NORMATIVE ORDERS

Cluster of Excellence at Goethe University Frankfurt/Main

Normative Orders Working Paper

02/2018

The Time is Right for Europe to Take the Lead in Global Internet Governance

Von Matthias C. Kettemann, Wolfgang Kleinwächter und Max Senges

Cluster of Excellence
The Formation of Normative Orders
www.normativeorders.net

Goethe-University Frankfurt am Main

matthias.kettemann@normativeorders.net
wolfgang.kleinwaechter@medienkomm.uni-halle.de
senges@stanford.edu

Table of Contents

The Time is Right for Europe to Take the Lead in Global Internet Governance

Von Matthias C. Kettemann (Goethe-Universität Frankfurt am Main), Wolfgang Kleinwächter (Universität Aarhus), Max Senges (Stanford University)

Abstract: Europe is a key normative power. Its legitimacy as a force for ensuring the reign of rule of law in international relations is unparalleled. It also packs an economic punch. In data protection and the fight against cybercrime, European norms have been successfully globalized. The time is right to take the next step: Europe must now become the international normative leader for developing a new deal on internet governance. To ensure this, European powers should commit to rules that work in security, economic development and human rights on the internet and implement them in a reinvigorated IGF.

1. THIS IS NOT A DRILL: INTERNET GOVERNANCE IS IN CRISIS

"Ballistic missile threat inbound to Hawaii. Seek immediate shelter. This is not a drill." This emergency alert was sent out to thousands of Hawaiians on 13 January 2018, at 8:08 am local time.[1] Luckily, it turned out to be not a drill, but rather the result of human error. An employee, it appeared, had pushed the wrong button (twice). The reactions on social media and in real life – the media was full of stories of scared Hawaiians hiding in garages – tells us a lot about our times both in terms of the unwelcome continuity of historic threats to international security (ballistic missiles threats were a Cold War staple) and in terms of cybersecurity: Human errors can cause real damages – and humans are an integral part of our cybersecurity.[2]

Now imagine what would have happened if the warning had been the result of a compromised alert system due to a state-sponsored attack on America, a digital "9-11". That thought is not without foundation. Conflicts online are on the increase. Threats to cyberstability and cybersecurity multiply. Is internet governance[3] implemented well enough

[1] "This is Not a Drill." Alana Abramson, 13 January 2018, Time.com, 'This Is Not a Drill.' Hawaii Just Sent Out an Incoming Missile Alert. It Was a Mistake, http://time.com/5102389/this-is-not-a-drill-hawaii-just-sent-out-an-incoming-missile-alert-it-was-a-mistake.

[2] Cf. Matthias C. Kettemann, "This is Not a Drill": International Law and Protection of Cybersecurity, in Wagner/Kettemann/Vieth (eds.), Research Handbook of Human Rights and Digital Technology (Routledge, 2019) (forthcoming); Kettemann, Ensuring Cybersecurity through International Law, Revista Española de Derecho internacional (2017), 281-290; and Kettemann, The Common Interest in the Protection of the Internet: An International Legal Perspective, in Benedek/de Feyter/Kettemann/ Voigt (eds.), The Common Interest in International Law (Antwerp: Intersentia, 2014), 167-184.

[3] While some prefer a more technical definition of internet governance, we understand internet governance to encompass the steering and shaping, the coordination and integration of rules and normative expectations regarding the development of the internet. We thus share the definition of the UN-backed Working Group on

so that fears of cyber instability and insecurity are effectively countered? Sadly, no. Can it be? Yes, we argue that it is Europe's turn to take up the baton of value-based normative internet governance approaches and run with it. By focusing on one actor pursuing one approach we overcome what psychologists call the selection paradoxon: that having to choose between multiple possible solutions makes choices more difficult. It's Europe's time.

Why - and why now? Simply put, the actors, normative instruments and processes of internet governance are in crisis. This might not surprise participants who have been criticizing the status quo for close to a decade. But the rhetoric at least seems to have become more gladitorial. Just recently, a high-level event was dedicated to outlining the conflicts in the "Battle for the Global Internet", a book sketched the *Global War for Internet Governance*[4] and a report attempted to "map the battleground" of internet governance. Does the martiality in tone and approach lend itself to optimal solutions? We have our doubts.

Rather, we suggest, Europe should take up the charge of reforming internet governance in light of its liberal, human rights-based values, prior legal commitments, normative pedigree in areas such as data protection and the fight against cybercrime, and powerful economic potential - and it should do so in the best form and forum possible, through coordinated multi-level activities in an invigorated IGF.

As the internet governance community seems evenly divided between the two argumentative hubs centered on dogmatic interpretation of norms and those arguing for a more technology-oriented reading of international law, we are faced with four dimensions of dysfunctionality plaguing current internet governance approaches. These are generalizations, but they hold true in essence:

(1) Internet governance actors do not substantially cooperate in all areas of governance, but increasingly pursue partially narrow self-interests. (Europe can provide a credible alternative approach by showing how global commons-oriented internet governance policy is better suited to develop an order where rights and goods are fairly distributed and political authority is checked).

---

internet governance as "the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the internet." Cf. Report of the Working Group on Internet Governance (2005), http://www.wgig.org/docs/WGIGREPORT.pdf.

[4] Laura DeNardis, The Global War for Internet Governance (New Haven and London: Yale University Press, 2014).

(2) Relatively new normative processes, such as the GGE, break down and existing ones, such as the IGF, seem to stall (which is why the IGF needs to be reinvigorated).

(3) Subsequent generations of different normative instruments - 'principles' and 'declarations of principles' first, now 'norms' - fail to convincingly alter the behavior of actors in light of cybersecurity threats. Those that convince normatively, such as a norm to protect the internet's public core, are too narrow to substantially influence internet governance policies on a macro level.[5] (This is why Europe's normative pedigree is an important source of legitimacy for norms).

(4) There are alarming tendencies to 're-silo' internet policies, that is to treat trade as unconnected to, say, human rights by using a sectoral approach. (This is why a holistic approach is needed – and Europe can provide it.)

To illustrate the challenges internet governance is faced with, take just the role of actors. For years the global Internet Governance discussion was overshadowed by debates between multilateralists and multistakeholderists. Truly, however, both approaches are necessary, depending on the normative subject matter at hand. In fighting cybercrime and forensic cooperation between police services, a treaty makes more sense than, say, when it comes to developing best practices to increase diversity in online environments. Further, even when treaties are elaborated, more attention is now paid to the process which is embedded into a multistakeholder environment in which non-governmental stakeholders with their resources, knowledge, and engagement make key contributions to develop and stabilize cyberspace.[6]

Today, however, the conflict dynamic has changed in tone and direction: a new threat to the globality of the internet has emerged: unilateralism coupled with populist illiberalism. The failure of the Group of Governmental Experts (GGE) in the field of cybersecurity in June 2017 as well as the inability of the World Trade Organisation (WTO) to draft a universal framework for global digital trade in December 2017 indicated that the road back

[5] At its fourth meeting in November 2017 in New Delhi, the GCSC issued a "Call to Protect the Public Core of the Internet": "Without prejudice to their rights and obligations, state and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace."

[6] Wolfgang Kleinwächter, EURODIG Tbilisi 2018: Positioning in the New Complexity of the Global Internet Governance Ecosystem, 28 June 2018, http://www.circleid.com/posts/20180618_eurodig_tbilissi_2018_positioning_in_the_new_complexity_of.

to constructive multilateral negotiations on internet-related public policy issues will be a long one.[7] It may be long, but it is notwithout existing commitment to internationa law and human rights. With the agreement already in the 2013 GGE report that, *first*, international law, and in particular the UN Charter, is applicable to the internet, *second,* that they are essential for world peace, and that *third,* international law is important for human development (via an enabling internet), a global consensus was reached,[8] even though some states have adopted very sovereignty-oriented interpretations.[9] Building on this consensus, the 2015[10] report of the GGE again confirmed that international law, the UN Charter and international legal principles apply to the internet,[11] stating inter alia that the international community aspired to regulate the internet in a peaceful manner "for the common good of mankind":[12] "[t]he adherence by States to international law, in particular their Charter obligations, is an essential framework for their actions in their use of ICTs and to promote an open, secure, stable, accessible and peaceful ICT environment".[13]

ICANN's IANA transition (2016) has demonstrated the feasibility of multistakeholder cross-community processes by transferring the responsibility for the management of key global Internet resources — domain names, IP addresses, and Internet protocols — to the empowered community. Intergovernmental silos are emerging and the new intergovernmental silo approach could become a big problem.[14] What is needed is a holistic approach to global Internet negotiations.[15]

The time has thus come for a fundamental normative restart in the processes seeking to stabilize the protection regime for the internet's core architecture in light of existing and growing challenges to cybersecurity and cyberstability. Discussions on issues from internet openness to threats to online freedom, from security threats through backdoors to

[7] Ibid.
[8] Schmitt and Vihul, The Nature of International Law Cyber Norms (2015), https://ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn%20Paper%20No%20%205%20Schmitt%20and%20Vihul.pdf: "12.
[9] Cf. Adam Segal, Chinese Cyber Diplomacy in a New Era of Uncertainty, Hoover Institution, Aegis Paper Series No. 1703, 2 June 2017, https://www.hoover.org/research/chinese-cyber-diplomacy-new-era-uncertainty.
[10] Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Secretary General, A/70/174 of July 22, 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 (hereinafter: "GGE report (2015)").
[11] GGE report (2015), para. 26.
[12] Ibid., para. 28 (c).
[13] Ibid., para. 25.
[14] Ibid.
[15] Cf. the commitment in the Bratislava meeting (May 2018) of the Global Commission on Stability in Cyberspace, Wolfgang Kleinwächter, EURODIG Tbilisi 2018: Positioning in the New Complexity of the Global Internet Governance Ecosystem, 28 June 2018, http://www.circleid.com/posts/20180618_eurodig_tbilissi_2018_positioning_in_the_new_complexity_of.

increasing internet resilience will be held at the Internet Governance Forum, the ITU Plenipotentiary, ICANN63 and in the framework of the UN Secretary General's High Level Panel on Digital Cooperation. It is in these forums, but especially in an reinvigorated IGF, that Europe must vigorously defend a normative approach to internet governance targeted at ensuring human rights-based cybersecurity.

We note that this normative restart must be designed in a way that does not hinder technical innovation but is based on rules: permissionless innovation is positive, innovation without a firm normative foundation can be dangerous. As with any normative approach, unwanted side-effects need to be taken into account.

2. EUROPE HAS A WINDOW OF OPPORTUNITY TO BECOME A NORMATIVE POWERHOUSE FOR INTERNET GOVERNANCE

Europe's strength is the rule of law. European institutions — from the Council of Europe with the European Court of Human Rights to the institutions of the European Union with the European Parliament, European Commission and European Court of Justice have produced instruments and offer procedures which make clear that cyberspace is ruled by law. Historically, data protection law was a European concept that successfully migrated internationally. A number of cases, from *Schrems* to *Google/Spain,*[16] have given Europe a judicial track record of holding companies to account. In terms of legislation, the recent GDPR[17] is respected and recognized (apart perhaps from it extraterritorial implications[18]) as an important example of how to weigh privacy, security and innovation. Europe must rely on its role as a normative actor, a legitimate norm-setter to compliance pulls. The soft power of the European Union can be combined with the substantial normative experience in standard-setting of the Council of Europe to form a convincing combination of mutually supporting normative actors.

To link Europe's manufacturing industry to digitalization has a lot of potential. Europe has a highly developed educational system which is able to produce the skill sets needed for tomorrow's digital economy. Europe is now trying to leapfrog into the digital platform

[16] CJEU, C-131/12, Google Spain and Google, judgment of 13 May 2014, CJEU, case C-362/14, Schrems v. Data Protection Commissioner, judgment of 6 October 2015. But also CJEU, C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger et al., judgment of 8 April 2014.
[17] General Data Protection Regulation, Regulation (EU) 2016/679 OJ L 119/1 of 4 May 2016.
[18] Pursuant to Article 3(2) the GDPR applies to controllers or processors of data not established in the EU in cases where "the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union."

economy via pushing industry 4.0, Internet of Things (IoT) [19]and Artificial Intelligence (AI)[20]. These issues need innovative, enabling governance. Europe can take up this baton, too.

But Europe's current weakness is to translate interesting normative approaches - the GDPR, the right to be forgotten - into effective policies and projects. The 28 member states of the EU have declared the establishment of a Digital Single Market as a high priority. Under the Estonian EU presidency (Fall 2017) there was a "Digital EU Summit". There is some progress, but progress is slow and Europe's implementation problem has not yet been overcome.[21]

Looking into the coming months, there is a window of opportunity for a big European Cyber initiative which could include also proposals for a holistic approach to global Internet negotiations. When the French president Macron announced that Paris will host this year's IGF in Paris (November 2018), he also indicated that time is ripe to speed up Europe's journey into the digital age. This journey, in our assessment, should be a journey of normative innovation that may start, but should definitely not end there. After Paris, The Hague will host EURODIG 12 in June 2019 and the 14th IGF is scheduled for Berlin (November 2019). What is needed now on the road to Paris, The Hague and Berlin is a more sustainable, holistic European approach.[22]

Similarly, the Council of Europe has, over the last years, developed innovative and normatively convincing standards regarding some of the thorniest issues of internet governance, including the roles and responsibilities of internet intermediaries, internet freedom, network neutrality, transboundary flow of information, rights of internet users, search engines, and social networking services.[23]

---

[19] Samuel Greengard, The Internet of Things (Cambridge, MA/London: MIT Press, 2015).
[20] Cf. the special section on Artificial Intelligence, *Science*, 15 July 2015 (vol. 349, no. 6245).
[21] Wolfgang Kleinwächter, EURODIG Tbilisi 2018: Positioning in the New Complexity of the Global Internet Governance Ecosystem, 28 June 2018, http://www.circleid.com/posts/20180618_eurodig_tbilissi_2018_positioning_in_the_new_complexity_of.
[22] Ibid.
[23] *Council of Europe*, Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries; *Council of Europe*, Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom; *Council of Europe*, Recommendation CM/Rec(2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality; *Council of Europe*, Recommendation CM/Rec(2015)6 of the Committee of Ministers to member States on the free, transboundary flow of information on the Internet; *Europarat*, Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users; *Council of Europe*, Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines; *Council of Europe*, Recommendation CM/Rec(2012)4 of the

Europe thus has a unique opportunity to become a global leader in internet governance based on its track record, rule of law focus, normative flexibility, experience with variable normative geometries and the curse and blessing of a lack of substantial, entrenched internet industry.

3. IN ORDER TO BECOME THE GLOBAL LEADER IN INTERNET GOVERNANCE, EUROPE HAS TO SHARPEN ITS NORMATIVE ONLINE AGENDA

Europe must step up with a more pronounced and vigorous internet governance agenda. That it can do so, is unquestionable. That it will do so, is not a foregone conclusion. Consider that during the June 2018 meeting of the G7 key European leaders, including French President Macron and German Chancellor Merkel, two of the world's most influential leaders on liberal internationalist politics, remained noticeably silent with regard to the broader challenges facing internet governance, including cybersecurity and digital trade.[24] In order to credibly be perceived as a key normative actor in internet governance, Europe has to sharpen its normative edge. It should do so by a combination of recommitting to past goals and globalizing - sensibly - key successful normative fields, such as data protection (including GDPR), privacy protection (including the right to be forgotten) and the fight against cybercrime.

We therefore call on Europe to

(1) recommit to the overarching goal of internet governance to contribute to securing world peace and international security (as enshrined in the UN Charter), ensuring human development (as codified in the Millennium Development Goals and the Sustainable Development Goals) and respecting, protecting and implementing human rights (as normatively ordered in the UDHR) which are in the global common interest; and

(2) recommit to internet governance as a policy priority and the achievements of multistakeholder governance as defined in the NetMundial Principles. This seems especially relevant in times when Brexit negotiations and the rise of populism and

Committee of Ministers to member States on the protection of human rights with regard to social networking services.

[24] They merely agreed on a "Commitment on Defending Democracy from Foreign Threats" which establishes a G7 Rapid Response Mechanism and seeks to identify, inter alia, opportunities for "coordinated response … in collaboration with governments, civil society and the private sector".

authoritarianism pose serious challenges to the internal stability of the EU; its time to look outward and reestablish Europe's role as a normative actor.

(3) In pursuing a vigorous normative approach to internet governance, Europe should not fall for technical determinism but premise all on the controlling power of normativity over technicity. Rather than letting a "technical medium […] define our societal values"[25] it is the values embedded in the normative order of the internet that define the evolution of the internet's underlying technologies through normative framing and regulatory interventions. Value-based normativity, it is hypothesized, must influence standard-setting to ensure the primacy of international legal commitments, and their national legal counterparts. Technology development is based on norms and normative choices are implemented through code and algorithms which are human-made.

(4) The lesson can stick if Europe leverages past normative successes into stabilizing its influence as a governance actor. Europe's power lies in its position as an exporter of norms and legitimate norm-based internet governance initiatives.

(5) Sharpening Europe's normative edge will only work if Europe engages all stakeholders. Being a non-traditional actor as well, the EU has a long history of engaging non-state actors in legislative processes. It must not only tolerate, but vigorously push for the inclusion of all stakeholders in the formation of its cyberstability approaches. To achieve this, it should rely on its long-standing and credible commitment to multistakeholderism and on the newly emerging notion of "digital cooperation"[26] (including legislating normatively across domains). In particular, Europe should empower individuals, companies, governmental organizations and networks as accelerators of progress towards cybersecurity and cyberstability[27]. Due to the private nature of the majority of online networks and

[25] Indra Spiecker gen. Döhmann, Online- und Offline-Nutzung von Daten: Einige Überlegungen zum Umgang mit Informationen im Internetzeitalter, in Michael Bartsch und Robert G. Briner (eds.), DGRI-Jahrbuch (Cologne: Verlag Dr. Otto Schmidt), 39-53 (53): "[Das Internet] ist ein rechtsfreier Raum nur solange, wie wir zulassen, dass ein technisches Medium unsere gesellschaftlichen Werte bestimmt." (transl. by the author).

[26] Bruno Lété and Daiga Dege, NATO Cybersecurity: A Roadmap to Resilience, The German Marshall Fund, Policy Brief, 2017 | No. 23, p. 4, http://www.gmfus.org/publications/nato-cybersecurity-roadmap-resilience.

[27] Europe must engage individuals more in the process of aiming towards enhancing cybersecurity and cyberstability. Securing the rights of human beings it not only the ultimate end of internet governance (or any governance understood as processes distributing rights and goods legitimately). But individuals are also the first best "frontier of cyberdefense" and cyberstability. Digitally empowered and cyberaware Europeans can become global leaders in responsible online behavior and multiply the impact of their governments' policies.

services the notion of corporate statesmanship[28] is becoming more important in order to give them more “shaping power” as well as make them more accountable.

(6) All of this will only work if Europe commits to a new deal on internet governance. States, citizens and companies (in Europe and beyond) need to (be made to) understand why cybersecurity and cyberstability matter.

4. TOWARDS A NEW DEAL ON INTERNET GOVERNANCE

Europe has a unique opportunity to play a leadership role. Cybersecurity is a key functional condition for an era defined by information and communications technology. A secure internet lies in the interest of each individual state and also collectively in the interest of all states of the world as a global community. Cybersecurity thus lies in the global common interest. It has a key security interest for which all the states of the world bear separate and common responsibility.[29]

Consequently, each state has protection obligations vis-à-vis the international community – to avert threats to the stability, integrity and functionality of the internet – which can be derived from customary international law. At the same time, states may not restrict freedom on the internet without limitation under the guise of imposing "security." The global, cross-border internet traffic may not be adversely affected or in any way destabilized by states due to national legislation and policy.[30]

The solution is not the adoption of a news cybersecurity treaty, as has been proposed by a number of countries that try to gain more control over the ‘national’ internets. They see such an instrument as a tool to redefine (in their sense) notions of human rights and freedom of expression and the importance of cross-border data flows: our approach is

[28] Martin Reeves, Georg Kell, and Fabien Hassan (BCG), The Case for Corporate Statesmanship, 1 March 2018. Europe can integrate companies to a much larger degree. Until now, they are often objects of regulation or (less willingly) regulated self-regulation. This must change. Ensuring cybersecurity is a classic case of a prisoner’s dilemma in business with everybody aiming for security, but no one feeling the need to invest too much. Here, Europe must help companies understand that they can profit immensely from assessing their impact in terms of the total societal function they perform and not as engines to increase shareholder’s net worth.

[29] Kettemann, Matthias C., The Normative Order of the Internet (2019).

[30] Kettemann, Matthias C., The Common Interest in the Protection of the Internet: An International Legal Perspective, in Benedek/de Feyter/Kettemann/Voigt (eds.), The Common Interest in International Law (Antwerp: Intersentia, 2014), 167-184; Kettemann, Matthias C., Völkerrecht in Zeiten des Netzes: Perspektiven auf den effektiven Schutz von Grund- und Menschenrechten in der Informationsgesellschaft zwischen Völkerrecht, Europarecht und Staatsrecht (Bonn: Friedrich-Ebert-Siftung, 2015), http://library.fes.de/pdf-files/akademie/12068.pdf.

different. Firmly grounded in human rights and international law, Europe must build support around the idea that the internet presents different iterations and scaling of existing problems. These problems are not new. We therefore no need a new treaty, but rather new approach, a 'New Deal' based on multistakeholderism and accepted internet governance principles.

Just as international law has been aptly termed a "gentle civilizer of nations",[31] Europe has the unique opportunity to become the (not quite so) "gentle civilizer of the internet". It must support, based on norms and convincing justification narratives that engage all stakeholders, the establishment and implementation of a multi-tiered, comprehensive, integrative, value-based and human being-oriented cyberstability. Normative steps towards a 'New Deal' on internet governance must be based on the UN Charter, the Sustainable Development Goals and the Universal Declaration on Human Rights. Different economic and political global 'deals' over the years have had their own finalities: the Bretton Woods system ensured a liberal economic world order after WW II; the global bipolarity during the Cold War ensured a certain measure of stability; the 'One World One Internet' mainstreamed development and globalization. However, a clear - and realistic - vision of a rule of law-based order of the internet is missing: this is where our proposal of a 'New Deal' fills a gap.

Within this 'New Deal' Europe's normative approaches an be separated into three baskets and, additionally, must include the regulation of AI:

(1) security: put the normative frame in place to counter socioeconomic forces leading to digital catastrophes in form of a Digital Peace Plan;

(2) economics and trade: introduce and deploy a Digital Marshall Plan;

(3) human rights: protect, respect and implement human rights and ensure that Europe's policies are based on law and oriented towards safeguarding the individual.

(4) Artificial Intelligence Governance: deploy Europe's extensive network of international actors to garner input for legitimate, effective and enabling norms ensuring *agency, automation, augmentation and accountability* for research and development of AI and AI use.

[31] Cf. Martti Koskenniemi, The Gentle Civilizer of Nations. The Rise and Fall of International Law 1870–1960 (Cambridge: CUP, 2001).

Security: Europe must proactively establish a legislative approach to ensuring cybersecurity and cyberstability and avoid digital catastrophes.

Reducing the risks of a cyberwar is a common goal for internet governance endeavors, as is the introduction of confidence-building measures and norms for good state behavior in cyberspace. These are a good foundation. Further, Microsoft's proposal for a Digital Geneva Convention is now on the table. It has provoked controversial discussions, and it remains to be seen how such an idea can be turned into a concrete political project. Elon Musk's proposal to ban killer robots goes in the same direction. Both initiatives signal that the private sector has no interest to be pulled into political power games, which could lead to a cyberwar.

Another concrete project open for discussion is the proposed norm to protect the public core of the internet made by the Global Commission on Stability in Cyberspace (GCSC). Today's internet is so important for the daily life that an attack on its basic functioning could damage a society. The GCSC proposal says: "State and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet." By giving the "public core of the Internet" a special status, the proposed norm would allow treating attacks against the basic functioning of the internet as violations of erga omnes norms which each state of the world can legitimately raise.

Europe must take this important commitment one step further: There is a need to enhance special protection for the electric power systems, for transportation and financial services as well as electoral procedures, if these are essential services. There are a lot of common interests even among states diverging in their internet policies. What is missing at the moment is the political will to translate these common interests into arrangements which will benefit all sides. As a flexible and credible provider of diplomatic solutions over decades, Europe can fulfill an important role here.

Different levels of internet security awareness and capabilities globally matter to all states because of the interconnectedness of ICTs and the networked nature of the internet. “These vulnerabilities are amplified”, the UN’s Group of Governmental Experts on IT and Security complained in 2013, “by disparities in national law, regulations and practices

related to the use of ICTs."[32] Only international cooperation in the protection of and from the internet can help meet these challenges. The role of the internet's integrity in ensuring international security and the threats posed by international cybercrime and cyberterrorism are further reasons for considering that the protection of the integrity of the internet lies in the common interest.[33]

In other words: we have the norms, we have (to a certain degree) a common will, what we need now is strong European leadership in taking the norms to the next level and institutionalizing a cyberstability architecture. This can work along the lines of the Budapest Convention, which is an important European success story to build on.[34]

Economics and trade: a Digital Marshall Plan should be adopted and deployed to increase the productive forces within global trade relations regarding the internet and improve development opportunities for all.

As an economic powerhouse Europe is well suited to encourage trade. As a block of nations that has been discussing common trade policies for over five decades, the EU, especially, is ideally placed to ensure that the digital economy is on every political agenda.

The G20 adopted already under the Chinese presidency in 2016 a "G20 Digital Economy Development and Cooperation Initiative" which was reconfirmed under the German G20 presidency. Certainly, every country will benefit from broadband deployment, digital skills, and eCommerce. But like in the field of cybersecurity, the political will to connect the world and to bridge the digital divide reaches its limits, if the protection of national interests is seen as more important than contributions to the common interest that lies in the establishment of a legitimate cyberstability architecture. This would be a core element of the normative project Europe should pursue.

This would unite human rights-based and human development-oriented internet policy development in that the right to access the internet (and through it receive and impart ideas) (and to information on the internet) is a key enabling right to realize the potential of human rights online and ensure human development. This approach has emerged as a

[32] GGE report 2013, para. 10.
[33] Kettemann (2019), 70.
[34] Kleinwächter (2018).

common theme in development policy which Europe should closely tie to its economic policy in what we could term a Digital Marshall Plan - and a reversed one at that.

The UN 2030 Agenda for Sustainable Development identified the building of resilient infrastructure, the promotion of inclusive and sustainable industrialization and the fostering of innovation as key goals of sustainable development. In Target 9.c of the Sustainable Development Goals (SDG) states commit to "[s]ignificantly increase[ing] access to information and communications technology and striv[ing] to provide universal and affordable access to the internet in least developed countries by 2020". There exists thus a commitment by UN member states to strive for universal internet access by 2020, which is deeply connected to increases in digitale trade.

Even if this commitment is difficult to realize, the importance of the commitment which evidences states' opinion vis-à-vis the internet is hard to overstate. Committing to universal access means, by implication, that internet integrity as a precondition for meaningful access needs to be ensured and is therefore in the common interest.[35]

The recent 11th WTO Ministerial meeting in Buenos Aires in December 2017 was a good illustration of what paper commitments mean if it comes to concrete projects. In the G20 meeting in Düsseldorf (April 2017) the G20 ministers agreed to "engage constructively in WTO discussions relating to E-commerce." But the "constructive engagement" was not strong enough to avoid a split of the WTO. Efforts to set up a central e-commerce negotiating forum within the WTO failed. It is up to Europe to restart the process by engaging all stakeholders, including through Jack Ma's eWorld Trade Platform.

The human dimension: As a region with a strong track record of human rights protection, Europe must make sure to orient all policies towards the human being.

In 2005, at the end of the two-phased World Summit on Information Society (WSIS), states affirmed in the *Tunis Commitment* their goal to build a "people-centred, inclusive and development-oriented Information Society" premised on the "purposes and principles of the Charter of the United Nations, international law and multilateralism, and respecting fully and upholding the Universal Declaration of Human Rights".

As the New Mundial Declaration from 2014 has reaffirmed, Internet Governance has to be based on the respect of human rights. There is no need to invent "new human rights." But

[35] Kettemann (2019), 66.

there is a need to analyze the implications of new technological developments for the existing human rights. This is relevant in particular for the right to freedom of expression and the right to privacy.

The UN Human Rights Council has appointed Special Rapporteurs for both of these rights, who are functioning as watchdogs, produce critical reports to the UN General Assembly and make their own suggestions on how to strengthen the protection of human rights in cyberspace. Europe must continue its support for these initiatives.

But we do not need an “international law 2.0”. The emergence of the internet and the pervasiveness of ICTs in today’s societies have not *fundamentally* changed or challenged international human rights law. Recall the WSIS documents referring to the importance of international law and the commitments by both GGE reports in 2013 and 2015. Applying existing and developing new rules in light of changing technological realities, economic developments and social mores speaks to the essence of a dynamic international legal order: its ability to be normatively responsive with a view to a certain finality.

These commitments have not (yet) been stabilized by conventional norms, however, as will customary international law and general principles of international law provide for the protection of and from the internet. The continued absence of a treaty regime complicates the analysis of norms applicable to the internet and its use. Normative preferences for a rule of law-based international internet-related governance model are counterindicated by destabilizing state actions including cyberattacks, pervasive state surveillance via the internet and attempts by states to create national internet segments. The complexity of regulating for these challenges suggests the need for a comprehensive human rights protection regime for the internet.

Luckily, in many regards, the EU is the world’s foremost ‘soft power’. I needs to toughen up and mainstream human rights protection into all internet governance policies.

Harnessing ICTs in order to ensure human rights, human security and human development (and, as a means towards these ends, economic growth) is premised upon the integrity of the internet. If ensuring these goals lies in the common interest – as it indubitably does –, the latter needs to be protected in the common interest.

This applies to technology governance as well. Recently, RFC 8280 on Research into Human Rights Protocol Considerations[36] provided a detailed model for considering human rights for protocol developers, providing "questions that engineers should ask themselves when developing or improving protocols if they want to understand their impact on human rights". These range from issues of connectivity, privacy, 'content agnosticism' and security to censorship resistance, accessibility, and transparency.

Europe must seek to set an ethical framework and policy options for the development and use of AI for the benefit of all.

The debate about the IANA transition is over. But this does not mean that there are no controversies anymore at the technical layer of the internet. And it is not only IoT (the Internet of Things) and AI which raise new problems with political implications. One cannot exclude that some groups have the interest to politicize the technical debate, to challenge the "rough consensus and running code" philosophy and to use technology to push for national political or economic interests.

Technologies are not spaces, but technologies enable human behavior in these spaces, and states need to respect, protect and fulfil their human rights obligations through law. Even in times of shifting media of law, states need to regulate with a view to certain values that are extrinsic to technology and must be imported through a controlling normative order which Europe must establish and immunize against technocratic capture.[37]

The design and use of algorithms can interfere with human rights.[38] The rights to fair trial and due process can be impacted by biased use of algorithms in court proceedings, including through the use of reoffending 'risk scores' in probation vs. jail decisions. Privacy and data protection rights are impacted through the collection, processing and use of vast amounts of data, online tracking algorithms.[39]

Freedom of expression, which includes the right to receive information, is interfered with when predictive algorithms shape the content users see in light of prior interests or, more harmful, biased economic incentives of third actors, even though the fear of "filter

[36] Internet Research Task Force (IRTF), RFC 8280, Research into Human Rights Protocol Considerations, https://tools.ietf.org/html/rfc8280.
[37] Kettemann (2019).
[38] Council of Europe, MSI-NET: Study on the Human Rights Dimensions of Automated Data Processing Techniques (in Particular Algorithms) and Possible Regulatory Implications, MSI-NET (2016)06rev6.
[39] Chris Jay Hoofnagle, Behavioural Advertising: The Offer You Cannot Refuse, Harvard Policy & Law Review 6 (2012), 273-296.

bubbles", that is selective publics with ever more extreme views among ingroup members, seems to be empirically overblown.[40] Algorithms are also used by internet platforms to scan for problematic content, which can lead to overblocking and to select and recommend news, which impacts the way broadcasters can reach and engage with their audiences.

In light of the growing critique of 'black box' algorithms, some approaches to hold authors and operators of algorithms accountable have emerged. It is especially the EU's new General Data Protection Regulation[41] which establishes standards for data collection through algorithms, including a limited right to information or 'explanation'. Article 13 (2) (f) EU GDPR forces controllers to provide data subjects, in cases where personal data is collected from them, with information about the existence of automated decision-making and, at least in cases of profiling in the sense of Article 9, "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing." Article 9 prohibits processing of certain personal data (revealing inter alia racial or ethnic origin, political opinions, religious or philosophical beliefs) unless the data subject has given consent (Article 9 (2) (a)) or the processing is necessary for reasons of substantial public interest. While this does not amount to a full right to explanation of the logic behind algorithms (which is often very difficult to present in an understandable way), it does amount to a right to be sufficiently informed to be able to give informed consent to data processing.

In 2016 and 2017 the notion of algorithmic accountability slowly gathered momentum. Engineering and computer associations understood the challenge and committed to "algorithmic transparency"[42] or "ethically aligned design", underlining the need for accountability that can help "[prove] why a system acts in certain ways to address legal issues of culpability, and to avoid confusion or fear within the general public". The most extensive normative approach, the *Principles for Accountable Algorithms – Fairness,*

[40] Jan-Hinrik Schmidt, Filterblasen und Algorithmenmacht. Wie sich Menschen im Internet informieren, in C. Gorr, M. C. Bauer (eds.), Gehirne unter Spannung: Kognition, Emotion und Identität im digitalen Zeitalter (Berlin/Heidel-berg: Springer, 2018), 35-51. See further Jan-Hinrik Schmidt, Jannick Sørensen, Stephan Dreyer, Uwe Hasebrink, Algorithmische Empfehlungen. Funktionsweise, Bedeutung und Besonderheiten für öffentlich-rechtliche Rundfunkanstalten (Hamburg: Verlag Hans-Bredow-Institut, 2018), Hans-Bredow-Institut Working Papers No. 45, https://www.hans-bredow-institut.de/uploads/media/default/cms/media/w188msk_45AlgorithmischeEmpfehlungen.pdf.

[41] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1 of 4 May 2016.

[42] Cf. Association for Computing Machinery, Statement on Algorithmic Transparency and AccountabIEEE, Ethically Aligned Design, December 2016, http://standards.ieee.org/develop/indconn/ec/ead_v1.pdf.ility (2017), http://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf.

Accountability and Transparency in Machine Learning (2016), considers accountability through five principles: responsibility (redress mechanisms for adverse effects must be provided), explainability (concerned parties must be able to understand how algorithms reach a decision), accuracy (errors and worst case scenarios need to be logged and planned for), auditability (third parties must be able to study and monitor the algorithm), and fairness (discriminatory or unjust impacts must be avoided).[43]

An example of a norm-based approach are the Universal Guidelines for Artificial Intelligence of October 2018.[44] The non-governmental drafters called for the guidelines to be included in **"**ethical standards, adopted in national law and international agreements, and built into the design of systems". They include a right to transparency, a right to human determination, the obligation for an institution using the AI system to self-identify and to not use AI with unfair biases, to use only AI that leads to accountable, accurate, reliable and valid decisions. Nation states using AI have to refrain from establishing systems of unitary scoring. Such guidelines can serve as valuable normative instruments for the European approach.

We have now described what Europe should do. We now turn to where Europe can most effectively implement these policies: in an reinvigorated IGF.

5. WHERE EUROPE SHOULD MAKE ITS STAND: AT A REINVIGORATED IGF

The next EURODIG and two subsequent IGFs take place in Europe, with the IGFs in Paris and Berlin being organized by powerful European states that can shape policies across the continent, without, of course, interfering with the multistakeholder structure of both the EuroDIGs and the IGF. This gives Europe - its states, but also its other stakeholders, including IT companies and non-governmental organizations, technical community and academic community - a chance to show the advantages of its normative approach. EURODIG has in the past innovated the IGF processes with new ideas, including interactive formats of sessions, tangible output in form of clear and short messages, a

[43] Fairness, Accountability, and Transparency in Machine Learning (FATML), Principles for Accountable Algorithms and a Social Impact Statement for Algorithms (2017), http://www.fatml.org/resources/principles-for-accountable-algorithms.
[44] Universal Guidelines for Artificial Intelligence, 23 October 2018, https://epic.org/international/AIGuidleinesDRAFT20180910.pdf, Brussels, Belgium.

Youth IGF, open calls for themes, and decentralized and bottom-up management procedures.[45]

Yet fundamentally the IGF has a serious problem that Europe needs to address and fix if the IGF meetings in Paris 2018 and Berlin 2019 should become loci for true internet governance innovation. Currently, states merely pay lip service to the multistakeholder approach, but prefer to negotiate internet-related issues behind closed doors. In doing so, they rob the IGF of their full potential as a global clearinghouse of internet governance innovation.

The IGF and its regional and national subsidiaries — like EURODIG — provide the needed framework for such a discussion across constituencies, stakeholders, state and nonstate organizations. The problem is that some governments and some businesses underestimate the potential of the IGF and are looking for alternative venues. This must change, and can change, if Europe finds a way (in concert with other actors) to reinvigorate the IGF.

It is certainly true that the IGF has some weaknesses. The UNCSTD IGF Improvement Working Group has made some recommendations which have been reaffirmed by the UN General Assembly in its WSIS+10 Resolution in December 2015. Progress is slow but there is improvement, including more intersessional work, more tangible output, more interlinkage with national and regional initiatives.[46] These developments need to be more systematically applied in light of a new self-perception of the IGF as a locus of issue identification, framing challenges and tracking normative progress.[47]

As a private-sector approach to reforming the IGF noted, the meeting has a chance to become a "global clearinghouse and deliberation space tasked with (1) identifying emergent internet governance challenges, (2) framing them so that experts from all relevant institutions can cooperate in developing and implementing innovative solutions, and (3) assuring that the progress and discourse are archived and available for analysis. This option would allow those institutions to devise solutions while maintaining existing systems and processes for those who still wish to use them."[48] This seems to be the very

[45] Kleinwächter (2018).
[46] Ibid.
[47] Vint Cerf, Patrick Ryan, Max Senges, Richard Whitt, A Perspective from the Private Sector: Ensuring that Forum Follows Function, in William J. Drake and Monroe Price (eds.), Beyond NETmundial: The Roadmap for Institutional Improvements to the Global Internet Governance (August 2014), https://global.asc.upenn.edu/publications/beyond-netmundial-the-roadmap-for-institutional-improvements-to-the-global-internet-governance-ecosystem/
[48] Ibid., 33.

approach that Europe should push for (and use in order to implement the necessary policy changes outlined in the previous sections).

Europe can help transform the IGF - through the meetings in 2018 and 2019 - into leveraging its clearing house functions to develop in the foremost transnational platform for facilitating governance of the internet. As a previous contribution by Vint Cerf, Patrick Ryan, Max Senges and Richard Whitt[49] has shown, three functions are particularly important for an reinvigorated IGF.

(1) identify issues: The IGF should help to find solutions to significant problems that arise in the current practices of users, companies and governments, including by making the workshop proposal process more transparent and collaborative, and the workshops themselves more structured and participatory.

(2) frame challenges: experts within the IGF should help in stratifying the challenges involved, e.g. through processes such as deliberative democracy, and frame them by assigning them to different institution. The European Union should seek to contribute to establishing a methodology for selecting the optimal multistakeholder-based structure for solving the normative challenge. This allows for competing or parallel approaches and positions the IGF as facilitator rather than responsible for finding solutions.

(3) document and track normative progress: Regular updates and tracking normative developments from issue identification to the way that other institutions have dealt with normative challenges of previous IGFs ensure transparency and continuity across IGFs. It is important in this context to distinguish between documenting the activities (and processes), tracking the progress (using metrics and methods used by the stakeholders working on the challenges) and archiving the evolution of the issues addressed in a way that makes it accessible. Especially the archiving function can position the IGF as an accountability mechanism by documenting the activities of the institutions identified as relevant to address an issue.

The three functions are not fulfilled sequentially. Rather, they influence each other and – taken together – can reposition the IGF as the most central and normatively relevant multistakeholder discourse forum for internet governance. One institution that can develop this approach further is the High Level Group on Internet Governance within the European

[49] Ibid., 36. The following section draws from their contribution.

Commission. Europe should use the valuable resources and pedigree the IGF has built over the years and its unparalleled legitimacy as a normative forum. It is at the IGF – in 2018 in Paris and in 2019 in Berlin – and at the EuroDIGs of the same years that can function as normative prep 'schools' for the IGFs, that Europe should make a stand. How it can do so, has been outlined in this article.

6. CONCLUSIONS

Internet governance has become the connector between almost all policy challenges on the internet and stakeholders are taking part in a multitude of deliberations and negotiations in various forums. They engage in normative exercises under the auspices of a number of institutions. But too many norms, too many meetings might be counterproductive. Psychologists refer to the paradox of selection. Too many choices, including normative choices, make decisions harder, not easier. As an exercise to reduce complexity, the present contribution aims to present one single, normative European approach to ensuring better cyberstability in the 2020s.

What are its key elements? We can apply values to standards and code and 'renormativize' them. Just as has happened with industrial norms in the last century, codes and standards are shown to be part of the normative order of the internet and not technical artefacts.

The key critical internet resources – internet routing, the domain name system, certificates and trust, and communications cables – have also been called the 'public core of the internet' and deserve special protection. The hypothesis that value-based normativity must influence technical standard-setting to ensure, inter alia, the protection of the common interest is shown to be valid. Far from being a space where only adhoc norms develop, essential elements of the internet's architecture are based on stable normative arrangements.[50] Stability, legitimacy and normativity all bring us back to the EU who can grow into a powerful online actor.

This paper has elaborated how the EU can strengthen its position as a legitimate global leader in internet governance. It must take up the baton now. The darth of comprehensive political approaches to safeguarding human rights and security and ensuring economic progress and innovation is obvious. Therefore, Europe's time to act has come. In order to functionally do so, it must sharpen its normative approaches. The goal must be to

[50] Kettemann, The Normative Order of the Internet (2019).

establish a legitimate normative order of internet, based on common standards and commitments – a 'New Deal for Internet Governance', implemented through an reinvigorated IGF, which can exercise substantial normative pull.

Together with other stakeholders in their respective roles Europe should engage in a forward-looking process of establishing the contours of '**New Deal for internet governance**'. This deal could take the form of a legally non-binding framework of commitments by state and non-state actors on how to stabilize and develop cyberspace to the benefit of all. Such a deal would go beyond normative precursors, such as the Global Compact proposed by the Bildt Commission, and include (based on pre-existing commitments) norms for good behavior in cyberspace for state and non-state actors (**Digital Peace Plan**), clear commitments to reinvigorating global trade while ensuring the realization of human development through digital SDGs (**Digital Marshall Plan**), a framework of interpretation for the protection and the respect of human rights in the digital age (**Digital Human Rights Document**) and guidelines for the development of internet protocols, codes and algorithms for the Internet of Things and for AI (**Guidelines on Norms and Code**).

In light of the challenges ahead, we end as we started: This is not a drill. Europe's time to act is now.