Turnkey tyranny? Struggles for a new digital order

Thiel, Thorsten

Postprint / Postprint
Sammelwerksbeitrag / collection article

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Hessische Stiftung Friedens- und Konfliktforschung (HSFK)

Empfohlene Zitierung / Suggested Citation:
Thiel, T. (2017). Turnkey tyranny? Struggles for a new digital order. In S. Gertheiss, S. Herr, K. D. Wolf, & C. Wunderlich (Eds.), *Resistance and change in world politics: international dissidence* (pp. 215-242). Basingstoke: Palgrave MacMillan. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-61839-4

Pre-Print (the final version differs slightly)
Thorsten Thiel (2017): Turnkey Tyranny. Struggles for a New Digital Order. In: Gertheiss et. al: Resistance and Change in World Politics International Dissidence. Basingstoke, p. 215-242

Turnkey Tyranny? Struggles for a New Digital Order

Thorsten Thiel

> 'Bingo,' Jolu said. 'I'm not saying it wasn't terrible in the Great Depression or whatever. But we've got the power to organize like we've never had before. And the creeps and the spooks have the power to spy on us more than ever before, to control us and censor us and find us and snatch us.'
> 'Who's going to win?' I said. 'I mean, I used to think that we'd win, because we understand computers and they don't.'
> 'Oh, they understand computers. And they're doing everything they can to invent new ways to mess you up with them. But if we leave the field, it'll just be them. People who want everything, want to be in charge of everyone.'
> (Cory Doctorow, *Homeland*)

Over the last two decades, the establishment of the Internet as a global mass medium, the increased economic importance of information and communications technology (ICT), and the almost total replacement of analogue methods of information-processing by digital ones have changed modern societies more profoundly and more rapidly than has any previous technological advance. Networking and digital communication now pervade every area of life. As a consequence, the political management of the Internet, both as a piece of technical infrastructure and as a communicatively constituted 'cyberspace,' has also gained in importance. Although the 'hands-off' approaches that were seen as an appropriate way of working—or indeed the only way of working—in the early stages of digital development now have very few supporters, the process of creating a new digital order is far from complete: norm formation on the Net is a hotly disputed process; power relations between different political institutions and social actors are extremely unclear; and the area as a whole is riddled with fault lines.

One thing that can be observed, however, is the emergence of a battle-front running between one (admittedly very diversely constituted) bloc comprising private business and national and international politics and another consisting of a very vocal group of Internet activists. The first bloc has the greater share of power-resources at its disposal, but achievement of a hegemonial position, in the Gramscian sense of the production of ideas capable of commanding consent, seems so far to have been denied it. In fact, the increase in regulatory ambitions has resulted in Internet activists banding together to form a counterforce and this in turn has led to attempts to exclude them as dissidents. Control-oriented practices—such as criminalisation and

surveillance—have burgeoned, and on the dissident side this has in turn lent plausibility to dystopian accounts of the new order and fuelled the tendency of activists to portray what they do as freedom-loving.

In what follows here, I shall reconstruct this growth in Internet control and the stages of resistance to it. I shall begin by describing the evolution of the new order, its main drivers and characteristics, and I shall then correlate this with the emergence of dissidence and its various manifestations. My thesis is that in the wide-ranging policy-area of digitalisation, dissidence has found a particularly conducive setting for its operations and that thanks to the open starting-position and an astute use of the expanding protest-repertoire, it has managed to generate considerable public interest. Many forms of digital dissidence—at least in the West—are viewed as legitimate, and this despite the attempts made to criminalise them. But to what extent politicisation and dissident practice will succeed in countering the fundamental trend towards the establishment of an order regulating Internet architecture and cyberspace, remains to be seen. This is because in the current hybrid regulatory structure there is no coherent, authoritative power capable of responding to general issues, with the result that, even where there is a high degree of acceptance in the public discourse, this does not translate directly into political decisions.

The emergence of order and the shaping of governance on the Internet

In order to be able to make sense of the struggles over order that characterise an increasingly digitalised world, we first have to understand the 'beating heart' of that world—namely, the Internet and the manner of its organisation. The Internet can initially best be understood, technically speaking, as a protocol that allows networks to link up with other networks, and computers with other computers.[i] From this perspective, the history of the Internet is, at the basic level, the story of how a standard was developed and diffused, making it possible for technical devices to communicate with each other and providing a substructure onto which more and more services were built (one such is the World Wide Web, which is now widely regarded as synonymous with the Internet) (Leiner et al. 2011). Because these standards of exchange and communication—in other words, Internet protocols—are intrinsically 'dumb' (in the sense that they merely facilitate the transfer of data and say nothing about the latter's content), and because of the boundless versatility of the architecture built on to this system, there is no fixed authority operating beyond the level of data-normalisation. Anyone can communicate with anyone via the network; it is only the end-user devices that process the content. But if this is so, how can communication be ordered?

To answer this question, we need to distinguish between (1) the technical dimension and (2) the content-related dimension of the Internet as a space for communication. We then need to demonstrate, for each dimension, how ordering processes are set in motion there.

(1) At the technical level, it is in regard to the previously mentioned enforcement and universalisation of standards that regulatory mechanisms are having to be established and pushed through against alternatives—such as the closed 'Minitel' system in France and AOL's scheme to set up an 'internet within the Internet.' Infrastructure providers in particular—these include phone companies and content providers—are continually seeking to create an Internet that is less versatile but more commodifiable.[ii] But the exponential growth of the Net would hardly have been possible without the system's open structure—the feature most often cited as the reason for the Net's irresistible rise and currently the basis that is allowing ever more devices to link up with one another and communicate autonomously (Internet of Things). In this sense, connectivity is now largely a given and regulated consensually—though the increase in the number of functions dependent on data-transfer via the Internet brings with it an ongoing need for accommodation.

Even this seemingly purely technical development, however, has a political dimension. This becomes evident when one looks at the decision-making involved in establishing and refining standards. The major role which educational establishments and the military played at the outset in the development of the Internet clearly points to early state influence in this area. However, this influence did not translate into a state-dominated decision-making system. Instead, a highly differentiated, hybrid structure grew up, in which the emphasis was on expertise-based legitimation. Commercial actors such as Internet service providers and hardware developers (and later also content providers and Internet-based suppliers of services) have always played a major part in the cooperative structures of Internet governance. This does not mean, however, that the state is disappearing from the scene—in fact it currently looks to be making a comeback (DeNardis 2013, Drezner 2004, Hofmann 2009).

Even more importantly, however, the neutrality that has been inferred from the Internet's technocratic, cooperation-based set-up has increasingly revealed itself to be an illusion. Technical decisions can have highly political effects and at the same time as the importance of these decisions is growing in the modern world, acceptance of the technocratic bodies that take them is declining. As a result, over the last few years the governance institutions that regulate the technical aspects of the infrastructure have been increasingly called into question and currently find themselves in a state of upheaval. The experiments with multi-stakeholder arrangements are

regarded in many quarters as having failed, and states in particular—Russia and China, for example—have woken up to the challenge and are trying to institute a different kind of Internet-management that would give them a tighter hold on technical decisions (DeNardis 2009, 2014, Ebert/Maurer 2013).[iii] In line with this, options for control and filtering are becoming an increasingly important focus of interest—not only for these actors, but also (for different reasons) for liberal states and Internet services. This has led, overall, to the Internet's technical infrastructure being thought of as something other than a domain of hierarchical intervention and has resulted in the creation, or political exploitation, of "points of control" (DeNardis 2012, Benkler 2016, Zittrain 2003).[iv]

(2) The second level at which digital communication has experienced a consistent push in the direction of order-formation is that of 'content,' in other words in regard to the regulation of communication and/or the policing of cyberspace.

In this connection, the argument that because of the specifics of digital communication, the Internet is a 'regulation averse' space was long regarded as compelling. It was assumed that in order to be able to assert its statehood, the state must be in a position to make full use of its 'traditional' instruments—the law, controls, and sanctions—and that these, in turn, were based on clearly defined systems of accountability, hierarchies, and territorial spheres. But these realities, it was argued, were cast into doubt by digital communication—by the extensive opportunities it offered for anonymous activity, by the possibility of individual, loss-free and (largely) cost-free duplication of content, and by the territorial indeterminacy of data-flows. In combination, so ran the argument, all this would permanently undermine any attempt at regulation via the law.[v] What this early debate overlooked, however, was that there are numerous functional equivalents to direct control (filters, for example, or control through intermediaries). Eventually classic state sovereignty was not only restored; it actually gained in strength and intensity (Goldsmith/Wu 2006, Thiel 2014b).

There are in fact numerous ways in which digital communication—even allowing for its enduring peculiarities—can be regulated by government and business. As part of this process, controls that need to be applied to data-flows for technical reasons are increasingly mutating into surveillance of those flows (meaning examination of their content and prioritisation or tracking of particular communications) (Sprenger 2015). What is more, over time the possibilities of doing this on a permanent basis have increased yet further because infrastructure changes (see above), big data, and algorithmic processes have greatly reduced the problems of capacity hampering legal enforcement and control. Thanks to the rise of the mobile Internet, for example,

it has become much easier to pinpoint communications geographically, and nowadays the content of digital communication is much more frequently captured and classified in transit (Bendrath/Mueller 2011).

Even more important than these state endeavours to keep a grip on communications-content is the comprehensive commercialisation of the Net. The Internet is now one of the most important drivers of economic productivity; it pervades every aspect of economic and social life and in developed states it is the means by which a hefty proportion of the gross national product is generated. One of the major features of actual money-making on the Internet is its reliance on the generation and collection of data. In addition, both in the telecommunications sector (i.e. among Internet providers) and in the information economy, there are signs of a trend towards monopolisation. This arises from the obvious expediency of economies of scale in the case of digital goods—as when, for example, search algorithms become more efficient precisely as a result of being used by large numbers of people (Tufekci 2016).

There are at least three ways in which commercialisation and increased economic importance have created political incentives for a more thoroughgoing regulation of the Internet. First, the growth in importance of digital communication has upped the requirements in regard to regulation. This is evident, for example, in the area of security, where the individual notion of computer safety has increasingly morphed into the all-encompassing notion of cyber security. Centrality is here translated into vulnerability and this is used as justification for state intervention (Nissenbaum 2005, Hansen/Nissenbaum 2009). Secondly, being a force that sets in motion global, communication-enabling processes of exchange, the Internet has triggered the desire, on the part of many states, to impose controls in relation to particular social discourses. Motives here may range from, at one end, the wish to safeguard cultural specifics or the freedom of expression of particular social groups and, at the other, fear of political criticism. Thirdly, the mass collection of data by business also entices states to write access to these stocks of information into their own regulatory practice. From this point of view, the task which states currently face in regard to regulatory management of the Net is totally different from that which they faced even twenty years ago. And it is a task they have set about tackling with determination—if not always with unqualified success.

The quest to get a policy implemented on the Net that is both effective and as consistent as possible with regulation in the 'offline world' is being pursued not only at the political and legal level, but also in relation to coding and technical infrastructure. Attempts are constantly being made, for example, to align the Internet more closely to the logic of territorial sovereignty

(Mueller 2015). Examples here range from China's sealing-off and censoring of the Internet, through Britain's blanket filtering of Net content, to 'soft interventions' such as the German endeavour to get Facebook to apply rules on hate speech. Another facet of developments here is the attempt to increase the extent to which Internet communication is classified and organised automatically, a measure which, in turn, necessitates the collection of data by private and/or public bodies ('data retention') and drives moves against earlier Web standards such as those on anonymity.

This brief account of developments indicates how and in which areas order is being formed in regard to digital issues. Overall, we can safely say there is a marked increase in the extent of regulation. Commercial and state actors are contributing in equal measure to this intensification—though there may sometimes be profound differences of opinion and conflicts of interest between, or indeed within, these groups of actors, depending on the context or subject-matter. The planned aspects of rule-making and sovereign control are not the only significant factors here. Of equal importance are non-intended effects—for example, the shifting configuration of the incentive-structure for data-collection, which is bringing about an exponential increase in the generation and linkage of data and is thus itself prompting new calls for order and rules.

All in all, it is clear that economic and technical developments are being secured and strengthened through a process of juridification and regulation. In this connection, it serves no purpose to ask who is ultimately the key player in this multi-layered process, or to what extent the process is an intentional or directed one. What matters is that the process has clear winners—actors who occupy, and seek to extend, the resultant positions of power. This threatens, in the medium to long term, to result in the closing-down of the Internet's open communications-structure (an unsurprising turn of events when viewed in the broader historical context of the development of information and communications technologies: Wu 2010, Clark 2016).[vi]

Digital dissidence: Convictions and strategies

We now have a rough outline of the way in which order and norms have taken shape in the digital sphere over the last few years. Unsurprisingly, this process has encountered resistance at many different levels—and has done so in particular because networks and digitalisation have a progressive and emancipatory connotation in public discourse and are associated with a whole raft of utopian aspirations (Thiel 2014a). The commercial and state-led reshaping of digital space

has thus been met with various acts of resistance and attempts to create alternative structures and it is to these that I shall turn my attention in what follows, first describing and then classifying them.

Digital dissidence—by which I mean dissidence relating to digital issues rather than dissidence in general, made possible or promoted by digitalisation and networking—is undoubtedly on the increase. This is clear just on an anecdotal level: we are all familiar with the kinds of protests that have made headlines in recent years, often perceived, and talked of, as being highly revolutionary in their forms and concerns. Prominent players here include the WikiLeaks organisation, the activists from 'Anonymous' and the closely related 'Lulzsec' group—and, of course, the whistleblower Edward Snowden. Also of importance, however, are the protest actions mounted against norm-changes targeted specifically at Internet infrastructure. These include the global protests against SOPA, PIPA, and ACTA, which succeeded in blocking a complex international set of regulations backed by a number of powerful interests. At the national level too, it is possible to point to a whole host of high-profile cases: in Germany, for example, these included the opposition to web blocking, the demonstrations mounted by the *Freiheit statt Angst* ('Freedom Not Fear') alliance, the campaign on ancillary copyright, and the 'treason' controversy over the bloggers from netzpolitik.org. Key to the momentum of these debates is the prestige of a number of charismatic and media-savvy rallying-figures—from Aaron Swartz, through Julian Assange, to Edward Snowden—who have become household names (and, it has to be noted, are all male, as is so often the case in the technology sector). What are the distinguishing features of this resistance? What are the convictions that drive it and what are its different strategies and approaches?

Convictions

As far as conviction/ideological position is concerned, what strikes one in particular is that recognising a dissident stance is easier than specifying what lies at its ideological heart. Internet activism initially grew out of a relatively large, now quite well-established and very vibrant subculture—a fact that is reflected in the wealth of symbolic codes it uses (from cat-images to Guy Fawkes masks). By contrast, the politicisation of Internet-related issues, the engagement with 'high' politics and representative institutions, the discourse with a broad social public, and the forging of alliances are more recent developments and place heavy demands on a community which, though ideologically outspoken, is often vague and lacking in coherence.[vii]

Nonetheless, it is possible, at an abstract level, to identify at least two overarching motifs running through the great majority of cases of digital dissidence. The first is the ideal of free speech.

Many activists take a liberal-to-libertarian line, combined, to varying degrees, with a participatory notion of democracy. Politically speaking, therefore, many of the stances adopted by cyber dissidents tally with democratic norms and practices as established in Western states, but what they frequently do is 'radicalise' those norms and reject their institutional embodiment and practical implementation.[viii]

The second, directly related, motif is the battle against surveillance. Here, the aspect of freedom of opinion and expression is, as it were, turned up a notch, in the sense that any form of surveillance or control is assumed to curtail freedom of opinion and permanently hobble democracy. Criticism here is directed both at businesses and at states, but it is noticeable that, where businesses are targeted, the objections are not formulated in terms that are particularly critical of capitalism (instead adopting a 'consumer protection' or 'individual choice' line), whereas when political power-formations, notably states, are the target, the criticism is voiced much more in terms of principles (for example, little distinction is made between authoritarian and liberal regimes).[ix]

When it comes to ideological motivation, however, what has to be remembered, overall, is that what unites the activists and guides the political actions is not an overarching political-cum-ideological construct. Rather, actions are largely issue-led and are targeted at real-world developments that are seen as being off course (the tightening-up of copyright, for example, or web blocking, or various other concrete legislative schemes). Whereas activism in this area has traditionally been geared to technical issues, over the last few years general trends—from the expansion of the security state to broader developments in democracy—have also begun to feature more prominently as triggers for these kinds of activities.[x] Overall, this demonstrates the way in which digital dissidence is maturing—a process that is expressing itself in the increased politicisation of the movement and which, in turn, is being bolstered by the criminalisation of many of the actions involved (see below).

Strategies

Even more indicative than ideological stance when it comes to identifying digital dissidence is the choice of strategies and means. And these themselves, in their turn, often have the effect of shaping or reinforcing identity—particularly since, in many protest-actions, the media preoccupation with means is just as important, if not more so, than the substance of the position taken. What, then, are the means and strategies employed by digital dissidents?

One important fact to note at the outset is that acts of dissidence are not the only response to have been triggered by the increasing politicisation of Internet policy. On the contrary, what one predominantly sees is a growth in, and professionalisation of, that section of civil society that takes an interest in Internet-related issues. Actors such as the European-based Chaos Computer Club (CCC), Digitale Gesellschaft, and iRights, and the US-based Electronic Frontier Foundation (EFF) only, or mostly, use strategies that would fall under the rubric of opposition (these range from participation in commissions of inquiry, through litigation, to the organisation of large-scale protests).[xi] In individual cases, these interventions have clearly been a success. This was spectacularly so with the blocking of SOPA, PIPA, and subsequently ACTA, but the actions against data retention or in favour of Internet neutrality have also scored considerable successes. Those involved have repeatedly managed to introduce even complex issues into the public discourse and frame them in line with their own convictions (Leifeld/Haunss 2012) give an empirical account of this process using the example of the campaign against software patents; see also Faris et al. 2015). In recent years, this type of opposition-politics has also shown itself open to alliance-building and has sometimes been pursued in close cooperation with parties and political institutions, and also with businesses from the Internet economy—in other words quite deliberately from within the political system, using the legal processes and other classic means associated with the latter (on general developments in the German case, see Beckedahl 2015, Ganz 2015). Possibly the most far-reaching manifestation of this opposition-politics is the Pirate Party, which has tried to make gains primarily by tackling genuinely Net-related issues and has managed to notch up a number of major successes inside various European political systems.[xii]

The second strategy, which is linked to articulation and public education but is difficult to transpose adequately to the dissidence/opposition spectrum, is the creation of technical alternatives to the platforms and communications-mechanisms of the commercial Internet. In many cases, these products operate directly counter to the forces that engender order. The spectrum here extends from free and open-source software (well-known examples of which are Linux and Firefox) (Coleman 2009, 2012, Kelty 2005), through alternative Internet platforms such as Indymedia (Kidd 2003, Winter 2008, Ludlow 2001, Milan 2013a) and collaborative endeavours such as Wikipedia (Benkler 2013), to communications-resources such as TOR. Many of these structures are deliberately decentralised and aim to preclude, or actively impede, the operation of both state-based and commercial surveillance-mechanisms.[xiii] Despite this, the great majority of these activities are not perceived as dissidence or criminalised as such. In fact, they have a firm place in the developing digital universe, because many of the 'enclaves' in question act as important motors for innovation and in some cases supply common goods. By contrast,

projects that aim more deliberately at the anonymisation and encryption of communications are seen much more often as having criminal overtones. One example here is peer-to-peer networks, which are widely viewed as criminal on account of their role in file-sharing; another is the TOR encryption software, which, though developed and supported partly with government funds, has been increasingly criticised over the last few years—for example, for helping to facilitate illegal activities such as drugs- and arms-trafficking—and has therefore been subject to attempts to infiltrate or actually ban it (Moore/Rid 2016).

Not until we go beyond oppositional Internet politics and the creation of alternative technologies do we find dissidence in the stricter sense, as a mode of challenging hegemonial political actors and norms through actions that fall outside the established rules of the game. In general terms, this kind of dissidence can be summed up under the rubric of 'hacktivism.' More specifically, it can be divided into three core types: the practice of leaking; blockade strategies such as 'Ddosing' that function like collective forms of protest; and forms such as hacking that are aimed directly at altering virtual environments.

- Leaking or leaktivism (White 2016) is a mode of challenge in which material from inside an organisation is made public in an attempt to produce a political effect. It is closely akin to whistleblowing but is, as it were, given an added boost by digitalisation in the sense that disclosure of material is easier and can be achieved even without the involvement of gatekeepers. Above all, the quantity of leakable documents has increased thanks to digital storage, and at the same time the cost and effort involved in copying data have declined sharply. Leaking presupposes access to an organisation, either in the form of an internal source or via enforced entry from outside. In the wake of the WikiLeaks and Snowden affairs, leaking has come to be seen in a largely positive light and its image is that of an effective 'emergency resort' against increasingly hard-line institutions (for an overview of leaking and the discussion surrounding it, see, for example, Benkler 2011, de Lagasnerie 2016, Lovink/Riemens 2013, Pozen 2013, Greenberg 2012).
- DDoSing (distributed denial-of-service attack) is here cited as a stand-in for the kinds of digital protest-actions that aim to replicate the effects of real-world demonstrations—in other words, that look to create the combined impression of broad-based support and blockading. In practical terms, DDoSing means the deliberate, targeted overloading of a server. It does not require access to an organisation and taking part is a relatively easy and widely accessible process. It came to fame notably as the tactical method of choice

of the Anonymous group (on DDoSing and other essentially digital protest-practices, see Sauter 2014, McCaughey/Ayers 2003, Milan 2013b, 2013c).[xiv]

- Hacking, the last category here, has a much higher technical content.[xv] The term denotes the unauthorised and unscheduled modification of the functions of particular digital artefacts and often implies unauthorised access. Because it aims at fundamental change rather than surface protest or the enforcement of transparency, there are almost no bounds to the creativity of this kind of protest (on the persona of the hacker and on hacking as a strategy or form of protest, see, for example, Funken 2010, Hempel 2015, Jordan 2008, Powell 2016, Himanen 2004).

One thing common to all three of these forms of hacktivism is that they generate a lot of interest. In both general and scholarly debate, they are very often construed as practices from, or successors to, civil disobedience. This is because in many cases their choice of means in itself conveys what is at issue and their performative breaches of the law point up the inadequacy of the existing order and/or indicate alternatives (on the question of whether digital disobedience is civil disobedience, see, for example: Celikates 2015, Kleger/ Makswitat 2014, Scheuermann 2014, Züger 2014, Züger/Milan/Tanczer 2015). Although, as a result, all three variants are credited with a high degree of legitimacy in public debate, they are also subject to a high degree of criminalisation (a study published by the German Federal Criminal Police Office conveys the general idea here: Bundeskriminalamt 2015; see also the critical response to some of the findings in Haase/Züger 2015). Manifestations of this criminalisation include: the institution—or threat—of legal proceedings and the imposition of long prison-sentences if conviction ensues (the cases of Edward Snowden, Julian Assange, and the netzpolitik' bloggers André Meister and Markus Beckedahl illustrate the first practice, the fate of Chelsea Manning the second); unequal legal treatment of virtual blockades/protests and their real-world equivalents (an early but memorable case of this involved the online protest against Lufthansa's deportation-practice: Kartenberg 2011; also Gertheiss in this volume); particular zeal in the prosecution of hackers; and the especially harsh penalties imposed under relevant legislation (one example of which is the US Computer Fraud and Abuse Act, applied, for example, in the case of Aaron Swartz: Peters 2016).

Having reviewed the political convictions and different strategies and permutations of digital dissidence, we are in a position to broach the question—raised in the introduction to the present volume—of what motivates dissidence. The answer, in the case of digital dissidence, seems to be that identity-related factors (dissidence by choice) and external labelling (dissidence by ascription)

play equal parts. The players in question take care to stage their dissidence in highly visible ways and they deliberately exploit media interest in order to get attention for their causes.[xvi] As a result, they have succeeded in making the creeping regulation of the Net described in the first part of this chapter into a political issue. Because of the actions of digital dissidents, the idea that there is no alternative to the current technical and commercial development of the Net no longer prevails. Instead, the emancipatory promise of digitalisation has been reawakened and has secured a key place for itself in the public debate. This being so, self-stylisation as dissident should here be seen primarily as identity- and norm-related. Self-reinforcing dynamics also play an important role, but interest-based explanations, by contrast, are of very little relevance when it comes to accounting for the motives of the dissenting camp in this particular policy-area.

Another point to note is that in the field of digital policy there is no transition from opposition to dissidence. Instead, there is a simultaneous upsurge in both, operating as complementary strategies. Acts of digital dissidence have a reinforcing, boosting effect and are deliberately used by oppositional actors as a way of creating awareness. Hence, dissidence is not excluded from discourse by oppositional actors but actively defended and justified. Meanwhile, as the arguments hot up, the opposing camp engages in deliberate denigration and criminalisation. The order currently entrenching itself on the Internet adopts a strongly exclusionary attitude to its critics, portraying divergent norms and platforms as problematic and presenting legal oppositional strategies as endangering security.

Order and dissidence: Why we got to where we are

The present case-study differs somewhat from the others in this book in that, when it comes to digital policy, it is not possible to classify the struggles over order, as they currently stand, as straight successes or failures. This area of policy is still too young for that, its themes are too varied and multi-layered, and the different stances and alliances need time to establish themselves. Another distinctive feature is that the side with the greater resources, which is seeking to transpose the status quo of the non-digital world in as wholesale a form as possible to digital environments, does not enjoy an 'incumbency bonus' and has, by its own efforts, to demonstrate the plausibility of its regulatory ambitions and push these through amidst great scepticism and in the face of numerous kinds of resistance. The politicisation and polarisation of digital policy is thus pursued from two sides; it is not a case of dissenting actors facing an adamantine order. This also means that digital dissidents occupy a special position, particularly in regard to public recognition and legitimacy, and can claim a number of sometimes far-reaching successes in the sphere of practical policy.[xvii] Although digital policy must be viewed overall as a fiercely contested

and extremely ill-defined domain, its core dynamics are nonetheless amenable to description according to the classificatory scheme developed for the present book.

Features of the normative context

With regard to the significance of norm characteristics, we should begin by noting that in the case under investigation here it was not one, more or less solidly identifiable, norm that was under scrutiny but a meshwork of norms—in fact, a whole policy-area. In-depth study of individual norms such as Internet neutrality or censorship would produce more concrete results. This means that the type of norm conflict is, likewise, not very easy to isolate: in the field examined here, conflicts of interpretation and fundamental clashes between norms crop up in equal measure. That said, the overwhelming majority of the disputes outlined here would have to be classed as clashes of principle—a fact which helps to explain the impassioned nature of the argument and the irreconcilability of the various positions.

Key to the explanation in the case analysed here, however, is the third aspect of the normative context identified as causally relevant in the book's introduction, namely institutional particularities. Specifically, the absence of robust institutions—in other words, bodies with the power to make decisions and the ability to respond to interventions—often prevents public demands, even those that are viewed as legitimate and enjoy strong support, from being realised. The field of digital policy is characterised by an enormous degree of transnationality and in the area of positive regulation in particular cooperation (including, quite regularly, with commercial actors) is unavoidable. The power of civil-society actors has, it is true, found expression in a proliferation of deliberative forums (the UN-convened two-stage World Summit on the Information Society, and the Internet Governance Forum that was set up in its wake, are examples of this). However, when it comes to anything beyond highly technical standard-setting, and particularly where substantive issues relating to the regulation of cyberspace are concerned, the internal weaknesses of these institutions, and, even more importantly, the problems associated with enforcing positions agreed within them, are such that the chances of participation are slight (Dany 2012). As a result, digital dissidence continues to be at its most successful when it is geared to national—or, in the case of the European Union, regional—arenas. Even here, however, getting policies enforced poses an ongoing problem.[xviii]

Actor characteristics and strategies

As far as the digital dissident line-up is concerned, the professionalism, organisation, and connectivity of its members indicate that we are dealing with a highly organised and efficient

civil-society phenomenon. The sphere of Internet policy boasts a number of well-established and now well-tried transnational alliances; actors here have the ability to generate media publicity for their causes; and the level of organisational capacity in this domain would have to be classed as high (one study that throws light on skills-acquisition and efficiency in this area—but also on weaknesses—is Bennett's in-depth study of privacy advocates: Bennett 2008). Odd groups, particularly at this dissident end of the spectrum, are less well organised and connected, but they are greatly helped by the technology available to them to network and organise protests. Thus, even isolated whistleblowers have been able to prevail against state and commercial actors and draw on broad-based support-networks which, for example, organise physical demonstrations or ensure media awareness. Needless to say, resources here are always limited and initiatives that are seeking not only to devise but also to realise practical alternatives are dependent on high inputs of money and personnel that are constantly having to be replenished. The result is that even actors of some status in the broader Internet economy—those, for example, on the Free and Open Source Software scene—are reliant on donations, which, in their turn, wax and wane very much according to the popularity of the issues in question. Alliances with the commercial Internet economy are sometimes also of importance here.

The domain of strategies and means has already been explored in some detail above. An obvious recurrent feature here is the ability of digital dissidence to call upon a wide-ranging and in some cases novel repertoire of approaches. Apart from bringing with it a number of strategic advantages, this facility helps to explain the huge public interest in this area. One particularly important element, in addition to the previously mentioned alliance-building within—but also beyond—the civil-society scene, is the successful framing of issues. Questions relating to digitalisation and Internet regulation are necessarily abstract and in public discourse they have to be discussed via metaphors and analogies. As a result, the battle over imaginaries assumes particular importance (Singh 2013; an overview of state strategies aimed at shaping the conceptual landscape is given in Kamis/Thiel 2015). Dissident actions such as the Snowden leaks have, in their turn, played a major and discourse-defining role in upping the visibility of particular issues. As regards consistency of position in different cases and across time, this is generally a given in the sphere of digital dissidence and is reinforced as the debate intensifies.

Contextual change

External developments obviously play a major role in the field of Internet policy, as elsewhere, and they do so both in the form of unexpected events and as a continuous process of technological change. Thus, the security discourse that flares up after every terrorist attack is

undoubtedly a crucial factor in pressing home pro-regulation points of view. The debates about the restriction or infiltration of encryption, about mandatory registration, and about the redirection of resources to surveillance-players, for example, are directly connected to events and, what is more, become a permanent feature even if they prove ineffective. (This is true, for example, of the perennial debate about data-retention that resurfaces in Germany after every terrorist attack and seems to survive even the highest-level legal rulings.) More important still, however, is the influence of technological and commercial change, because such transformation shapes the policy-field itself at a fundamental level. The development of the mobile Internet, for example, has created entirely new possibilities as regards the collection and monitoring of locational data; and the commodification of the Internet and the establishment of data-based business-models have dramatically increased the need for political regulation. We should, however, be warned against the kind of technological determinism that currently pervades discussion about the Net. Such a position will not bear closer scrutiny, either in its progressive version (networks as an irresistible force that will ultimately transform hierarchical and capitalist arrangements or render these obsolete—see Shirky 2008 and, for a more nuanced account, Castells 2004 and 2010) or in its fatalistic permutation (Enzensberger 2014). Besides this, it ignores the many and varied opportunities we have to shape and influence the 'fourth revolution' that is currently enveloping us in so many different ways (Floridi 2014).

Conclusion

As a case-study, digital dissidence has turned out to be intriguing and enlightening in equal measure. Because norm-building in the field of digital policy is an unfinished and much-contested project, individual explanatory factors stand out clearly. It turns out that the protagonists of Internet policy have built up a considerable capacity for action and for pressing home their point of view. This in turn helps to explain the high degree of public legitimacy enjoyed by the causes these actors champion, and examination of individual conflicts often shows it to be a determining factor. At the same time, contextual changes (particularly technological developments and the marketisation of information and communications technologies) combined with the distinctive structural character of a policy-area equipped with only weak transnational institutions militate against the translation of ideas—even if widely shared—into concrete policies. Overall, then, the dynamics in this area of policy indicate that resistance is likely to become fiercer, with the emergent order being perceived as both gaining in strength and largely unresponsive. For civil-society actors in the field of Internet policy, therefore, the creation or refinement of political institutions that can make any kind of effective

policy possible will continue to be a vital consideration. Such institutions—which must therefore also be responsive—are, after all, a prerequisite if the actors in question are to see the high levels of legitimacy enjoyed by their ideas translated into concrete policies. The strategy of building up alternative forms of communication and exchange, and of maintaining or developing existing projects, will also play a part in determining the success or failure of digital dissidence. With this in mind, the essentially open architecture of the Internet must be preserved, because it is a precondition for the design of independent communications-platforms. However, this open architecture is not in itself a guarantee of success—as the cyber-utopians of the nineties rather too hastily assumed. To this extent, the politicisation of Internet policy has been a logical development. The next few years will show us along what lines our communicative norms and possibilities will develop and what kind of digital order will prevail.

References

Assange, Julian (2006). 'Conspiracy as Governance' and 'State and Terrorist Conspiracies', reproduced at https://cryptome.org/0002/ja-conspiracies.pdf, accessed 8 April 2016.

Assange, Julian (2010). 'Don't Shoot Messenger for Revealing Uncomfortable Truths', *The Australian,* 8 December.

Barbrook, Richard and Cameron, Andy (1996). 'The Californian Ideology', *Science as Culture*, 6: 1, 44–72.

Barlow, John Perry (1996). 'A Declaration of the Independence of Cyberspace', https://projects.eff.org/~barlow/Declaration-Final.html, accessed 23 May 2016.

Beckedahl, Markus (2015). 'Die digitale Gesellschaft: Netzpolitik, Bürgerrechte und Machtfrage', *Journal of Self-Regulation and Regulation*, 1: 1, 11–30.

Bendrath, Ralf and Mueller, Milton (2011). 'The End of the Net as We Know it: Deep Packet Inspection and Internet Governance', *New Media & Society*, 13: 7, 1142–60.

Benkler, Yochai (2011). 'A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate', *Harvard Civil Rights-Civil Liberties Law Review*, 46: 2, 311–97.

Benkler, Yochai (2013). 'Practical Anarchism: Peer Mutualism, Market Power, and the Fallible State', *Politics & Society*, 41: 2, 213–51.

Benkler, Yochai (2016). 'Degrees of Freedom, Dimensions of Power', *Daedalus*, 145: 1, 18–32.

Bennett, Colin J. (2008). *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge, MA: MIT Press.

Bundeskriminalamt (2015). *Hacktivisten: Abschlussbericht zum Projektfeld der Hellfeldbeforschung*, www.bka.de/nn_193924/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/SonstigeVeroeffentlichungen/2015HacktivistenProjektteilHellfeldbeforschung,templateId=raw,property=publicationFile.pdf/2015HacktivistenProjektteilHellfeldbeforschung.pdf, accessed 4 January 2016.

Castells, Manuel (2004). 'Informationalism, Networks, and the Network Society: A Theoretical Blueprint', in Manuel Castells (ed.), *The Network Society. A Cross-cultural Perspective*. Cheltenham: Edward Elgar, 3–45.

Castells, Manuel (2010). *The Rise of the Network Society*. 2nd edn. Chichester: Wiley-Blackwell.

Celikates, Robin (2015). 'Digital Publics, Digital Contestation: A New Structural Transformation of the Public Sphere?', in Robin Celikates, Regina Kreide and Tilo Wesche (eds.), *Transformations of Democracy*. London: Rowman & Littlefield International, 159–74.

Clark, David D. (2016). 'The Contingent Internet', *Daedalus*, 145: 1, 9–17.

Coleman, Gabriella (2009). 'Code Is Speech: Legal Tinkering, Expertise, and Protest among Free and Open Source Software Developers', *Cultural Anthropology*, 24: 3, 420–54.

Coleman, Gabriella (2012). *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton: Princeton University Press.

Coleman, Gabriella (2014). *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London: Verso Books.

Crawford, Susan P. (2007). 'Internet Think', *Journal on Telecommunications & High Technology Law*, 5, 467–86.

Dany, Charlotte (2012). 'Ambivalenzen der Partizipation: Grenzen des NGO-Einflusses auf dem Weltgipfel zur Informationsgesellschaft', *Zeitschrift für Internationale Beziehungen*, 19: 2, 71–99.

Deibert, Ronald J. (2013). *Black Code: Surveillance, Privacy and the Dark Side of the Internet*. Toronto: Signal.

Deibert, Ronald and Rohozinski, Rafal (2010). 'Liberation vs. Control: The Future of Cyberspace', *Journal of Democracy*, 21: 4, 43–57.

DeNardis, Laura (2009). *Protocol Politics: The Globalization of Internet Governance*. Cambridge, MA: MIT Press.

DeNardis, Laura (2012). 'Hidden Levers of Internet Control: An Infrastructure-based Theory of Internet Governance', *Information, Communication & Society*, 15: 5, 720–38.

DeNardis, Laura (2013). 'The Emerging Field of Internet Governance', in: William H. Dutton (ed.), *Oxford Handbook of Internet Studies*. Oxford: Oxford University Press, 555–77.

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

Diffie, Whitfield and Landau, Susan (2007). *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, MA: MIT Press.

Drake, William J., Cerf, Vinton G. and Kleinwächter, Wolfgang (2016). *Internet Fragmentation: An Overview*, World Economic Forum (Future of the Internet Initiative) White Paper. Geneva: World Economic Forum.

Drezner, Daniel (2004). 'The Global Governance of the Internet: Bringing the State Back In', *Political Science Quarterly*, 119: 3, 477–498.

Earl, Jennifer (2006). 'Pursuing Social Change Online: The Use of Four Protest Tactics on the Internet', *Social Science Computer Review*, 24, 362–77.

Earl, Jennifer and Kimport, Katrina (2011). *Digitally Enabled Social Change*. Cambridge, MA: MIT Press.

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

Elliot, Williams (2016). 'Hackers and Heroes: A Tale of Two Countries', http://hackaday.com/2016/01/11/hackers-and-heroes-a-tale-of-two-countries/, accessed 7 April 2016.

Enzensberger, Hans Magnus (2014). 'Wehrt Euch', *Frankfurter Allgemeine Zeitung*, 1 March, 9.

Faris, Robert, Roberts, Hal, Etling, Bruce, Othman, Dalia, and Benkler, Yochai (2015). *Score Another One for the Internet: The Role of the Networked Public Sphere in the U.S. Net Neutrality Policy Debate*, Berkman Center Research Publication 4. Cambridge, MA: Berkman Center Harvard University.

Floridi, Luciano (2014). *The 4th Revolution: How the Infosphere is Reshaping Human Reality*. Oxford: Oxford University Press.

Funken, Christiane (2010). 'Der Hacker', in Stephan Moebius and Markus Schroer (eds.), *Diven, Hacker, Spekulanten: Sozialfiguren der Gegenwart*. Berlin: Suhrkamp, 190–205.

Ganz, Kathrin (2015). 'Zehn Jahre Netzbewegung: Konflikte um Privatheit im digitalen Bürgerrechtsaktivismus vor und nach Snowden', *Forschungsjournal Soziale Bewegungen*, 28: 3, 35–45.

Goldsmith, Jack and Wu, Tim (2006). *Who Controls the Internet: Illusions of a Borderless World*. Oxford: Oxford University Press.

Greenberg, Andy (2012). *This Machine Kills Secrets: How WikiLeakers, Hacktivists, and Cipherpunks are Freeing the World's Information*. New York: Dutton.

Haase, Adrian and Züger, Theresa (2015). 'Hacktivismus = Cybercrime? Eine Replik auf die Studie des BKA zu Hacktivisten', www.sicherheitspolitik-blog.de/2015/02/26/hacktivismus-cybercrime-eine-replik-auf-die-studie-des-bka-zu-hacktivisten/, accessed 8 April 2016.

Hansen, Lene and Nissenbaum, Helen (2009). 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53, 1155–75.

Hempel, Leon (2015). 'Technisierter Protest, Hacking und die Absorptionskraft des Designs', *Forschungsjournal Soziale Bewegungen*, 27: 4, 112–21.

Himanen, Pekka (2004). 'The Hacker Ethic as the Culture of the Information Age', in: Manuel Castells (ed.), *The Network Society: A Cross-cultural Perspective*. Cheltenham: Edward Elgar, 420–31.

Hofmann, Jeanette (2009). 'Formierung und Wandel des Politischen in der Regulierung des Internet', in Ulrike Bergermann, Isabell Otto and Gabriele Schabacher (eds.), *Das Planetarische: Kultur–Technik–Medien im postglobalen Zeitalter*. Paderborn: Wilhelm Fink, 175–186.

Hofmann, Niklas (2011). 'Der Gegenverschwörer', in Heinrich Geiselberger (ed.), *Wikileaks und die Folgen: Netz, Medien, Politik* Berlin: Suhrkamp, 47–54.

Howard, Philip N. (2010). *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam*. Oxford: Oxford University Press.

Johnson, David R. and Post, David G. (1996). 'Law and Borders: The Rise of Law in Cyberspace', *Stanford Law Review,* 48, 1367–402.

Jordan, Tim (2008). *Hacking: Digital Media and Technological Determinism*. London: Polity.

Kahn, Richard and Kellner, Douglas (2005). 'Oppositional Politics and the Internet: A Critical/Reconstructive Approach', *Cultural Politics*, 1: 1, 75–100.

Kamis, Ben and Thiel, Thorsten (2015). *The Original Battle Trolls: How States Represent the Internet as a Violent Place*. PRIF Working Paper 23.

Kartenberg, Hans-Peter (2011). 'Das Netz als Ort des Protests: Gilt die Demonstrationsfreiheit auch im Internet?', *Bürgerrechte & Polizei,* 98, 57–63.

Kehl, Danielle, Wilson, Andi and Bankston, Kehl (2015). 'Doomed to Repeat History: Lessons from the Crypto Wars of the 1990s', Open Technology Institute Policy Paper, June.

Kelty, Christopher (2005). 'Geeks, Social Imaginaries, and Recursive Publics', *Cultural Anthropology*, 20: 2, 185–214.

Kidd, Dorothy (2003). 'Indymedia.org: A New Communications Common', in Martha McCaughey and Michael D. Ayers (eds.), *Cyberactivism: Online Activism in Theory and Practice*. London: Routledge, 47–70.

Kleger, Heinz and Makswitat, Eric (2014). 'Digitaler Ungehorsam: Wie das Netz den zivilen Ungehorsam verändert', *Forschungsjournal Neue Soziale Bewegungen*, 27: 4, 8–17.

Kubitschko, Sebastian (2015). 'The Role of Hackers in Countering Surveillance and Promoting Democracy', *Media and Communication*, 3: 2, 77–87.

Lagasnerie, Geoffroy de (2016). *Die Kunst der Revolte: Snowden,* Assange, Manning. Berlin: Suhrkamp.

Leifeld, Philip and Haunss, Sebastian (2012). 'Political Discourse Networks and the Conflict over Software Patents in Europe', *European Journal of Political Research*, 51: 3, 382–409.

Leiner, Barry M., Cerf, Vinton G., Clark, David D., Kahn, Robert E., Kleinrock Leonard, Lynch, Daniel C., Postel, Jon, Roberts, Larry G., Wolff, Stephen (2011). 'Brief History of the Internet' www.internetsociety.org/brief-history-internet, accessed 23 May 2016.

Lovink, Geert and Riemens, Patrice (2013). 'Twelve Theses on Wikileaks', in Benedetta Brevini, Arne Hintz and Patrick McCurdy (eds.), *Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society*. Basingstoke: Palgrave Macmillan, 245–53.

Ludlow, Peter (ed.) (2001). *Crypto Anarchy, Cyberstates, and Pirate Utopia*. Cambridge, MA: MIT Press.

Mansfield-Devine, Steve (2015). 'The Ashley Madison Affair', *Network Security,* 9, 8–16.

McCaughey, Martha and Ayers, Michael D. (eds.) (2003). *Cyberactivism: Online Activism in Theory and Practice*. London: Routledge.

Milan, Stefania (2013a). 'Indymedia (The Independent Media Center)', in David Snow, Donatella della Porta, Bert Klandermans and Doug McAdam. (eds.): *Wiley-Blackwell Encyclopedia of Social and Political Movements*. Oxford: Wiley-Blackwell, 603–05.

Milan, Stefania (2013b). *Social Movements and Their Technologies: Wiring Social Change*. Basingstoke: Houndmills.

Milan, Stefania (2013c). 'Wikileaks, Anonymous, and the Exercise of Individuality: Protesting in the Cloud', in Benedetta Brevini, Arne Hintz and Patrick McCurdy (eds.), *Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society*. Basingstoke: Palgrave Macmillan, 191–208.

Moore, Daniel and Rid, Thomas (2016). 'Cryptopolitik and the Darknet', *Survival: Global Politics and Strategy*, 58: 1, 7–38.

Morozov, Evgeny (2011). *The Net Delusion*. London: Allen Lane.

Mueller, Milton (2015). 'Gibt es Souveränität im Cyberspace', *Journal of Self-Regulation and Regulation,* 1: 1, 65–80.

Musiani, Francesca, Cogburn, Derrick L., DeNardis, Laura, and Levinson, Nanette S. (eds.) (2016). *The Turn to Infrastructure in Internet Governance*. Basingstoke: Palgrave Macmillan.

Nissenbaum, Helen (2004). 'Hackers and the Contested Ontology of Cyberspace', *New Media & Society*, 6: 2, 195–217.

Nissenbaum, Helen (2005). 'Where Computer Security Meets National Security', *Ethics and Information Technology,* 7: 2, 61–73.

O'Hagan, Andrew (2014). 'Ghosting Julian Assange', *London Review of Books,* 36: 5, 5–26.

Olson, Parmy (2012). *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. New York: Little, Brown and Co.

Peters, Justin (2016). *The Idealist: Aaron Swartz and the Rise of Free Culture on the Internet*. New York: Scribner.

Powell, Alison (2016). 'Hacking in the Public Interest: Authority, Legitimacy, Means, and Ends', *New Media & Society,* 18: 4, 600–16.

Pozen, David E. (2013). 'The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information', *Harvard Law Review*, 127, 512–635.

Sagar, Rahul (2011). 'Das mißbrauchte Staatsgeheimnis: Wikileaks und die Demokratie', in Heinrich Geiselberger (ed.), *Wikileaks und die Folgen: Netz, Medien, Politik*. Berlin: Suhrkamp 201–23.

Sauter, Molly (2014). *The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet*. New York: Bloomsbury Academic.

Scheuermann, William E. (2014). 'Whistleblowing as Civil Disobedience: The Case of Edward Snowden', *Philosophy & Social Criticism,* 40: 7, 609–28.

Shantz, Jeff and Tomblin, Jordon (2014). *Cyber* Disobedience*: Re://presenting Online Anarchy*. Winchester: Zero Books.

Shirky, Clay (2008). *Here Comes Everybody: The Power of Organizing without Organizations*. London: Penguin Books.

Singh, J.P. (2013). 'Information Technologies, Meta-power, and Transformations in Global Politics', *International Studies Review,* 15: 1, 5–29.

Sprenger, Florian (2015). *Politik der Mikroentscheidungen: Edward Snowden, Netzneutralität und die Architekturen des Internets*. Lüneburg: meson press.

Thiel, Thorsten (2014a). 'Die Schönheit der Chance: Utopien und das Internet', *Juridikum. zeitschrift für kritik | recht | gesellschaft,* 15: 4, 459–71.

Thiel, Thorsten (2014b). 'Internet und Souveränität', in Friederike Kuntz and Christian Volk (eds.), *Der Begriff der Souveränität in der transnationalen Konstellation*. Baden-Baden: Nomos, 215–39.

Timberg, Craig (2015). *The Threatened Net: How the Web Became a Perilous Place*. New York: Diversion Books.

Tufekci, Zeynep (2016). 'As the Pirates Become CEOs: The Closing of the Open Internet', *Daedalus*, 145: 1, 65–78.

Turgeman-Goldschmidt, Orly (2005). 'Hackers' Accounts: Hacking as a Social Entertainment', *Social Science Computer Review,* 23: 1, 8–23.

Turner, Fred (2006). *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago: University of Chicago Press.

Weinberger, David (2015). 'The Internet That Was (and Still Could Be)', *The Atlantic*, 22 June.

White, Micah (2016). 'The Panama Papers: Leaktivism's Coming of Age', *The Guardian* 5 April, www.theguardian.com/news/commentisfree/2016/apr/05/panama-papers-leak-activism-leaktivism, accessed 6 April 2016.

Winter, Rainer (2008). 'Perspektiven eines alternativen Internets', *Aus Politik und Zeitgeschichte,* 39, 23–8.

Wolfson, Todd (2014). *Digital Rebellion: The Birth of the Cyber Left*. Urbana (Ill.): University of Illinois Press.

Wu, Tim (2010). *The Master Switch: The Rise and Fall of Information Empires*. New York: Alfred A. Knopf.

Zittrain, Jonathan (2003). 'Internet Points of Control', *Boston College Law Review,* 44: 2, 653–88.

Zittrain, Jonathan (2009). *The Future of the Internet: And How to Stop It*. New Haven: Yale University Press.

Zittrain, Jonathan (2010). 'Protecting the Internet without Wrecking It: How to Meet the Security Threat', in Berin Szoka and Adam Marcus (eds.): *The Next Digital Decade: Essays on the Future of the Internet*. Washington, DC: TechFreedom, 91–112.

Züger, Theresa (2014). 'Digitaler ziviler Ungehorsam: Spurensuche der Dissidenz im digitalen Zeitalter', *Juridikum. zeitschrift für kritik | recht | gesellschaft,* 15: 4, 472–81.

Züger, Theresa, Milan, Stefania and Tanczer, Leonie M. (2015). 'Sand in the Information Society Machine: How Digital Technologies Change and Challenge the Paradigms of Civil Disobedience', *Fibreculture Journal,* 26, 108–35.

[i] There are at least two other, equally key, notions of the Internet: as a space for communication (an idea I look at in greater detail later on) and as a physical structure (An overview of the different concepts and their implications is given in Crawford 2007.) Although the second view is playing an increasingly important role in the control of the Internet (DeNardis 2012, Musiani et al. 2016), it is only dealt with indirectly here.

[ii] There is currently much discussion as to how far we are experiencing the return of closed spaces in this regard. What has triggered this debate is the appearance of ever more 'closed gardens', particularly in relation to the mobile Internet and its 'restricted app' logic and to access in developing countries, as exemplified in Facebook's 'internet.org' initiative, which allows no-cost access to Internet services but only to specific ones. These changes to the Internet, and the various rationales underlying them, are discussed in e.g.: Weinberger 2015, Wu 2010, Zittrain 2009, Clark 2016, Timberg 2015.

[iii] On closer analysis, two (complementary) processes are observable that represent a departure from the original multi-stakeholder model: transposition to multilateral institutions (internationalisation) and sharper definition of networks within the 'network of networks'—the 'fragmentation thesis' (Drake/ Cerf/Kleinwächter 2016).

[iv] Civil-society actors too have stinging criticisms to make of the present set-up and its institutional predecessors. The conclusions they draw, however, differ from the arguments advanced by the state and the corporate sector. Whereas to begin with a minimally regulated Internet was seen as a better guarantor of freedom on the Net, the defects in the security-architecture (Zittrain 2010) and the possibility of utilizing open protocols for commercial purposes have undermined this belief (Tufekci 2016). Hence, the idea of an increase in regulation is no longer rejected on principle and instead ways are sought of creating an institutional landscape that is more committed to freedom and more open to democratic influence.

[v] This position is known by the name of 'internet exceptionalism' (Johnson/Post 1996) and received what was perhaps its most famous exposition in John Perry Barlow's 'Declaration of the Independence of Cyberspace' (Barlow 1996). Music- and software-piracy were early cautionary developments which seemed to demonstrate the inability of political sanctions or commercial clout to prevent the upheavals caused by the shift from analogue to digital formats and networks.

[vi] Those that derive particular benefit from digital juridification and order-formation often include—speaking in particular of the state—executive bodies such as secret services. Ironically, these bodies themselves are subjected to very little legal regulation. On the contrary: they operate in a broad, loosely defined legal framework that both permits and ensures their expansion. Illustrations of this include the framing of objectives in very general terms, e.g. 'countering terrorism', and the definition of a task in terms that are too vague or too narrow—as when the analysis of communications-content is regulated but analysis of meta-data has no limit imposed on it. As far as private actors are concerned, a renewed increase in sensitivity to issues of data collection and analysis is observable over the last decade, particularly in Europe. The paralysis that had resulted from the assumption that actors operating at global level could not be regulated is beginning to wear off. Parliaments and courts of law in particular have set new trends here, identifying and enforcing regulations that curtail particularly far-reaching practices and in some cases have led to enhanced consumer-awareness.

[vii] It is also clear that, overall, cyber dissidence is located almost exclusively at the left/progressive end of the political spectrum (Wolfson 2014). Naturally, there are also a good many right-wing and nationalist movements that actively exploit Internet networking or use it as a way of doing politics. However, this 'right-wing' activity does not relate to issues of norm-development or regulation on the Net; it merely uses the Net as a means of tackling non-digital concerns.

[viii] Only in a very few cases are the demands so radical that they fall outside the bounds of the fundamental consensus that obtains in Western states. In this regard, Julian Assange, for example, is something of a chameleon: there are certainly writings by him that break radically with the notion of statehood and the possibility of representative democracy—see Assange 2006, and, for more general anarchistic observations, Shantz/Tomblin 2014. Having said that, we should bear in mind that Assange's position, and the WikiLeaks notion of democracy, is ambiguous in places and has undergone several mutations. On this, see Assange 2010, Hofmann 2011, O'Hagan 2014, Sagar 2011. In essence, Assange assumes that, overall, technological developments provide better, i.e. more direct, opportunities for influencing and participating in, politics but that the basis for this is the essential openness of all decision-making bodies. The broader Internet discourse also includes libertarian voices, which seek to extend the principles of free expression and absolute transparency not only to public institutions but also to private activities. defending trolling as a form of freedom of expression, for example, or attempting to hallow unfiltered leaking with an air of moral or political rectitude. The best known instance of this is the Ashley Madison hacking episode (Mansfield-Devine 2015). Within the public discourse, numerous voices have been raised against the transparency ideal, often taking the form of literary/fictional treatments of the theme. Jonathan Franzen's *Purity*, for example, or Dave Eggers's *The Circle*, predict totalitarian consequences for society as a whole.

[ix] One can probably also draw a distinction here between an American and a European Internet culture. The former is much more influenced by *Californian ideology* and the culture of Silicon Valley, with its mixture of libertarian and 1960s counter-culture stances. (The classic critique of this mix was formulated early on by Barbrook and Cameron (1996). For a general account of developments, see Turner 2006.) The European position is less tied to business and permeated to a greater degree by a culture of data-protection (on the cultural differences in general, and on status within the social system, see Elliot 2016).

[x] Examples of activism that is Net-based but not Net-related include the WikiLeaks publications regarding Iraq and Afghanistan. They also include many of the 'Anonymous' group's actions, in which the choice of means is Internet-related but the substance at issue is not. (The interplay between Net-related and general opposition is explored in Kahn/Keller 2005.) A case in point was Project Chanology, which sought to challenge the Church of Scientology and played a key role in politicizing the group. Here too, however, there was a crucial digital connection, namely the attempt by the Church to have a video of Tom Cruise—one of its members—removed from the Internet (excellent descriptions of the evolution and politicisation of Anonymous are given in Coleman 2014 and Olson 2014).

[xi] The digital dissidence described here is largely a phenomenon of Western liberal societies. Dissidents in authoritarian regimes do share many of the ideals in question, and in some cases use similar means; however, given the repressive context, the efforts to get the right to freedom of expression and other Internet standards accepted are more of a means to an end. Equally, under an authoritarian regime, much smaller acts are required to turn opposition into dissidence. In general, one should take care not to construe information and communications technologies one-sidedly as 'liberation technologies'. One has

to weigh up what instruments and opportunities also find their way into the hands of the state as a result of the expansion of the digital sphere (on this debate, see: Morozov 2011, Deibert/Rohozinski 2010, Deibert 2013, Howard 2010).

[xii] Interestingly, in this case the name of the party itself constitutes a call to dissidence. Also, battles against copyright-provisions (and thus also indirectly against the liberal system of property ownership) have had a high profile in the party's country of origin—Sweden.

[xiii] The passing of technical expertise to non-expert users in order to make these open structures accessible (CrytoParty is one such initiative) must be included in these activities. Much of what is done by classic hacker-organisations—the CCC, for instance—comes under the development, deployment, and dissemination of an open infrastructure in a way that does not seek confrontation with the commercial/political shaping of the digital order (Kubitschko 2015).

[xiv] As well as these forms of online protest, there are many net-based but non-disruptive kinds (e-petitions, for example, which come in for frequent use at the oppositional end of the spectrum—see Earl 2006 and Earl/Kimport 2011).

[xv] It is important to bear in mind that hacking does not necessarily have a political component and is instead pursued out of technical curiosity, say, or for fun (or indeed may actually be done exclusively or chiefly for these reasons) (Turgeman-Goldschmidt 2005). One reason why hacking has become increasingly politicised is because the ontology of digital communication has undergone a change and what was once a mode of play for experts has turned into a heavily regulated area of human action deemed to be of crucial social importance (Nissenbaum 2004).

[xvi] It would be instructive at this point to look a little further afield and consider the kinds of world-views that are associated with digital dissidence—views that appear to play an important part in recruiting new activists and maintaining the digital-dissidence movement in society. Popular culture's fascination with digital dissidence is evident. It finds expression in admiring narratives about hackers—in the 'Mr Robot' television series, for example, and in countless feature films. Iconic images of columns of green figures and successions of programme codes flashing past elevate computer-expertise to the realms of wizardry. At the same time, these admiring accounts always have an undertone of considerable ambivalence, partly because they convey the feeling that anything may happen, that there is no control, and partly because the hacker is often portrayed as a loner and an unstable person.

[xvii] One example of successful endeavour by civil-society actors that remains as telling as ever is the series of so-called 'crypto wars' conducted during the 1990s. As a result of these, comprehensive and accessible systems of coding were made available to end-users in the face of strong reservations on the part of political actors. This example also shows, however, that the successes achieved by the Internet movement need constant safeguarding: the Snowden leaks make clear just how keen secret services are to undermine encryption standards (Kehl/Bankston. 2015, Diffie/Landau 2007). Similarly, the discussions about 'back doors' and 'golden keys' in commercial applications demonstrate that the ideal of control-averse network-structures faces strong resistance from both the state and, to some extent, business, meaning that norm-formation must be viewed as an incomplete and contested project.

[xviii] This is clear from the case of data-protection. Thus, the successful challenges mounted against the 'Safe Harbour' arrangement both in the courts and in parliament seem at first sight to signal victory, but the updated version of the instrument, entitled 'Privacy Shield', contains as many major implementation-problems as ever and these are explained—at least by the actors involved in the negotiations—as being due to the impossibility of pushing through any broader-based agreements.