

HIIG Discussion Paper Series

Discussion Paper No. 2017-07

Risk Management in the Digital Constellation – A Constitutional Perspective

IDP Conference Barcelona 2017

October 2017

Ingolf Pernice*

ingolf.pernice@hiig.de
Alexander von Humboldt Institute
for Internet and Society
Humboldt-Universität zu Berlin

* Former Professor of Public, International and European Law, Humboldt-Universität zu Berlin, Director of the Alexander von Humboldt Institute for Internet and Society (www.hiig.de). I would like to express my deep gratitude to Dr. Christian Djéffal and Jörg Pohle, research assistants at the HIIG, for their invaluable comments and observations on an earlier version of this paper.

Abstract

The digital revolution is creating new risks, together with multiple opportunities for communication, commerce and political participation. What Ulrich Beck described as the world risk society, and – from another perspective – Jürgen Habermas calls the »postnational constellation« – is a challenge to our concepts of society and democracy. Digitisation is pushing this development towards a new dimension that allows us to speak of the »digital constellation«. Social relations are denser across borders and continents; what happens abroad matters here, as if it were happening on our own doorstep. New kinds of risks are arising as a side-effect of the increasing use of information technologies, while the internet also offers – for the first time ever – an infrastructure that makes formerly unrealistic concepts of cosmopolitan democracy (David Held) a real option. This includes the establishment of a constitutional framework for normative processes aiming at, among other global challenges, effectively managing cyber-risks at national, supra-national and global levels in a coherent way. Multilevel Constitutionalism has been proposed as a means of providing a normative theory for conceptualising the constitutional structure of a layered system of governance that provides for a maximum degree of self-determination for the individual and, thus, for the democratic legitimacy of decisions made at each level, from local to global. Thus, the constitution for democratically legitimate action at the global level does not question democracy at other levels, but should be understood as complementary, based upon functioning states, and designed to deal with issues that are beyond their reach, including cyber-security.

Keywords

Digitisation, Multilevel Constitutionalism, Global Constitutionalism, Digital Constellation, Democracy, Risk Society, Risk Management, Legitimacy

Contents

INTRODUCTION	1
I. RISK SOCIETY AND THE DIGITAL CONSTELLATION	2
1. Risk Society and World Risk Society (Ulrich Beck)	3
2. The Postnational Constellation (Jürgen Habermas)	6
a. Democracy Theory Revisited	6
b. »The Political Constitution of World Society«	9
3. Conceptualising the »Digital Constellation«	10
a. A New Communicative Density for the Global Society	10
b. A New Infrastructure for a Global Digital Democracy	11
c. New Risks and Challenges	12
II. RISK MANAGEMENT AND MULTILEVEL CONSTITUTIONALISM	15
1. Risk Management: Strategy and Measures	19
2. Constitutional Framework: Multilevel Constitutionalism	22
a. Deficiencies of the International Law and Cooperation Approach	22
b. What »Multilevel Constitutionalism« Means and Offers	25
(1) The Individual in the Centre	26
(2) Sharing Sovereignty – or the Principle of Attribution	26
(3) The Principle of Subsidiarity: Maximising Political Self-Determination	28
(4) The Citizen’s Multiple Identities in a Composed Constitutional System	29
c. Towards Global Constitutionalism	29
3. Global Risk Management and Multilevel Constitutionalism	30
CONCLUSION	32

Introduction

The digital revolution is a revolution affecting all our societies, one which is creating great opportunities and great risks. The result is an emerging digital society that differs from industrial society in many respects. Talking about risk management today necessarily involves explaining what the new risks in this digital society are, before considering the tools and processes to deal with these risks, and this seems particularly interesting in a constitutional theory and law perspective.

Some preliminary general questions need to be answered nevertheless. First of all, we need to understand what we mean by the terms »risk« or »risk society«, and what the concept of »Digital Society« denotes. Secondly, managing risks is about more than risk assessment, precaution, protection or defence, in particular in the digital age. This paper takes a broader view and discusses governance aspects, as well as political and, in particular, normative instruments with the aim of exploring a constitutional approach to the choice and implementation of appropriate strategies for cyber-risk management.

Here is my first proposition: As we talk about the new risks that are being created by digitisation, which, in turn, is creating a multitude of opportunities regarding governance at large, we have to deal with a new kind of risk in a new kind of »constellation«, to use a term coined by Jürgen Habermas. With regard to his concept of »postnational constellation«¹, the internet today is carrying us one step further to what I would call the »digital constellation«. This will be discussed in the first part of the present paper.

In the »digital constellation« we are confronted with new risks and threats on a global level, regardless of borders and geographical distances. There are also great opportunities, the internet offers, for developing new concepts of governance that seem to be particularly relevant also for risk-management. As has been mentioned in earlier studies, digitisation has the particular potential to make democratic regulation possible at the global level and also to manage risks of the kind involved by the worldwide application of ICT.² In other words, the

¹ Jürgen Habermas, *The Postnational Constellation and the Future of Democracy*, in: id., *The Postnational Constellation. Political Essays* (Polity Press, Cambridge 2001), p. 58.

² Ingolf Pernice, *Global Constitutionalism and The Internet. Taking People Seriously*, in: Rainer Hofmann & Stefan Kadelbach (eds.), *Law beyond the State. Past and Futures* (Campus, Frankfurt am Main, 2016), pp. 151-206; id., *E-Democracy, the Global Citizen, and Multilevel Constitutionalism*, in: Corien Prins, Colette Cuijpers, Peter L. Lindseth, Mônica Rosina (eds.), *Digital Democracy in a Globalised World* (Edward Elgar, Cheltenham 2017), pp. 27-52,

global dimension of the internet and, consequently, of the risks it entails for digital society at large is comparable to the global dimension of other great challenges like climate change, mass migration, nuclear power, genetic engineering or international terrorism. The risks they entail are somehow inherent products of our society, and so are the cyber-risks.³ In order to manage them, instruments of the state and international cooperation in most cases will not suffice. Global solutions are necessary, and one such solution is global regulation – global cybersecurity regulation that is democratically decided and globally effective.

Here is my second proposition – perhaps still a bit utopian: establishing mechanisms of democratically legitimised regulation at the global level as part of a multilayer system of governance organised in accordance with »multilevel constitutionalism«. Some thoughts on this will be presented in Part II of this paper.

I. Risk Society and the Digital Constellation

There is a correlation between the problem as I see it and the solution I envisage: With the progressive use of the internet the risk society has assumed a new character and proportions with new, so far unknown risks; this is the problem. On the other hand, modern information technologies and, in particular, the internet are opening up new possibilities for managing the risks we are facing; this is the solution. A first question is this: with regard to the risks that are accompanying the digital revolution, what kinds of risk exactly are making the risk society in the digital age different from the risk society of the kind described by Ulrich Beck? It appears that the (world) risk society described by Ulrich Beck (infra 1) corresponds in many respects to the »postnational constellation« of Jürgen Habermas in that our societies face the challenges of globalisation and we are compelled by a need to rethink democracy (infra 2). However, an answer to the open question of how to organise democracy beyond the state at the global level seems to be possible as a result of the opportunities presented by the digital revolution only. Besides its concomitant new risks, therefore, digitisation is also

forthcoming; id., Cybersecurity Governance. Making Cyberspace a Safer Place, in: Global Constitutionalism 2017 (in review process), available as HIIG Discussion Paper Series No. 2017-05, available at: <https://ssrn.com/abstract=3012136> (accessed 22 September 2017).

³ See already Pernice, Cybersecurity Governance (note 2), p. 5.

fundamentally changing the conditions for political processes in such a way that it is fair to conceptualise the new situation as the »digital constellation« (infra 3). Thus, with the internet it seems to be possible to develop an answer. And yet only the new risks and opportunities presented by digitisation and the internet seem to compel us – but also allow us – to conceptualise and establish a global system of democratic norm-setting as required under the new circumstances (infra 4.).

1. Risk Society and World Risk Society (Ulrich Beck)

We owe the term »risk society« to Ulrich Beck's works on the society of the 1980s, which presented new risks of a kind and magnitude hitherto unknown and equally affecting all members of society.⁴ In contrast to the industrial society described by Marx and Weber, the question is not how best to utilise nature, to release men from traditional constraints and to produce and redistribute wealth in a society of inequalities. The risk society has to deal with problems arising from socio-economic development, the risks produced by industrialisation and new technologies: nuclear accidents, genetic engineering, climate change, air pollution and the dying forests, to name but a few. These risks are man-made, and they are transnational, in part global.⁵ This is why Beck extended his concept of risk society to »World Risk Society«.⁶ The risks are unintended and »implicit« side-effects of industrialisation, »risks of modernisation«; they are universal and affect the poor as much as the rich, they are »self-referential«, unpredictable and difficult to attribute to particular individuals.⁷ And they produce inequalities at all levels, including the international one.⁸ Ulrich Beck distinguishes these risks from personal risks, such as those taken by Columbus when discovering new continents and having the connotation of adventure and courage. Instead, the new risks are general, they have the potential to cause mankind to destroy itself.⁹ Also, »external« risks like natural disasters or pandemics, unforeseeable and

⁴ Ulrich Beck, *Risikogesellschaft. Auf dem Weg in eine andere Moderne* (Suhrkamp, Frankfurt a. M. 1986), pp. 17-18, 25-30, 48, 52-58.

⁵ *Ibid.*, p. 26.

⁶ Ulrich Beck, *World Risk Society* (Polity Press, Cambridge 1999); see also *id.*, *Weltrisikogesellschaft. Auf der Suche nach der verlorenen Sicherheit* (Suhrkamp, Frankfurt a. M. 2008), and particularly pp. 40-42, where he emphasises the »cosmopolitan momentum« of the world risk society; and *id.*, *Critical Theory of the World Risk Society*, in: 16 Constellation (2009), pp. 3-22, available at: <https://www.jus.uio.no/smr/om/aktuelt/arrangement/2015/ulrich-beck-cosmopolitan-view.pdf> (accessed 17 July 2017).

⁷ *Ibid.*, pp. 29-30, 36, 42-43.

⁸ *Ibid.*, pp. 54-58.

⁹ *Ibid.*, p. 28.

unattributable to anyone as they are, are not the kind of risks that Beck is referring to in his concept of risk society.¹⁰

Cyber-risks are of a different kind as well. They can be very explicit, concrete and visible. Cyber-threats, as experienced, affect individuals, business, public services and authorities, critical infrastructures, energy grids, nuclear plants, and whatever is connected to the internet¹¹ or depends on its operation. These threats are not unintended, general and implicit but intended and focused. Cyber-risks can have a global dimension, like the risks Ulrich Beck is concerned with. Cyber-threats, however, are not from diffuse sources, as in the case of air pollution or dying forests, but always arise from a well-determined source, often individuals, but also from groups, businesses or states. As attribution is not technically possible; for the potential victims, they give the appearance of natural disasters. However, they are not »external« to the society, but »internal«. They are »risks of modernisation« like the risks described by Ulrich Beck. In contrast to those, however, they arise from intentional planned attacks on IT systems, starting with smartphones and individual computers up to critical infrastructures. In this respect, cyber-risks are distinct from risks qualified as unintended side-effects, if they are not the unintended side-effects of digitisation at large.

Interestingly, in his book on the »World Risk Society«, Beck places particular emphasis on the global dimension of the new risks: »they destroy national borders and mix the domestic with the foreign«.¹² With regard to the environment, he observes a de-coupling of the social location of the responsible decision-maker from the place and time where foreign people become the object of the physical and social injury the decisions cause.¹³ The complexity of the interaction and accumulation of disorders and destructions, he concludes, are challenging the survival of the planet itself, while international risk management is becoming progressively necessary and influential.¹⁴ Cyber-risks may not be

¹⁰ Ibid., p. 300, where he emphasises that an essential characteristic of the risk society is the fact that we cannot make external factors accountable for the risk situations (»Unmöglichkeit externer Zurechenbarkeit von Gefahrenlagen«).

¹¹ Stuxnet is said to be a case where the attack was possible even when there was no connection to the internet, see: David Kushner, The Real Story of Stuxnet. How Kaspersky Lab tracked down malware that stymied Iran's nuclear-fuel enrichment program, in: IEEE Spectrum 26 February 2013, available at: <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet> (accessed 8 August 2017).

¹² Beck, World Risk Society (note 6), p. 40, mentioning the »cosmopolitical moment« as an indication for a »meta-change« of the society of the 21st century: *ibid.*, p. 41 (my translation). See also *ibid.*, pp. 287-91.

¹³ *Ibid.*, p. 288.

¹⁴ *Ibid.*, pp. 288-89.

challenging the survival of the planet, but they do stretch across borders and continents because of the global reach of the internet itself.

With regard to civil society, Beck detects approaches supporting a »world-risk-civic right«. In a new social theory, he states, society must be de-coupled from the state. What he strives to sketch out is a historico-empirical social theory of the world-risk-society.¹⁵ Beck also takes a cosmopolitan view of sociology, based upon the insight that reality is no longer national or international, but borderless and global: decision-makers have to take account of the people their decisions potentially affect, wherever they are in the world.¹⁶ He shares the call made by David Held for the establishment of institutions for global coordination, while emphasising that, prior to institutionalisation, global norms are emerging merely from the general indignation felt about facts that are considered to be simply unacceptable: norms, he says, do not only emerge »positively« from legislative processes but also »negatively« from an evaluation of crisis and threats.¹⁷ But he goes one step further. The ethical principle of hospitality in the sense meant by Immanuel Kant, who regarded the duty to welcome strangers as a key feature of his normative cosmopolitanism, for Beck would not be applicable in what he calls »the global space or responsibility of global risks«. ¹⁸ The category of hospitability would not be »appropriate to expressing the inescapability of moral proximity over geographical distance«. For Beck, the global risks trigger a kind of »compulsory cosmopolitanism« instead, »in a world whose boundaries are as porous as Swiss cheese, at least as regards communication and economics«. ¹⁹ The global risks create a »globalised neighbourhood« among people worldwide, though unequally because of the different vulnerabilities in different regions of the world. »In legal terms« he says, »the ethical principle of recognition involves a kind of cosmopolitan law of global risk«. It is »the ›living side effects‹ of the risk decisions of others«, in his view, that create the right to have a say in these decisions.²⁰ These are the external effects of national policies in an interconnected world, and many of the global risks analysed by Beck are the result. This leads to the normative claim:

¹⁵ Ibid., p. 291.

¹⁶ Ibid., pp. 322-23. For his understanding of the term »cosmopolitan« see also *ibid.*, p. 314.

¹⁷ Ibid., p. 326.

¹⁸ Ibid., pp. 339-40; in English: Ulrich Beck, *Critical Theory of World Risk Society: A Cosmopolitan Vision*, in: *16 Constellations* (2009), p. 5.

¹⁹ Ibid., p. 4.

²⁰ Ibid., p. 6.

»Global risks produce harms that transcend national borders. Thus the cosmopolitan law of risk is possible only if the boundaries of moral and political communities can be redefined so that the others, strangers and outsiders, are included in the key decisions which jeopardize and violate their existence and dignity.«²¹

Consequently, for him the future of politics is cooperation: »no nation can master its problems alone«. Beck calls this »an insight of political realism«, and he qualifies it as the »fundamental law of cosmopolitan Real politik«. ²² As will be shown below, all this applies to cyber-risks, the management of which requires more than cooperation.

2. The Postnational Constellation (Jürgen Habermas)

Beck's analysis, after all, draws attention to important aspects of globalisation. The risks include environmental, economic and terrorist risks. They are distinct from each other, and each of them requires different responses. ²³ He insists, however, that they have two key features in common: »First, they all promote or dictate a policy of proactive countermeasures that annuls the basis of the existing forms and alliances of international politics, necessitates corresponding redefinitions and reforms and calls forth new political philosophies«. Second, they cannot be understood as »external«, but are »the risks of civilisation«, as Beck says, that »may give rise to a more acute global normative awareness, create a public space and perhaps even a cosmopolitan outlook«. ²⁴

a. Democracy Theory Revisited

At this point, though from a different perspective, the analysis corresponds not only to the cosmopolitan approach of David Held but also to the »postnational constellation« of Jürgen Habermas. Habermas, too, paves the way towards a revisited and extended approach to democracy as a democratic necessity. ²⁵ His concept not only offers an opening-up of democracy theory, ²⁶ but also indicates

²¹ Loc. cit.

²² Ibid., p. 18.

²³ Ibid., pp. 13-15.

²⁴ Ibid., p. 15.

²⁵ Habermas, Postnational Constellation (note 1), pp. 58-112.

²⁶ For the construction of democracy beyond the state see already Ingolf Pernice, Multilevel Constitutionalism and the Treaty of Amsterdam: European Constitution-Making Revisited, in: 36 Common Market Law Review (1999), pp. 703-9, also available at: <http://www.whi-berlin.eu/documents/whi-paper0499.pdf> (accessed 25 July 2017); see also, with a comprehensive

a number of fundamental points for democratic risk management at the global level. In contrast to the »historical constellation« that has existed since Rousseau and Kant, in which the democratic process assumed the more or less convincing institutional form of the territorial state or the nation, faced with the effects of globalisation,²⁷ Habermas looks for »appropriate forms for the democratic process to take beyond the nation-state«. There is what he calls a »paradoxical situation«, described as follows:

»The idea that one part of a democratic society is capable of a reflexive intervention into society as a whole has, until now, been realized only in the context of nation-states. Today, developments summarized under the term »globalization« have put this entire constellation into question.«²⁸

Democracy organised within nation-states is limited to the borders of each state: The state is regarded as the home of sovereignty. The self-determination of the »sovereign« people cannot reach beyond these borders, except for international cooperation or war. The former is often ineffective, the latter unacceptable. Though the external effects of national politics have always existed in history, the world has changed with the progress of globalisation. As Claus Offe stated in 1986, »national communities by no means exclusively make and determine decisions and policies for themselves, and governments by no means determine what is appropriate exclusively for their own citizens«. ²⁹ Ten years later, David Held argued on the basis of this observation that traditional concepts of democracy have to be rethought and to this end »a new agenda will have been created for democratic theory and practice.«³⁰ As he demonstrates, the interdependence and interconnectedness of states, the external effects of national political decisions on other countries and the need for instruments for effective joint decision-making at the global level on common problems exceeding the reach of national politics have notably increased; hence his call for »cosmopolitan

analysis, Anne Peters, *Elemente einer Theorie der Verfassung Europas* (Duncker & Humblot, Berlin 2001), pp. 93-166.

²⁷ Ibid., p. 60.

²⁸ Ibid., pp. 60-61.

²⁹ David Held, *Democracy and the Global Order. From the Modern State to Cosmopolitan Governance* (Stanford University Press, 1995), p. 16-7, with reference to Claus Offe, *Disorganized Capitalism* (Polity Press, Cambridge 1985), pp. 286, who focussed, however, on the influence of private powers. See also David Held, *Global Transformations: Politics, Economics and Culture* (Stanford University Press, 1999), p. 445. Recently, Stephen Coleman, *Can The Internet Strengthen Democracy?* (Polity Press, Cambridge 2017), describes this as one of four factors that »profoundly disrupted« the system of the existing political communication system that »resulted in predictable relations between political elites, journalistic mediators and citizens«.

³⁰ Held, *Democracy* (note 29), pp. 16-23; see also Beck (note 4), p. 310, as an aspect of politics losing boundaries (»Entgrenzung von Politik«, *ibid.*, p. 300).

democratic law»³¹ in a »cosmopolitan democracy«. ³² In the same vein, in »The Postnational Constellation« (2001) Habermas envisages that politics in future will become a substantial part of »world domestic politics« implemented in the name of, for and by the »citizens of the world«. ³³

Whether the responsible political leaders of the world have learned from these analyses or not, we still have no appropriate institutional settings for exercising democracy beyond the state at the global level. Would their establishment be a threat to the democracy of the nation-state? In his book on the crisis of the European Union, taking the EU as a model for his propositions on the establishment of a global regulatory capacity to meet global challenges, Habermas argues that establishing institutions and processes for regulation at the global level would not be at odds with democracy, but in fact the opposite: it is a requirement of democracy:

»In view of a politically unregulated growth in the complexity of the world society which is placing increasingly narrow systemic restrictions on the scope for addition of nation states, the requirement to extend political decision-making capabilities beyond national borders follows from the normative meaning of democracy itself.«³⁴

In some way, the EU can indeed be taken as a model for a democratic constitution of such decision-making capabilities. Habermas develops some important thoughts on a politically constituted world society and on designing institutions and processes along these lines at the global level. ³⁵ Globalisation, interconnectedness, environmental imbalances, the external costs of national politics and the economic crisis, as described in the emerging world society with all its complexities, are taken as a challenge to the traditional, nation-state-related democratic system. The incapacity of the nation-state to fully meet its original tasks of providing peace and security in a broad sense, particularly through an effective risk management in the postnational constellation, has placed even the self-determination of people at risk. Whatever democratic processes the internal

³¹ Held, Democracy (note 29), p. 31, 239-266, based upon a brilliant description of five »disjunctures« of the modern society, *ibid.* p. 99-140.

³² *Ibid.*, pp. 267-286

³³ See already Habermas, Postnational Constellation (note 1), p. 104-112: »make a change of course toward a world domestic policy possible without a world government«.

³⁴ Jürgen Habermas, The Crisis of the European Union. Response (Polity Press, Cambridge 2012) p. 15; see also *ibid.*, p. 55.

³⁵ *Ibid.*, p. 2, pp. 53-70.

constitutional system may look like, as a consequence of globalisation the classic nation-state has an increasingly growing democratic deficit.³⁶ This deficit needs to be repaired through an extension of the concept and practice of democracy.

b. »The Political Constitution of World Society«

Though not a purely intellectual construction, »social reality« is itself imposing a »shift in perspective from classical international law to the political constitution of world society«. Habermas, therefore, argues that »environmental imbalances and the risks generated by large-scale technology have given rise to a similar global need for regulation«.³⁷ The constitutional solution proposed for the »postnational constellation« is to extend democracy beyond national borders with a central role for the (reformed) United Nations and a representation of the world's citizens through an elected global parliament.³⁸ The United Nations »should be reorganized as a politically constituted community of states *and* citizens«.³⁹ With regard to the problems of legitimation at this level, though, Habermas envisages a split between two areas of competence: tasks of global security, the prohibition of violence and human rights protection have to be decided by the »world organisation«, and while »tasks of world domestic politics with distributive implications are not included in the hierarchically constructed arrangement of competences«; they must be »negotiated transnationally«.⁴⁰ The world parliament, composed of representatives of the world's citizens and states would have a general deliberative function and would, in particular, »ensure that the competing justice perspectives of world citizens, on the one hand, and of national citizens, on the other, would be taken into account and brought into balance«.⁴¹

Many challenges of globalisation, however, and the global risks dealt with by Ulrich Beck and recognised by Habermas, as well as the new cyber-risks, would not be manageable with such an arrangement. These are basically questions of world domestic politics in need of globally applicable and enforceable regulation which, owing to its limited legitimacy and representation of the world's citizens,

³⁶ Habermas, Postnational Constellation (note 1), pp. 69-76.

³⁷ Habermas, Crisis (note 34), p. 55.

³⁸ Ibid., p. 60-66.

³⁹ Ibid., p. 56.

⁴⁰ Ibid., p. 67-68.

⁴¹ Ibid., pp. 58-59.

the UN as an institution, even together with a world parliament, is unable to ensure.

3. Conceptualising the »Digital Constellation«

Digitisation not only entails new challenges and risks but also involves a far more important change that is essential for what could be called the »digital constellation«. This change is about organising legitimacy, beyond what Habermas has already assumed when proposing to extend the chain of legitimacy to the »world organisation«:

»that the global, in part digitally produced, communication processes extend beyond porous national public spheres in such a way as to enable all peoples to form a reasoned judgment about the moral core content of decisions taken at the UN level.«⁴²

There are three major changes to observe that characterise the new constellation that can be called the »digital constellation« and, thus, one step beyond Habermas' postnational constellation: A new communicative density of the global society (infra a), new opportunities for democratic processes (infra b), which could allow the development of global responses to the new risks of digitisation (infra c).

a. A New Communicative Density for the Global Society

The new information and communication technologies do more than change markets into e-markets, allow financial transactions globally at lightning speed and on a massive scale, and change industrial processes, labour markets as well as administrative structures and processes. Overall, they are pushing society into a new constellation, with a new kind of density of social and communicative relations, and with a so far unknown proximity between people from all over the globe.

The »globalizing impact of the modern communications media« has been described by David Held as »part of a process of ›cultural globalization‹«; it is one of the five disjunctures he has determined.⁴³ He observes that »the development of the new communication systems creates a world in which the

⁴² Ibid., p. 66.

⁴³ Held, Democracy (note 30), p. 122.

particularities of place and individuality are constantly mediated by regional and global communication networks«, with the effect that »the traditional link between ›physical setting‹ and ›social situation‹ is broken.«⁴⁴

Held could not foresee the dramatic developments of the internet, which not only confirms his observation but also carries it to a new dimension. Today, the internet reaches all points of the globe, we get news from everywhere, not filtered through established media only, but directly from people of other continents, in real time. So we can communicate our ideas, opinions, actively participate in public debates and influence political processes, wherever we like. In the »global village« we can observe and have a greater sense than we could in the past of how politics and actions at one place in the world potentially affect people at other places around the globe. The internet allows us even to have a direct personal voice in politics abroad, in real time – and not through diplomatic channels only.

b. A New Infrastructure for a Global Digital Democracy

With the internet, we can observe the emergence of a new potential for open, deliberative democracy also at the global level: Borderless, real-time communication and information; access to knowledge and education regardless of geographical distances; social networks, discussion platforms and deliberative spaces across borders and continents etc. are allowing the emergence of a global public sphere, which is one of the conditions of global democracy. With the new dimension of proximity, social interrelation and discourse among people worldwide, opportunities for democratic rule-making at the global level are thus visible and they need further consideration.⁴⁵ The distinction between »them« and »us« is fading away, like the other distinctions Ulrich Beck says have already disappeared in the world risk society.⁴⁶ Human dignity and solidarity are felt more and more to apply across borders and continents too, and the emergence of global norms arising from the indignation about crises and disasters in other parts of the world, described by Beck,⁴⁷ is increasing.

The term »digital constellation«, therefore, corresponds to the digital society, which is global like the risk society. It reflects a level of social and communicative relations among people that is comparable to those at the local, regional, national

⁴⁴ Ibid., p. 123.

⁴⁵ See Pernice, E-Democracy (note 2).

⁴⁶ Beck, World Risk Society (note 6), pp. 335-36. English: Beck, Critical Theory (note 18), pp. 4-5.

⁴⁷ See supra, note 17.

and supranational levels of society, though still more informal and with less attachment. Its potentials, however, include the formation of a global political will across continents, as is already practiced in the areas of internet governance and as can be further developed as a fundamental part of a global order that is capable of meeting global challenges through democratically established rules and concepts.⁴⁸ Among these challenges are the new risks that need to be managed at all levels, and for which regulation is required also at the global level: One example is cyber-security.

c. New Risks and Challenges

The risks attending the use of computers and the progressive digitisation of our societies were observed early on,⁴⁹ but with the changing context and spread of the technologies the proportions they assume are somewhat unexpected and surprising. New products and applications are often put on the market without sufficient care being taken over security. The producers need to learn that a sound security and privacy engineering⁵⁰ is part of the deal. The internet grew out of efforts in military and academic circles to allow computers to connect and to ensure safe communication within the army or easy communication among students. As Oliver Burkeman of the Guardian newspaper says in an article commemorating forty years of the internet in 2009, »hobbyists« played a major role in the early developments of the internet in civil contexts, and safety of the net or cybersecurity was not among the concerns leading their work.⁵¹ Early warnings on privacy issues⁵² however, and the revelations about mass

⁴⁸ For the theoretical concept and a model of global regulation along these lines see Pernice, Global Constitutionalism (note 2).

⁴⁹ See the study by the Swedish Minister of Defence, Vulnerability of the Computer Society (1976), and the summary given by the U.S. Government Accountability Office available at: <http://www.gao.gov/products/100059> (accessed 12 August 2017).

⁵⁰ Precious insights into the issue and methodology are provided by Michelle Finneran Denny, Jonathan Fox and Thomas Finneran, The Privacy Engineer's Manifesto. Getting from Policy to Code to QA to Value (Apress Open/Springer, New York, 2014).

⁵¹ For the history see: Oliver Burkeman, Forty Years of the Internet: How the World Changed For Ever, in: The Guardian, 23 October 2009, available at: <https://www.theguardian.com/technology/2009/oct/23/internet-40-history-arpnet> (accessed 27 June 2017).

⁵² For an analysis based upon the RFC's of 10 years' previous development see Sandra Braman, Privacy by Design: Networked Computing, 1969-1979, New Media Society (online 26 December 2011), available at: <http://nms.sagepub.com/content/early/2011/12/25/1461444811426741> (accessed 13 August 2017).

surveillance by intelligence services⁵³ received little public attention or had only little impact in real terms on enhanced oversight.⁵⁴

In the internet's early stages of development, it was difficult to foresee the enormous threats we are discussing today as a by-product of digitisation. Here are but four issue areas that are far from being resolved:

- a. Privacy is one of the major concerns in the public debate on the new techniques of data collection, storage, transfer and processing, including big data analysis and profiling. Human dignity and personal rights are also threatened by hacking-attacks on private computers, e-mailing systems or databases. Last but not least, individual surveillance by law enforcement authorities and mass surveillance by intelligence agencies, as known from the Snowden revelations in 2013, have been made possible in the age of digitisation and have reached an intensity, depth and extent that have changed the very nature of intelligence. Espionage among states and governments was broadly accepted in the past, but what we are seeing now is intelligence activities affecting the whole of society. Such systematic threats to privacy affect everybody's private life and human dignity, they produce chilling effects on the exercise of fundamental rights and freedoms and, in particular, of the freedom to expression. They can, at least indirectly, even harm democratic processes.
- b. Democratic processes, including elections and democracy at large, are also threatened by other kinds of cyber-attack, such as massive disinformation campaigns through fake news in social media, botnets and systematic manipulation of people on the basis of individualised profiles and psychographic targeting. The case of Cambridge Analytica is a striking example.⁵⁵ Such threats may come from inside a country, but

⁵³ For one of the most striking examples see the 2001 Report (Gerhard Schmid) of the European Parliament, on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) of the »Five Eyes«, running since the 1960s until its discovery in 1990, available at: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN> (accessed 12 August 2017). Today, based upon a comparative analysis, Richard Morgan recommends the »Five Eyes« model as an international norm for intelligence oversight: »Oversight through Five Eyes. Institutional convergence and the structure and oversight of intelligence activities«, Zachary K. Goldman and Samuel J. Rascoff (eds), *Global Intelligence Oversight. Governing Security in the Twenty-First Century* (OUP, Oxford 2016) 37.

⁵⁴ For a comparative analysis see: Zachary K. Goldman and Samuel J. Rascoff (eds), *Global Intelligence Oversight. Governing Security in the Twenty-First Century* (OUP, Oxford, 2016).

⁵⁵ For an account of the method see: Hannes Grassegger und Mikael Krogerus, »Ich habe nur gezeigt, dass es die Bombe gibt. Der Psychologe Michal Kosinski hat eine Methode entwickelt, um Menschen anhand ihres Verhaltens auf Facebook minutiös zu analysieren. Und verhalf so Donald Trump mit zum Sieg«, *Das Magazin* N°48 – 3. Dezember 2016, available at: <https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/> (accessed 14 August 2017); for attempts by Cambridge Analytica to calm down the discussion

equally from abroad, as in the case of the alleged Russian activities in the latest American election campaign. Hate speech, xenophobia, extremist and populist postings in social media risk poisoning political discourse and culture in western democracies. As it is not possible to determine with certainty the origins of these actions, the platforms and intermediaries are made responsible. Compelling internet platforms to take down illegal content, as the German legislator is doing with the new »Netzdurchsetzungsgesetz«, however, is only a very partial and limited solution, which itself raises many questions.⁵⁶

- c. Security, from the personal computer or smartphone up to nuclear power plants, traffic systems or the entire energy grid, is under increasing threat from private or state hacking or cyber-attacks. 28.4000 cyber-attacks against its IT equipment were registered by the German Ministry of Defence within the first nine weeks of 2017 alone. The yearly damage in Germany is estimated to cost 50 billion euros per year. But more importantly, in the case of the crash of a nuclear plant or the breakdown of the energy supply system, the damage can be unimaginable – not to mention the damage caused by cyberwar, given the new capacities established in many countries, including Germany, not only for cyber-defence troops but also with offensive cyber-weapons. New incidents like WannaCry and NotPetya hitting thousands of internationally active companies and even public hospitals are but the latest of the publicly visible cyber-attacks rolling around the globe.⁵⁷

The digital revolution with its power, spread and intensity, including the new threats as we are experiencing them today, has changed public awareness of the

see: Patrick Beuth, »Die Luftpumpen von Cambridge Analytica«, in Zeit Online, 7 March 2017, available at: <http://www.zeit.de/digital/internet/2017-03/us-wahl-cambridge-analytica-donald-trump-widerspruch> (accessed 14 August 2017).

⁵⁶ See also the critical remarks of Eileen Donahoe, Protecting Democracy from Online Disinformation Requires Better Algorithms, Not Censorship, in: Council of Foreign Relations 21 August 2017, available at: <https://www.cfr.org/blog/protecting-democracy-online-disinformation-requires-better-algorithms-not-censorship> (accessed 22 September 2017). See also Mark Scott and Laurens Cerulus, Europe struggles to find united front to combat illegal content online, in: Politico of 20 September 2017, available at: <http://www.politico.eu/article/europe-hate-speech-jihad-terrorist-propaganda-theresa-may-google-facebook/> (accessed 22 September 2017).

⁵⁷ See Lily Hay Newman, The Ransomware Meltdown Experts Warned About Is Here, in: WIRED 12 May 2017, available at: <https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/> (accessed 17 July 2017); Johannes Steger, Der nächste Erpresser-Virus kommt bestimmt, in: Handelsblatt, 14 July 2017, available at: <http://www.handelsblatt.com/unter-nehmen/it-medien/petya-wannacry-und-co-der-naechste-erpresser-virus-kommt-bestimmt/20057630.html> (accessed 17 July 2017). Olivia Solon & Alex Hern, »Petya« ransomware attack: what is it and how can it be stopped?, in: The Guardian, 28 June 2017, available at: <https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how> (accessed 17 July 2017).

risks and the need for action. As we can see, all the values at stake, as listed above, are closely linked with fundamental rights or principles, including cybersecurity.⁵⁸ As the risks we are facing in the digital society are not external, from outside like a thunderstorm, but self-made risks produced by society itself, it is our joint social responsibility to find appropriate ways of managing them.

National legislation can strive to limit these risks, but threats from sources outside the country, even if detected, are difficult to counter. The country of origin may have different laws and allow the activities that create the threats, and in any event, sanctions cannot be imposed on other countries. Attacks ranging from those on the dignity of the person and privacy to the integrity of information systems, private property or the democratic system and the whole of society at large can vary in scope and gravity. The internet allows attacks across borders from any place in the world, striking targets in any other part of the world. Even if one knew where the attack had originated, the law of the country struck by it would not be applicable to an attacker situated abroad. The rules on state responsibility under international law are difficult to enforce. The risks characterising the digital constellation cannot be managed with the traditional toolbox of national politics. Along with the progressively creative and universal application of the internet, creative and universal strategies for risk management in the digital constellation are needed.

II. Risk Management and Multilevel Constitutionalism

Accordingly, steps towards an effective risk management aiming at an adequate level of rights protection and security at home and worldwide have to be assessed in a new perspective: The risks – and also the risk society – extend from private life and local communities up to the global level. Therefore, risk management has to be undertaken at all levels. Certain measures may be aimed, as appropriate, at private individuals, while others may be devised for business corporations, public authorities, states and supranational or international organisations. All these players are potential attackers and victims, but they are

⁵⁸ See also Sebastian Leuschner, *Vom Grundrecht zum Grundsatz. Sicherheit als Schutzgut der europäischen Grundrechtecharta – eine grundrechtsdogmatische Rekonstruktion und ihre Folgen für die Sicherheit im Cyberraum*, Dissertation Berlin 2017 (Mohr Siebeck, Tübingen 2017), forthcoming.

also responsible and relevant as actors in the field of risk management. It is their shared interest and common responsibility to respect and protect privacy and human dignity, property rights and personal freedoms, as well as the fundamental right to security as spelled out in the constitutions and the European and international instruments for the protection of human rights. And they need to act in a coherent and cooperative way, respectful of their respective responsibilities and powers, following a coordinated strategy to achieve a common objective.

At present, individual states⁵⁹ and also the European Union⁶⁰ are each developing their own cybersecurity strategies.⁶¹ The 2015 U.S. Cyber Strategy was based upon defensive and offensive capabilities for cyber-security, including hit-back and deterrence, but also resilience and stigmatising markets for »zero-day exploits«, though it is said to have bought itself vulnerabilities on this market allowing it to intrude foreign digital systems, or may be developing them itself.⁶² Interestingly, the new U.S. administration does not seem to have adopted a

⁵⁹ For an overview see the NATO Cooperative Cyber Defence Centre of Excellence (DDCDOE), Cyber Security Strategy Documents, 23 May 2017, available at: <https://ccdcoe.org/cyber-security-strategy-documents.html> (accessed 14 August 2017). For the UK see the policy paper 5 »A safe and secure cyberspace – making the UK the safest place in the world to live and work online«, Department for Digital, Culture, Media & Sport (1 March 2017), available at: <https://www.gov.uk/government/publications/uk-digital-strategy/5-a-safe-and-secure-cyber-space-making-the-uk-the-safest-place-in-the-world-to-live-and-work-online> (accessed 15 August 2017), with a strong emphasis on defence and deterrence, based upon the strong involvement of intelligence and also offensive capabilities. For a telling account of the present cyber threats see, for example: »Cyber-Sicherheitsstrategie für Deutschland 2016«, available at: https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (accessed 17 July 2017). See also the Law on the Federal Office for IT Security (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)) of 2009/17, available at: https://www.gesetze-im-internet.de/bsig_2009/BSIG.pdf (accessed 26 July 2017), and the Law on Enhanced Security of IT Systems (»IT-Sicherheitsgesetz«) of 2015, available at: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#_bgbl_2F2F2F5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D_1501068552430 (accessed 26 July 2017).

⁶⁰ See the 2013 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, available at: http://www.eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (accessed 17 July 2017); the Eighth Progress Report Towards an Effective and Genuine Security Union (COM(2017) 354 final), promises a revision of this Strategy by September 2017, available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20170629_eighth_progress_report_towards_an_effective_and_genuine_security_union_en.pdf (accessed 22 September 2017) see also Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (»Cyber Diplomacy Toolbox«), available at: <http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf> (both accessed 17 July 2017). For an overview see the EU Commission's Factsheet EU cybersecurity initiatives (2017), available at: <https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-initiatives-working-towards-more-secure-online-environment> (accessed 26 July 2017).

⁶¹ For a renewed strategy see: ENISA, Principles and Opportunities for a Renewed EU Cybersecurity Strategy (Version B I July 2017), available at: <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-input-to-the-css-review-b> (accessed 22 September 2017).

⁶² On all this see Monkey Cage, What is new in the U.S. cyber strategy, in: The Washington Post 24 April 2015, available at: <https://www.cfr.org/blog/cybersecurity-2015-national-security-strategy> (accessed 14 August 2017).

strategy yet,⁶³ though some important ideas for a »new cyber security agenda« had been submitted to the U.S. government in November 2016.⁶⁴ In the introduction of this policy paper the authors stress their belief that »cyber security needs to be thought of as an existential risk to core American interests and values, rising close to the level of major armed conflict and climate change«.

The German Ministry of Defence has established a new military commando unit for cyber-defence, including offensive capabilities.⁶⁵ This is part of the German »Cyber Security Strategy« (2016), which is characterised by a cooperative approach with both business and European and international partners.⁶⁶ Apart from an updated »EU Cybersecurity Strategy« announced for September 2017⁶⁷, an important EU document is the »Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities («Cyber Diplomacy Toolbox«), adopted by the EU Council in June 2017. It rightly emphasises »the need for coherence among the EU cyber initiatives to effectively strengthen the cyber resilience«.⁶⁸ The NIS-Directive⁶⁹ is referred to as the main instrument for achieving this, but the Council also insists on the full application of international law. It confirms »the strong commitment« of the EU and its Member States »to actively support the development of voluntary, non-binding norms of responsible State behaviour

⁶³ For some points on cybersecurity in the 2015 U.S. National Security Strategy see Adam Segal, Cybersecurity in the 2015 National Security Strategy, blogpost 6 February 2015, available at: <https://www.cfr.org/blog/cybersecurity-2015-national-security-strategy> (accessed 14 August 2017). Clicking on the »strategy« to find it on the White House website, leads to the following White House message: »Thank you for the interest in this subject«, with no further information. See, however, the report by Cage, What is new in the U.S. cyber strategy (note 61).

⁶⁴ Center for Long-Term Cybersecurity, Cybersecurity Policy Ideas for a New Presidency (Berkeley 2016), available at: https://cltc.berkeley.edu/files/2016/11/Center_for_Long_Term_Cybersecurity.pdf (accessed August 2017).

⁶⁵ See Bundesministerium der Verteidigung, Entwicklung des Organisationsbereichs bei der Bundeswehr, available at: <https://www.bmvg.de/de/themen/cybersicherheit/cyber-verteidigung/entwicklung-des-org-bereich-bei-der-bw> (accessed 14 August 2017).

⁶⁶ »Cyber-Sicherheitsstrategie« (note 59), p. 33.

⁶⁷ See, meanwhile, the EU Commission and the High Representative of the Union for Foreign Affairs and Security Policy Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN(2017) 450 final of 13 September 2017, available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=JOIN:2017:450:FIN&from=EN> (accessed 24 September 2017). Part of the Strategy is the new Proposal for a REGULATION of the European Parliament and of the Council on ENISA, the »EU Cybersecurity Agency«, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (»Cybersecurity Act«); available at: <https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF> (accessed 22 September 2017).

⁶⁸ Council Conclusions (9916/17) on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (»Cyber Diplomacy Toolbox«), available at: <http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf> (accessed 26 July 2017). See already Commission Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC_0410&from=DE (accessed 22 September 2017).

⁶⁹ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194/1, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG (accessed 26 July 2017).

in cyberspace and the regional confidence-building measures agreed by the OSCE». The Framework makes clear that »all of the EU's diplomatic efforts should as a priority be aimed at reducing the risk of misperception, escalation and conflict that may stem from ICT incidents«. ⁷⁰ With regard in particular to the problem of attribution it reminds us that this »remains a sovereign political decision based on all-source intelligence and should be established in accordance with international law of State responsibility«. ⁷¹ Not all measures of a joint diplomatic response to malicious cyber-activities, however, would require attribution. There is an EU toolbox but, except for a list of general principles and an invitation to the institutions and the Member States to further develop the Framework, the box is empty and crying out for concrete initiatives. Even a recent strategic note of the European Commission is relatively poor regarding efficient action at the global level. ⁷² The new EU Commission and the High Representative of the Union for Foreign Affairs and Security Policy's Joint Communication to the European Parliament and the Council ›Resilience, Deterrence and Defence: Building strong cybersecurity for the EU‹ of 13 September 2017 uses stronger words and, in particular, calls for »robust alliances and partnerships with third countries« as a fundamental tool for »the prevention and deterrence of cyber-attacks – which are increasingly central to international stability and security«. ⁷³ It declares itself ready to enhance »cyber-dialogues« and continue its efforts on »cybersecurity capacity building« in third countries so promoting a »rights-based capacity building model, in line with the Digital4Development approach«. ⁷⁴ And it also includes close cooperation with NATO that includes »countering hybrid threats« with a view to »strengthen resilience and response to cyber crises«, and »parallel and coordinated exercises in response to a hybrid scenario with NATO«. ⁷⁵

⁷⁰ Council Conclusions (note 64), para 3.

⁷¹ Ibid., para 4.

⁷² See the EU Commission's European Political Strategy Centre, Building an Effective European Cyber Shield. Taking EU Cooperation to the Next Level, Issue 24 of 8 May 2017, available at: https://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_24.pdf (accessed 14 August 2017), p. 14: »It will be indispensable to establish an agreed international regime, underpinned by three principles: (i) applicability of international law to cyberspace, just as to land, air or sea; 8ii) agreement on norms concerning acceptable behaviour of states in times of peace, voluntarily adhered to by states (e.g. no deliberate action against critical infrastructures); and (iii) confidence-building measures to build trust, reduce risks and increase transparency«.

⁷³ Joint Communication (note 67), point 4.1.

⁷⁴ Ibid., point 4.2., this including the setting up of »a dedicated EU Cyber Capacity Building Network... bringing together the EEAS, Member States' cyber authorities, EU agencies, Commission services, academia and civil society«.

⁷⁵ Ibid., point 4.3.

The examples given show that, so far, in spite of certain efforts at national and European level, we are far from having developed efficient instruments of cyber-risk management. A comprehensive approach to cybersecurity governance includes private individuals, business corporations and civil society in addition to the public authorities at all levels.⁷⁶

From a constitutional perspective, however, the focus here will be on public authorities and the question of how the public interest in cybersecurity can best be articulated democratically and effectively implemented at the diverse levels. Following a short discussion below of the strategy and measures to be considered for an appropriate risk management (infra 1), multilevel constitutionalism will then be presented as a normative theory (infra 2) that can offer a basis for implementing the strategy and taking action in an ordered, effective and democratic way (infra 3).

1. Risk Management: Strategy and Measures

Cybersecurity is often understood to mean defence against cyber-attacks in a classic warlike sense, particularly within the military context of cyberwar: deterrence, hack-back, and the protection of civilians are discussed in the same way as the Geneva Conventions. The most striking example is the ›Tallinn Manual‹ that seeks to interpret international law, including the terms of armed attack, self-defence and humanitarian law in a way applicable to cyberwarfare.⁷⁷ While this is an important work, in respect of the risks arising from governmental threats, the underlying approach largely misses the point.

Given the difficulties of attribution, a meaningful strategy needs to be based upon a different approach: The key features of this approach are enhanced resilience of the entire IT environment, digital literacy and an enhanced diligence

⁷⁶ See details in: Pernice, Cybersecurity Governance (note 2), pp. 18-26.

⁷⁷ Michael N. Schmitt (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence (Cambridge University Press, 2013), available at: <https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf> (accessed 24 September 2017). For some comments on this impressive document see Ingolf Pernice, Vom Völkerrecht des Netzes zur Verfassung des Internets. Privacy und Digitale Sicherheit im Zeichen eines schrittweisen Paradigmenwechsels, in: HIIG Discussion Paper Series No. 2017-02, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959257 (accessed 10 June 2017), p. 14-21. A second edition of this Manual has been published as ›Tallinn Manual 2.0‹ in 2017, see: http://assets.cambridge.org/9781107177222/frontmatter/9781107177222_frontmatter.pdf (accessed 24 September 2017). It takes a broader perspective and also covers cybersecurity in peace situations. According to the book information provided by CUP, ›...it addresses such topics as sovereignty, state responsibility, human rights, and the law of air, space, and the sea. Tallinn Manual 2.0 identifies 154 ›black letter‹ rules governing cyber operations and provides extensive commentary on each rule‹.

of suppliers and users of IT products.⁷⁸ Public authorities must have a common responsibility, derived from internationally agreed fundamental rights, to promote and ensure, for example:

- the awareness of the developers, producers and owners of IT systems as well as of the users for the risks in all diverse applications. This awareness is coupled with their co-responsibility for the functioning of the entire system;
- a responsible choice and diligent use of IT devices by everybody, taking account of the possible vulnerabilities of the technology and the need for regular backups of documents and of software updating;
- the elaboration, observance and implementation by producers of the highest technical standards regarding the privacy and security of hardware and software through privacy- and security-engineering;
- the development and application of strong encryption technologies for the protection of communication among users and with private or public service providers, including e-government and e-democracy;
- intensive research and development in security and resilience technologies both at universities and in industries, to be promoted and sponsored by private foundations as well as public finances;
- systems of instant information about attacks on, or abuses of data, as well as about cyber-incidents, allowing those potentially exposed to such attacks to take timely measures of self-protection;
- regulation on minimum security requirements for hardware and software, on liability for the negligent offering or use of unprotected or vulnerable IT products, as well as on cyber-crime;
- the development of an international cybersecurity culture including the sincere commitment of all governments to abstain from cyber-attacks on foreign infrastructures and political processes and to engage in a coordinated common cybersecurity policy.⁷⁹

⁷⁸ On this line see now the Joint Communication (note 67), in particular at point 2: »Building EU Resilience to Cyber Attacks« proposing the strengthening of ENISA, the adoption of an »EU cybersecurity certification framework«, the »screening of foreign direct investment in the European Union«, but also »resilience through rapid emergency response« as well as »a cybersecurity competence network with a European Cybersecurity Research and Competence Centre« and »building a strong Eu cyber skills base«. Also »promoting cyber hygiene and awareness« is among the list of actions to be taken.

⁷⁹ For a step-by-step approach, starting with a code of conduct with regard to the establishment, by international agreement, of an international »Special Necessity Regime for Cyber Incidents«, see Christian Schaller, *Beyond Self-Defence and Countermeasures. A Critical*

There should be a general ban on any state launching cyber-attacks on others, just as there are international agreements on a ban on biological and chemical weapons.⁸⁰ Malicious cyberactivities against other states must be understood as new and specific forms of intervention in the internal affairs of the targeted state, contrary to the principle of equal sovereignty in Article 2 (1) of the Charter of the United Nations.⁸¹ In the field of cyberspace state responsibility under international law fully applies not only to states⁸² but also – within the limits of the due diligence obligations – to the malicious activities of private bodies acting from their territory.⁸³ States have a duty to prevent cyber-attacks being launched from their territory on foreign territories. Since these international principles cannot easily be enforced, not least because of the problem of attribution, risk management in the digital constellation requires the consideration of a broader set of measures and enhanced precautions. Apart from the kinds of action mentioned above, an important precondition for the safe use of the internet and cybersecurity is a reliable and safe identification tool both for the user and for those who provide services, including public administration. Beyond the call for secure e-identity based upon the application of the electronic identity card nationwide,⁸⁴ there is a need for a much broader, globally accepted and applicable system of authentication and e-identity as a corollary of the global use of the internet in markets, social networks, information and politics, and as a condition for democratic processes at the global level.⁸⁵

Cybersecurity in the digital constellation, therefore, requires joint efforts by all participants and actors and an appropriate coordination of their action globally so as to achieve the common objectives. If public authorities at all levels have a particular constitutional duty to take effective action with the aim of achieving a

Assessment of the Tallinn Manual's Conception of Necessity, in: 95 Texas Law Review (2017), pp. 1619,1636-38.

⁸⁰ On the history, reasons and effects of the conventions of 1972 and 1993 see: ICRC, Chemical and biological weapons, available at: <https://www.icrc.org/en/document/chemical-biological-weapons> (accessed 14 August 2017).

⁸¹ For this interpretation and practice under Article 2 (1) UN-Charter see: Knut Ipsen, Völkerrecht, 4th ed. (C.H. Beck, München 1999), pp. 955-61; for the duty, or principle, of non-intervention connected with Article 2(1) UN-Charter see also Ian Brownlie, Principles of Public International Law, 7th ed. (OUP, Oxford 2008), pp. 289, 292.

⁸² See the Tallinn Manual 2.0 (note 72), pp. 79-80.

⁸³ *ibid.*, p. 83; see also *ibid.*, Rule 7, with comments (p. 43)

⁸⁴ See the German ›Cyber-Sicherheitsstrategie‹ (note 59), p. 16.

⁸⁵ A first step has been achieved at the EU level with the entry into force in June 2016 of Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ 2016 L 257/73, available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=DE> (accessed 15 August 2017). It is based upon the mutual recognition of national identification schemes notified to the Commission by each of the Member States, and so does not provide for a common e-identity scheme for the EU citizen.

high degree of resilience of the IT systems, this excludes, in particular, keeping secret and making use of previously undisclosed flaws («zero-day» exploits) in software by intelligence services to penetrate into a targeted network; on the contrary, it requires protecting as many computer systems as possible by adequate information.⁸⁶

2. Constitutional Framework: Multilevel Constitutionalism

Public authorities at all levels, states and the European Union have a constitutional obligation, therefore, in accordance with their respective constitutional powers, to take action in the form of legislative and administrative instruments in order to make cyberspace a safer place. And they have already undertaken, as has already been mentioned, the first few steps to meet the challenges. With regard to the global dimension of the internet and the related risks, however, such actions, though well-intended and of great value, may well be ineffective, at least with regard to activities originating in other parts of the world.

It is for this reason that action has also been taken at the global level both in the form of international conventions and intergovernmental coordination within international bodies such as the UN. Yet the effectiveness of the approach based upon international law is questionable. Increasing new risks require innovative strategies of risk management and, in particular, the need to overcome traditional concepts like national sovereignty and international cooperation. Let me explain, first, the deficiencies of the international law approach and, second, give an outline of what multilevel constitutionalism offers instead. It seems to allow the establishment of a constitutional framework for risk-management also at the global level without establishing a world-state.

a. Deficiencies of the International Law and Cooperation Approach

Regarding cooperation through international conventions, the only instrument in force is the «Budapest Convention on Cybercrime» of 2001. It was adopted

⁸⁶ For the problem and debate on this issue see Zachary K. Goldman and Samuel J. Rascoff, Introduction. The New Intelligence Oversight, in: Goldman/Rascoff, Global Intelligence Oversight (note 54), p. xvii, xxvii, xxxi.

within the framework of the Council of Europe, and is open for ratification by non-member countries too.⁸⁷ Other conventions, like the ›African Union Convention on Cyber Security and Personal Data Protection‹, adopted in June 2014, have not yet been ratified. Given the urgency of effective action, the negotiation, conclusion and ratification of a convention takes more time than is available, and anyway international conventions lack both enforceability and instruments for judicial protection. They are binding only on states that have ratified the agreement, and they need to be implemented by national legislation in order to have an effect on individuals and business. Though examples like the ›Rome Statute of the International Criminal Court‹ of 1998 establishing an individual criminal responsibility,⁸⁸ or the ›Bilateral Investment Treaties‹ (BIT) allowing, through provisions for investor state dispute settlement (ISDS), for the worldwide enforcement of damages by private investors against states violating their rights under such agreements,⁸⁹ these special cases are difficult to replicate, the treaties have no general global application and, above all, even if states accept that there is a need for an international convention on cybersecurity with a similar degree of effectiveness, there is no time to wait for this to be achieved.

This does not mean that international cooperation and agreements are useless. The 2016 ›Technical Arrangement on Cyber Defence‹, concluded between the NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team of the European Union (CERT-EU), for instance, provides as a technical arrangement an important »framework for exchanging information and sharing best practices between emergency response teams«.⁹⁰ The ›EU-NATO joint declaration‹ of 8 July 2016 in particular emphasises the determination to »expand our coordination on cybersecurity and

⁸⁷ The Convention has been in force since 1 July 2004, with 55 ratifications so far. For details see: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185> (accessed 27 June 2017).

⁸⁸ Rome Statute of the International Criminal Court, 1998, see: <https://www.icc-cpi.int/NR/rdonlyres/ADD16852-AEE9-4757-ABE7-9CDC7CF02886/283503/RomeStatutEng1.pdf> (accessed 8 August 2017).

⁸⁹ For an overview on the existing 2954 BITs worldwide see: UNCTAD Investment Policy Hub, available at: <http://investmentpolicyhub.unctad.org/IIA>. For an overview of the ISDS arrangements see *ibid.*, available at: <http://investmentpolicyhub.unctad.org/ISDS>, and for the cases decided or pending see the country-by-country overview available at: <http://investmentpolicyhub.unctad.org/ISDS/FilterByRulesAndInstitution> (all accessed 8 August 2017). With regard to specific EU problems of ISDS in the cases of CETA and TTIP see the contributions of: Piet-Jan Cuijper/Steffen Hindelang/Ingolf Pernice, *Investor-State Dispute Settlement (ISDS) Provisions in the EU's International Investment Agreements*, Vol. 2 – Studies (European Parliament, INTA 2014), available at: [http://www.europarl.europa.eu/thinktank/en/document.html?reference=EXPO_STU\(2014\)534979](http://www.europarl.europa.eu/thinktank/en/document.html?reference=EXPO_STU(2014)534979) (accessed: 24 September 2017).

⁹⁰ See: NATO and the European Union enhance cyber defence cooperation, 10 February 2016, on the NATO website, available at: http://www.nato.int/cps/en/natohq/news_127836.htm (accessed 8 August 2017).

defence including in the context of our missions and operations, exercises and on education and training«.⁹¹ This is a little step in the right direction, but with its limitations, geographically as well as in substance, it is far from being a satisfactory solution to the problem of tackling global cybersecurity threats.

Already the UN General Assembly Resolution 64/211 rightly recognises »that a robust global culture of cybersecurity needs to be encouraged, promoted, developed and vigorously implemented«.⁹² In this vein, the United Nations »Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security« (GGE), has been created as a forum for discussing and reporting on key questions such as the applicability of international law to cyber space and state responsibility.⁹³ Its 2015 report »on Developments in the Field of Information and Telecommunications in the Context of International Security« particularly emphasises the »need for confidence-building measures«.⁹⁴ A new report is expected in September 2017. As the topic is politically sensitive and states are not yet ready to act effectively in common, it will not include any recommendation on a global cybersecurity strategy. Another relevant actor at the international level is the International Telecommunications Union (ITU).⁹⁵ It has been given the role of building »confidence and security in the use of Information and Communication Technologies (ICTs)«. It runs a Global Cybersecurity Index (GCI), which is a multi-stakeholder initiative monitoring the cybersecurity commitments of countries. And it has launched, already in 2007, the »Global Cybersecurity Agenda« (GCA), establishing a »framework for international cooperation aimed at enhancing confidence and security in the information

⁹¹ Joint declaration by the President of the European Council, Donald Tusk, the President of the European Commission, Jean-Claude Juncker, and the Secretary General of NATO, Jens Stoltenberg, Warsaw 8 July 2016, available at: http://www.consilium.europa.eu/press-releases-pdf/2016/7/47244644040_en.pdf (accessed 24 September 2017).

⁹² Resolution 64/211. Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, 21 December 2009, available at: <https://ccdcoe.org/sites/default/files/documents/UN-091221-CultureOfCSandCI.pdf> (accessed 24 September 2017). Similarly, already the UN General Assembly Resolution 58/199, available at: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/58/199 (accessed 24 September 2017).

⁹³ See the overview on national reports available at: <https://www.un.org/disarmament/topics/informationsecurity/> (accessed 22 September 2017). The latest examples of GGE reports to the UN Secretary General are the Report of 22 July 2015 at: <http://undocs.org/A/70/174> (accessed 24 September 2017) and the Report of 19 July 2016, available at: <http://undocs.org/A/71/172> (accessed 24 September 2017).

⁹⁴ UN General Assembly Doc. A/70/174 of 22 July 2015, available at: <https://undocs.org/A/70/174> (accessed 24 September 2017).

⁹⁵ See: <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx> (accessed 22 September 2017).

society».⁹⁶ The ITU is active in standard-setting, and a subgroup has issued a technical report of high quality on »Cyber-security, data protection and cyber resilience in smart sustainable cities«.⁹⁷

Raising awareness of the risks and the need for action, perhaps a degree of exchange and joint learning about best practices, are valuable aspects of the work of these international bodies. All of this is a first step, but insufficient in terms of the increasing need for rapid and effective action within a coordinated strategy of risk management worldwide.

b. What »Multilevel Constitutionalism« Means and Offers

To make risk management in the digital constellation effective, some kind of global system of decision-making and binding regulation is required. Norms have to be set that are binding not only on states or organisations but also directly on individuals. There must be provision for enforcement, judicial review and for an effective protection of fundamental rights. Furthermore, the system must be designed and also recognised as being democratically legitimate. Such requirements remind us of the model of a constitutional state, yes. But to some extent, they are also met by the constitution of the European Union. It seems to be possible to extend the constitutional approach beyond the state and apply it to the statute of a framework for regulation at the global level.⁹⁸ While this framework cannot look like the constitution of a state, it may follow the logic of constitutionalism. Diverse attempts to conceptualise a cosmopolitan concept lack plausibility, for they do not explain the relationship of existing states and their constitutions, including the idea of sovereignty, to cosmopolitan democracy.

Here is where »multilevel constitutionalism« seems to offer a perspective of thinking beyond traditional patterns of constitutional theory.⁹⁹ In short, this

⁹⁶ See: <https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx> (accessed 24 September 2017). For the Chairmen's Report of the first year's work and recommendations see: <https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf> (accessed 24 September 2017).

⁹⁷ See: ITU-T Telecommunication Standardisation Sector of ITU, Focus Group on Smart Sustainable Cities (2/2015), link to pdf available at: <https://www.itu.int/en/ITU-T/focusgroups/ssc/Pages/default.aspx> (accessed 24 September 2017).

⁹⁸ Supra, note 3.

⁹⁹ For the concept see: Ingolf Pernice, Multilevel Constitutionalism and the Treaty of Amsterdam: European Constitution-Making Revisited, in: 36 Common Market Law Review (1999), pp. 703-50, also available at: <http://www.whi-berlin.eu/documents/whi-paper0499.pdf> (accessed 22 September 2017); id., Europäisches und nationales Verfassungsrecht, Bericht, in: 60 Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer (De Gruyter, Berlin 2001), pp. 148-93, also available as WHI-paper at: <http://www.whi-berlin.de/documents/whi-paper1301.pdf> (accessed 22 September 2017). Spanish translation (by A. Lopez-Pina): Derecho constitucional europeo y Derecho constitucional de los Estados miembros, in: 8 Revista española de Derecho Europeo (2003), pp. 601-38. For a critique of the concept from a legal theory point of view see: Matthias Jestaedt, Der Europäische Verfassungsverbund – Verfassungstheoretischer

concept consists of four assumptions: (1) It is centred not in states and national sovereignty, but in the individual sovereignty of each human being. (2) Sovereign powers are attributed by the people of the community to the institutions at each respective level of political action and shared with institutions at the other levels of action. (3) The allocation of powers to the levels of action is guided by the principle of subsidiarity that ensures a maximum of effectiveness and of democratic control at each level, allowing the greatest degree possible of political self-determination of the individual. (4) The different levels of political action and their respective constitutional statutes are not independent and isolated from each other, but components of a composed interwoven and layered constitutional system based upon the rule of law.

(1) The Individual in the Center

The point of departure of »multilevel constitutionalism« is as simple as it is challenging: There is no other person, body or institution we can call sovereign but the human person. I draw this from the idea of human dignity which means, in normative terms, the original right of self-determination and the duty to respect the dignity – or otherness – and the right of self-determination of the other.¹⁰⁰ As we can learn from contractual political philosophy – from Hobbes to Rousseau and Locke –, people confer powers on common institutions, established in order to protect the security of all citizens against attacks from others, and to lay down binding rules as necessary for ensuring peaceful life in a community. This arrangement is what we call the Constitution of the political body - the State - whose people define themselves and their respective rights as citizens.

(2) Sharing Sovereignty – or the Principle of Attribution

If this admittedly very short description is correct, we can go one step further: Jean Monnet and Robert Schuman understood, after two terrible wars and several centuries of brutal military conflicts among European nations, that the Westphalian model of the sovereign state – including international law – had

Charme und rechtstheoretische Insuffizienz einer Unschärferelation, in: R. Krause et al. (eds.), *Recht der Wirtschaft und der Arbeit in Europa*, Gedächtnisschrift für W. Blomeyer (Duncker & Humblot 2004) p. 638, also published in C. Calliess (ed.), *Verfassungswandel im europäischen Staaten- und Verfassungsverbund*, Göttinger Gespräche zum deutschen und europäischen Verfassungsrecht (Mohr Siebeck, Tübingen 2007) pp. 93-127. For a reply: Ingolf Pernice, *Theorie und Praxis des Europäischen Verfassungsverbundes*, *ibid.*, pp. 61-92. See also the critiques of René Barents, *The Fallacy of European Multilevel Constitutionalism*, in M. Avbelj and J. Komárek, (eds.), *Constitutional Pluralism in the European Union and Beyond* (Hart 2012) p. 153, and as a reply Ingolf Pernice, *Multilevel Constitutionalism and the Crisis of Democracy in Europe*, 11 *EuConst* (2015), pp. 541-62.

¹⁰⁰ See in more detail: Pernice, *Global Constitutionalism* (note 2), pp. 152-55.

failed. It was unable to preserve peace, the basic condition for a life of freedom and prosperity. This insight led Monnet and Schuman to propose the new, somewhat revolutionary concept of supra-nationalism. It means sharing sovereignty and results in a process of »integration through law«,¹⁰¹ made by a supranational public authority vested with limited legislative, executive and judicial powers. While it was to be established through the means of international law, the EU Treaties created a new, legally autonomous level of political action. Specific provisions of the national constitutions open the way for the establishment of such a supranational power by authorising, in different ways, the democratic legislator to confer such power upon the institutions that have been established and organised by these treaties. This is the European Union.

You can argue, like the German Federal Constitutional Court and many others, that the authors of this creature, the »masters of the Treaties«, are the Member States, sovereign states.¹⁰² Yes, they can remain in the Union, but since the Treaty of Lisbon, they have also the »sovereign« power to leave it. Brexit seems to be a first example of an attempt to leave. But this case suggests that exit is not an easy process and may even not happen at all.¹⁰³

In my view, the masters of the Treaties, ultimately, are the citizens of the Member States. Let us take one step back: Who are the Member States, whom are governments representing in our democracies, when they negotiate and conclude international – or EU – treaties? Who could this be, if not the citizens of the states? And when a Parliament is ratifying such a treaty, who is it representing? The ratification entails the indirect consent of the people in the representative democracy, which is ultimately the same as in the case of a referendum required by the Constitution: The citizens are represented, or the people that form the citizen body. And why should we not say that, in the form of an international treaty, the citizens of the participant states as a whole, in ratifying, in accordance with their respective constitutional provisions by act of

¹⁰¹ For the term see already the series: Mauro Cappelletti/Monica Secombe/Joseph Weiler (eds.), *Integration Through Law. Europe and the American Federal Experience* (Walter de Gruyter, Berlin 1986) and, more recently, Andreas Voßkuhle, »Integration durch Recht« – Der Beitrag des Bundesverfassungsgerichts, 71 *Juristenzeitung* (2016), pp.161-68.

¹⁰² Particularly clear in this vein is: German Federal Constitutional Court (GFCC), case BVerfGE 89, 155 *Maastricht*, judgment of 12 October 1993, para 190. See also: GFCC, case BVerfGE 123, 267 *Lisbon*, judgment of 30 June 2009, paras 231, 235, 271, 289 and 334, available at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/06/es20090630_2bve000208en.html (accessed 8 August 2009).

¹⁰³ See Ingolf Pernice, *Brexit – exercise of democracy or a challenge to democracy?*, to appear at: SSRN.

parliament or directly by referendum, the EU Treaties, are concurring and agreeing upon the »constitution« of their new supranational union as an instrument to achieve their common goals?

(3) The Principle of Subsidiarity: Maximising Political Self-Determination

The term »constitution« is used for this special kind of agreement, for the EU Treaties contain – in essence – exactly what constitutions are about: People are establishing institutions, conferring powers on these institutions, organising their decision-making processes and laying down the objectives of the new organisation as well as the rights and duties of the individuals who, by doing this, define themselves as the citizens of the Union. The form of an international treaty is irrelevant: the content counts.

What can be seen here is this: people – together with people from other states – convene upon a common constitution that is applicable to themselves in addition to and beyond their respective constitutions. This common constitution does not compete with but builds upon and is complementary to the national constitutions. It is created for different purposes and objectives, objectives that cannot be achieved by one single Member State on its own. Like the national constitution, therefore, it is a self-referential act of sovereignty of people defining themselves as the citizens of the supranational (or potentially global) community.¹⁰⁴ It does not take away sovereignty from the Member States, for the matters it is given competence for are beyond the reach of national sovereignty. In this sense, establishing this additional framework for political action in the common interest even adds sovereignty to the people(s), allows the citizens better self-determination through options that enable the Union to act effectively even beyond the borders and powers of the individual state. The statement by Jürgen Habermas quoted above exactly reflects what is meant here: insofar as the state is unable to act effectively, it is a requirement of the normative meaning of democracy to extend decision-making capabilities beyond the state. Pooling sovereignty at the supranational level, therefore, means the democratic self-empowerment of the citizens, allowing them to do what they could not achieve otherwise.

¹⁰⁴ For a theoretical foundation of the idea of sovereignty of the citizen see: Majid Behrouzi, *Democracy as the Political Empowerment of the Citizen. Direct-Deliberative e-Democracy* (Lexington Books 2005), pp. 2-5, 13-17, 27-33, 131-70; see also Ingolf Pernice, *Europäisches und nationales Verfassungsrecht, Bericht*, in: 60 *Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer* (Walter de Gruyter, Berlin 2001), pp. 148, 162-63, 166, 174-75.

The steering principle, both for the attribution of powers and for the exercise of the conferred competences, is the principle of subsidiarity. It means that – with a view to ensuring a maximum of individual self-determination – your family steps in when you cannot help yourself, the local community does so if the family is unable to help, the regional government is called upon to rule where local authorities cannot effectively act, and then the state, and then the European Union do the same and so on and so forth. Can we imagine that one day there will be a global governing body or structure deciding upon matters of common concern of the global society? Why not if there is a need for global regulation? And indeed, there is a need.

(4) The Citizen's Multiple Identities in a Composed Constitutional System

Multilevel constitutionalism allows us, thus, to conceive of a pluralism of constitutions as components of one multilevel system of governance, the source of legitimacy of which is the citizen. These citizens have multiple political identities: They may be Barcelonian, but also Catalán, Spanish, European and global citizens. From the perspective of the citizen, these identities can be represented by a series of concentric circles: Each circle comprises the citizens of the other polities of the same level: the local community, the region, the nation-state, the EU and, at some time, the global community. While the relative political influence of each individual decreases with its distance from the centre, the horizon – or reach – of the action taken increases at each supplementary level. Democratic self-determination is not limited to nations or bounded by national borders any more, as long as the principle of subsidiarity is respected and the necessary provision is made for an equal voice of every citizen in the decision-making processes at each level. According to the idea of subsidiarity, and for the sake of democratic self-determination, decisions must be taken »as closely as possible to the citizen«. This is what Article 1 (2) TEU requires, but it is true for whatever supranational or global entity might be established to manage global risks.

c. Towards Global Constitutionalism

In some way similar to the federalist model and in spite of important structural differences, the EU can be understood as a materialisation of multilevel

constitutionalism. It is open to being extended to the global level¹⁰⁵ with due regard, though, for the very different conditions we are confronted with in a context of more than 7 billion people living in more than 190 states, some of which are failed states, and many of which are anything but democratic. Yet it is quite possible that over time and with the increasing spread of the internet and online-services the interest in cybersecurity, like that in managing other global risks, may grow stronger, worldwide, and come to take priority over national sovereignty that more and more reveals as a dangerous illusion. The need to preserve security in cyberspace, together with the desire to benefit from the opportunities offered by the ICTs, may even become a driving force for establishing a global constitutional frame for common regulatory solutions applicable throughout the world.

3. Global Risk Management and Multilevel Constitutionalism

Multilevel constitutionalism, therefore, can add a constitutional perspective to the debate about risk management in the digital constellation. It allows us to conceptualise a framework for regulation at the global level with a high level of democratic legitimacy, rooted in the will of the people of the globe. This regulation could concern cyber-crime and the establishment of information and alert systems, include minimum requirements on cybersecurity and privacy by design, and guidelines for technical standardisation and certification, lay down globally applicable provisions for data protection and cybersecurity in line with initiatives at the UN level, and even concretise the responsibilities and duties of states and supranational organisations regarding cybersecurity.

Granted, we already have concerns about the democratic deficit in the EU. Would these problems not be multiplied with a global constitutional setting of this kind? This is difficult to say, but a provisional answer would consist of three considerations: First, digitisation also has the potential to remedy some of the

¹⁰⁵ For first attempts in this direction see: Ingolf Pernice, *The Global Dimension of Multilevel Constitutionalism: A Legal Response to the Challenges of Globalisation*, in: P.M. Dupuy/B. Fassbender/M.N.Shaw/K.-P. Sommermann (Hrsg./Editors), *Völkerrecht als Wertordnung. Common Values in International Law, Festschrift für/Essays in Honour of Christian Tomuschat*, (N.P. Engel, Kehl-Strasbourg-Arlington 2006), pp. 973-1005, also available at: <http://www.wi-berlin.eu/documents/whi-paper0908.pdf> (accessed 24 September 2017). Span. translation (Osvaldo Saldías): *La dimensión global del Constitucionalismo Multinivel. Una respuesta global a los desafíos de la globalización*, Documento de Trabajo. Serie Unión Europea y Relaciones Internacionales, no. 61/2012, available at: <http://www.idee.ceu.es/Portals/0/Publicaciones/Docuweb%20doc%20%2061%20UE.pdf> (accessed 24 September 2017).

legitimacy problems of the EU.¹⁰⁶ Second, the constitutional setting for democratic decision-making and regulation at the global level could not be a simple clone of a national or the EU constitution; much more room must be given to deliberation and state responsibilities regarding action taken by new public authorities established at the global level.¹⁰⁷ And third, the potential of the internet to make global democracy a reality is far from being exhausted.¹⁰⁸

Constitutionalism is based upon the ownership of the individual and trust in the legitimacy and proper functioning of an institutional setting for political action, a system that is rooted in its own will and participative engagement. It requires a legal statute, providing for equal fundamental and political rights and their effective protection, transparency, accountability and the respect of the rule of law. Global constitutionalism, accordingly, is about appropriate institutions, procedures and equal rights of the citizens of the global community established through this statute, a legal statute, which would be complementary to and based upon the constitutions of states and supranational organisations according to the principles of multilevel constitutionalism.

Both for the processes of establishing and designing this statute, and for its operation and the exercise of the specific and limited powers attributed to the global institutions, the internet with the opportunities it offers for a borderless, open and transparent political discourse seems to play a key role. It also allows for an integrated scheme of e-identity for the global citizens who will be at the root of this global constitutional frame for common policies. At the same time, cybersecurity, including provision of protection against »information operations« by foreign powers or private actors against democratic processes in states, massive disinformation campaigns and manipulation through psychographic targeting,¹⁰⁹ is a condition for the beneficial use of the internet in these contexts.¹¹⁰ The need for effective action here may become one of the

¹⁰⁶ See Ingolf Pernice, E-Government and E-Democracy: Overcoming Legitimacy Deficits in a Digital Europe, in: Lina Papadopoulou/Ingolf Pernice/Joseph H.H.Weiler (eds.), *Legitimacy Issues of the European Union in the Face of Crisis* (Nomos 2017), pp. 287-316, see also WHI-paper 4/2015, available at: http://www.whi-berlin.eu/tl_files/WHI-Papers%20ab%202013/WHI-Paper%20042015.pdf (accessed 22 September 2017) and HIIG Discussion-Paper 2016/01, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2723231 (accessed 22 September 2017).

¹⁰⁷ For a tentative outline see Pernice, *Global Constitutionalism* (note 48).

¹⁰⁸ For a very balanced study of the potential of the internet see Coleman (note 29), p. 57, 84-119.

¹⁰⁹ See Donahoe, *Algorithms* (note 56).

¹¹⁰ In this vein also the Joint Communication (note 67), point 2.7: »Awareness-raising in relation to online disinformation campaigns and fake news on social media specifically aimed at undermining democratic processes and European values is equally important«.

driving forces of a constitutional process for the framework that makes possible effective action at the global level.

Experiences of open deliberation models in internet governance and multi-stakeholder processes will be of great value in this process,¹¹¹ as will be an open, creative and cooperative spirit in governments and political leaders who understand the urgent need for a democratic global risk management in the digital constellation.

Conclusion

Much work, commitment and idealism are required for turning theory into practice. My optimism is fed by the simple assumption that the digital constellation does not leave much time and room for hesitation or alternatives. It may be possible to encourage the big internet corporations operating in the global market to agree among each other upon common rules on cybersecurity, rules they would enforce through their sheer market power. Or they work closely together with state actors having understood the common interest in safe communication systems worldwide. An attempt to initiate this kind of cooperation is the ›Tech Accord‹, proposed recently by Microsoft, an agreement among business undertakings requiring them not to assist »offensive cyber operation«, to protect customers, and to bolster first-response efforts.¹¹² This approach could be an important step forwards, though nobody can ensure that it would be respected by all relevant business undertakings worldwide and therefore effective. Equally, the attempts to rely upon institutions established under private law, like ICANN, or upon private standardisation or multi-stakeholder processes of internet-governance, are not likely to bring about binding law nor to be effective where public authority is called upon to play its role. ICANN seems to be unique regarding its key role in the functioning of the internet, its governance structure and its effectiveness.¹¹³ It was established and

¹¹¹ For an attempt to explain the theoretical foundations and a possible design of such a framework see: Ingolf Pernice, E-Democracy, the Global Citizen, and Multilevel Constitutionalism, in: Corien Prins, Colette Cuijpers, Peter L. Lindseth, Mónica Rosina (eds.), *Digital Democracy in a Globalised World* (Edward Elgar, Cheltenham 2017), pp. 27-50.

¹¹² See the proposals made by Microsoft: A Tech Accord to protect people in cyberspace, available at: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW6iCh> (accessed 12 June 2017).

¹¹³ Conceptualizing ICANN and in particular the Domain Name Dispute Resolution Policy (UDRP), as a case of »self-constitution« in a multi-stakeholder process: Lars Viellechner, *Transnationalisierung des Rechts* (Velbrück, Weilerswist 2013), pp. 253-64 (emergence of constitutional norms: »Eigenkonstitutionalisierung«).

grew during a pioneering period of the internet,¹¹⁴ but it is difficult to imagine that a new organisation would be accepted for the effective management of the problems mentioned above concerning privacy, property, freedom and democracy. Finally, with valuable ideas and the best intentions, the recent Microsoft initiative for the establishment of a ›Digital Geneva Convention to Protect Cyberspace‹,¹¹⁵ perhaps combined with the proposed establishment of an »Attribution Organisation« as a »private sector-led, independent and transparent« body to provide a »foundation of a fact-based, global dialogue about the nature of significant cyber-attacks«,¹¹⁶ could be a starting point for a public-private-partnership in cyber-risk management at the global level. Yet, there is little hope that such international agreements can be concluded more rapidly and that they will be more effective than other international arrangements.

The discussion about a constitutional framework for democratically legitimate regulation at the global level, therefore, is about to begin. The digital constellation is creating new risks and new instruments to make it a reality. The internet empowers the individual as a global citizen, and it is for each global citizen to take responsibility in the organisation of a system of self-rule on matters of global concern. One is risk management in the global risk society. Even if it is true that many countries in this world do not even comply with standards of democracy internally and so may not be willing to accept these standards for global regulation – they may even work in an opposite direction – it is a question of determination, time, negotiation and good diplomacy to find common ground and, step by step, establish, perhaps starting within a »coalition of the willing«,¹¹⁷ processes from which a global regime for risk management in the digital constellation will emerge.

¹¹⁴ Ibid., pp. 128-41.

¹¹⁵ For the document see: Microsoft, A Digital Geneva Convention to protect cyberspace, available at: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH> (accessed 12 June 2017).

¹¹⁶ Microsoft, An attribution organisation to strengthen trust online, available at: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QI> (accessed 12 June 2017).

¹¹⁷ For an analysis of the concept, once applied by George W. Bush, see Christian Callies/Georg Nolte/Peter-Tobias Stoll (eds.), *Coalitions of the Willing: Avantgarde or Threat?* (Carl Heymanns, Köln-München 2007).