IDP
REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

ARTICLE

Risk management in the digital constellation – a constitutional perspective (part II)*

Ingolf Pernice
Humboldt-Universität zu Berlin

Submission date: November 2017
Accepted date: April 2018
Published in: September 2018

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 what – 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 there 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 – 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 managing effectively, among other global challenges, cyber-risks at national, supra-national and global levels in a coherent way. Multilevel Constitutionalism is proposed as a means of providing a normative theory for conceptualising the constitutional structure of a layered system of governance that ensures 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 complementary, based upon functioning states, and designed to deal with issues that are beyond their reach, including cybersecurity.

* This paper is part II of an extended and updated version of a key-note given at the Congrés IDP 2017 'Managing Risk in the Digital Society. Internet, Dret i Política', in Barcelona 30 June 2017. I would like to express my deep gratitude to Dr Christian Djeffal and Jörg Pohle, research assistants at the HIIG, for their invaluable comments and observations on an earlier version of this paper.

Keywords

risk society, democracy, postnational constellation, digitization, cybersecurity, risk management, digital constellation, global citizen, multilevel constitutionalism, shared sovereignty, subsidiarity, multiple identities, global constitutionalism

Topic

Law, constitutional theory

La gestión de riesgos en la constelación digital — una perspectiva constitucional (parte II)

Resumen

La revolución digital está creando nuevos riesgos y, a la vez, múltiples oportunidades para la comunicación, el comercio y la participación política. Lo que Ulrich Beck describió como la sociedad mundial del riesgo y –desde otra perspectiva– lo que Jürgen Habermas llama la «constelación postnacional» es un desafío a nuestros conceptos de sociedad y democracia. La digitalización está impulsando este desarrollo hacia una nueva dimensión que nos permite hablar de la «constelación digital». Las relaciones sociales son más densas a través de las fronteras y los continentes; lo que ocurre ahí importa como si ocurriera en nuestra propia puerta. Surgen nuevos tipos de riesgos como efecto secundario del uso creciente de las tecnologías de la información, mientras que Internet también ofrece – por primera vez – una infraestructura que hace de los conceptos hasta ahora poco realistas de democracia cosmopolita (David Held) una opción real. Esto incluye el establecimiento de un marco constitucional para los procesos normativos que trata, entre otros desafíos mundiales, de gestionar de manera coherente y eficaz los riesgos cibernéticos a nivel nacional, supranacional y mundial. El constitucionalismo a varios niveles se propone como un medio de aportar una teoría normativa para conceptualizar la estructura constitucional de un sistema de gobernanza en capas que garantice el máximo grado de autodeterminación del individuo y, por tanto, la legitimidad democrática de las decisiones tomadas en cada nivel, desde lo local hasta lo global. Por lo tanto, la constitución para una acción democráticamente legítima a nivel global no cuestiona la democracia en otros niveles, sino que debe ser complementaria, basada en estados que funcionen y diseñada para tratar temas que están fuera de su alcance, incluyendo la ciberseguridad.

Palabras clave

sociedad del riesgo, democracia, constelación postnacional, digitalización, ciberseguridad, gestión del riesgo, constelación digital, ciudadano global, constitucionalismo a varios niveles, soberanía compartida, subsidiariedad, identidades múltiples, constitucionalismo global

Tema

Derecho, teoría constitucional

II. Risk Management and Multilevel Constitutionalism

According to the challenges and opportunities of the digital constellation, set out in Part I of this study, steps towards 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 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 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 – or the principle of – security as spelled out in the constitutions and the European and international instruments for the protection of human rights.[1] 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 states[2] and also the European Union[3] are each developing their own cybersecurity strategies.[4] The 2015 U.S. Cyber Strategy was based upon defensive and offensive capabilities for cybersecurity, 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.[5] The new U.S. administration has adopted a strategy only very recently,[6] while some important ideas for a "new cyber security agenda" had been submitted to the U.S. government already in November 2016.[7] In the introduction of this policy paper the authors stressed 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.[8] It is part of the German Cyber-Security Strategy (2016), which is characterised by a cooperative approach with both business and European and international partners.[9] Apart from an updated EU

1. See details in Leuschner (2018).
2. For an overview see the NATO Cooperative Cyber Defense Centre of Excellence (DDCDOE) (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, 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" (Bundesministerium des Innern, 2016). See also the Law on the Federal Office for IT Security (Gesetz über das Bundesamt für Sichereheit in der Informationstechnik (BSIG) of 2009/17, at <https://www.gesetze-im-internet.de/bsig_2009/BSIG.pdf> [Accessed: 26/072017] and the Law on Enhanced Security of IT Systems ("IT-Sicherheitsgesetz") of 2015 at <https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1501068552430> [Accessed: 26/07/2017].
3. See the 2013 "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", JOIN(2013) 1 final, at: <http://www.eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf> [Accessed: 17/07/2017); the "Eighth Progress Report Towards an Effective and Genuine Security Union" (COM(2017) 354 final), promises a revision of this Strategy by September 2017, 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>; see also Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") (2017). For an overview see the EU Commission's "Factsheet EU cybersecurity initiatives" (2017).
4. For a renewed strategy see: ENISA (2017).
5. On all this, see Cage (2015). See, however recently, White House (2017); and the important proposals of Sven Herpig (2018).
6. For some points on cyber security in the 2015 U.S. National Security Strategy, see Segal (2015). 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 (2015). The US Department of Homeland Security has adopted the "Cybersecurity Strategy" (2018).
7. Center for Long-Term Cybersecurity (2016).
8. See Bundesministerium der Verteidigung (2017).
9. ENISA (2017).

Cybersecurity Strategy announced for September 2017,[10] 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".[11] The NIS-Directive[12] 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 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".[13] 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".[14] 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.[15] 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".[16] It declares itself ready to enhance "cyber-dialogues" and continue its efforts on "cybersecurity capacity building" in third countries, thus promoting a "rights-based capacity building model, in line with the Digital4Development approach".[17] And it also includes close cooperation with NATO that embraces "countering hybrid threats" with a view to "strengthen[ing] resilience and response to cyber crises", and "parallel and coordinated exercises in response to a hybrid scenario with NATO".[18]

The examples given show that, thus far, in spite of certain efforts at the national and European levels, we are far from having developed efficient instruments for cyber-risk management. A comprehensive approach to cybersecurity governance would include private individuals, business corporations and civil society in addition to the public authorities at all levels.[19]

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

10. See the EU Commission and the High Representative of the Union for Foreign Affairs and Security Policy (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"); at: <https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF> [Accessed: 22/09/2017].
11. European Council (2017). See European Commission (2016).
12. 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: 26/07/17].
13. European Council, para. 3.
14. Ibid., para. 4.
15. See the EU Commission's European Political Strategy Centre (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; (ii) agreement on norms concerning acceptable behavior 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".
16. EU Commission and the High Representative of the Union for Foreign Affairs and Security Policy (2017, point 4.1).
17. 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".
18. Ibid., point 4.3.
19. See details in: Pernice (2017b, pp. 18-26).

measures to be considered for 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 cyber warfare.[20] While this is important work as regards 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 of suppliers and users of IT products.[21] 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 their users about 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 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 vulnerabilities as well as on 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 and certification 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.[22]

20. Schmitt (2013). For some comments on this impressive document see Pernice (2017a, p. 14-21). A second edition of this Manual has been published as 'Tallinn Manual 2.0' (Schmitt, 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."
21. On this line see now the Joint Communication (note 159), 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". "Promoting cyber hygiene and awareness" is also among the list of actions to be taken.
22. 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 Schaller (2017, p. 1619, 1636-38).

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.[23] Malicious cyber activities 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.[24] In the field of cyberspace, state responsibility under international law fully applies not only to action of states[25] but also – within the limits of due diligence obligations – to the malicious activities of private bodies acting from their territory.[26] 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,[27] 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.[28]

Cybersecurity in the digital constellation, therefore, requires joint efforts by all participants and actors and 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 high degree of resilience of 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.[29]

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 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 risk management strategies and, in particular, the need to overcome traditional concepts such as national sovereignty and international cooperation. Let me explain,

23. On the history, reasons and effects of the conventions of 1972 and 1993 see: ICRC (2013).
24. For this interpretation and practice under Article 2 (1) UN Charter see: Ipsen (1999, pp. 955-61); for the duty, or principle, of non-intervention connected with Article 2(1) UN Charter see also Brownlie (2008, pp. 289, 292).
25. Schmitt (2017, pp. 79-80).
26. Ibid., p. 83; see also ibid., Rule 7, with comments (p. 43).
27. Bundesministerium des Innern (2016, p. 16).
28. 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, at: <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=DE> [Accessed: 15/08/17]. 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 EU citizens.
29. For the problem and debate on this issue see Goldman and Rascoff (2016, p. xvii, xxvii, xxxi). A differentiated approach in cases where the retention of the information may be needed for urgent security reasons, see the proposals of Herpig (note 4). With a call for "responsible disclosure" see Leisterer (2018, pp. 332-337). Weighing public security against inherent cybersecurity will need to be done in each particular case in the light of constitutional principles and fundamental rights.

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 within the framework of the Council of Europe and is open for ratification by non-member countries too.[30] 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. Despite examples like the Rome Statute of the International Criminal Court of 1998 establishing an individual criminal responsibility,[31] and 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,[32] 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 cyber security 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".[33] The "EU-NATO joint declaration" of 8 July 2016 in particular emphasises the determination to "expand our coordination on cyber security and defence including in the context of our missions and operations, exercises and on education and training".[34] 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 cyber security threats.

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".[35] 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.[36] Its 2015 report "on Developments in the Field of Information and Telecommunications in the

30. 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: 27/06/17].
31. Rome Statute of the International Criminal Court, 1998, see: <https://www.icc-cpi.int/NR/rdonlyres/ADD16852-AEE9-4757-ABE7-9CDC-7CF02886/283503/RomeStatutEng1.pdf> [Accessed: 08/08/2017].
32. For an overview on the existing 2954 BITs worldwide see: UNCTAD Investment Policy Hub, at: <http://investmentpolicyhub.unctad.org/IIA> [Accessed: 08/08/17]. For an overview of the ISDS arrangements see ibid., at: <http://investmentpolicyhub.unctad.org/ISDS> [Accessed: 08/08/17], and for the cases decided or pending see the country-by-country overview at: <http://investmentpolicyhub.unctad.org/ISDS/FilterByRulesAndInstitution> [Accessed: 08/08/17]. With regard to specific EU problems of ISDS in the cases of CETA and TTIP see the contributions of Cuijper, Hindelang and Pernice (2014).
33. See NATO (2016).
34. 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, at: <http://www.consilium.europa.eu/press-releases-pdf/2016/7/47244644040_en.pdf> [Accessed: 24/09/17].
35. UN Resolution 64/211 (2010). Similarly, the UN General Assembly Resolution 58/199 (2004).
36. See the overview on national reports at <https://www.un.org/disarmament/topics/informationsecurity/>. 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>, and the Report of 19 July 2016, at: <http://undocs.org/A/71/172>.

Context of International Security" particularly emphasises the "need for confidence-building measures".[37] 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 recommendations on a global cybersecurity strategy. Another relevant actor at the international level is the International Telecommunications Union (ITU).[38] 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 launched, as early as 2007, the Global Cybersecurity Agenda (GCA) establishing a "framework for international cooperation aimed at enhancing confidence and security in the information society".[39] The ITU is active in standard-setting and a subgroup has issued a technical report of high quality on "Cybersecurity, data protection and cyber resilience in smart sustainable cities".[40]

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 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.[41] 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 because 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.[42] In short, this 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 maximum effectiveness and 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 Centre

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

37. UN General Assembly Doc. A/70/174 of 22 July 2015, at: <https://undocs.org/A/70/174> [Accessed: 24/09/17].
38. See <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx>.
39. See <https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>. 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>.
40. See: ITU-T Telecommunication Standardisation Sector of ITU, Focus Group on Smart Sustainable Cities (2/2015).
41. Part I, note 3.
42. For the concept see: Pernice (1999, pp. 703-50; 2001, pp. 148-93). For a critique of the concept from a legal theory point of view see: Jestaedt (2004, p. 638). For a reply: Pernice (2007, pp. 61-92). See also the critiques of Barents (2012, p. 153) and as a reply Pernice (2015, pp. 541-62).

right of self-determination of the other.[43] As we can learn from contractualist 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 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",[44] 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.[45] 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.[46]

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 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 is what 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

43. See in more detail: Pernice (2015b, pp. 52-55).
44. For the term see the series: Cappelletti, Seccombe and Weiler (1986) and, more recently, Vosskuhle, (2016, pp. 161-68).
45. 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, para. 231, 235, 271, 289 and 334, available at:* <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/06/es20090630_2bve000208en.html> [Accessed: 08/08/09].
46. See Pernice (2017c).

of the supranational (or potentially global) community.[47] 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) and 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.

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, therefore, 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 Catalonian, 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 one 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 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 level[48] with due regard, nevertheless, 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 the interest in cyber security, like that in managing other global risks, may grow stronger worldwide and come to take priority over national sovereignty that is, ultimately, nothing more than an illusion. The need to preserve security in cyberspace, together with the desire to benefit from the opportunities offered by 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

47. For a theoretical foundation of the idea of sovereignty of the citizen see: Behrouzi (2005, pp. 2-5, 13-17, 27-33, 131-70); see Pernice (2001, pp. 148, 162-63, 166, 174-75).
48. For first attempts in this direction see Pernice (2006, pp. 973-1005).

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 cyber security and privacy by design, and guidelines for technical standardisation and certification, lay down globally applicable provisions for data protection and cyber security in line with initiatives at the UN level, and even concretise the responsibilities and duties of states and supranational organisations regarding cyber security.

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 legitimacy problems of the EU.[49] 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 democratic deliberation and state responsibilities regarding action taken by new public authorities established at the global level.[50] And third, the potential of the internet to make global democracy a reality is far from being exhausted.

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 respect for 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,[51] is a condition for the beneficial use of the internet in these contexts.[52] The need for effective action here may become one of the driving forces of a constitutional process for the framework that makes effective action at the global level possible.

Experiences of open deliberation models in internet governance and multi-stakeholder processes will be of great value in this process,[53] as will be an open, creative and cooperative spirit in governments and political leaders who understand the urgent need for 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 with each other upon common rules on cyber security, rules they would enforce through their sheer market power. An example may be 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

49. See Pernice (2017d, pp. 287-316).
50. For a tentative outline see Pernice (2015b, p. 151; 2017e, p. 27).
51. See Donahoe (2013).
52. In this vein also the Joint Communication (note 15), 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."
53. For an attempt to explain the theoretical foundations and a possible design of such a framework see: Pernice (2015b).

bolster first-response efforts.[54] This approach could be an important step forward, 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 or 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.[55] It was established and grew during a pioneering period of the internet,[56] 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",[57] 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",[58] 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",[59] processes from which a global regime for risk management in the digital constellation will emerge.

References

BARENTS, R. (2012). "The Fallacy of European Multilevel Constitutionalism". In: M. AVBELJ and J. KOMÁREK (eds.). *Constitutional Pluralism in the European Union and Beyond*. Hart, p. 153.

BEHROUZI, M. (2005). *Democracy as the Political Empowerment of the Citizen. Direct-Deliberative e-Democracy*. Lexington Books, pp. 2-5, 13-17, 27-33, 131-70.

BROWNLIE, I. (2008). *Principles of Public International Law*. Oxford: OUP, p. 289, 292.

BUNDESMINISTERIUM DER VERTEIDIGUNG (2017). "Entwicklung des Organisationsbereichs bei der Bundeswehr" [Accessed: 14/08/17] <https://www.bmvg.de/de/themen/cybersicherheit/cyber-verteidigung/entwicklung-des-org-bereich-bei-der-bw>

54. See the proposals made by Microsoft: "A Tech Accord to protect people in cyberspace", at: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW6iCh> [Accessed: 12/06/2017].
55. Conceptualising ICANN and in particular the Uniform Domain-Name Dispute-Resolution Policy (UDRP) as a case of "self-constitution" in a multi-stakeholder process: Viellechner (2013, pp. 253-64), rep. in: Thornhill (2017, pp. 206-9): emergence of constitutional norms: "Eigenkonstitutionalisierung".
56. Ibid., pp. 128-41.
57. For the document see: Microsoft Policy Papers "A Digital Geneva Convention to protect cyberspace", <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH>.
[Accessed: 12/0617].
58. Microsoft Policy Papers: "An attribution organisation to strengthen trust online", <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QI> [Accessed: 12/06/17].
59. For an analysis of the concept, once applied by George W. Bush, see Callies, Nolte Stoll (2007).

BUNDESMINISTERIUM DES INNERN (2016). "Cyber-Sicherheitsstrategie für Deutschland 2016". [Accessed: 17/07/17] <https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf>

CAGE, M. (2015). "What is new in the U.S. cyber strategy". *The Washington Post*, 24 April 2015. [Accessed: 14/08/17] <https://www.cfr.org/blog/cybersecurity-2015-national-security-strategy>

CALLIES, C.; NOLTE, G.; STOLL, P. T. (eds.) (2007). *Coalitions of the Willing: Avantgarde or Threat?*. Köln-München, Carl Heymanns.

CAPPELLETTI, M.; SECCOMBE, M.; WEILER, J. (eds.) (1986). *Integration Through Law. Europe and the American Federal Experience*. Berlin: Walter de Gruyter. <https://doi.org/10.1515/9783110909227>

CENTER FOR LONG-TERM CYBERSECURITY (2016). "Cybersecurity Policy Ideas for a New Presidency", Berkeley. [Accessed: 14/08/17] <https://cltc.berkeley.edu/files/2016/11/Center_for_Long_Term_Cybersecurity.pdf>

CUIJPER, P. J.; HINDELANG, S.; PERNICE, I. (2014). "Investor-State Dispute Settlement (ISDS) Provisions in the EU's International Investment Agreements". Vol. 2 – Studies. European Parliament, INTA. <http://www.europarl.europa.eu/thinktank/de/document.html?reference=EXPO_STU(2014)534979>

DEPARTMENT FOR DIGITAL, CULTURE, MEDIA & SPORT (2017). "5 A safe and secure cyberspace – making the UK the safest place in the world to live and work online". [Accessed: 15/08/17] <https://www.gov.uk/government/publications/uk-digital-strategy/5-a-safe-and-secure-cyberspace-making-the-uk-the-safest-place-in-the-world-to-live-and-work-online>

DONAHOE, E. (2013). "Protecting Democracy from Online Disinformation Requires Better Algorithms, Not Censorship". In: Council of Foreign Relations, 21 August 2017 [Accessed: 22/09/2017] <https://www.cfr.org/blog/protecting-democracy-online-disinformation -requires-better-algorithms-not-censorship>

ENISA (2017). "Principles and Opportunities for a Renewed EU Cybersecurity Strategy (Version B I July 2017)". [Accessed: 22/092017] <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-input-to-the-css-review-b>

EU COMMISSION AND THE HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY (2017). 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. [Accessed: 24/09/2017] <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=JOIN:2017:450:FIN&from=EN>

EU COMMISSION'S EUROPEAN POLITICAL STRATEGY CENTRE (2017). "Building an Effective European Cyber Shield. Taking EU Cooperation to the Next Level". Issue 24 of 8 May 2017. [Accessed: 14/08/17] <https://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_24.pdf>

EUROPEAN COMISSION (2016). "Commission Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final". [Accessed: 22/09/2017] <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0410&from=DE>

EUROPEAN COMISSION (2017). "Factsheet EU cybersecurity initiatives". [Accessed: 17/07/17] <https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-initiatives-working-towards-more-secure-online-environment>

EUROPEAN COUNCIL (2017). "Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities" ("Cyber Diplomacy Toolbox"). [Accessed: 17/07/17] <http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf>

HERPIG, S. (2018). "Governmental Vulnerability Assessment and Management. Weighing Temporary Retention versus Immediate Disclosure of 0-Day Vulnerabilities. A proposal supported by the

Transatlantic Cyber Forum". [Accessed: 28/08/18] <https://www.stiftung-nv.de/en/publication/governmental-vulnerability-assessment-and-management>

GOLDMAN, Z. K.; RASCOFF, S. J. (2016). "Introduction. The New Intelligence Oversight". In: *Intelligence Oversight*, p. xvii, xxvii, xxxi.

ICRC (2013). "Chemical and biological weapons". [Accessed: 14/08/17] <https://www.icrc.org/en/document/chemical-biological-weapons>

IPSEN, K. (1999). *Völkerrecht*. München: C.H. Beck, pp. 955-61.

ITU (2007). "Report of the chairman of hleg". *Global cybersecurity agenda*. <https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf>

ITU (2015). "Focus Group on Smart Sustainable Cities" (2/2015). <https://www.itu.int/en/ITU-T/focusgroups/ssc/Pages/default.aspx>

JESTAEDT, M. (2004). "Der Europäische Verfassungsverbund – Verfassungstheoretischer 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, p. 638. Also published in C. CALLIESS (ed.) (2007). *Verfassungswandel im europäischen Staaten- und Verfassungsverbund. Göttinger Gespräche zum deutschen und europäischen Verfassungsrecht*. Mohr Siebeck Tübingen, pp. 93-127.

LEUSCHNER, S. (2018). *Sicherheit als Grundsatz. Eine grundrechtsdogmatische Rekonstruktion im Unionsrecht am Beispiel der Cybersicherheit*, Mohr Siebeck, Tübingen

LEISTERER, H. (2018). *Internetsicherheit in Europa. Zur Gewährleistung der Netz- und Informationssicherheit durch Informationsverwaltungsrecht*, Mohr Siebeck, Tübingen

NATO (2016). "NATO and the European Union enhance cyber defence cooperation". [Accessed: 08/08/17] <http://www.nato.int/cps/en/natohq/news_127836.htm>

NATO COOPERATIVE CYBER DEFENSE CENTRE OF EXCELLENCE (DDCDOE) (2017). "Cyber Security Strategy Documents". 23 May 2017 [Accessed: 14/08/17] <https://ccdcoe.org/cyber-security-strategy-documents.html>

PERNICE, I. (1999). "Multilevel Constitutionalism and the Treaty of Amsterdam: European Constitution-Making Revisited". *Common Market Law Review,* no. 36, pp. 703-50. Also available as *WHI-paper* 04/1999. [Accessed: 28/09/18] <http://www.whi-berlin.eu/documents/whi-paper0499.pdf>

PERNICE, I. (2001). "Europäisches und nationales Verfassungsrecht, Bericht". In: *60 Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer*. Berlin: de Gruyter, pp. 148-93. Also available as *WHI-paper* 13/2001 [Accessed: 28/09/18] <http://www.whi-berlin.de/documents/whi-paper1301.pdf>. Spanish translation (by A. Lopez-Pina): "Derecho constitucional europeo y Derecho constitucional de las Estados miembros". *Revista española de Derecho Europeo* (2003, 8, pp. 601-38).

PERNICE, I. (2006). "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 (eds). *Völkerrecht als Wertordnung. Common Values in International Law, Festschrift für / Essays in Honour of Christian Tomuschat*. Kehl-Strasbourg-Arlington: N.P. Engel, pp. 973-1005. Also as *WHI-paper* 9/08. [Accessed: 28/09/18] <http://www.whi-berlin.eu/documents/whi-paper0908.pdf>. Spanish translation (by 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 Internationales, no. 61/2012 [Accessed: 28/09/18] <http://www.idee.ceu.es/Portals/0/Publicaciones/Docuweb%20doc%20%2061%20UE.pdf>

PERNICE, I. (2007). "Theorie und Praxis des Europäischen Verfassungsverbundes". *WHI Paper*, 08/2008. [Accessed 28/09/18] <http://www.whi-berlin.eu/documents/whi-paper0808.pdf>

PERNICE, I. (2015a). "Multilevel Constitutionalism and the Crisis of Democracy in Europe". *EuConst*, no. 11, pp. 541-62 <https://doi.org/10.1017/S1574019615000279>

PERNICE, I. (2015b). "Global Constitutionalism and the Internet. Taking People Seriously". *HIIG Discussion Paper Series,* No. 2015-01. <https://ssrn.com/abstract=2576697> <http://dx.doi.org/10.2139/ssrn.2576697>

PERNICE, I. (2017a). "Vom Völkerrecht des Netzes zur Verfassung des Internets. Privacy und Digitale Sicherheit im Zeichen eines schrittweise Paradigmenwechsels". *HIIG Discussion Paper Series No*. 2017-02, p. 14-21. [Accessed: 10/06/18] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959257>

PERNICE, I. (2017b). "Global cybersecurity Governance. A constitutional approach". In: *Global Constitutionalism 2017* (in review process), 112-141. Available as a draft version "Cybersecurity Governance. Making Cyberspace a Safer Place" in *HIIG Discussion Paper Series* No. 2017-05. [Accessed: 22/09/17] <https://ssrn.com/abstract=3012136>

PERNICE, I. (2017c). "Brexit – exercise of democracy or a challenge to democracy?". *WHI-Paper,* 03/2017. [Accessed: 01/11/17] <https://www.rewi.hu-berlin.de/de/lf/oe/whi/publikationen/whi-papers/2017/whi-paper-03-2017.pdf>

PERNICE, I (2017d). "E-Government and E-Democracy: Overcoming Legitimacy Deficits in a Digital Europe". In: L. PAPADOPOULOU, I. PERNICE, J. H. H. WEILER (eds.). *Legitimacy Issues of the European Union in the Face of Crisis*, pp. 287-316. See also *WHI-paper* 4/2015 and *HIIG Discussion-Paper* 2016/01. [Accessed 28/09/18] <http://www.whi-berlin.eu/tl_files/WHI-Papers%20ab%202013/WHI-Paper%20042015.pdf> <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2723231>

PERNICE, I. (2017e). "E-Democracy, the Global Citizen, and Multilevel Constitutionalism". In: C. PRINS, C. CUIJPERS, P. L. LINDSETH and M. ROSINA (eds.). *Digital Democracy in a Globalised World*. Edward Elgar, Cheltenham, p. 27. <https://doi.org/10.4337/9781785363962.00009>

SCHALLER, C. (2017). "Beyond Self-Defense and Countermeasures. A Critical Assessment of the *Tallinn Manual's* Conception of Necessity". *Texas Law Review,* no. 95, pp. 1619, 1636-38.

SCHMITT, M. N. (ed.). (2013). *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. [Accessed 28/09/18] <https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf>

SCHMITT, M. N. (ed.) (2017). *Tallinn manual 2.0 on the International Law applicable to cyber operations*. [Accessed: 28/09/18] <http://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf>

SEGAL, A. (2015). "Cybersecurity in the 2015 National Security Strategy". [Accessed: 14/08/17] <https://www.cfr.org/blog/cybersecurity-2015-national-security-strategy>

THORNHILL, C. (2017). "Lars Viellechner: Transnationalisierung des Rechts, Weilerswist, Velbrück, 2013". *Zeitschrift für Rechtssoziologie*, vol. 37, no. 1, pp. 206-209. [Accessed: 27/08/18]. <https://doi.org/10.1515/zfrs-2017-0009>

VIELLECHNER, L. (2013). *Transnationalisierung des Rechts*. Velbrück, Weilerswist, pp. 253-64

UNITED NATIONS (2004). "UN General Assembly Resolution 58/199. Creation of a global culture of cybersecurity and the protection of critical information infrastructures", 23 December 2003. [Accessed: 28/09/18] <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/58/199>

UNITED NATIONS (2010). "UN Resolution 64/211. Creation of a global culture of cyber security and taking stock of national efforts to protect critical information infrastructures", 21 December 2009. [Accessed: 28/09/17] <https://ccdcoe.org/sites/default/files/documents/UN-091221-CultureOfCSandCI.pdf>

UNITED NATIONS (2015). "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", 22 July 2015. [Accessed: 24/09/17] <http://undocs.org/A/70/174>

UNITED NATIONS (2016). "Developments in the field of information and telecommunications in the context of international security", 19 July 2016. [Accessed: 28/09/17] <http://undocs.org/A/71/172>

US DEPARTMENT OF HOMELAND SECURITY (2018). "Cybersecurity Strategy", May 15, 2018. [Accessed: 28/08/19] <https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf>

VOSSKUHLE, A. (2016). "Integration durch Recht – Der Beitrag des Bundesverfassungsgerichts". *Juristenzeitung,* no. 17, pp. 161-68. <https://doi.org/10.4337/9781785363962.00009>

WHITE HOUSE (2017). "Vulnerabilities Equities Policy and Process for the United States Government (VEP)", November 15, 2017 [Accessed: 28/08/18] <https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF>

Recommended citation

PERNICE, Ingolf (2018). "Risk management in the digital constellation – a constitutional perspective (part II)". *IDP. Revista de Internet, Derecho y Política.* No. 27, pp. 79-95. UOC [Accessed: dd/mm/yy] <http://dx.doi.org/10.7238/idp.v0i27.3125>

About the author
Ingolf Pernice
pernice@hiig.de

Director of the Alexander von Humboldt Institute for Internet and Society

Ingolf Pernice served as principle administrator at the European Commission's Legal Service before he became Professor for Public, European and International Law at the Johann Wolfgang Goethe-Universität, Frankfurt and, from 1996 to 2015, at the Humboldt-Universität of Berlin. Here he founded the Walter Hallstein-Institut for European Constitutional Law. He directed the DFG-funded junior research program "Multilevel Constitutionalism – European Experiences and Global Perspectives" from 2006 to 2015. He was visiting professor at Paris II (Panthéon-Assas) in 1998. In 2008/9 he was a LAPA-fellow at the Woodrow Wilson School for Public and International Affairs and Visiting Professor at Princeton University. He acted as the agent of the German Bundestag in case 2 BvE 2/08 und 2 BvR 1010/08 (Treaty of Lisbon). Since 2013 he has been co-director of the Alexander von Humboldt Institute for Internet and Society at the Humboldt-Universität of Berlin. His main research areas are European constitutional law, privacy and data protection, cyber security law, smart government as well as global constitutionalism and the internet.

Hiig
Französische Straße 9
10117 Berlin