties
	Standards-Based Patent Policies	Standards-Setting Organizations
	Enacting Trade Secrecy in Content Intermediation	Search Engines, Reputation Engines

b) Need for a user-centered and community-related approach

Due to the lack of equivalence,[732] a replication of the physical world model is not possible in cyberspace.[733] Obviously the most serious consequence of embedding the wrong (business) model in cyberspace rule-making is its effect on the behavior of those who are subject to the law: Cyberspace participants may adopt behaviors which they believe will enable them to comply with the respective cyberspace rules, but these rules are often different from what the rule-makers originally intended.[734] Instead of purely replicating physical world models the online rules are to be designed in a way which addresses the needs and requirements of cyberspace communities, i.e. the approach must be user-centered and community-related in order to be suitable for cyberspace.

The user-centered approach may be described in short as follows: "Digital information is really just people in disguise".[735] In more moderate words it could be said that persons and information about them are very closely linked in cyber-

732 For a detailed analysis see Reed, 2010, 248 et seq.

733 See the detailed analysis (incl. the aspects of guessing wrong and rigging the market), underlined by many examples from the (mainly European Union) legislation, outlined by Reed, 2012, 158 et seq.

734 Reed, 2012, 170.

735 Lanier, 2013, 15.

space. On the basis of the information available online a clear picture of an individual is usually identifiable; therefore, the individual must have a direct influence with regard to the design and contents of such information. The user-centered approach includes the task of rule-makers to design a normative order for the benefit of the "citizens" of cyberspace.[736]

Openness also encompasses the need to implement neutral rules not favoring any specific (societal) model, i.e. rules based on a clear identification of the regulatory objectives; this process helps to release rules seeking to persuade cyberspace stakeholders to comply with them, not impose laws with command and control functions.[737] A particular measure in the neutral rule-making context is the realization of the network neutrality principle[738] that also needs regulatory action in transparency, switching and contract exit.[739]

Furthermore, the fundamental rights of individuals are only guaranteed if several specific issues are properly addressed:[740] (i) What measures should be taken to create greater transparency and dialog between consumer groups, other civil society stakeholders, and standards experts? (ii) How can it be ensured that the benefits of rapid standards-making are maintained even with the additional scrutiny suggested in increasing multistakeholder arrangements?

A stronger emphasis on user-orientation has been expressed for example in the context of privacy protection. Cyberspace users should be provided with understandable and (in the light of the good faith principle) acceptable terms of service including options to influence the collection of personal information as follows *(Table 19):*

Example: Privacy

The following general principles are to be considered as milestones of an online privacy system:[741] (i) Individuals should have the choice of sharing or not sharing their information. (ii) The technical system must be designed in a way that choice can be easily executed by the individuals. (iii) Individuals whose information is used by third persons are to be notified about such use. (iv) The legal framework should provide means to verify whether the information is correct and in compliance with existing privacy policies. (v) The legal framework must provide mechanisms that ensure compliance with applicable privacy policies and give recourse for legal action.

736 See also Kulesza/Balleste, 2013, 1326.
737 See Reed, 2012, 173–178 giving many examples from legislations not taking into account the mentioned fact.
738 See below V.C.4.c)(i).
739 See Brown/Marsden, 2013, 185/86.
740 See Brown/Marsden, 2013, 200.
741 Weber, 2012c, 281.

The user-orientation of rule-making can also be seen in the recent Recommendation 2014/6 of the Council of Europe releasing a Guide to human rights for Internet users (April 2014).[742] Amongst others, users should receive support to understand and effectively exercise their human rights online in case their freedoms have been restricted and interfered with; furthermore, users should be empowered to use the Internet as participatory form of democratic life (No. 4).

An interesting user-centered approach has been developed by Brown/Marsden who argue that the term "user" as such would correspond to a poor description of the potential creativity of the individual user in cyberspace; rather the (in fact ugly) term *prosumer* (the online creator, after Toffler[743]) should show "the potential for the individual to move far beyond a caterpillar-like role as a producer of raw silk and encompass their ability to regenerate into a butterfly or a moth".[744] Reality evidences that the verb "to surf" is indicating the user-generated agenda of the prosumer, as does the weaving of the web by billions of prosumer-created sites.[745]

A partly similar approach has been outlined by Braithwaite/Drahos, pleading for the transformation of the consumer movement into a pro-competitive constituency.[746] Since the consumer movement has credentials in competition law and policy it could offer trained vigilance for regulatory transformation that diminishes monopolization and enhances economic efficiency, thereby simultaneously increasing the sovereignty of civil society.[747] In this understanding, consumer advocates, organized in epistemic communities, would constitute a distributed network of information workers who are competition watchdogs.[748]

2. Identification of the relevant substantive principles of cyberspace

A global legal framework for cyberspace regulation with a broader scope than Internet governance, which mainly looks at protocols, technical standards, and address allocation system issues, should identify the most relevant substantive principles and seek to find the appropriate regulatory mechanisms that are suita-

742 Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users of April 16, 2014 (adopted at the 1197th meeting of the Ministers' Deputies).

743 Alvin Toffler, The third wave, New York 1980.

744 Brown/Marsden, 2013, 184.

745 Brown/Marsden, 2013, 184.

746 Braithwaite/Drahos, 2000, 620 and 623–628.

747 Braithwaite/Drahos, 2000, 623.

748 Braithwaite/Drahos, 2000, 625; for further details of the concept see *ibid.*, 625–628.

ble for the implementation of a normative order. Such framework cannot be developed purely in an abstract way; moreover, the rule-makers must have an understanding of how cyberspace is actually used (or how an expected use can occur) in order to identify the behaviors, which the norms should attempt to influence.[749]

In theory, two groups of principles (with some grey zones) can be distinguished, namely (i) those principles of the real world which can be applied in cyberspace without major adjustments or amendments (for example many fundamental rights) and (ii) those principles which need significant adjustments or amendments in order to cover the particularities of cyberspace.[750] The inherent advantage of principles compared to legal norms consists in the fact that principles functioning as guidelines do not require strict compliance or observance.[751]

The list of possible substantive principles[752] is (or can be) quite long; as mentioned, sometimes the topics are relatively similar to the offline world, at other times completely new issues arise.[753] Notwithstanding the existing or lacking neighborhood of cyberspace norms to traditional provisions, however, there is no way that an easy analogy may be drawn. Even if some (vague) routes to meaningful equivalence between offline and online problems can be established, the importance of equivalence should not be exaggerated, but it might have a symbolic value since cyberspace users might be more inclined to follow an equally applicable general offline/online rule than two different rule-sets whose combination and outcome merely aspire to be equivalent.[754]

The objective of this book consists in the attempt to assess possible normative foundations of cyberspace regulation, not to discuss specific legal issues being of concern to cyberspace lawyers, not at least due to the fact that vast literature is available on most of these issues. Therefore, only a short overview to the substantive principles is given hereinafter.

The structuring of the substantive topics can be done in different ways, for example by distinguishing market entry, infrastructure stability, ownership and distribution systems (intellectual property rights, privacy), and content as broad category.[755] In order to exemplify the substantive topics by way of easily understandable charts without going into the details of a legal interpretation, the

749 Reed, 2012, 156.
750 See also Kulesza, 2012, xiv.
751 See Uerpmann-Wittzack, 2011, 1248.
752 Mathiason, 2009, 59, uses the notion "regulatory imperatives" instead of substantive principles.
753 A thorough discussion of the substantive topics is not the objective of this book; for a detailed description of current national practice see Kulesza, 2012, 85–124.
754 See also Reed, 2012, 119–121 and Reed, 2010, 248 et seq.
755 This approach has been chosen by Weber, 2002, 101–203.

categories chosen by Brown/Marsden will be shown in form of an overview. The five substantive topics discussed are (i) privacy and data protection[756], (ii) copyright[757], (iii) censorship/filtering[758], (iv) social networking services[759], and (v) smart pipes.[760]

The main merits of the classification of Brown/Marsden can be seen in the fact that special attention is allocated to social networking services and smart pipes which opens the possibility to specifically address new issues such as user-generated contents and their regulation[761], the specific data protection requirements for social networking services[762] and the regulatory problems related deep pocket inspection[763]. However, some important substantive issues are not covered by this classification, for example the general application of human (fundamental) rights in cyberspace[764], the provisions on electronic commerce[765], the rules related to the liability of Internet service providers,[766] or the legal environment for cybersecurity.[767]

The mentioned five substantive topics[768] can be put into relation with the relevant impact and policy driver issues. The respective diagram allows drawing lessons for public policy and market failure as follows *(Table 20)*:[769]

[756] Brown/Marsden, 2013, 47–68; see also Reed, 2012, 158–163; Kulesza, 2012, 54–62; for a recent detailed analysis of the international perspective see Bygrave, 2014.

[757] Brown/Marsden, 2013, 69–91; see also Murray, 2007, 169–202; Reed, 2012, 152–155; Kulesza, 2012, 33–41.

[758] Brown/Marsden, 2013, 93–116; see also – under the heading digital content – Murray, 2007, 205–229.

[759] Brown/Marsden, 2013, 117–138.

[760] Brown/Marsden, 2013, 139–162; to the systems convergence in particular see Kulesza, 2012, 49–54.

[761] Brown/Marsden, 2013, 126–128.

[762] Brown/Marsden, 2013, 134/35.

[763] Brown/Marsden, 2013, 146–148.

[764] To this topic see Kulesza, 2012, 44–49; Jørgensen, 2013.

[765] To this topic see Kulesza, 2012, 69–75.

[766] To this topic see Tambini/Leonardi/Marsden, 2008, 6–9 and 14–19; Kulesza, 2012, 62–65; Lipton, 2012, 144 and 147/48, re-conceptualizes cyberlaw mainly from an Internet service provider angle which appears to be too narrow as a perspective.

[767] To this topic Kulesza/Balleste, 2013, 1313/14 with further references.

[768] To the basic considerations for doing the five case studies see Brown/Marsden, 2013, 18/19 and 163 et seq.

[769] This diagram is based on Brown/Marsden, 2013, 168/69.

	Data protection	Copyright	Censorship/ filtering	Social networking	Smart pipes
Social impact of technology	Bandwidth, processing capacity, storage scope, surveillance	Digital reproduction at marginal cost, peer-to-peer nets, cyberlocker sites	Ubiquitous use of broadband, widespread use of blogs, private censorship, governmental surveillance	Mass diffusion of information, need for protection (children, etc.)	Monitoring of traffic, mobile broadband, streaming video
Policy drivers: entry barriers, networks, scale effects, competition	Single market in data flows, data hoarding by enterprises and governments	Incentivation of creativity, granting of exclusive rights, highly concentrated markets (music, film, software)	Entry costs through technology for blocking, traffic monitoring enables surveillance	Costs of providing safer environment, tipping effect of dominant network	Quality-of-service technology imposes network costs (but reduced by scale economies)
Fundamental rights in policy design	International legal instruments available (ICCPR, ECHR)	Right to remuneration and moral right accepted	Lack of due process and appeal, little democratic scrutiny	Little effective government policy, mainly private actor business model	Limited regulatory oversight and rights-based discussion
Lessons	Privacy as key human right, to be protected by government	Higher protection of creators' rights at the expense of freedom of speech/privacy	Improved transparency needed; focus on content producers desirable in the long term	Only self-regulation	Risk of implementation of invasive systems, telecom regulations with too limited perspective

The five substantive issues can also be related to the institutional political economy of cyberspace regulation showing an interesting dialogue between property rights holders and governments as illustrated in the following diagram *(Table 21)*:[770]

[770] This diagram is based on Brown/Marsden, 2013, 170/71.

	Data protection	Copyright	Censorship/ filtering	Social networking	Smart pipes
Key actors: national, global, regional	Data protection regulators, consumer protection agencies, coordination in EU, APEC, etc.	Rightsholder associations, State legislators (US, EU, Japan) and international instruments (WIPO, ACTA)	ISPs, multinational content companies, user groups, multinational coders (WWW Consortium)	ISPs, intermediaries, local user groups, child protection groups, coders in Silicon Valley	Telecoms regulators, ISP, intermediaries, content companies, surveillance-industrial complex
How legitimate and accountable?	If legislative, democratically accountable, less so with self-regulatory solutions	Much policy laundering, forum shifting, exclusion of civil society and developing world	Limited transparency and accountability, remote engineering ethics	Some control by user-generated regulation, opaque terms and application means	Parliamentary supervision of telecom regulators, less so with self-regulatory solutions
Multistake-holderism	Internet governance through IGF, RFID process	Civil society involvement in WIPO, actions against ACTA	Little representation for free speech organizations (except in hotline governance)	Little formal multistake-holder consultations by corporates	Limited activities of stakeholders in telecoms regulatory environment
Key technical actor buy-in	Apple Safari, Firefox (DNT), privacy framework of RFID industry	Trusted Computing Group (TCG) and operating system vendors with limited effect involved, partial role of ISP	ISP-level filtering, need for standards and best practices	More open environments needed, prevention of high-walked gardens	Corporate vendors and mobile industry support quality-of-service, technical opposition given
Lessons	Strong intervention from legislators/ regulators is needed	Code instead of business innovation, limitation of freedom of expression, low multistake-holder involvement	Private censorship, limited governmental initiatives, control of "critical" material	Ineffective user-generated regulation, civil society ineffective	Little traction for policy initiatives, some initiatives of technical community

A further perspective concerns the various layers of protocol stack, not merely the application layer, which can be mirrored against the five case studies according to the following diagram *(Table 22)*:[771]

	Data protection	**Copyright**	**Censorship/ filtering**	**Social networking**	**Smart pipes**
Layer	RFID focus, browser code (do not track, cookies), privacy by design, privacy impact assessment	Failure of technological protection measures, ISP blocks, three-strikes	Application or network or both, supported by filtering software	Application and platform	Network or transport-layer
Location (manufacturer, ISPs, servers, clients)	Software and system architects	Previously hardware and software vendors, now ISP	Transport-level filters and clients filters	Server side with some mobile-based features	DPI solutions (hardware/ software vendors), traffic management solutions
Enforcement of code	Threat of data protection rules' enforcement	Ban of devices and circumvention measures	"Plug pulling", Green Dam local filter, Golden Shield national solution	Terms of use (amended by contractual terms with third parties)	Termination monopoly of ISP, nontransparent terms, competition regulation

A specifically important perspective concerns the outcomes and divergences of the five substantive issues in respect of key parameters of cyberspace regulation as of the following diagram *(Table 23)*:[772]

[771] This diagram is based on Brown/Marsden, 2013, 176.
[772] This diagram is based on Brown/Marsden, 2013, 179/80.

	Data protection	Copyright	Censorship/ filtering	Social networking	Smart pipes
Transparency	Limited impact of opaque privacy policies and user education	Unclear causation: Does more transparency lead to more just solutions?	Private block lists, no generic reporting duty on ISP	Often obscure in software updates and privacy policy changes, little evidence of good practice	Creating greater transparency through regulation
Enforcement	Data breach requirements and code solutions, limited effect of State enforcement	Problem of second user, business models and licenses effective in enforcement, three-strikes disproportionate	Private censorship limits user rights, put-back "enforcement"	Nudges and defaults (not individual reuses of data) useful ("distributed enforcement")	Network neutrality as solution to prevent protocol and application blocking
Inter-operability	Cross-border-adequacy assessments drive interoperability	DRM closes off interoperability	Cleanfeed instead of DNS blocking	Portability not sufficient	Limited transparency related to adaption of vender off-the-shelf solutions to ISP
Efficiency	Efficiency by internalized data controller self-enforcement?	New business models required	Source treatment: Tackling producers not blocking views	Improvement of corporate governance conformity needed	Co-regulation between legislators and industry desirable

3. Realization of multistakeholder participation

Without any doubts, civil society is the most active user of the Internet and therefore the most affected player; in the meantime, practically all aspects of the Internet have an impact on the daily life of civil society. Therefore, whether the organization of the Internet, its governance, access, operability or other topics are concerned, the understanding of members of civil society and non-state actors has to be taken into account.[773] This concept of including all possibly concerned actors in a participatory framework is now usually called multistakeholder model.

[773] Weber, 2011a, 6–8; Weber/Weber, 2009, 94.

For the time being, the multistakeholder discussion is mainly of a descriptive nature. Further research should rather concentrate on normative aspects.[774]

a) General foundations

Internet governance is not the first field attempting to implement multistakeholder models. Participatory democracy having directed the way for multistakeholder participation can already be found in the debates of economic governance models.[775] Furthermore, the realization of the interests of global public goods requires the involvement of all stakeholders concerned.[776]

Multistakeholder participation must be designed in view of the applicable social and environmental conditions. Commonly used evaluation criteria encompass the following aspects:[777]

- *Level of the standards:* The level issue can concern different objectives to be realized, for example high technical security standards or limits to living standards.
- *Completeness of the standards:* The completeness aspect depends on the question whether the standards refer to multiple issues or are limited to a single issue only.
- *Market coverage:* The broader the market coverage, the more likely is a widespread functionality of the multistakeholder involvement.
- *Accountability:* It is important to ensure that the standards contain regulations regarding the monitoring, reporting or verification of actions taken by an entity as well as potential sanctions.
- *Economic model:* A decentralization of economic decisions and an easy market access lead to a higher chance of having several stakeholders involved.
- *Extent of the involvement of stakeholders:* Entry barriers for stakeholders should be lowered and participation possibilities facilitated.
- *Impact of the existing standards on the decision-making of an entity:* Corporate governance frameworks as well as corporate social responsibility concepts are supporting the involvement of multistakeholders in participating in the entity‘s decision-making processes.

774 Normative aspects are discussed hereinafter, however, this book’s objective does not allow extending the considerations into all potential details and must remain the topic of another publication.

775 See Elinor Ostrom, Governing the commons: the evolution of institutions for collective action, Cambridge 1990.

776 See Weber/Menoud, 2008, 24–27; Doria, 2013, 119.

777 Van Huijstee, 2012, 45.

Already Aristotle explained the best regime to be a combination of various features for the sake of the commons, however, he did not perceive democracy as the mandatory best regime, but rather aristocracy.[778] In aristocratic regimes, only a few are able to act as representatives for the benefit of the community; these ruling persons should act "with a view to what is best for the city and for those who participate in it".[779] This (historic) perception shows that the bottom-up process may be implemented in practice by establishing a hierarchical framework encompassing representatives from various parts of civil society and/or from different regions who themselves can elect legitimate individuals for the participation in the final decision-making processes.[780]

From a theoretical perspective, it should be differentiated between the groups of involved actors and the authority relations between these actors. A possible approach may be structured as follows:

Often four different groups of actors are distinguished playing a role in the multistakeholder debates related to cyberspace regulation, namely (i) States, (ii) formal intergovernmental organizations (IGO), (iii) business entities, and (iv) non-governmental organizations (NGO), technical and academic community, civil society and the individuals acting on their own behalf. The last group obviously combines a wide variety of actors but a further refinement would lead to an unmanageably complicated typology.[781]

Apart from the distinction of different actors governance arrangements can also vary according to the authority relations between these actors. Four ideal-typical possibilities are available for consideration, namely (i) hierarchy, (ii) homogeneous polyarchy, (iii) heterogeneous polyarchy, and (iv) anarchy.[782] Hierarchy entails relations of super- and subordination (command and obey structure), usually given in the context of States, polyarchy encompasses situation where the authority is distributed among several actors, having either (homogeneously) similar formal powers or (heterogeneously) different formal powers. In case of anarchy no authority relations exist.

778 Aristotle, The Politics of Aristotle, translated by Benjamin Jowett, Oxford 1885, Vol. 1, Book III, Chapter 7, 1279b.
779 *Ibid.*, 1279a.
780 See also Weber/Weber, 2009, 94/95.
781 See also DeNardis/Raymond, 2013, 9.
782 DeNardis/Raymond, 2013, 10.

b) Important elements of multistakeholder participation

The analysis of the general foundations of multistakeholder participation has shown that the inclusion of civil society calls for a bottom-up process. Even if the various actors of civil society are independently organized, common strategies and goals can be developed; the bottom-up approach also enables the creation of new networks and facilitates the enlargement of the fundament for the active participation of Internet users.[783] The multistakeholder models must rely on ever increasing participation by those with interests, capacities, and needs.[784]

In elaborating the substantive issues of multistakeholder participation in more detail, the specific legitimacy strategies are to be developed; thereby, the following factors should be taken into account:[785]

- *Openness:* Access to discussions, negotiations and decisions must be open for interested and concerned persons.
- *Transparency:* Procedures have to be transparent in formal and substantive respects thus ensuring an appropriate representation of the situation.
- *Accessibility:* Information sources need to be accessible for interested and concerned persons.
- *Accountability:* Decision-makers must be accountable to those being exposed to the respective decisions, i.e. responsibility is an important element in corporate structures.
- *Credibility:* Decision-makers should seek to achieve an acknowledgment of their credibility by the persons concerned.
- *Adequately resourced:* Multistakeholder involvement and participation requires sufficient human and financial resources in order to enable the respective processes.
- *Consensus-based:* Acceptability for decisions taken will increase if they are reached by consensus of all concerned persons and not by (sharp) majority votes;
- *Opportunity for appeal/challenge:* An entity of any nature should provide for the possibility to file a complaint against a given decision to an independent panel of „judges".
- *Ability to resist capture:* Decision-making bodies must avoid to be captured by lobbying groups.

783 Weber/Weber, 2009, 94.
784 Doria, 2013, 135.
785 Waz/Weiser 2012, 242/43; to the strategies see Tamm Hallström/Boström, 2010, 141 et seq.

A proper treatment of these aspects requires an enlargement of the scope of traditional research. A multidisciplinary examination of the relevant questions incorporating social-legal, economic, policy-oriented and game theory studies as well as interdisciplinary information studies drawing on socio-economic and political analysis is indispensable.[786] For the time being, an integrated approach has not yet been developed: The disciplines still remain "somewhat stove-piped in different silos"[787] without bringing together the many approaches into a holistic and coherent scientific framework as well as associated evaluation and design methodologies. Developing a multidisciplinary catalog of methodologies as well as the corresponding multidisciplinary tools can improve comprehension of challenges of better participative decision-making, including consideration of governance concepts.[788]

Major substantive issues of the multistakeholder concept are the access to and the participation in cyberspace rule-making. By enhancing the respective possibilities for the multistakeholder communities, better use can be made of the public service value of the Internet. In fact, no other medium is able to spread information within such a short period of time, making it possible for members of civil society to communicate on current topics. Furthermore, organizing events as has been shown during the Arab spring[789] and helping persons in need is facilitated due to the easy information flow and the activation of people.[790]

The realization of the multistakeholder participation is particularly appropriate if a co-regulation system exists which balances the often mutually exclusive interests of the State, the businesses, and civil society.[791] If society becomes more integrated, a more "communitarian" framework will evolve over time.[792]

A specific problem related to responsiveness and participation concerns the scope of impact actually reached. Obviously, a multistakeholder regime is not accomplished by merely providing the preconditions for the participation of civil society; moreover, a real opportunity to shape policy output needs to be provided.[793] Therefore, an evaluation of the influence that the voices of the various stakeholders have on the decision-making process should be conducted; listening to

786 Brown/Marsden, 2013, 200.
787 Brown/Marsden, 2013, 200.
788 Brown/Marsden, 2013, 201.
789 See for example Rolf H. Weber, Politics Through Social Networks and Politics by Government Blocking: Do We Need New Rules?, International Journal of Communication 5 (2011), 1186–1194.
790 See Weber/Weber, 2009, 101.
791 See Tambini/Leonardi/Marsden, 2013, 30o; Dutton/Peltu, 2007, 73.
792 See also Koskenniemi, 2005, 599.
793 Dany, 2008, 61.

the voices of the members of civil society may not become an alibi since in this case the outcome of the deliberations will not result in everyone's welfare.[794] In addition, attempts by certain groups to advance their own interests must be critically analyzed.

In addition, the multistakeholder concept should not be viewed as a value in itself to be applied homogenously to a multiple of governance functions, i.e. the concept is not a one-fits-all solution for cyberspace governance.[795] For example in respect of cyberspace regulation, an appropriate and effective approach must attempt to determine what types of governance are optimal for promoting a suitable regime in any particular functional and political context. As the NetMundial in late April 2014 showed, the multistakeholder concept has to be seen as a compromise with caveats, and a couple of "blocks" stand in the way of a reloaded multistakeholder development.[796] The multistakeholder concept should be based on a granular taxonomy which most likely leads to different results in respect of the manifold substantive topics such as freedom of expression, cybersecurity, standard setting (protocols, routers), interoperability, operational stability, treatment of Internet service providers, etc.[797]

c) Multistakeholder participation in Internet governance debates

Notwithstanding the fact that other markets and areas have known the inclusion of a variety of stakeholders for quite some time[798], the multistakeholder debate has particularly evolved in connection with Internet governance. The discussions are based on the definition contained in the Tunis Agenda for the Information Society: "A working definition of 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 programs that shape the evolution and use of the Internet."[799]

After the agreement on the Tunis Agenda and the implementation of the Internet Governance Forum the topic of multistakeholder participation (or – in shorter form – multistakeholderism[800]) became a major discussion issue in the context of

794 Weber/Weber, 2009, 101.
795 DeNardis/Raymond, 2013, 2.
796 See Francesca Musiani/Julia Pohle, NETmundial: only a landmark event if „Digital Cold War" rhetoric abandoned, available at http://policyreview.info/articles /analysis/net-mundial-only-landmark-event-if-digital-cold-war-rhetoric-abandoned.
797 See also DeNardis/Raymond, 2013, 2.
798 See the examples listed by Mena/Palazzo, 2012, 534/35.
799 World Summit on the Information Society (WSIS), Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6(Rev.1)-E, 18. November 2005, Para 34.
800 To the -ism discussion in more details see Doria, 2013, 117/118.

Internet governance.[801] The multistakeholder concept is more than a bottom-up process or an equal footing principle and cannot be replaced by a sole democracy understanding[802] even if Drake (in his own words "misquoting" Winston Churchill on democracy) argues that "multistakeholderism is the worst form of governance, except all others that have been tried".[803]

Governance policies involve a variety of actors operating at different layers of a structured system, from the physical infrastructure to content and behavior; these activities encompass the development of standards and protocols as well as the offering of applications and services with the consequence that a cross-mapping governance should be realized.[804] This fact clearly shows that non-state actors such as engineers, entrepreneurs, and citizens need to find appropriate cooperation forms.[805] Civil society can even be considered to be the glue making cyberspace regulation happening in reality.

The key to the multistakeholder concept must be seen in the concretization of the "respective roles" of the stakeholders.[806] The Report of the Working Group on Internet Governance (WGIG) of June 2005 and the Tunis Agenda are silent on the interpretation of the term "respective roles".[807] The problems for the interpretation of this term due to its ambiguity have caused substantive impediments to the success of the multistakeholder model.[808] The reference to the technical and academic community does also not help to describe the involvement of civil society. The complexity of defining the "respective roles" has led to the assessment that the cyberspace is left with an unfinished task.[809]

The already described four groups of actors and the four ideal-typical possibilities of authority relations between these actors need a concretization in respect of Internet governance; a first attempt has been undertaken by DeNardis/Raymond.[810]

---

801 To the historical development of the multistakeholder concept in the WSIS I and WSIS II context see Mathiason, 2009, 97–125.

802 Doria, 2013, 120–123; see also Weber, 2011a, 7/8.

803 Drake, 2011, 69.

804 See also Brown/Marsden, 2013, 202.

805 See Mathiason, 2009, 32–48.

806 Doria, 2013, 123–127; Uerpmann-Wittzack, 2011, 1261/62; Kulesza/Balleste, 2013, 1329/30 and 1342.

807 See de la Chapelle, 2011, 15, calling the wording "in their respect roles" a perfect example of what diplomats usually describe as constructive ambiguity, namely an agreement on terms that conceal a disagreement of substance.

808 Doria, 2013, 123.

809 Doria, 2013, 126/27.

810 See DeNardis/Raymond, 2013, 11/12.

Their approach, which convincingly excludes the anarchy relation, can be summarized as follows *(Table 24)*:[811]

Stakeholder Types	Authority Relations		
	Hierarchy	Polyarchy	
		Homogeneous	Heterogeneous
States, IGO, Firms, NGO	ITU		ICANN
States, IGO, Firms		IOSCO	
IGO, Firms, NGO			Global Compact
States, Firms, NGO		IETF, W3C	

Apart from the more theoretical aspects practical considerations must also gain importance, for example in respect of the following questions: (i) How can greater transparency and dialog between different civil society groups and standards experts be introduced? (ii) How can it be ensured that the benefits of rapid standard-making are maintained even with the additional scrutiny due to increasing multi-stakeholder arrangements?[812]

Recently, the European Commission has also taken up the multistakeholder concept and in its Communication of February 2014 proposes the principle "to defend and promote fundamental rights and democratic values, and multistakeholder governance structures that are based on clear rules that respect those rights and values",[813] " (…) governed by a genuine multistakeholder model (…) where the necessary inter-governmental discussions are anchored in a multistakeholder context in the full understanding that the Internet is built and maintained by a variety of stakeholders, as well as governments; (…) where decisions are taken on the basis of principles of good governance, including transparency, accountability, and inclusiveness of all relevant stakeholders" as a basis for a common European vision for Internet governance.[814] In No. 5 of the mentioned Communication, the European Commission describes the multistakeholder process under the headings of transparency, inclusiveness and balance, and accountability[815] leading to the following conclusion *(Table 25)*:[816]

811 The chart is a shortened version taken from DeNardis/Raymond, 2013, 12.
812 See also Brown/Marsden, 2013, 200.
813 European Commission, 2014, 2.
814 European Commission, 2014, 3.
815 European Commission, 2014, 6.
816 European Commission, 2014, 7

• The European Commission is firmly committed to the multistakeholder model of Internet governance. The Commission calls upon stakeholders to further strengthen the sustainability of the model by making actors and processes more inclusive, transparent and accountable.
• The Commission will work with stakeholders on the exchange of best practice.

On the national level, many countries do now have an event comparable to the Internet Governance Forum conference that gathers interested stakeholders for a yearly exchange of ideas and comments. In particular Brazil has made remarkable experiences of multistakeholder cooperation for the discussion of Internet-related issues, embodied in the Brazilian Internet Steering Committee (CGI.br).[817] The regional IGF for Europe, namely the European Dialogue on Internet Governance (EuroDig), nicely combines the theoretically contradicting terms of "dialogue" and "governance".

In the context of Internet governance, Wolfgang Kleinwächter developed a sophisticated model composed of the "United Nations" as organization of sovereign States and the "United Constituencies" representing networks, non-governmental groups, businesses, technical/academic community and civil society. Even if the two governance cultures are rather different, they do not need to be antagonistic, but can co-exist in a meaningful way.[818] A formal and rough comparison between "national hierarchies" of the "United Nations" and "global networks" of the "United Constituencies" could lead to the following diagram *(Table 26)*:[819]

[817] See OII-Paper, 2013, 13–16.
[818] Kleinwächter, 2011, 571.
[819] Kleinwächter, 2011, 571/72.

Issue	United Nations	United Constituencies
Actors	Governments	Private Industry/Civil Society
Structure	Hierarchies	Networks
Codification	National Laws	Universal Codes
International Agreements	Legally Binding Treaties	Memorandum of Understanding
Mission	Broad	Narrow
Policy Development	Top Down	Bottom Up
Decision-Making	Formally specified Majority Voting	Informally specified Rough Consensus
Representation	Elections by All	Delegation by competent Constituencies or via NomComs
Policy-Making	Formally Restricted Access and limited Participation	Formally Open Access and broad Participation
Negotiations	Mainly closed to outsiders	Mainly transparent and open for outsiders
Result	Stability and Predictability	Flexibility

The table shows that both the "real places" and the "virtual places" are linked to each other; since reality does not allow a separation, an objective need for collaboration in a multistakeholder framework is given.

Furthermore, it is important that all stakeholders need to recognize the dynamic nature of the respective roles of the stakeholders in the cyberspace environment.[820] Not only do new actors appear and have to be integrated, but also iterative consultation processes and governance workflows change over time.[821] Therefore, pitfalls in the design of participatory processes need to be avoided, for example by ensuring really inclusive participation, by fighting information overload, by synthesizing discussions, by preventing capture(s), and by ensuring the neutrality of the framework.[822]

820 Doria, 2013, 135.
821 De la Chapelle, 2011, 16/17 and 20.
822 De la Chapelle, 2011, 22/23.

4. Compliance with basic socio-legal values

a) Acknowledgement of cultural diversity

In view of the global extension of the Internet it appears to be obvious that different cultural attitudes and expectations about the best possible way of implementing a legal framework exist and may cause conflicts. Culture can be defined as the integrated system of socially acquired values, beliefs, and rules of conduct delimiting the range of accepted behaviors in any given society.[823]

Due to the vast new opportunities offered by cyberspace, many Internet cultures exist, made up by different members of civil society, all trying to maintain their own voice and identity.[824] Virtual communities and online identities are spreading out, showing how people interact within a given social space; "meet" and "face" are becoming different notions as compared to the real world; inclusion and exclusion from communities follow different patterns.[825] Therefore, Lovink calls for a new kind of cultural criticism, capable of analyzing different positions that are the hallmarks of potential conflicts.[826] The form of governance in view of different perceptions also depends upon the fact that technologies do not only tie up with changes in society, but that the organizational power of communication is adequately realized.[827]

Sociologists argue that globalization creates entirely new kinds of social relations, i.e. new ways of identifying, managing, disciplining and profiting from human relations through the use of the technologies that connect people.[828] As a consequence, studies of cyberspace culture have started to focus on new virtues such as the commons-based-peer-production (Benkler)[829], on youth practices[830] and on social network sites.[831] Furthermore, culture also influences the way online practices affect the formation of identity.

Upholding the values of openness and sharing in the Internet leads to the promotion of a free culture movement. According to Lessig, the social practices associated with cyberspace represent a creative revolution fostering new means for participation in cultural production.[832] The new forms of collaboration create the

823 Jørgensen, 2013, 122; to the aspect of solidarity in particular see Benkler, 2011b, 89–95.
824 Bowry, 2005, 14/15.
825 Jørgensen. 2013, 123.
826 Lovink, 2003, 10.
827 Bowry, 2005, 25–29.
828 Bowry, 2005, 177.
829 For further details see above IV.D.2.
830 Palfrey/Gasser, 2008.
831 Jørgensen, 2013, 125.
832 Lessig, 2004.

situation that "many minds produce knowledge"[833]; thereby, the contributors develop a distinct attitude towards authorship no longer based on the notion of "owner" but of partnership.[834]

In this context, it should not be underestimated that law itself can be seen as a cultural product; treating law as a cultural reality means looking at the material structure of the law to see it in play and at play as signs and symbols, fantasies and phantasms.[835] The analytical problem for rule-makers consists in the attempt to escape the artificial construction of autonomous categories and principles of law.[836] Cultural analysis should strive to combat common sense understandings of law as formal and rule-bound, and instead seek to justify an alternative approach showing the law as discipline moving beyond legal realism.[837]

Consequently, rule-makers should look at broader ways of thinking about what law is and about how law was constituted. A cultural analysis of law not only helps in challenging traditional ideas of culture, it also may help advance new concepts of law.[838] For example, as experience over the last two decades showed, international law and some human rights (for example right to development and right to cultural/linguistic diversity) must accommodate broader aspirations for all members of civil society. From a scholar point of view, empirical research on civil society advocacy should be improved.[839]

The acknowledgment of cultural values, however, should not be misinterpreted in a way that "maintaining social habits", the protection of "morality", and safeguarding "social standards" may be used to interfere with central fundamental rights. Practice has shown that governments of many countries refer to such terms as justification for interventions into open communication networks by declaring these values part of "national security".[840] Thereby, cultural values are perverted into political interests of the individuals that hold the power in a State.

During the last decade, cultural diversity has become a legally established principle for the international community. Foremost, the UNESCO Universal Declaration on Cultural Diversity, adopted by the UN Assembly in 2005, merits more at-

833 Sunstein, 2006, 151.
834 See also Jørgensen, 2013, 132.
835 Austin Sarat/Jonathan Simon, Cultural Analyses, Cultural Studies and the Situation of Legal Scholar-ship, in: Austin Sarat/Jonathan Simon (eds.), Cultural Analyses, Cultural Studies, and the Law: Moving Beyond Legal Realism, Durham 2003, 13.
836 Bowry, 2005, 19.
837 See the respective title of the book of Sarat/Simon (note 835).
838 Bowry, 2005, 17.
839 Bowry, 2005, 190.
840 Kulesza, 2012, 120/21.

tention.[841] In fact, nowhere is the diversity of the world's communities more vivid than in cyberspace, enabling cultures to simultaneously interact at all possible levels.[842] The need to respect and promote cultural diversity is specifically enshrined in many WSIS documents.[843] The practical application of the principle of cultural diversity in the context of the Domain Name System also led to the introduction of internationalized domain names in early 2010.[844]

b) Recognition of cyberspace openness

Freedom of information/communication and freedom of access to networks are of utmost importance in the cyberspace environment.

(i) In line with the well-known slogan "information wants to be free"[845] Lessig proclaimed in his book "The Future of Ideas"[846] that free resources are essential for creativity and innovation. The importance of "free information" became most obvious with the beginning of the age of convergence, which allowed a cheap and simple cross-media delivery, some thirty years ago. Communications theorist Ithiel de Sola Pool popularized the term "convergence" in his seminal book "Technologies of Freedom" stating that "electronic technology is bringing all modes of communication into one grand system".[847] As follow-up to Pool's pronounced vision and the emergence of the World Wide Web in the early nineties of the last century Nicholas Negroponte predicted in his famous book on digitization ("Being Digital") that by 2005 (i.e. 10 years later) Americans would spend more hours on the Internet than on watching network television[848]; this prediction turned out to be quite wrong at the time, partly due to the lack of sufficient digital distribution chains for information deliveries.[849]

---

841 UNESCO, Convention on the Protection and Promotion of the Diversity of Cultural Expressions, 20 October 2005, available at http://portal.unesco.org/en/ev.php-URL_ID=31038&URL_DO=DO_TOPIC&URL_SECTION=201.html.

842 Kulesza, 2012, 140; see also Kurbalija, 2012, 163/64.

843 WSIS, Plan of Action, WSIS-03/GENEVA/DOC/5-E, 12 December 2003, para. 23; WSIS, Declaration of Principles, Building the Information Society: a global challenge in the new Millennium, WSIS-03/GENEVA/DOC/4-E, 12 December 2003, paras. 52–54; WSIS, Tunis Agenda (note 799), 20.

844 Kim Davies, ICANN Blog, First IDN ccTLDs now available, 5 May 2010, available at http://blog.icann.org/2010/05/idn-cctlds/.

845 This slogan was coined by Stuart Brand at the first Hackers' Conference in fall 1984; see Murray, 2007, 76/77 note 7.

846 Lessig, 2001.

847 Pool, 1984, 28.

848 Negroponte, 1995, 58.

849 See Murray, 2007, 78.

Notwithstanding the fact that Lessig also assumed a faster realization of convergence his theoretical analysis about the available options for society is correct. According to Lessig, on the one hand, there is the model of the perfectly controlling cable providers (owning and controlling the physical, logical and content layer of its network); on the other hand, there is the Internet model in principle not exerting any control over a physical layer beyond the decision to include specific equipment and enabling the free exchange of content over a code layer that remains open.[850] Vertical integration and anticompetitive behavior, however, could jeopardize the second model driving at openness.

(ii) As Benkler stated, networks can be characterized as systems partly overlapping and, therefore, requiring "bridges"; freedom and power are affected by the degree of openness, i.e. by the extent "to which individuals can bob and weave between networks to achieve their designed behavior, perceptions, or outcomes".[851] The relation between freedom and the mentioned three objectives can be described as follows *(Table 27)*:[852]

- **Relation freedom/behaviors:**

  "A facility that allows a user to get a desired content without being exposed to advertising provides a degree of freedom and affordance to be free of this particular modality of power."

- **Relation freedom/actions or perceptions:**

  "A system of unencrypted music gives users technical freedom to use music files as they please. Note: They may still not be "free" of all restraints, due to, say, the legal system's constraints, but they do have freedom in the technical distribution system from the particular kind of technical power."

- **Relation freedom/outcomes:**

  "Critiques of systems designed to bundle payment for cultural materials with the basic ISP service have so far succeeded in preventing this pathway of exerting power over outcomes from being established. Users may still be susceptible to power over behavior in the form of digital rights management (DRM), but not to power over outcomes in this form."

850 Lessig, 2001, 167.
851 Benkler, 2011a, 721.
852 Benkler, 2011a, 732–734.

The relations can be deepened and combined to complex configurations depending on the democratizing environment. In preparing norms it is important to understand the level of freedom and its sources, thereby enabling the rule-makers to design a structure that leads to an equilibrium of the diverging interests.[853]

(iii) The openness of cyberspace is also threatened by governmental and private control regimes: The security-industrial complex applying extensive surveillance measures even by co-opting private actors has a significant potential in the hand of dictatorial regimes; its technologies of control and lobbying power, mostly obscured from public gaze, might increase over the coming decade and thereby cause serious threats to individual human freedoms in the cyberspace.[854]

In addition to the above mentioned encrypted music and the digital rights management by rightsholders, the openness of cyberspace can only be ensured on the private side if dominant stakeholders are restricted in blocking rival content threatening their own commercial interests, for example by transforming open platforms into "walled gardens".[855] A vigorous enforcement of the openness rules to maintain access to innovation is needed in times of increasing establishment of horizontal and vertical bottlenecks over distribution.[856]

(iv) Recently, the inventor of the World Wide Web, Tim Berners-Lee, proposed to implement a "Magna Carta" in order to protect and enshrine the independence of cyberspace since the web he had created 15 years ago has come under increasing attack from governments and corporate influence making it necessary to ensure an "open, neutral" system.[857] Berners-Lee's Magna Carta plan is supposed to be taken up as part of an initiative called "the web we want" which calls on people to generate a digital bill of rights and an open Internet.[858]

Openness of cyberspace corresponds to the principle that the Internet must be seen as a public sphere in a universality concept encompassing multiple publics with manifold interests.[859] Looking from this perspective, openness is also a prerequisite for combatting the fragmentation of network structures. As outlined by the European Commission, the vision for cyberspace governance must consist in a single, un-fragmented network.[860] The aspect of one un-fragmented resource is

853 See also Benkler, 2011a, 751.
854 See also Brown/Marsden, 2013, 162.
855 See Mehra, 2011, 894 et seq.
856 See also Brown/Marsden, 2013, 199.
857 See http://www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web.
858 See also the statements of Vint Cerf as cited by Kulesza/Balleste, 2013, 1312.
859 Jørgensen, 2013, 83–89; Uerpmann-Wittzack, 2011, 248.
860 European Commission, 2014, 2.

endangered if each State develops its own national network with the objective to intervene into the cross-border flow of information.

The right to free Internet access being an emanation of the right to free speech and free communication was mentioned in all WSIS documents.[861] In 2011, universal Internet access has been declared a human right in the Report of Frank La Rue, presented to the United Nations General Assembly.[862] Regional and national human rights instruments also know this principle; Switzerland was the first of several countries[863] introducing a universal right of access to the broadband Internet as part of the widely acknowledged universal service obligation. Notwithstanding these principles many countries still apply extensive Internet filtering and censorship. Recently, the Council of Europe clearly included the right of access to the Internet into the Recommendation 2014/6 on a Guide to human rights for Internet users.[864] Therefore, the implementation of an "openness" principle is to be seen as a central pillar for an international cyberspace framework.[865]

The openness of cyberspace also is a key element of the "Internet Universality" concept of UNESCO as presented in a working paper in September 2013. The "Internet Universality" is constituted by the R-O-A-M approach designing Rights, Openness, Accessibility, and Multistakholder.[866] Based on this approach the relevant issues can be summarized in a diagram as follows *(Table 28):*

861 See Kulesza, 2012, 141 with further references.

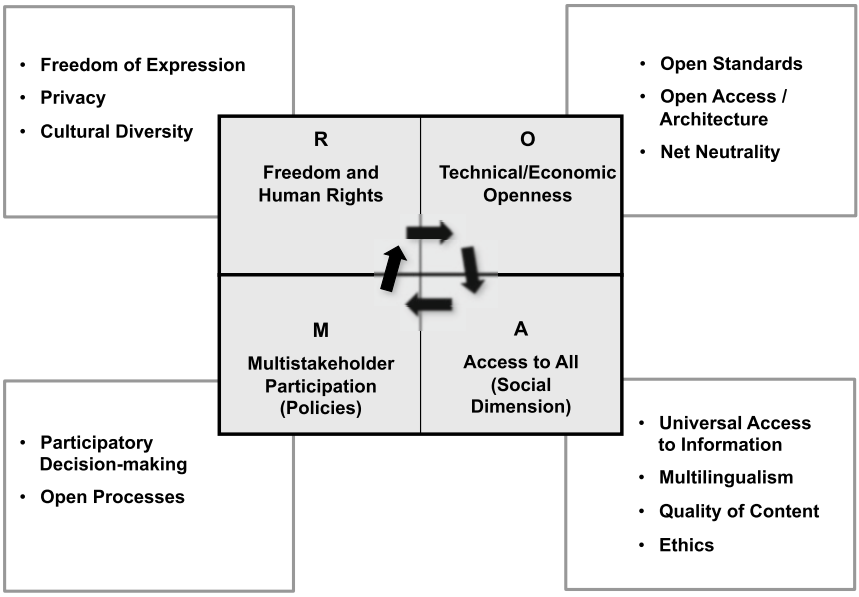
862 La Rue, 2011.

863 Not Finland as stated in many publications (for example Brown/Marsden, 2013, 38) only looking at EU countries.

864 Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users of April 16, 2014 (adopted at the 1197th meeting of the Ministers' Deputies).

865 See also Kulesza, 2012, 143.

866 See http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/internet_universality_en.pdf.



c) Implementation of corresponding technological values: neutrality and interoperability

The technological environment also contributes to the realization of social values. Two principles are insofar of major importance, namely the principle of technology neutrality and the principle of interoperability.

(i) The term *technology neutrality* means that normative rules should abstain from favoring or discriminating against any particular technology. The basic nature of this principle is clear, however, the implementation can cause problems. Often, at least if the rule-maker is careful, a legal norm does not opt for a specific technology, but the norm could lead to the result that technology 1 is norm-compliant without further modification, whereas technology 2 needs a (possibly expensive) modification. In such a situation, the norm would have an indirectly discriminating effect.[867]

Other objectives to be achieved by applying the technology neutrality principle can encompass (i) the achievement of particular effects (for example related to the behavior of people or the outcome of activities), (ii) the functional equivalence between different modes of activities (for example offline and online), (iii) the

867 See Reed, 2012, 192.

non-discrimination between technologies with equivalent effects, and (iv) the drafting techniques in respect of the developed rules (for example flexible norms in order not to hinder the future design of technologies and sustainable norms which do not require over-frequent revisions to cope with technological change).[868]

Rule-making techniques to be adopted for the realization of technology neutrality encompass the technology indifference model, the implementation neutrality principle, and the concept of potential neutrality.[869] Indifferent laws are applicable irrespective of the technology used. If a specific technology is preferred for policy reasons the law should at least not favor one or more implementations of that technology. Finally, a rule-maker can achieve a basic level of neutrality between different technological implementations by providing the possibility to modify a non-compliant implementation in a way that it becomes compliant.

Certain doubts that technology neutrality can achieve its aims, however, have been expressed and need to be overcome.[870] Apart from the fact that neutrality is not always desirable (for policy reasons or competition concerns) the business models often change with the consequence of jeopardizing technology neutrality irrespective of the technological developments. Furthermore, language is not always technology-neutral and literal interpretation can keep the law connected to the technology.

(ii) The term *interoperability* is open to be defined in a broad way, namely as a tool to interconnect networks (including the aspect of standardization), but also as measure to interconnect individuals. Palfrey/Gasser distinguish interoperability functions on four broad layers of complex systems:[871] (i) The first layer concerns technology (ability to transfer and render data and other information across systems, applications, or components). (ii) The second layer is the data layer (ability to read the data). (iii) The third layer is the human layer (ability to communicate, for example through a common language). (iv) The fourth layer looks at institutional aspects (ability to work together).

Open participatory standards (for example an open source operating system such as Linux) are partly claimed to be better for the development of fundamental rights and to grant better access to information than a proprietary operating system (such as Windows).[872] Interoperable systems usually make life easier and in-

868 See Koops, 2006, 83–90.
869 For more details see Reed, 2012, 193–199.
870 See Reed, 2012, 199–204.
871 Palfrey/Gasser, 2012, 5/6.
872 Further to this discussion Brown/Marsden, 2013, 22.

crease efficiency.[873] An open environment can also stimulate innovation since State censorship and corporate control of the value chain might be more difficult; the wider the choice that is available to users, the higher their ability to take advantage of their freedoms will be, however, a guarantee of fundamental rights is not given.[874] Usually, a combination of instruments is needed to get optimal levels of interoperability.[875]

Interoperability, mostly addressed from the perspective of technology, is a widely discussed topic among cyberspace scholars. In a broad sense, conditions for open interoperability can encompass (i) access to the decision-making process, (ii) transparent and undistorted procedures, (iii) pro-competitive goals, (iv) objective and relevant criteria for technology selection, and (v) no over-standardization.[876] In a more narrow sense, interoperability between networks refers to the possibility to easily link two different structures; this issue has been dealt with in the literature to a very detailed extent.[877]

From a theoretical perspective interoperability issues can be mapped by differentiating between private-sector-led approaches and government-driven measures on the one hand, as well as between unilateral and collaborative approaches on the other.[878] Private initiatives are reverse engineering, licensing, technical collaboration, and open standards initiatives; governmental actions are disclosure of information, transparency for consumer, public procurement, and framework for cooperation.[879]

In respect of the mentioned private interoperability the possibility of encryption as user-led regulation must be considered:[880] Encryption software gives the individual the possibility to protect the exchange of information against interference by third persons, however, this technical measure can also make communication more difficult and thereby jeopardize human interoperability. Additionally, the use of encryption software is confronted with governmental prohibition provisions in many countries and the software's application is partly complicated.

---

873 Palfrey/Gasser, 2012, 11; to the competitive advantages of interoperability see Palfrey/Gasser, 2012, 168/69, 173/74 and 232.

874 See also Brown/Marsden, 2013, 23.

875 Palfrey/Gasser, 2012, 160.

876 Brown/Marsden, 2013, 28/29; to the legal operability in particular see below V.D.2.

877 Instead of repeating the contents of previous valuable studies reference is made to the detailed publications of Palfrey/ Gasser, 2012, and DeNardis, 2011; see also Beydogan, 2010, 304–317; Brown/Marsden, 2013, 36–43, 157/58 and 187–192; to the common carriage regulation in particular see Weiser, 2009, 537 et seq.

878 See Palfrey/Gasser, 2012, 14 who, however, label (contrary to this study) a private-sector-led-approach as "non-regulatory" approach.

879 Palfrey/Gasser, 2012, 15.

880 See Brown/Marsden, 2013, 22–28.

5. Implementation of structural governance principles

a) Organizational management requirements

A cyberspace regulatory framework also needs to address organizational elements: a stable order will only be realizable if the degree of "organization" is high enough, enabling and facilitating the implementation (and enforcement) of the agreed harmonized substantive standards. As past experience has shown, the implementation of autonomous soft law and non-state standards based on the principle that they are considered by the concerned persons as benchmark for the behavior can lead to a gradual process of institutionalization.[881]

Such insight has led the school of institutional analysis to develop the concept of the new institutional economics, acknowledging the contribution of sociological institutionalism on historical institutional path dependency and thus providing a broader explanation of the incremental development of policy.[882] Similar considerations are discussed in connection with the constitutionalism of global developments.[883] Relevant questions are the institutional response to dynamic economic change, the functionality of the utility and geometry of regulation and the democratic deficit in case of institutional underdevelopment.[884] Responses to these aspects with regard to available tools can encompass the following aspects: (i) Responses of regulatory institutions to dynamic change in economic conditions; (ii) influence of political, social, cultural, ideological, and economic factors on governance reforms; (iii) divergence of national and regional regulators in their response to global technological factors.

Organizational and decision-making procedures are not any longer solely defined by States and established international organizations; moreover, representatives of other "public" groups (such as business and civil society) have taken a seat at the negotiation table, i.e. these "social actors" have also become accredited participants in the relevant fora.[885] In the last few years, not only private persons and businesses, but also representatives of national governments and international organizations have recognized that the establishment of adequate decision-making structures is important, irrespective of the legal quality of the normative order (hard law or soft law).[886] Without any doubt, appropriate coverage of concerned

881 Weber, 2010b, 517/518.
882 For further details see North, 1990.
883 See Diggelmann/Altwicker, 2008, 643–645.
884 To these issues and the following questions see Brown/Marsden, 2013, 16.
885 Franklin, 2013, 50.
886 Koskenniemi, 2007, 1; see also Senn, 2011, 200 and 270 et seq. to the institutional transformation.

stakeholders with adequate reputational and retaliatory rules can generate a sufficient degree of compliance.[887] Reputational constraints are usually derived from the fact that illegitimacy itself can create "costs", i.e. members in standard-setting bodies must keep reputational discipline by refraining from overtly biased or self-serving decision-making.[888]

New organizational structures also require the development of new governance principles enshrining a range of meanings such as regulating influence, directing, controlling, commanding etc.[889] Typical assays of globalized governance, encompassing the notion of government (in the perception of Foucault) and of governed behavior or regulatory techniques[890] can be seen in the following aspects that need to be addressed:[891]

- Governance must refer to an "order, characterized in part by porous borders and power sharing amongst states, non-state actors and geographic/or functional entities".[892]
- Governance must encompass collective efforts enabling the concerned persons to identify, understand and address worldwide problems going beyond the capacity of individual States to solve.[893]

As the observations to the substantive cyberspace legal framework have evidenced, the future problems by their nature require a broader and more collective decision-making process than in the past; the different interests and needs call for the mentioned establishment of multi-layer mechanisms ensuring that the voices of all concerned participants are heard and appreciated.[894] In terms of a well-known approach of economic theory, law should not mainly use sticks, but through global governments mechanisms rather prefer to use carrots.[895]

The absence of hierarchical structures and the fact that responses to new issues are complex must be acknowledged. Flat structures on different appropriate levels facilitate the decision-making by including the relevant persons and organizations at the actual point of their respective concern. Thereby, the interests of the parties involved should not be defined by any specific group, but through procedural par-

887 Weber, 2012b, 9.
888 Brummer, 2011, 309.
889 See also Senn, 2011, 256/57; Mathiason, 2009, 16–18.
890 See also Senn, 2011, 257/58; for the sake of completeness it may be added that the Canon Law already dealt with the power of governance (see Canons 129–144 and Myriam Wijlens, in: Beal/Coriden/Green, 2000, 183–194).
891 Waters, 2009, 33; Weber, 2010a, 15.
892 Winchester, 2009, 22.
893 See Weiss/Thakur, 2006.
894 Weber, 2010a, 15.
895 Frydman, 2004, 231.

ticipatory mechanisms that reflect the views of the whole society.[896] The mentioned multistakeholder approach calls for different forms of "co-governance" in a multi-layer multi-player mechanism of coordination and collaboration.[897] In practice, these mechanisms are now tested in different forms of "enhanced cooperation";[898] for Internet governance the task of making policy recommendations regarding future forms of multistakeholder inclusion into the regulatory cyberspace processes is mainly performed by the Working Group on Enhanced Cooperation (WGEC).[899]

Based on such an understanding, future governance can be seen as a broad "array of changes in the distribution of authority, legitimacy, decision-making and participation by individuals and organizations in ordering human society, in response to similarly broad changes to material, social, technological, and economic conditions".[900] Consequently, an increased interconnectedness and complexity of life must be taken into account, leading to the formation or legitimization of aggregated networks of sub- or cross-state communities as rule-producing and rule-enforcing actors.[901]

If this kind of governance regime is implemented in social life, civil society will act according to (aligned) incentives with the public interest;[902] this is even more the case with market participants in business matters. Consequently, the degree to which rules are binding should not be conflated with whether they imply a formal legislative obligation; insofar, hard law and soft law are not dichotomous or qualitatively different forms of regulatory control.[903] Lack in confidence in the organizational law and skepticism about the legal framework of governance is detrimental and cannot be helpful in relation to the institution that provides a regime with which civil society and the commercial world should operate.[904]

The problem of soft law or "informal" law-making consists in the fact that such kind of law can hardly provide a protection against extraneous influences. This issue concerns the relationship between the system's own design and the environment in which it operates.[905] This fact calls for the development of new elements covering accountability, institutional differentiation and elaborated procedural

896 Weber, 2012b, 8.
897 Kleinwächter, 2011, 573.
898 See also Franklin, 2013, 191.
899 See http://unctad.org/en/Pages/CSTD/WGEC.aspx.
900 Waters, 2009, 35.
901 Cottier/Hertig, 2003, 261 et seq.; Petersmann, 2011, 23 et seq.
902 Weber, 2012b, 9.
903 Brummer, 2011, 306.
904 Susskind, 1996, 40.
905 Weber, 2012b, 9.

techniques. In the last few years the international regulatory system has undergone a significant evolution and accepted increasing prominence of public notice and consent procedures.

b) Enforcement and dispute resolution requirements

The establishment of an effective and efficient dispute settlement mechanism with the objective to complement and "enforce" soft law or informal international/Internet-ional rule-making is of major importance in order to attribute higher acceptance to a newly established substantive normative order.[906] As many examples show,[907] the possibility of invoking a dispute settlement mechanism tends to lead to better voluntary compliance with the rules.[908]

The need to improve the system of judicial review is especially apparent in connection with decisions taken by the ICANN board. The possibility of appealing against an ICANN decision to the competent court in California is not a suitable solution; moreover, new appeals procedures need to be implemented, for example the establishment of an independent body of experts being vested with the power to review the respective decisions and to release new guidelines, if necessary.[909]

The term dispute settlement mechanism should be understood in a broad sense, including not only theoretical "proceedings" in a traditional form (such as arbitration), but also all conceivable forms of mediation. Governmental legislators and private rule-makers have developed different forms of alternative dispute resolution (ADR) mechanisms; these models apply many types of binding effects of norms and range from negotiated solutions to clear recommendations and finally to enforceable judgments. The suitability of the discussed approaches depends on the given circumstances.[910]

Dispute settlement mechanisms can equally be necessary to clarify which legal obligations are potentially incomplete or inadequate. In this respect, the dispute settlement regime should be able to establish the predicate for, and limit the scope of, retaliation. There is no suitable forum for complaints in the cyberspace world available yet; however, consideration should be given on how to implement new structures dealing with the settlement of disputes.[911]

---

906 See Thompson, 2011, 183.

907 For example consumer disputes, financial services disputes etc.

908 Weber, 2012a, 17.

909 For more details see Weber/Gunnarson, 2012, 68 et seq.

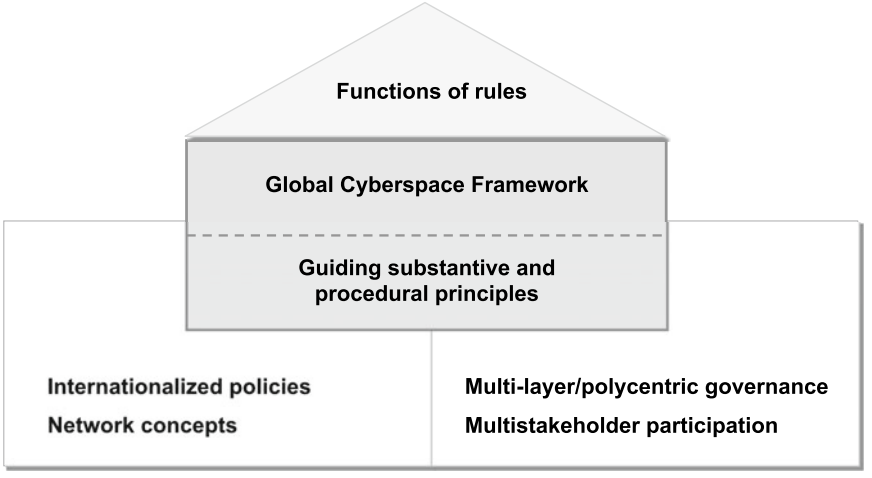
910 For an overview see the still basic contribution of Harry T. Dewards, Alternative Dispute Resolution: Panacea or Anathema?, Harvard Law Review 99 (1985/86), 668 et seq.

911 Weber, 2012b, 9/10.

The availability of dispute settlement mechanisms is also a pre-condition for the introduction of (reputational or/and monetary) sanctions. Examples could be the imposition of some sort of disciplinary and enforcement powers, that would attach costs to the failure of complying with applicable rules. The universally applicable Canon Law of the Catholic Church also contains reputational sanctions. However, such a "sanctioning" requires the implementation of adequate mechanisms making the "environment" of the normative order clearly transparent and including accountability principles that bind the responsible persons.[912]

D. Incorporation of a Global Cyberspace Framework

Based on the assessed policy parameters for cyberspace rule-making and the guiding principles of a normative online order the structural design of a corresponding framework can be outlined. Cyberspace should not be a regulatory vacuum; global challenges require global solutions. The core of the concept must consist in a "Global Cyberspace Framework" (GCF), which should be embedded into internationalized policy structures, and a procedural regime, which relies on the multi-layer/polycentric governance model and on multistakeholder participation and which takes proper account of the functional dimensions of a normative order. Shown in a table the house to be built may have the following shape *(Table 29):*



912 See above IV.C.4.

1. Need for internationalization of policy structures

The question of who should run the Internet is intrinsically political because it is a sociocultural concern[913], i.e. cyberspace regulation cannot evade political considerations.[914] However, the question remains whether the power of digital networks is so great that traditional politics can no longer retain their former status.[915] A preliminary answer has already been given by Marshall McLuhan more than fifty years ago: The communication networks allow a "collective interplay" and constitute a "global village".[916]

Without any doubt, cyberspace requires (and deserves) universal protection and regulation.[917] Since cyberspace functions independently of State borders, online human activities need a minimal legal framework giving guidelines as to the compliance with important substantive principles of the concerned community. In addition, sensitive topics might even need surveillance and intervention mechanisms, which led Vint Cerf to propose the creation of a "cyber fire-department".[918] Nevertheless, the "crossing the Rubicon" metaphor recalling Julius Caesar's river crossing on the way to Rome from Gaul appears to overestimate the changes needed to adapt international policies.[919]

Since traditional rule-making is connected to the physical territory according to the sovereignty principle, civil society might be prepared to comply with norms stemming from an authority which acts in the territory of domicile. In contrast, a legal framework that has been developed at another place and is "transported" through cyberspace can hardly expect to become acceptable. This assessment is particularly true for the enforcement of rights against cyberspace actors that do not have assets in the concerned jurisdiction.[920] Looking from a general perspective, rule-makers need to avoid becoming unwitting prisoners of history by looking at the pre-cyberspace physical world developed piecemeal instead of addressing the new technological appearances.[921]

---

913 Franklin, 2013, 139 with further references.

914 For more details see Franklin, 2013, 176–180; Brousseau/Marzouki/Méadel, 2012.

915 Lanier, 2013, 328.

916 McLuhan, 1962, 5.

917 See also Kulesza, 2012, 136.

918 Vint Cerf mentioned the "cyber fire-department" being an international organization that would stand guard over international cybersecurity and coordinate international efforts in fighting cyber-crime at the IGF Meeting 2010 (Session 123) in Vilnius, Lithuania; a transcript is available at http://www.afilias.info/webfm_send/138.

919 Demchak/Dombrowski, 2011, 32, evoke this metaphor in connection with the Stuxnet worm attack.

920 Reed, 2012, 223; Goldsmith, 1998, 1216/17.

921 See also Reed, 2012, 151.

Therefore, Post has (recently again) proposed[922] that national legislators should abandon all their claims in the cyberspace context and not act as authority over cyberspace anymore, but – moreover – recognize a right to self-determination for cyberspace actors, namely "their right – perhaps even their inalienable right – to govern themselves as they see fit".[923] According to Post this approach is a consequence of the fact that national law can no longer guide the behavior of those subject to it in any meaningful way.[924] Surprisingly enough, these statements do not stem from the early days of cyberspace, but only date a few years back (2009). Nevertheless, as Reed points out, this "proposition is more than a little idealistic".[925] It can hardly be imagined that States would be willing to give up their law-making authority and their jurisdiction, to the contrary, as the recent experiences during and in the aftermath of the WCIT 2012 (Dubai) have shown, national interventions are in the process of being strengthened.[926]

However, even in view of the expressed reservation it cannot to be excluded that an incentive exists for States to substantially reduce their claims to authority over cyberspace.[927] The reason for this assumption lies in the growing awareness of States that reality does not allow them to make a claim with a global extension and does not offer the corresponding power. Competences could potentially be moved from the State level at least to a regional level.[928] The effectiveness element calls for a limitation of the claim for compliance with national laws to those cyberspace actors who are likely to recognize the implemented norms since they consider themselves part of the concerned community (civil society). Such a limitation would also contribute to a certain reduction of confusion with respect to the normative force of available laws and overcome the dilemma of existing power paradoxes.[929]

---

922 Already at a time when the Internet became more widely used by civil society the promoters of the libertarian movement proclaimed the independence of cyberspace (see above II.B.2).

923 Post, 2009, 185.

924 Post, 2009, 168.

925 Reed, 2012, 223.

926 See above V.B.1.

927 Reed, 2012, 224.

928 From a technological perspective the most recent attempts of network engineers, mainly of a team of the Swiss Federal Institute of Technology in Zurich, developing a decentralized structure (instead of a global structure) of the Internet with some regional outlets (as far as network order and control authority is concerned) should not be overlooked (see NZZ am Sonntag of June 1, 2014, 53–57).

929 See also Franklin, 2013, 18–20.

Nevertheless, this assessment is subject to two reservations which merit attention:

- Members of civil society in cyberspace cannot be divided into two categories, namely those who deliberately break the law ("bad people") and those who intend to act lawfully ("good people"). Such a distinction[930] does not reflect reality in cyberspace and the assumption that "good" norm-compliant persons would benefit from better laws can hardly be defended.[931]
- The States' acknowledgement of the fact that a practically unlimited extension of their laws' applicability does not correspond to the nature of cyberspace should not be interpreted as a complete denial of the need for a legal framework. Moreover, apart from the existence of voluntarily observed social norms based on soft law arrangements or customary habits, some basic principles need universal protection (and regulation).[932] As a result, a basic set of commonly accepted rules will allow for efficient and flawless international cooperation in all cyberspace-related matters.[933]

Summarizing this aspect in a nutshell it can be stated that the political dimensions of rule-making in cyberspace must take into account the manifold interests of cyberspace users and rule-makers acting in different cultural environments.

2. Need for multi-layer/polycentric approach with multistakeholder participation

For the time being, the attempt of introducing cyberspace regulations takes place in multiple international, regional and national fora according to the described multi-layer approach based on polycentric rule-making processes.[934] Most fora, however, that have not been established according to binding multilateral agreements (and not many fora in the cyberspace field fulfill this requirement of a multilateral incorporation) so far lack decision-making power; this assessment is particularly relevant for the most important forum, namely the Internet Governance Forum (IGF). Its establishment at the second WSIS in Tunis (2005) was conditional of a design only allowing discussions and deliberations (often in form of so-called dynamic coalitions) without extending the right to release binding motions.[935]

930 This distinction is partly made by Reed, 2012, 55–57.
931 Critical to this approach also Julia Hörnle, Book Review, International Journal of Law and Information Technology 20 (2012), 370, 380/81.
932 Kulesza, 2012, 136; to these generally acknowledged principles hereinafter V.D.3.
933 See also Kulesza, 2012, 138.
934 See above V.B.3.
935 See Weber, 2009, 70/71; Franklin, 2013, 154 et seq.; Brown/Marsden, 2013, 13/14.

This fact, however, does not mean that fora such as the IGF should be vested with sovereign power. Moreover, the principle of a multi-layer regime requires accepting different forms of rule-making developed by different institutions and stakeholders. This assessment is particularly relevant in view of the fact that many types of cyberspace users are actors in the online world and conflicts of interest between them need to be balanced and solved.[936] The realization of a multistakeholder regime is not an easy task; all participants need to build and constantly regain trust and confidence.

Notwithstanding the different perceptions of the various stakeholders in cyberspace the principles agreed upon in the manifold fora need to be linked into a comprehensible structure. This objective can be achieved if — apart from the technical interoperability[937] — the legal interoperability is also improved. Legal interoperability is the process of making legal rules work together across jurisdictions.[938] Whether new laws are implemented or existing laws are adjusted/reinterpreted depends on the given circumstances. Due to the increasing fragmentation of cyberlaw, efforts should be undertaken to achieve higher levels of legal and policy interoperability in order to reduce costs in cross-border business and to drive innovation and economic growth.[939]

In view of the complex cyberspace structures that make it advisable to implement a multi-layer regime composed of polycentric rule-making processes[940] and in consideration of the impossibility to define an optimal level of legal interoperability the model of total harmonization should not be the approach to follow even if the judgment based on a specific national law does not comply with general principles of another national law as the case "LICRA c. Yahoo!" demonstrated.[941] Moreover, it is important to find the appropriate degree of legal interoperability (instead of an all-or-nothing solution), which considers the substantive principles (such as freedom of expression, privacy, etc.) in different circumstances.[942] In-

936 Reed, 2012, does not really differentiate between the manifold cyberspace users and follows a relatively "monolithic" approach; see also the critical remark made by Julia Hörnle, Book Review, International Journal of Law and Information Technology 20 (2012), 370, 381.

937 See above V.C.4.c) (2).

938 Palfrey/Gasser, 2012, 178.

939 Palfrey/Gasser, 2012, 178/79.

940 See above V.B.3.

941 The "Tribunal de grande instance" in Paris confirmed the illegal nature of the sale of memorabilia of the Nazi period under French law in 2000 (thereby approving the competence of the French courts in a complaint against the US firm Yahoo!; decision RG:00/0538 of May 22 and November 22, 2000). Later Yahoo! started legal action in the US arguing that the sale's prohibition would contradict the First Amendment of the US Constitution.

942 For more details see Palfrey/Gasser, 2012, 180–183.

stead of debating a multilateral treaty system against a multistakeholder approach a new collaborative approach should be realized.

Furthermore, some variability is also caused by the enforcement mechanisms ("law in action") that might drive the decision on implementing a top-down approach (governed by large international bureaucracies) or a bottom-up process (developed step-by-step within multistakeholder institutions).[943] The multi-layer model attempting to achieve the suitable legal interoperability can insofar be seen as variable geometry model or as example of the described polycentric regulation.[944]

3. Need for consensus on guiding principles

In order to avoid a fragmentation of the applicable legal regime and to improve legal interoperability, the academic perspective calls for the implementation of a Global Cyberspace Framework (GCF); such a Framework should (i) adhere to the specific nature of cyberspace, (ii) envisage implementing the multistakeholder concept in the decision-making processes by realizing an appropriate multi-layer regime and (iii) incorporate the mentioned substantive principles into the framework.[945]

a) General declaration and additional protocols

The form of a Global Cyberspace Framework should not be identical to the traditional multilateral treaties designed as agreements between sovereign States, but should rather have the character of a declaration, a protocol or a commitment, based on the creation of a wide contractual consensus[946] acceptable to sovereign States, international organizations, businesses, and civil society.[947] The inclusion of private actors in internationally binding regimes has already been executed in other fields (for example Montreux Protocol[948]) and is also achievable in future cyberspace regulations.

---

943 Palfrey/Gasser, 2012, 184/85.

944 See above IV.E.2.

945 See also Kulesza, 2012, 152–154 with a proposal for an "Internet Framework Convention" which, however, is not fully identical with the proposal in this book; the idea of the "Convention" has been taken up in Kulesza/Balleste, 2013, 1345.

946 Such kind of consensus corresponds to the notion of "social contract" (see above IV.C.1).

947 Kulesza, 2012, 153.

948 The Montreux Document on pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict, 17 September 2008, available at: http://www.icrc.org/eng/assets/files/other/icrc_002_0996.pdf; see also Weber, 2011a, 11–13.

The "agreement" on a global normative order is not a completely new thing that never happened in the past: the (ecclesial) *jus canonicum* of the Catholic Church is a legal body with a global reach being independent from national legislation. The Canon Law is usually defined as a set of norms created by reason enlightened through faith that intends to bring order into the life of ecclesial community,[949] i.e. the Canon Law attempts to assist people in the reception of God's saving mysteries. Law is a specific instrument in this process, prompting and binding the community to strive for its perfection and giving directions for its progress.[950] This comparison does not mean that Canon Law should be taken up (by analogy) in cyberspace, however, it shows that normative orders can exist for centuries in parallel to the traditional national legislation.

A Global Cyberspace Framework could be complemented by additional protocols addressing specific social policy issues.[951] The respective topics might often be of a substantive matter (guiding principles)[952] but also encompass specific Internet issues (e.g. protocol standards and their interoperability, domain name allocation system). Such an approach leads to a desirable sequential rule-making process according to the prevailing needs. In addition, heuristic categories could be developed building a system and further evolving into a normative order.

Potential material topics are civil law (e.g. protection of privacy), trade law (e.g. provisions on e-commerce and international consumer protection as well as copyright and trademark principles), administrative law (e.g. trans-border online offer of medical services), financial law (e.g. e-banking), or criminal law (in particular cybersecurity).[953] Further input could be drawn from the 2005 WGIG Report[954], even if it cannot be overlooked that this document mainly addresses social policy issues essential to Internet governance and its already existing supervisory mechanisms.[955]

949 See Ladislav M. Örsy, in: Beal/Coriden/Green, 2000, 6.
950 *Ibid.*, 2.
951 See also Kulesza, 2012, 154.
952 See above V.C.2.
953 See Kulesza, 2012, 137/38.
954 Report of the Working Group on Internet Governance, June 2005, available at: http://www.wgig.org/docs/WGIGREPORT.pdf.
955 For this reason the approach of Kulesza, 2012, 154, for the design of the additional protocol appears to be too narrow.

b) Agreement on guiding principles

The most central issue of a Global Cyberspace Framework consists in the need for reaching a consensus on the applicability of some guiding principles.[956] Since law cannot operate as a mechanism for controlling the behavior of all cyberspace actors in a satisfactory way[957], the model with normative principles helps to systemize and explain a set of appropriate normative rules; furthermore, principles are an element of legal reasoning.[958] General principles are a recognized source of international law according to Article 38 (1) (c) of the Statue of the International Court of Justice; furthermore, general principles should be observed by the States and other cyberspace stakeholders since compliance with them leads to foreseeability in respect of the other actors' behavior; insofar, compliance pays off.[959] Even if different cultural identities do not necessarily acknowledge the same substantive principles some key values appear to be globally accepted.[960] At the forefront, human (fundamental) rights, ethics, and democratic participation merit strong protection. Such an approach could systematically benefit from the concept of "regulatory gravity".[961]

Human rights can be seen as values common to a major part of (or even the whole) global community. Not only are there several international legal instruments in place protecting human rights for more than fifty years, but also human rights are not exclusively a matter, which concerns States. Private enterprises are equally bound to conduct their business in a way that individuals are able to exercise their guaranteed freedoms. The efforts of the Global Network Initiative encompassing the major IT and Internet firms show that the cyber-community no longer relies on States as the only capable entities to protect fundamental rights.[962] In a comparative view, the mentioned Canon Law is also perceived as normative

956 At the NetMundial in Sao Paulo the participants agreed in the Multistakeholder Statement of April 23/24, 2014, on a set of governance principles, available at http://www.netmundial.br/.

957 See Reed, 2012, 242.

958 Uerpmann-Wittzack, 2010, 1246.

959 Kulesza/Balleste, 2013, 1344.

960 To the freedom of expression in the global governance debate see in particular MacKinnon, 2012, 2013–219; Anne-Claire Jamart, Internet Freedom and the Constitutionalization of Internet Governance, in: Roxana Radu/Jean-Marie Chenou/Rolf H. Weber (eds.), The Evolution of Global Internet Governance. Principles and Policies in the Making, Zürich 2013, 57 et seq.

961 See Reed, 2012, 100; Murray, 2010, 195 et seq.

962 See Global Network Initiative, available at: http://www.globalnetworkinitiative.org; see also Kulesza/Balleste, 2013, 1348.

order for a truly human community; some norms are borne from a human need for order, entrusted to individuals and linking the order to values.[963]

Ethics is another central principle. By identifying ethical standards, common to civil society (and thereby also to cyber-communities), a consensus as far as behavior in cyberspace is concerned might be achievable.[964] For quite some time ethics has not been deeply addressed in cyberspace rule-making circles, however, recently the perspective seems to convincingly change. For example, the European Commission expressed the intention to include ethics in the efforts for implementing suitable governance structures in cyberspace.[965] Ethical behavior enshrines many related principles, such as acting in good faith or building trust.

Experience in cyberspace has shown that the online civil society is more likely prepared to acknowledge general principles that have become customary ("Internet-ional rulemaking") instead of strict laws. General principles need to be derived from the acknowledged perceptions of the civil society's members. Therefore, an important element of the Global Cyberspace Framework conception should consist in designing customary legal rules for online communities that are based on recognized general principles; by identifying, for example, ethical standards, common to all online communities (along the concept of the "civic virtue" as developed by Johnson/Post), a consensus satisfying all concerned individuals and entities in cyberspace might be achievable.[966]

A further issue of a Global Cyberspace Framework concerns the delineation of the addressed actors in cyberspace. Apart from the usually mentioned multistakeholders (States, international organizations, businesses, civil society), Internet intermediaries also merit special attention. Particularly with respect to their role in cyberspace activities, that may cause harm and require remedies, a more intermediary-focused approach of a Global Cyberspace Framework seems justified.[967] As mentioned[968], appropriate dispute settlement mechanisms can equally be helpful in clarifying which legal obligations are potentially incomplete or inadequate. There is no suitable forum for complaints in cyberspace matters available yet; therefore, it appears to be reasonable to consider implementing new structures dealing with the settlement of disputes.

963 See Ladislav M. Ösry, in: Beal/Coriden/Green, 2000, 2 and 4.
964 See also Kulesza, 2012, 151.
965 European Commission, 2014, 9.
966 See Kulesza, 2012, 151.
967 Lipton, 2012, 148.
968 See above V.D.5.b).

c) Quality of rule-making

As outlined, a Global Cyberspace Framework should be composed of basic principles, not of narrowly worded legal norms. Therefore, the body of these principles can hardly be called a "law". Consequently, no specific term such as *"lex digitalis"* or *"Jus Internet"*[969] is proposed as terminological classification for the Global Cyberspace Framework.

Irrespective of the chosen form of a Global Framework Convention it is necessary to ensure that the norm-setting reaches an adequate level of quality. A consensus of all concerned cyberspace actors on the rule-making body does not suffice if the norms are so defective that they do not achieve the envisaged normative objectives. Three problems are particularly noteworthy in this context:[970]

- In developing new norms rule-makers have to avoid creating conflicts with other rules that are already part of the cyberspace users' law system. Therefore, rule-makers should research the norms currently applied and considered to constitute a part of the concerned community and only then define the new rules in a way that they fit into the existing framework; this kind of procedure can contribute to the required regulatory quality of a Global Cyberspace Framework.[971] Depending on the given circumstances, new rules may be able to modify existing norms by gradually extending their scope into the rule-makers' desired direction, if this direction is not irreconcilable with the existing framework.[972]
- Another problem consists in the concrete drafting of new rules; if cyberspace actors do not understand the wording, compliance with the rules can hardly be expected and/or achieved. In other words, the linguistic quality of norms is of importance; insufficient quality is a widely known issue in rule-making processes.[973] In addition, if new rules do not take up the requirements of the socio-technological environment obedience by cyberspace actors is not facilitated.[974]
- A third pitfall occurs if the law is framed in terms, which have no apparent connection to what the cyberspace actors actually do.[975] If the relation between the demands of the rule-maker and the behavior of cyberspace actors is not recognizable, a rejection (non-compliance with new rules) by cyberspace

969 This is the terminology recently used by Kulesza/Balleste, 2013, 1343–1345.
970 For further details see Reed, 2012, 226–228.
971 For more details to the regulatory quality requirements see above III.C.2.
972 Reed, 2012, 227.
973 See Reed, 2012, 129 et seq.
974 To the aspect of respect for the implemented normative order see Reed, 2012, 20–25.
975 Reed, 2012, 228.

actors is likely since the new rule does not appear to be established on the basis of a meaningful concept.[976] Only meaningful and respectful laws will not encounter resistance from the addressees of the norms (i.e. civil society).[977]

As known from general law-making theories, an appropriate trade-off between simplicity and certainty in respect of the application of new rules is difficult to achieve; as a consequence, rule-makers have to carefully assess the cyberspace actors' required intentions, behaviors, and outcomes in some detail.[978] Furthermore, as designed by the form of a Global Cyberspace Framework, it appears to be imperative to have a flexible rule-making regime in an open systems' design.

Another general observation consists in the acknowledgement that law should be embedded in a social concept[979] and that law can hardly operate as a mechanism for controlling the behavior of cyberspace actors.[980] Therefore, the purpose of a rule-making process should be to regulate functions and effects, not means.[981]

The preparation, design, and implementation of an appropriate Global Cyberspace Framework cannot be the exclusive task of legally educated scholars. Moreover, a multidisciplinary approach should be applied and must include impact assessments in respect of different market structures and their dynamics, the development of pioneering international policies for cyberspace regulation and the monitoring of efficiency exercised by the implemented legal cyberspace framework.[982] The IGF has become a forum for multidisciplinary exchanges; the respective deliberations could even be made be more fruitful if comprehensive discussions between representatives of different disciplines, professional backgrounds, and cultural/geographical expertise would take place.

4. Need for improved emphasis on the functions of rules

When designing the future cyberspace legal framework[983] the fact should be considered that building designers, i.e. architects, are the experts in sketching "constructions". More than a hundred years ago the famous architect Louis H. Sullivan said: "It is the pervading law of all things, organic and inorganic, of all things, physical and metaphysical, of all things human and all things superhuman, of all

976 To the elements constituting meaning laws see also above III.A.1.
977 For more details to these aspects see Reed, 2013, 20–23.
978 See Reed, 2012, 241.
979 See Koskenniemi, 2005, 573.
980 See Reed, 2012, 242.
981 See Thompson, 2013, 45.
982 See also Brown/Marsden, 2013, 203.
983 The following comments are based on Weber, 2012b, 10.

true manifestations of the head, of the heart, of the soul that the life is recognizable in its expression, that form ever follows function. This is the law."[984]

The architect Sullivan uses twice the word "law" consisting in the key notion of making form dependent from function. Therefore, when designing an international legal framework for cyberspace, the function of law has to be considered in more depth; following Bentham's principle of utility and Luhmann's approach of stabilization of normative expectations, a functional approach that bodes for the political project should determine the normative order.[985] As a result, the main question could be phrased as follows: What social impacts should be caused by law? The answer is to be founded on the expectations of civil society. These expectations change over time, but some elements remain the same, such as legal certainty, stability, and reliability. In times of fast developing information technologies civil society is able to better rely on these principles in an informal law-making process and context than in the traditional legal regime.

Coexistence in an increasingly informal law-making environment makes it necessary to implement governance elements which encompass collective efforts enabling a proper identification and understanding of worldwide problems needed for global solutions, to have organizational structures in place which allow widespread participation by way of a multistakeholder model and to establish a dispute settlement mechanism which strengthens the accountability of all involved members of States' powers, international organizations, businesses, and civil society.

[984] Louis H. Sullivan, The tall office building artistically considered. Lippincott's Magazine 57, March 1896, 403–409, reproduced in: Leland M. Roth (ed.), America builds: Source Documents in American Architecture and Planning, New York 1983, 340, 345.

[985] See Thompson, 2013, 48/49; to the functional approach see also Reed, 2012, 179.