*Global Constitutionalism (2020), 9:2, 364–386*
doi:10.1017/S2045381720000167

# Authority conflicts in internet governance: Liberals vs. sovereigntists?

DANIËLLE FLONK
*Hertie School, Friedrichstrasse 180, 10117 Berlin, Germany*

Email: flonk@hertie-school.org

MARKUS JACHTENFUCHS
*Hertie School, Friedrichstrasse 180, 10117 Berlin, Germany*

Email: jachtenfuchs@hertie-school.org

ANKE S. OBENDIEK
*Hertie School, Friedrichstrasse 180, 10117 Berlin, Germany*

Email: obendiek@hertie-school.org

**Abstract:** We analyse conflicts over norms and institutions in internet governance. In this emerging field, dispute settlement is less institutionalised and conflicts take place at a foundational level. Internet governance features two competing spheres of authority characterised by fundamentally diverging social purposes: A more consolidated liberal sphere emphasises a limited role of the state, private and multistakeholder governance and freedom of speech. A sovereigntist challenger sphere emphasises state control, intergovernmentalism and push against the preponderance of Western institutions and private actors. We trace the activation and evolution of conflict between these spheres with regard to norms and institutions in four instances: the World Summit on the Information Society (WSIS), the World Conference on International Telecommunications (WCIT-12), the fifth session of the United Nations Group of Governmental Experts (UNGGE) and the Budapest Convention of the Council of Europe. We observe intense norm collisions, and strategic attempts at competitive regime creation and regime shifting towards intergovernmental structures by the sovereigntist sphere. Despite these aggressive attempts at creating new institutions and norms, the existing internet governance order is still in place. Hence, authority conflicts in global internet governance do not necessarily lead to fragmentation.

**Keywords:** contested multilateralism; internet governance; norm collisions; sovereignty

## I. Introduction

With its dramatic rise in importance, the analysis of internet governance increasingly moves from predominantly technical analyses to general conceptual lenses such as constitutionalisation (Celeste 2019; Fischer-Lescano 2016; Pernice 2018), the evolution of norms (Finnemore and Hollis 2016) or the role of state interests (Drezner 2007). We contribute to this mainstreaming by analysing conflicts between spheres of authority in internet governance over the last 20 years.

We find that despite the relative novelty and the extreme dynamism of the field where one might expect to find rapidly evolving governance structures and complex conflict constellations, there is relative stability and only slow change of spheres of authority. A prevailing *liberal* sphere is strongly supported by Western states but increasingly challenged by an assertive *sovereigntist* sphere spearheaded by China, Russia and a number of authoritarian as well as developing countries. Contrary to what one might expect, the growing number of institutions and fora in internet governance and the explicit activation of norm collisions has not (yet) led to the fragmentation of internet governance. Rather, the liberal sphere is undergoing slow internal change.

Our argument proceeds as follows: In the next section, we present our understanding of internet governance, of authority conflicts and our methodology for selecting cases and analysing these conflicts. The following four sections provide detailed studies of different cases for supporting our argument. We conclude by interpreting and generalising the results.

## II. Analytical concepts and methods

Defining internet governance has been subject to considerable debate by policymakers (WSIS 2005) and specialised scholars (DeNardis 2014: 19–20; Hofmann et al. 2016: 1418). As we aim to apply general concepts to the study of internet governance, we define (global) governance in line with a widespread use in international relations as 'the exercise of authority across national borders as well as consented norms and rules beyond the nation state, both of them justified with reference to common goods or transnational problems' (Zürn 2018: 4–5). This rather broad definition includes purely intergovernmental bodies as well as purely private or non-profit arrangements or mixed forms, and it refers to agreed norms and the exercise of authority (as opposed to power alone) but it is neutral with regard to the underlying social purposes.

Internet governance (like governance in other issue areas) takes place in distinct spheres of authority. A sphere of authority is more than just a group of like-minded states, which the literature on internet governance frequently

https://doi.org/10.1017/S2045381720000167 Published online by Cambridge University Press

identifies (Deibert and Crete-Nishihata 2012: 346; Maurer and Morgus 2014: 3; Nye 2014: 13), but ‘a governance space with at least one domestic or international authority, which is delimited by the involved actors’ perception of a common good or goal at a given level of governance’ (Kreuder-Sonnen and Zürn, this issue: 255). Spheres of authority can comprise a diversity of actors such as states, intergovernmental organisations, private actors and multistakeholder fora, with some actors as focal points and some more at the periphery. In line with the definition of governance above, spheres of authority are not just functional or technocratic bodies but normative orders about common goods. For our empirical analysis, we distinguish between two ideal types, a *liberal* and a *sovereigntist* sphere. Our description emphasises their characteristic and distinctive features. As ideal types, they are not meant to be an accurate representation of a complex reality but rather constitute an abstraction from this reality in order to use them as analytical concepts.

The proponents of the *liberal sphere* see the internet as an opportunity and as an emerging transnational space that should mostly be governed by private self-regulation based on voluntary participation and substantive expertise. Institutions should be flexible and stakeholder-based whereas the role of the state should be limited to providing security and enforcing hard rules when needed. Their social purpose is to encourage the development of the internet as much as possible by giving individuals, firms and civil society organisations as much freedom as possible. Intergovernmental organisations are perceived as too status quo oriented for achieving this purpose. The underlying ideology is a combination of free market and pluralist civil society thinking.

The proponents of the *sovereigntist sphere* see the internet as a threat rather than as an opportunity. It should therefore be governed by intergovernmental institutions in order to respect domestic sovereignty and avoid external encroachments. Firms, civil society or experts should at best have an advisory role. The social purpose of this sphere of authority is to protect sovereignty and core domestic values and goals against domestic or international actors empowered by the internet. The underlying ideology is a world in which governments decide about domestic policies without external intervention and constraints and enter into international agreements on the basis of sovereign equality.

The added valued of constructing two competing views of internet governance stems from the fact that while there is often a myriad of social purposes, institutional architectures and social or legal norms, these highly specific elements often come in packages. As analytical concepts, our two ideal-typical spheres of authority are located at a rather high level of abstraction. There is room for variety within each sphere but no third way which is categorically distinct from the liberal and the sovereigntist sphere.

https://doi.org/10.1017/S2045381720000167 Published online by Cambridge University Press

The libertarian views mainly popular in the 1990s as well as calls for tighter regulation and a more active state voiced in recent years are variants and possible trajectories of the liberal sphere.

Also, the diverging regulatory regimes of the US and the EU in the area of data privacy (Farrell and Newman 2019) constitute struggles within it. The sovereigntist sphere encompasses the views of authoritarian states that wish to control the internet in order to maintain domestic rule as well as views of developing countries eager to have a greater say in a governance system they perceive as dominated largely by Western states and firms. When we speak of 'adherents' or 'proponents' of the liberal or the sovereigntist sphere, this is a shorthand for expressing the positions of states and other actors towards alternative ways of organising internet governance. It does not say anything about their positions towards other issues and is not to be confounded with formal membership. Although the concept is neutral with regard to actors and could also include firms and civil society actors, we focus largely on states in this article for reasons of space.

We use these two spheres of authority for understanding the evolution of conflicts about how internet governance should be organised. This shows the applicability of the concept of spheres of authority beyond established spheres (see Gholiagha *et al.*, this issue) such as trade or drug control in rapidly evolving fields without a settled institutional structure like internet governance. We use our two ideal-typical spheres of authority for identifying stability, continuity and incremental change in a seemingly highly dynamic and unsettled policy area. We argue that underneath the surface of dynamism, the underlying social purposes, institutional preferences and norms remain relatively stable over time and are structured along a conflict line between two spheres of authority of which the liberal one is dominant and evolving over time while the sovereigntist one is a growing challenger.

For the analysis of these two spheres, we look at two dimensions where they clearly differ and where conflict is most pronounced. With respect to *institutions*, we analyse 'contested multilateralism' and assess state strategies in terms of whether they attempt 'regime shifting' (e.g. moving an issue from a multistakeholder forum to an existing intergovernmental institution) or 'competitive regime creation' (e.g. creating a new intergovernmental institution (Morse and Keohane 2014)). The advocates of the liberal sphere prefer private or multistakeholder fora. They are not in principle opposed to formal institutions but support them in some cases, mainly for dealing with core state powers such as security provision and crime control. For these issues, they prefer Western organisations such as the Council of Europe. The sovereigntists want a different institutional setup that is not dominated by large and powerful Western states and firms but gives primacy to sovereign states and equal representation and use regime shifting and competitive

https://doi.org/10.1017/S2045381720000167 Published online by Cambridge University Press

regime creation for achieving this goal. Their preferred institutional venue is the UN or its specialised organs such as the International Telecommunication Union (ITU).

With respect to *norms* (understood as shared standards of appropriate behaviour for actors with a given identity; Finnemore and Sikkink 1998: 891), we analyse conflict over specific norms for governing the same substantive issues between the adherents of the two spheres, for instance whether they prefer to strengthen human rights and freedom of expression or rather stress norms of information security or criminal law. As is typical for internet governance, these norm collisions often involve general principles or social norms rather than hard law, which is the focus of other contributions in this Special Issue (e.g. Moe and Geis, this issue; Krisch *et al.*, this issue). They often (but not exclusively) take place in political and deliberative fora rather than in institutions for formal law-making and adjudication. The proponents of the liberal sphere emphasise human rights, freedom of expression and a limitation of state control. Their sovereigntist contenders see the content of internet-based communication as a threat to domestic values and domestic stability that needs to be controlled rather than encouraged. Sovereigntists strive for the recognition and legitimisation of state control over the internet. Table 1 provides an overview of the differences.

In order to trace developments over time and to analyse conflicts over norms and institutions in some detail, we provide four case studies on the conflict over the World Summit on the Information Society (WSIS) and the Tunis Agenda from 2003 to 2005, the clash over seemingly technical details

Table 1. Spheres of authority in internet governance.

| Conflict over | liberal sphere | sovereigntist sphere |
|---|---|---|
| institutions | • private or multistakeholder<br>• institutional status quo<br>• Western institutions<br>• consensus-basedinclusive deliberation | • intergovernmental<br>• institutional change<br>• UN or non-Western institutions<br>• state veto power, one country/ one vote |
| norms | • individual human rights<br>• freedom of speech<br>• free flow of information<br>• universal values<br>• unfragmented and global internet | • state rights<br>• information security<br>• territorial integrity, domestic stability<br>• national sovereignty<br>• national internet segments |

https://doi.org/10.1017/S2045381720000167 Published online by Cambridge University Press

during the World Conference on International Telecommunications (WCIT-12) in 2012, the debates in the fifth session of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) in 2017 and the disputes over cybercrime and law enforcement online in the context of the Budapest Convention of the Council of Europe from 2017 onwards. We selected these four instances of conflict because they are moments of high conflict and intense debate where norm conflicts are activated and competing institutional proposals are made. They show large shifts and breaks between the spheres of authority while covering a wide scope of actors, issue areas and time. They take place in different fora (a large UN conference, an international technical conference, a UN expert group and a European intergovernmental institution), cover highly different substantial topics (general principles of internet governance, technical norms, the role of international law and security issues) and stretch over more than 15 years. Showing that there is a constant pattern of conflict in highly divergent cases over an extended period strengthens the generalisability of the results.

In the following, we analyse the conflict presented above in a stylised form in more depth. We show that while some states changed sides during the evolution of the conflict and the substance of contestation shifted, the overall structure of two competing spheres of authority remained constant even in different issue areas. In the next four sections, we briefly describe the substantive content and context of each of the four instances, identify the most important conflicts over institutions and over norms after the conflict was activated and analyse the outcomes. A summary of our findings can be found below in Table 2. Despite a series of intense challenges, there is still little fragmentation in internet governance and the existing order remains in place.

## III. Emerging conflicts during the WSIS process and the Tunis Agenda

The first major conflict occurred at the first World Summit on the Information Society, which formally started at the International Telecommunication Union in Geneva in 2003 and continued in Tunis in 2005. With the burst of the dot-com bubble in 2000–2002, there was increasing recognition of a ‘regulatory void’ (Hofmann 2005: 10) that needed to be filled. The development of regulative norms and principles as well as a definition of ‘internet governance’ became a key objective during the preparatory meetings and a Working Group on Internet Governance was established. A group of sovereignty-oriented actors challenged the existing US-centric governance structures and the conference resulted in a compromise and established the

https://doi.org/10.1017/S2045381720000167 Published online by Cambridge University Press

Table 2. Overview of conflicts and outcomes.

| | | **WSIS** | **WCIT-12** | **UNGGE** | **Budapest** |
|---|---|---|---|---|---|
| **Topic** | | definition, scope and actors of internet governance | revision of 1988 technical ITU Treaty for internet age | applicability of international law to use of ICTs by states | cybercrime convention |
| **Forum** | | World Summit on the Information Society | World Conference on International Telecommunications | Fifth UNGGE (UN expert group) | Council of Europe, UN |
| **Time of conflict** | | 2003–2005 | 2012 | 2016/17 | since 2017 |
| **Actors** | **liberal** | US and ICANN, technical bodies; EU undecided and finally compromising | 55 countries (incl. Australia, Canada, EU Member States, India, Japan, New Zealand, US) | US, supported by EU Member States and others | CoE members including US, but except Russia, Japan, South Africa |
| | **sovereigntist** | Brazil, South Africa, China, Iran and ITU with internal rifts due to democratic vs authoritarian systems | 89 countries (incl. African countries, Brazil, China, Indonesia, Iran and Russia) | BRICS states, CIS, developing countries | Russia, China, authoritarian countries (e.g. Iran), sometimes global South |
| **Positions institutions** | **liberal** | private or multistakeholder body | maintaining multistakeholder model | no new regime, no multistakeholderism | globalise Council of Europe Budapest convention |
| | **sovereigntist** | UN, ITU | increasing role of ITU | creating a new intergovernmental regime | new UN treaty |

https://doi.org/10.1017/S2045381720000167 Published online by Cambridge University Press

Table 2. (Continued)

| | | WSIS | WCIT-12 | UNGGE | Budapest |
|---|---|---|---|---|---|
| **Positions norms** | **liberal** | freedom of expression | prevent increased authority of governments, prevent justification of content control, prevent mentioning internet in revised ITRs | apply right to self-defence, countermeasures and humanitarian law | human rights (esp. free speech), cooperation |
| | **sovereigntist** | first indications of content as threat | increased role of governments in governing content, e.g. in traffic routing, defining spam | development of *lex specialis*, recognition of sovereignty in cyberspace | sovereign control, non-interference, for some: content control |
| **Outcome** | **institutions** | attempted sovereigntist regime shifting largely failed | successful sovereigntist competitive regime creation | attempted sovereigntist regime shifting failed, liberal consolidation of existing regime failed | ongoing attempts at sovereigntist competitive regime creation |
| | **norms** | commitment to democratic internet governance, but also emphasis on sovereignty | no agreement on government authority in internet governance | no consensus on *how* norms of international law apply to cyber operations | ongoing clash between human rights and non-interference/ content control norms |

UN Internet Governance Forum (IGF) as a 'new forum for multi-stakeholder policy dialogue' (WSIS 2005).

With regard to institutions, different perspectives existed concerning the status quo at the outset of the WSIS conference. The US-centric governance system included a multiplicity of rather informal, technical bodies, such as the Internet Engineering Task Force (IETF), private actors, and ICANN. The emerging countermovement, led by China, Brazil, South Africa and supported by the ITU, favoured a more intergovernmental model (Wright 2005), emphasising the significance of political authority and its links to sovereignty and economic development (Kleinwächter 2004).

While initially mostly favourable of the US model, the US unilateral oversight of ICANN, which existed at the time, increasingly developed into a source of conflict in the EU–US relations as well (Mueller 2010: 74). In particular the simultaneous advertisement of private sector leadership was perceived as contradictory. Thus, a power battle emerged between the US and ICANN on the one side and both non-Western and European states on the other (Mueller 2010: 67).

The European Commission (EC) proposed a 'new cooperation model' on 'a more solid democratic, transparent and multilateral basis, with stronger emphasis on the public policy interest of all governments' (EC 2005) and thus implicitly questioned the status quo. It was severely criticised by the US as a concession to the sovereigntist push for an intergovernmental body (Wright 2005). Multistakeholderism in its current form with relatively equal opportunities for the various stakeholders, particularly governments, was only emerging (Weinberg 2011: 201). However, after significant diplomatic efforts, European and other democratic countries were willing to compromise due to concerns about the efforts by countries such as China, Saudi Arabia or Iran to increase cyber sovereignty (Palfrey 2010).

While there were significant divergences regarding the appropriate institutions for internet governance, there was less conflict over norms, probably because the low internet access rates in most but the highly industrialised countries kept issue salience low. Nevertheless, the narrative of the internet as a threat to domestic stability was already emerging. For instance, the Chinese representative's statement emphasises the need to 'stress social responsibility and obligation' (Ju 2005) in internet governance. In contrast, actors of the liberal sphere expressed concerns about threats to freedom of expression and emphasised principles of openness and participation as embodied by ICANN and the IETF as well as freedom of expression and opinion as enshrined in the Universal Declaration of Human Rights (WSIS 2005: 47).

The Tunis Agenda (WSIS 2005) and the accompanying Tunis Commitment concluded the WSIS process with a compromise. On the one hand, the

https://doi.org/10.1017/S2045381720000167 Published online by Cambridge University Press

Tunis Agenda emphasises that the '[p]olicy authority for Internet-related public policy issues is the sovereign right of States' (Article 35a) and brings attention to governments' 'equal role and responsibility' (Article 68). On the other hand, it legitimises the existing structures (Article 55) and, in a commitment to multistakeholderism, highlights the 'important roles' (Article 35b, c) of private actors and civil society. The creation of the IGF as a forum for deliberation de-escalated rather than resolved the conflict. Its weak institutional capacities, by some dismissed as a mere 'talkshop' (Zittrain 2008), did not significantly restrict the authority of ICANN or other technical bodies. Therefore, the novelty of the IGF consisted in the significant inclusion of non-state actors in governance processes (Mathiason 2008). Nevertheless, the creation of the IGF already shows the emerging conflict between the liberal and the sovereigntist sphere.

With regard to norms, WSIS merely showed first signs of the conflicts that erupted later. The Tunis outcome documents often avoided specific phrasing on contentious issues to allow diverging interpretations by different countries and stakeholders (Mueller 2010). However, in contrast to earlier discussions that emphasised less controversial 'bottom-up' processes, a commitment to a 'democratic' management of the internet featured prominently in the first paragraphs of the Tunis Agenda, which indicates that core norms of the liberal sphere prevailed.

After the conflict, the liberal sphere had further consolidated, despite the contradictions between the simultaneous emphasis on US government control and private sector responsibility. In contrast, the sovereigntist sphere was still in flux. The efforts of the democratic BRICS, in particular Brazil and South Africa, might have contributed to enhanced governmental responsibility in internet governance if the European states had backed their efforts towards increased transparency and public regulation (Ebert and Maurer 2013). However, their insistence on the inclusion of private actors and concerns about the empowerment of authoritarian states made the Europeans join the US and push for multistakeholderism as an institutional compromise. This move successfully stopped the attempt to shift the regime to the UN.

## IV. Fragmentation in a seemingly technical forum: WCIT-12

On the 2012 World Conference on International Telecommunications (WCIT-12), ITU member states wanted to amend the International Telecommunication Regulations (ITRs) treaty from 1988, which was widely regarded as outdated and unsuitable for dealing with growing threats of cybercrime, cyberwarfare, and cyberespionage. The ITRs established

https://doi.org/10.1017/S2045381720000167 Published online by Cambridge University Press

general principles about the provision and operation of international telecommunication services, and the underlying international transport means to provide these services (ITU 1988). Although the ITRs were technical and most proposed revisions not controversial (about 90 per cent, Hill 2013: 317), some proposals were highly conflictual. At the end of WCIT-12, 89 countries (under which many African countries, Arab states, China, Russia, Iran, and emerging economies like Argentina, Brazil, Indonesia, Mexico, South Korea, and Turkey) signed the revised ITRs whereas 55 countries (under which Australia, Canada, EU Member States, India, Japan, New Zealand, and the US) did not sign the revised treaty (ITU 2012b). This led to the creation of two institutional structures: one for the states which signed the revised 2012 ITRs and one for the states that stuck to the old 1988 ITRs (see Hill 2013 for a comprehensive overview).

There was strong disagreement between adherents of the liberal and the sovereigntist sphere over institutions (on the role of the ITU in internet governance) and norms (on the balance between human rights and security concerns). With regard to institutions, there was conflict over to what extent internet governance should be brought under UN auspices (Nocetti 2015: 125). Whereas adherents of the liberal sphere wanted to keep the role of the ITU limited, proponents of the sovereigntist sphere wanted to replace existing multistakeholder models by giving more authority to the ITU to regulate the internet. For instance, Russia submitted a proposal that member states should have equal rights to manage the internet with regard to naming and numbering (Russian Federation *et al.* 2012), aimed at creating an alternative to ICANN. Proponents of the liberal sphere were concerned that this kind of proposals would give more authority to the ITU and replace the multistakeholder model (US Majority Committee Staff 2012). For the US, '[c]entralised control over the Internet through a top-down government approach would put political dealmakers, rather than innovators and experts, in charge of the future of the Internet' (Verveer 2012).

With regard to norms, states disagreed on human rights norms and the possible justification of content control. For instance, adherents of the sovereigntist sphere submitted a proposal that governments should know how internet traffic is routed and that operating agencies should determine which international routes should be used (Algeria *et al.* 2012: Article 3) in order to improve cybersecurity. They also submitted a proposal about spam, defining it as information having no meaningful message transmitted in bulk over telecommunication networks (Russian Federation *et al.* 2012). Adherents of the liberal sphere were opposed to any proposal on cybersecurity and spam since this would have given national governments more authority over the internet and justify internet censorship in the name of national security (US Majority Committee Staff 2012). The US even wanted to prevent any

https://doi.org/10.1017/S2045381720000167 Published online by Cambridge University Press

mention of the internet in the revised ITRs because they feared limitations of freedom of speech online (Pfanner 2012). As the US gained the support of the EU, a liberal and a sovereigntist bloc with strongly diverging preferences were in opposition.

The ITRs revision process escalated over the accompanying non-binding Resolution 3, which states that ‘all governments should have an equal role and responsibility for international internet governance and for ensuring the stability, security and continuity of the existing Internet’ (ITU 2012a). Proponents of the liberal sphere were concerned that this would increase the role of the ITU and move internet governance more towards an intergovernmental model instead of a multistakeholder model (Hill 2013: 325). The process by which this resolution was adopted is characteristic for the intensity of the conflict. Although the ITU Secretary-General had assured that no voting would take place, the conference chair, Mohamed Nasser al-Ghanim, asked for an informal poll, on which member states used their nameplates to show whether they agreed or not with the resolution. After a majority of member states was in favour of the resolution, the chair ruled that it was approved. Whether this process counted as an official and authoritative vote was debated until the end of the conference (Maurer and Morgus 2014: 3). This incident activated the conflict and created concerns with adherents of the liberal sphere and greatly contributed to the later rejection of the revised ITRs by 55 countries.

In the end, 89 countries signed the revised ITRs, and 55 countries did not due to concerns over the ITU’s role in global internet governance and increased state control over internet content even though there was a consensus that outdated technical regulations needed to be updated. Adherents to the sovereigntist sphere successfully created a competitive regime, which entered into force in 2015 for those ITU member states who signed the revised ITRs. For the non-signatories, the 1988 ITRs are still in force. WCIT-12 thus led to a fragmentation of internet governance in a specific sector.

## V. Divisions over security at UNGGE 2016/2017

Since cybersecurity had become a global concern by 2015, the UN General Assembly (UNGA) tasked the fifth United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of International Security (UNGGE) to write a report on how international law applies to the use of ICTs by states (UNGA 2015). The UNGGE was established after a Russian proposal in 2001 and consists of government representatives. Since 2004, five UNGGEs have convened on common norms, rules and principles for responsible state behaviour in

https://doi.org/10.1017/S2045381720000167 Published online by Cambridge University Press

cyberspace. In 2013, the third UNGGE agreed *that* international law, and in particular the UN Charter, applied to the use of ICTs by states. The fourth UNGGE of 2015 articulated voluntary and non-binding norms of responsible state behaviour (Tikk and Kerttunen 2017: 11). However, during the fifth UNGGE in 2017, the working group could not reach a consensus on *how* norms of international law apply to cyber operations (UNGA 2017a) and did not adopt its final report.

The conflict was activated when proponents of the liberal (the US and EU Member States) and sovereigntist sphere (BRICS, Commonwealth of Independent States members and some developing countries) disagreed on a number of issues. Regarding institutions, adherents of the liberal sphere wanted to apply existing international law to cybersecurity without creating a new regime. However, adherents of the sovereigntist sphere preferred a new binding intergovernmental regime (Tikk and Kerttunen 2017: 16) but proponents of the liberal sphere were unwilling to initiate such a negotiation process in the UN (Rodríguez 2017).

Regarding norms, proponents of the liberal and sovereigntist sphere disagreed on what was concretely meant by the application of existing international law to issues such as the right to self-defence, countermeasures, and humanitarian law (Delerue 2018: 3–4). Adherents of the sovereigntist sphere feared that including the right to self-defence would legitimise retaliation with conventional weapons (Sukumar 2017). Particularly problematic for them was the formulation in the draft final report that the malicious use of ICTs by states was the same as an armed attack as defined in Article 51 of the UN Charter (which justifies self-defence) (Rodríguez 2017). Some states feared that the US would use such a reading of international law as a justification to launch retaliatory strikes against cyberespionage by countries like China (Segal 2017: 7). They also feared that the reference to countermeasures could recognise the right to reciprocate a cyberattack (Sukumar 2017). This would enable sanctions and punishment while bypassing existing mechanisms, such as the UN Security Council (Russian Federation 2017). Since the US has superior conventional and cyber capabilities, the inclusion of the right to self-defence and countermeasures is problematic for sovereigntists (Sukumar 2017). Moreover, they argued that a reference to Article 51 does not send a message of peaceful settlement of conflict prevention (Rodríguez 2017) since it suggests a legitimation of cyberwarfare. Whether or not these are valid legal arguments is debatable but they show the high degree of conflict over the topic of cybersecurity.

These disagreements escalated once some proponents of the sovereigntist sphere started to retract their support for the applicability of international law made in previous UNGGEs. This backsliding was not acceptable for proponents of the liberal sphere. The US stated that some participants believed that they are ‘free to act in or through cyberspace to achieve their political ends with no limits or constraints on their actions’ (Markoff 2017). The diverging views between the two spheres’ adherents proved to be insurmountable during the fifth UNGGE. The attempt of adherents of the liberal sphere to consolidate the existing information security regime failed when no final report was adopted. Likewise, the attempt of adherents of the sovereigntist sphere to shift the regime into their preferred direction or even creating a new regime failed when the UNGGE did not reach a consensus. Previously established reports were already fragile compromises and the chair of the fifth UNGGE, Karsten Geier, even argued that the establishment of a future UNGGE was unlikely since ‘continuing to do the same thing and expecting a different outcome is a sign of madness’ (Geier 2018).

The divisions continued when conflicting resolutions by the US and Russia were both adopted by the UNGA First Committee in 2018. The US resolution (139 votes) calls for the establishment of a new UNGGE to further study norms and to discuss how international law applies to cyberspace (UNGA 2018b). The Russian resolution (109 votes) establishes an open-ended working group (OEWG) to further develop the norms of the fourth UNGGE and to discuss models for regular institutional dialogue under the UN (UNGA 2018a). This recent attempt by the sovereigntist sphere actors to create an alternative to the UNGGE is a development similar to the WCIT-12 case. It shows proactive attempts to create a competitive regime with the support of a considerable amount of countries and to move debates to new venues (e.g. the OEWG) when they are considered unfruitful in other fora (the UNGGE). Although the outcome of these developments are not clear yet, it at least indicates that the conflict between the proponents of the liberal and sovereigntist sphere over cybersecurity continues.

## VI. Norm clash over cybercrime and law enforcement online

Cybercrime has become an increasingly significant global problem and is addressed by different global and regional institutions, such as the OECD, the G8, the African Union, or the Arab League. However, the Council of Europe’s (CoE) (2001) Convention on Cybercrime (Budapest Convention), in force since 2004, is the only legally binding and arguably most important international instrument. The CoE is an intergovernmental organisation focused on human rights, democracy and the rule of law in Europe. It has 47 member states, including all EU member states and Russia. The US and Canada have observer status. However, the Budapest Convention has

https://doi.org/10.1017/S2045381720000167 Published online by Cambridge University Press

explicitly been designed to have a global reach and at present has more than 60 parties to the convention, including the US, Canada, and Japan.

While not all CoE member states have ratified the convention, Russia is the only CoE member to refuse to even sign it, mainly due to concerns about cross-border law enforcement access during cybercrime investigations (CoE 2001: Article 32b). While the more intergovernmental character of the CoE should, in principle, find their support, sovereigntists under Russian leadership attempt to create a competing regime under the auspices of the UN that reflects a commitment to sovereignty and non-interference rather than strong human rights protections typical for the CoE. While Russia has been pushing for an international treaty in the area of cyber and information security since 1998, for instance at the UNGGE and other UN fora, these efforts are echoed by all BRICS states. The BRICS collectively stated after a meeting in late 2017 that they 'recognize the need for a universal regulatory binding instrument on combatting the criminal use of ICTs under the UN auspices' and 'acknowledge the efforts of the Russian Federation' (BRICS 2017).

Russia activated the conflict by proposing a UN Draft Convention on Cooperation in Combating Information Crimes (Lavrov 2017; Russian Federation 2017) at the UNGA in 2017. While this proposal received only limited attention, a Russian-sponsored resolution, backed by Brazil, China and South Africa, was adopted with 88 votes in favour in November 2018 (UNGA 2018c). Compared to the Draft Convention, the 2018 resolution is less ambitious but attempts to re-emphasise the role of the UN, including the Secretary-General, in the area of cybercrime.

Most parties to the Budapest Convention reject these attempts as unnecessary or 'premature' (T-CY 2017) in light of the existing framework and the significant time and effort necessary to negotiate a new agreement on the global level. The 2018 resolution was severely criticised by the US representative for its attempt at 'politicizing, polarizing and undermining' existing policies (US Department of State 2018). In response to criticism of the exclusive negotiation framework of the CoE as a European institution, the CoE makes strategic efforts to appeal to particularly countries of the Global South through outreach and capacity-building projects.

With regard to norms, the Russian-led efforts emphasise a commitment to cyber sovereignty, territorial integrity and non-interference. For instance, Russian Foreign Affairs Minister Lavrov (2017) referred to a UNGA Resolution (2017b) emphasising the right to non-interference and the rejection of extraterritorial use of national laws, which echoes criticisms of other sovereigntists. In contrast, proponents of the liberal sphere have voiced concerns about potential attempts to induce state control over the internet via a global treaty (UNGA 2016). Whereas human rights online, such as freedom of speech or freedom of opinion, are prominently mentioned in the Budapest Convention, they have a limited role in the Russian proposals or in the cybersecurity strategies of the Shanghai Cooperation Organization (SCO) or China and are replaced by references to 'stability and security of society' or the need for sovereignty (China 2017: Preamble). This conception of 'content as threat' for the internal stability of a country (Nocetti 2015: 116; Palfrey 2010) has been promoted increasingly since the Arab Spring by authoritarian countries. Liberal states consider these efforts as a 'Trojan horse' (Ebert and Maurer 2013: 1055) to introduce content control and thus circumvent constitutionalist principles. This also decreased support from the democratic countries among the sovereigntists. This conflict is still ongoing.

## VII. Conclusion

In this article, we analysed conflicts over norms and institutions in the field of internet governance. Beyond a multiplicity of seemingly unrelated issues, there is an overarching conflict between two fundamentally different views with different social purposes, institutional structures and specific norms (see Table 2 for an overview of our empirical findings). As internet governance is by and large not strongly legalised, this conflict rarely, and in contrast to other contributions to this Special Issue (see e.g. Moe and Geis, this issue; Krisch *et al.*, this issue), involves collisions of legal norms from different established spheres of authority. Rather, it is in many instances not yet established which norms apply to which issue of internet governance. The UNGGE even debated whether international law was applicable at all. In this situation of normative uncertainty and rapid development, two distinct groups tried and are still trying to establish the applicability of specific norms to particular policy problems. In doing so, they draw on different sets of norms emanating from different institutions, the liberals typically from the area of human rights, the sovereigntists usually referring to non-interference and the collective rights of societies.

The polycentric nature of internet governance (Scholte 2017), characterised *inter alia* by a low degree of legalisation, the lack of a strong core institution or formalised dispute settlement, in contrast to other areas, such as world trade (see Gholiagha *et al.*, this issue), and the rapid multiplication of formal and informal venues for dealing with internet governance, are factors that could have contributed to a quick fragmentation of internet governance. However, we find little fragmentation. Only one case can be interpreted as such. In the WCIT-12 case on the revision of the International Telecommunication Regulations (ITRs), a massive sovereigntist attempt at regime shifting was rejected by the adherents of the liberal sphere and led to the creation of a competitive parallel regime. The creation of the open-ended working group (OEWG) by Russia in 2018 shows the resolve of the sovereigntists but it is too early to assess whether this is a permanent fragmentation.

The underlying conflict between two spheres of authority is not limited to the four cases analysed here. Instead, these cases are indicators of a broad sovereigntist endeavour to challenge the existing internet governance norms and institutions and to shape an emerging and therefore still malleable field. There is a plethora of other examples of this conflict. For instance, Russia proposed a Convention on International Information Security in 2011 (Russian Federation 2011). Similarly, Shanghai Cooperation Organization member states promoted a Code of Conduct for Information Security at the UNGA in 2011 and 2015 (China *et al.* 2011, 2015). Furthermore, China organised an annual World Internet Conference (WIC) in Wuzhen, focused on creating global internet governance norms.

However, the liberal sphere is not only challenged from outside but also from within. Particularly after the Snowden revelations in 2013, conflicts in areas such as data privacy or the domain name system have challenged the hegemonic influence of the US Government and of US companies. For instance, Brazil aimed to create a new multistakeholder forum on internet governance and hosted a first meeting in 2014. However, despite backing from other actors in the liberal sphere, the NETmundial Initiative failed. The IANA transition between 2014 and 2016, which terminated the exceptional role of the US in global Internet infrastructure, was a response to criticism of US hegemony from both liberal and sovereigntist proponents. However, these challenges do not necessarily result in a weakening of the liberal sphere. As also demonstrated by Scholte (2018) the IANA stewardship transition actually resulted in a manifestation of, for example, the position of the US government and the (liberal) multistakeholder community. The liberal sphere adapts or even strengthens by reacting to challenges and thus prevents a fragmentation of internet governance. However, the liberal sphere suffers from two inconsistencies: (1) the weakness of political authority, and (2) domestic stability and security.

First, there is a strong reliance of the liberals on private self-regulation, soft law and discursive multistakeholder processes rather than on public international law. As a result, the liberal sphere is strong in technical authority but weak in legitimate political authority. The need for the latter is, however, increasingly felt with internet governance gaining increasing domestic political and economic importance. Particularly US technology companies have embraced a more proactive role, in some instances effectively pushing for or challenging governmental practices by positioning themselves as competing power centres or ‘Digital Switzerlands’ (Eichensehr 2019) in the liberal sphere. Tellingly, a proposal by a private

https://doi.org/10.1017/S2045381720000167 Published online by Cambridge University Press

firm (Microsoft) to adopt a 'Digital Geneva Convention' as a classical international law treaty dealing with cyberwarfare is seen with great reserve by Germany, a state which is usually a staunch supporter of multilateralism and international law. Particular developing countries criticise these efforts to keep the dominant liberal sphere under-legalised and under-institutionalised and thus dominated by large Western powers and large Western firms. This is also seen as a refusal of formalised specific rights and obligations, which are characteristic of the very idea of constitutionalisation (Fischer-Lescano 2016).

Second, the liberal attitude towards internet-based communication as a threat to domestic stability is changing. For a long time, the liberals have regarded this argument as a Trojan horse for strongly illiberal and undemocratic tendencies justifying internet shutdowns and censorship. Yet, for sovereigntist (and often supported by developing countries), the current configuration of norms and institutions is another instance of how a small number of Western states shapes and dominates institutions and rules with a global reach. Their core argument is that the current system for internet governance is deeply intrusive into legitimate domestic social purposes and domestic laws. Even among Western states, there is an increasing tendency to introduce legislation aimed at manifest violations of domestic criminal law, combating terrorist propaganda and disinformation, most notably when it interferes with elections, and export of dual-use technologies. The concerns of the liberal sphere in this respect sound increasingly similar to those of the sovereigntists. This weakens the liberal resistance against limitations of freedom of expression in the name of legitimate domestic concerns.

More recently, particularly the EU but also emerging powers have increasingly diverged from the current weak legalisation and constitutionalisation, which have raised the question whether there is a 'third way' between a 'Californian' and a 'Chinese cyberspace' as French President Macron put it during the 2018 IGF. Although it is too early to make a decisive call on this issue, we argue that it is more likely that the liberal sphere will accommodate requests for stronger internet regulation and a more proactive role of the state because this would not violate its normative core but allow the liberal sphere to remain dominant. Other liberal states, such as the US or New Zealand, are also facing increased internal contestations of their current internet policies and face public debates about, for example, hate speech, competition, data privacy, or intermediary liability (Frosio 2018). However, conflicts within the liberal sphere are likely to increase as the current US administration has in some areas worked against this trend, for example by dismantling net neutrality rules, refusing to join the widely

https://doi.org/10.1017/S2045381720000167 Published online by Cambridge University Press

supported Paris Call for Trust and Security in Cyberspace, or in recent attacks on French proposals for digital taxation.

Nevertheless, the concept of spheres of authority allows for these gradual shifts in constellations of actors, policy preferences and motivations for regulation, as long as the spheres are still meaningfully distinguishable from each other. Hence, the changing shape of spheres is not a new phenomenon. For example, early libertarian positions of internet pioneers have been abandoned once the internet became larger in scale and scope and China has remarkably expressed its support for the multistakeholder organisation ICANN, despite recent efforts to subject domain name registration to governmental licensing. As argued in the previous section, security concerns are an important driver for these changing constellations of the liberal sphere. External shocks such as terrorist attacks in Christchurch increase the demand for state regulation and the liberal sphere adjusts accordingly, creating new opportunities for sovereigntist challengers to shape global internet governance debates. Hence, the conflicts over adequate internet governance institutions and norms are ongoing, transforming and unlikely to be resolved in the future.

## Acknowledgements

The authors would like to thank participants at the Deutsche Vereinigung für Politikwissenschaft (DVPW) conference, the European Consortium for Political Research (ECPR) General Conference, the Overlapping Spheres of Authority and Interface Conflicts in the Global Order (OSAIC) research group for constructive comments. Special thanks go to Christian Kreuder-Sonnen, Martin Koch, Wolf Schünemann, Michael Zürn and two anonymous reviewers. We gratefully acknowledge funding by the *Deutsche Forschungsgemeinschaft* (DFG), FOR 2409, JA 772/8-1.

## References

Algeria, Saudi Arabia, Bahrain, China, United Arab Emirates, Russian Federation, Iraq, and Sudan. 2012. *Proposals for the Work of the Conference*, Document 47-E at: <http://files.wcitleaks.org/public/S12-WCIT12-C-0047!!MSW-E.pdf>.

BRICS. 2017. *9th BRICS Summit – BRICS Leaders Xiamen Declaration*. Xiamen, at: <http://www.mea.gov.in/Uploads/PublicationDocs/28912_XiamenDeclaratoin.pdf>.

Celeste, Edoardo. 2019. "Digital Constitutionalism: A New Systematic Theorisation." *International Review of Law, Computers & Technology 33*(1):76–99.

China. 2017. *International Strategy of Cooperation on Cyberspace* at: <http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm>.

https://doi.org/10.1017/S2045381720000167 Published online by Cambridge University Press

China, Kazakhstan, Kyrgyzstan, Russian Federation, Tajikistan, and Uzbekistan. 2015. *A/69/723. Letter Dated 9 January 2015 Addressed to the Secretary-General*, at: <https://digitallibrary.un.org/record/786846>.

China, Russian Federation, Tajikistan, and Uzbekistan. 2011. *A/66/359. Letter Dated 12 September 2011 Addressed to the Secretary-General*, at: <https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/Shanghai+Cooperation+Organization+Draft+International+Code+of+Conduct+for+Information+Security+9-14-2011.pdf>.

CoE. 2001. *Convention on Cybercrime*. Budapest: ETS No 185, at: <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>.

Deibert, Ronald J. and Masashi Crete-Nishihata. 2012. "Global Governance and the Spread of Cyberspace Controls." *Global Governance 18*(3):339–61.

Delerue, François. 2018. "ESIL Reflection: The Codification of the International Law Applicable to Cyber Operations: A Matter for the ILC?" at: <http://esil-sedi.eu/?p=12815>.

DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

Drezner, Daniel W. 2007. *All Politics Is Global: Explaining International Regulatory Regimes*. Princeton, NJ: Princeton University Press.

Ebert, Hannes and Tim Maurer. 2013. "Contested Cyberspace and Rising Powers." *Third World Quarterly 34*(6):1054–74.

EC. 2005. *Press Release – Commission Outlines EU Negotiation Principles for the World Summit on the Information Society in Tunis*. IP/05/672. Brussels, at: <http://europa.eu/rapid/press-release_IP-05-672_en.htm?locale=en>.

Eichensehr, Kristen. 2019. "Digital Switzerlands." *University of Pennsylvania Law Review 167*: 665–732.

Farrell, Henry and Abraham L. Newman. 2019. Of Privacy and Power: The Transatlantic *Struggle over Freedom and Security*. Princeton, NJ: Princeton University Press.

Finnemore, Martha and Duncan B. Hollis. 2016. "Constructing Norms for Global Cybersecurity." *American Journal of International Law 110*(3):425–79.

Finnemore, Martha and Kathryn Sikkink. 1998. "International Norm Dynamics and Political Change." *International Organization 52*(4):887–917.

Fischer-Lescano, Andreas. 2016. "Struggles for a Global Internet Constitution: Protecting Global Communication Structures against Surveillance Measures." *Global Constitutionalism 5* (2):145–72.

Frosio, Giancarlo F. 2018. "Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility." *International Journal of Law and Information Technology 26*(1):1–33.

Geier, Karsten. 2018. *Podcast: Cyberspace, International Norms, and a New Initiative in the UN?* at: <https://www.nupi.no/en/News/PODCAST-Cyberspace-international-norms-and-a-new-initiative-in-the-UN>.

Gholiagha, Sassan, Anna Holzscheiter and Andrea Liese. 2020. "Activating Norm Collisions: Interface Conflicts in International Drug Control." *Global Constitutionalism 9*(2):290–317.

Hill, Richard. 2013. "WCIT: Failure or Success, Impasse or Way Forward?" *International Journal of Law and Information Technology 21*(3):313–28.

Hofmann, Jeanette. 2005. "Internet Governance: Zwischen Staatlicher Autorität und Privater Koordination." *Internationale Politik und Gesellschaft 3*(2005):10–39.

Hofmann, Jeanette, Christian Katzenbach and Kirsten Gollatz. 2016. "Between Coordination and Regulation: Finding the Governance in Internet Governance." *New Media & Society* 1406–23.

ITU. 1988. *ITRs*, at: <https://www.itu.int/osg/spuold/wtpf/wtpf2009/documents/ITU_ITRs_88.pdf>.

https://doi.org/10.1017/S2045381720000167 Published online by Cambridge University Press

ITU. 2012a. *Final Acts of the WCIT*, at: <https://www.itu.int/en/wcit-12/documents/final-acts-wcit-12.pdf>.

ITU. 2012b. *Signatories of the Final Acts: 89*, at: <http://www.itu.int/osg/wcit-12/highlights/signatories.html>.

Ju, Huang. 2005. "Statement by Vice Premier Huang Ju, The State Council of The People's Republic of China." Presented at the WSIS (17 November) Tunis, at: <https://www.itu.int/net/wsis/tunis/statements/docs/g-china/1.html>.

Kleinwächter, Wolfgang. 2004. "Beyond ICANN Vs ITU? How WSIS Tries to Enter the New Territory of Internet Governance." *Gazette (Leiden)* *66*(3–4):233–51.

Kreuder-Sonnen, Christian and Michael Zürn. 2020. "After Fragmentation: Norm Collisions, Interface Conflicts, and Conflict Management." *Global Constitutionalism* *9*(2):241–67.

Krisch, Nico, Francesco Corradini and Lucy Lu Reimers. 2020. "Order at the Margins: The Legal Construction of Interface Conflicts over Time." *Global Constitutionalism* *9*(2):343–63.

Lavrov, Sergey. 2017. "Statement by Foreign Minister Sergey Lavrov at the 72nd Session of the UN General Assembly." (21 September) New York, NY: United Nations, at: <http://www.mid.ru/en/vizity-ministra/-/asset_publisher/ICoYBGcCUgTR/content/id/2870898>.

Markoff, Michele G. 2017. *Explanation of Position at the Conclusion of the 2016–2017 UN GGE*, at: <http://www.mid.ru/en/vizity-ministra/-/asset_publisher/ICoYBGcCUgTR/content/id/2870898>.

Mathiason, John. 2008. *Internet Governance: The New Frontier of Global Institutions*. London: Routledge.

Maurer, Tim and Robert Morgus. 2014. "Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate." *Internet Governance Paper Series* 7.

Moe, Louise Wiuff and Anna Geis. 2020. "From Liberal Interventionism to Stabilisation: A New Consensus on Norm-Downsizing in Interventions in Africa." *Global Constitutionalism* *9*(2):387–412.

Morse, Julia C. and Robert O. Keohane. 2014. "Contested Multilateralism." *Review of International Organizations* *9*(4):385–412.

Mueller, Milton. 2010. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press.

Nocetti, Julien. 2015. "Contest and Conquest: Russia and Global Internet Governance." *International Affairs* *91*(1):111–30.

Nye, Joseph S. 2014. "The Regime Complex for Managing Global Cyber Activities." *Global Commission on Internet Governance Paper Series* 1.

Palfrey, John. 2010. "Four Phases of Internet Regulation." *Social Research* *77*(3):981–96.

Pernice, Ingolf. 2018. "Global Cybersecurity Governance: A Constitutionalist Analysis." *Global Constitutionalism* *7*(1):112–41.

Pfanner, Eric. 2012. "Citing Internet Standoff, U.S. Rejects International Telecommunications Treaty." *The New York Times* (13 December) at: <https://www.nytimes.com/2012/12/14/technology/14iht-treaty14.html>.

Rodríguez, Miguel. 2017. *Declaration by Miguel Rodríguez, Representative of Cuba*, at: <https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf>.

Russian Federation. 2011. *Convention on International Information Security*, at: <http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666>.

Russian Federation. 2017. *Response to TASS' Question Concerning the State of International Dialogue in This Sphere*, at: <http://www.mid.ru/en/web/guest/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/2804288>.

https://doi.org/10.1017/S2045381720000167 Published online by Cambridge University Press

Russian Federation, United Arab Emirates, China, Saudi Arabia, Algeria, Sudan, and Egypt. 2012. *Proposals for the Work of the Conference, Document DT-X,* at: <http://files.wcitleaks.org/public/Merged%20UAE%20081212.pdf>.

Scholte, Jan Aart. 2017. "Polycentrism and Democracy in Internet Governance." In *The Net and the Nation State: Multidisciplinary Perspectives on Internet Governance*, edited by Uta Kohl, 165–84. Cambridge: Cambridge University Press.

Scholte, Jan Aart. 2018. "Complex Hegemony: The IANA Transition Global Internet Governance." Presented at the European Consortium for Political Research, Hamburg.

Segal, Adam. 2017. "Chinese Cyber Diplomacy in a New Era of Uncertainty." *Aegis Paper Series* 1703.

Sukumar, Arun Mohan 2017. "The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?" *Lawfare*, at: <https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well>.

T-CY. 2017. *Bureau Meeting Report*. T-CY (2017)22. Strasbourg, at: <https://rm.coe.int/t-cy-2017-22-bu-meeting-report-sep2017/1680760eaf>.

Tikk, Eneken and Mika Kerttunen. 2017. "The Alleged Demise of the UN GGE: An Autopsy and Eulogy." at: <http://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf>.

UNGA. 2015. *A/RES/70/237. Resolution Adopted by the GA on 23 December 2015*, at: <https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2016/01/A-RES-70-237-Information-Security.pdf>.

UNGA. 2016. *GA/DIS/3560. Calling for Norms to Stymie Cyberattacks, First Committee Speakers Say States Must Work Together in Preventing Information Arms Race*, at: <https://www.un.org/press/en/2016/gadis3560.doc.htm>.

UNGA. 2017a. *A/72/327. Report of the GGE*, at: <http://digitallibrary.un.org/record/1301308/files/A_72_327-EN.pdf>.

UNGA. 2017b. *A/RES/71/190. Promotion of a Democratic and Equitable International Order*. Adopted by the GA, 9 February 2017, at: <http://undocs.org/A/RES/71/190>.

UNGA. 2018a. *A/C.1/73/L.27/Rev.1. Developments in the Field of Information and Telecommunications in the Context of International Security*, at: <http://undocs.org/A/C.1/73/L.27/Rev.1>.

UNGA. 2018b. *A/C.1/73/L.37. Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, at: <http://undocs.org/A/C.1/73/L.37>.

UNGA. 2018c. *A/C.3/73/L.9/Rev.1. Countering the Use of Information and Communications Technologies for Criminal Purposes*, at: <http://undocs.org/A/C.3/73/L.9/Rev.1> https://usun.usmission.gov/explanation-of-vote-on-a-third-committee-resolution-on-countering-the-use-of-information-and-communication-technologies-for-criminal-purposes/.

US Department of State. 2018. *Explanation of Vote on a Third Committee Resolution on Countering the Use of Information and Communication Technologies for Criminal Purposes*. Bureau of Public Affairs, at: <http://www.state.gov/misc/415.htm/remarks/8803>.

US Majority Committee Staff. 2012. *Hearing on International Proposals to Regulate the Internet*, at: <https://www.govinfo.gov/content/pkg/CHRG-112hhrg79558/html/CHRG-112hhrg79558.htm>.

Verveer, Philip. 2012. *Testimony, Hearing on International Proposals to Regulate the Internet*, at: <https://www.govinfo.gov/content/pkg/CHRG-112hhrg79558/html/CHRG-112hhrg79558.htm>.

Weinberg, Jonathan. 2011. "Governments, Privatization and 'Privatization': ICANN and the GAC." *Michigan Telecommunications and Technology Law Review* 18:189–218.

https://doi.org/10.1017/S2045381720000167 Published online by Cambridge University Press

Wright, Tom. 2005. “EU Tries to Unblock Internet Impasse” *The New York Times* (30 September) at: <https://archive.nytimes.com/www.nytimes.com/iht/2005/09/30/business/IHT-30net.html>.

WSIS. 2005. *WSIS-05/TUNIS/DOC/6(Rev. 1)-E Tunis Agenda for the Information Society*. Tunis: World Summit on the Information Society, at: <http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html>.

Zittrain, Jonathan. 2008. *The Future of the Internet and How to Stop It*. New Haven, CT: Yale University Press.

Zürn, Michael. 2018. *A Theory of Global Governance: Authority, Legitimacy, and Contestation*. Oxford: Oxford University Press.

https://doi.org/10.1017/S2045381720000167 Published online by Cambridge University Press