International Cyber Norms:
Legal, Policy & Industry Perspectives,
Anna-Maria Osula and Henry Rõigas (Eds.),
NATO CCD COE Publications, Tallinn 2016

CHAPTER 5

Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace

Toni Erskine and Madeline Carr[1]

As in any realm of human activity, norms are unavoidable in cyberspace. Yet cyberspace is a singularly complex setting within which to understand and try to shape norms. The problem is not simply the nature of cyberspace, although, as we will address below, acknowledging the unique characteristics of cyberspace is crucial when exploring norms in this realm. Rather, the challenge lies in the often overlooked *nature of norms themselves* and how their defining features render them especially difficult to decipher – and, by extension, to attempt to design – in the context of cyberspace.

Norms are widely-accepted and internalised principles or codes of conduct that indicate what is deemed to be permitted, prohibited, or required of agents within a specific community. The modest aim of our chapter is to explore the challenges and potential of engaging with norms in cyberspace. By 'engaging with norms in cyberspace' we mean both *understanding existing norms* and the more prominent endeavour (prevalent in recent discussions of policies related to both cyber security and Internet governance) of what is variously described as *'cultivating', 'promoting'*

1 An initial iteration of this position was presented at the NATO CCD COE workshop on 'Cyber Norms & International Relations' in Stockholm, Sweden, 28-29 April 2014. We are grateful to Anna-Maria Osula and Henry Rõigas for the opportunity to develop our argument for this volume, to Nicholas Erskine, Nishank Motwani, Cian O'Driscoll and anonymous reviewers for their incisive written comments on an earlier draft, and to Campbell Craig for discussing particular points.

or *'developing' new norms.*[2] Our focus throughout most of this chapter will be on the former. Indeed, a central point of the argument that will follow is that one cannot hope to 'cultivate' norms in cyberspace without first understanding the existing normative landscape.

In order to explore the challenges and potential of engaging with norms in cyberspace, we will take five steps. First, we will elaborate upon the definition of 'norms' offered above. In doing this, we will draw on influential work from within the discipline of International Relations (IR), and specifically from the multifaceted approaches labelled 'normative IR theory' and 'constructivism'.[3] Second, we will introduce a task that is fundamental to understanding existing norms in any realm, including cyberspace: interpreting the norms themselves. Third, we will highlight the characteristics of cyberspace that render this crucial task particularly difficult; namely, that it is a new and rapidly changing realm in which underlying values are contested and relevant agents are often difficult to identify. Fourth, we will link the difficulties of addressing norms in such a realm with the tendency to invoke what we will call 'quasi-norms', or merely *purported* norms. Fifth and finally, we will turn to the potential to engage with norms in cyberspace, regardless of obstacles, by uncovering what we will call the 'norm of de-territorialised data' and, in the process, demonstrating how evidence for its status as such can be uncovered in the justifications and judgements that agents in international politics offer when it is violated. Our hope is that these preliminary steps will take us some distance towards establishing a conceptual framework for speaking more coherently about norms in cyberspace.

2 'Cultivating' is a term used by Martha Finnemore in 'Cultivating International Cyber Norms', in *America's Cyber Future: Security and Prosperity in the Information Age*, eds. Kristin M. Lord and Travis Sharp (Washington, D.C.: Center for a New American Security, 2011), 89-101, https://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20II_2.pdf. (She also employs 'formulating' and 'implementing' seemingly synonymously at page 99, which, for reasons that we will try to make clear below, is more problematic.). 'Promoting' is employed by, *inter alia,* Henry Farrell, 'Promoting Norms for Cyberspace,' *Council on Foreign Relations*, April 2015, 1-3, http://www.cfr.org/cybersecurity/promoting-norms-cyberspace/p36358. A series of workshops jointly held by Harvard, MIT and University of Toronto discussed 'developing' cyber norms. American Bar Association, 'A Call to Cyber Norms: Discussions at the Harvard-MIT-University of Toronto Cyber Norms Workshops, 2011 and 2012' (2015), https://www.americanbar.org/content/dam/aba/uncategorized/GAO/2015apr14_acalltocybernorms.authcheckdam.pdf.

3 For an overview of 'normative IR theory' (which is also referred to as 'international political theory' and 'international ethics'), see Toni Erskine, 'Normative International Relations Theory,' in *International Relations Theory: Discipline and Diversity,* eds. Tim Dunne, Milja Kurki and Steve Smith (Oxford: Oxford University Press, 2nd ed. 2010 and 4th ed. 2016), 236-258. For a general introduction to IR's 'constructivism', see Ian Hurd, 'Constructivism,' in *The Oxford Handbook of International Relations,* eds. Christian Reus-Smit and Duncan Snidal (Oxford: Oxford University Press, 2008), 298-316. For an essay that compares and contrasts these bodies of scholarship, see Toni Erskine, 'Whose Progress, Which Morals? Constructivism, Normative IR Theory and the Limits and Possibilities of Studying Ethics in World Politics,' *International Theory* 4 (2012).

1. Defining 'Norms': Insights from the Discipline of International Relations

In early 2015, Admiral Michael S. Rogers, head of the National Security Agency (NSA) and Cyber Command in the United States (US) announced his intention to 'do outreach in the academic world' in order to better understand norms in cyberspace. In making the case for 'a strong academic focus' in addressing norms in the cyber context, and comparing this current challenge to 'another cataclysmic change in national security in the middle of the previous century', namely the advent of the nuclear age, he noted that work that led to understanding and fostering 'established norms of behaviour' in relation to nuclear weapons, such as those surrounding deterrence, was 'done in the academic arena'.[4] Although Admiral Rogers did not elaborate on the precise source of this work, it seems clear that he was inclined in his outreach efforts to look particularly to the discipline of IR, within which prominent works on the political, ethical, psychological and security aspects of nuclear weapons and deterrence theory are found.[5] We will respond to Rogers' call for engagement with the academic community, and particularly with the discipline of IR, by suggesting that normative IR theory and constructivism, both relatively recently-established areas of scholarship within the discipline, are valuable places to begin acquiring the necessary conceptual tools for addressing the subject of norms in cyberspace.

Contributions to normative IR theory and what we will call 'mainstream constructivism' have engaged in separate analyses of norms, with distinct research aims and methodologies.[6] Nevertheless, they adopt valuable, shared assumptions about their common object of analyses. A 'norm' as it is generally understood within these IR approaches – and as we will use the term here – is a principle that displays two

4 Michael S. Rogers, 'A Conversation with Mike Rogers,' *Cyber Security for a New America: Big Ideas and New Voices*, February 23, 2015, https://www.newamerica.org/new-america/cybersecurity-for-a-new-america/.

5 This body of work has spanned IR's security studies, political realism, (early) normative IR theory, and, more recently, constructivism. Prominent works in security studies include, Thomas C. Schelling, *The Strategy of Conflict* (Cambridge: Harvard University Press, 1960 and 1980); Robert Jervis, Richard Ned Lebow and Janice Gross Stein (with contributions by Patrick M. Morgan and Jack L. Snyder), *The Psychology of Deterrence* (Baltimore: Johns Hopkins University Press, 1985); Daniel Deudney, 'Nuclear Weapons and the Waning of the Real-State', *Daedalus,* 124: 2 (Spring 1995), 209-231; and Lawrence Freedman, *Deterrence*, 1st ed. (Cambridge: Polity, 2004). For an overview of American realist engagement with nuclear weapons and the problem of deterrence, see Campbell Craig, *Glimmer of a New Leviathan: Total War in the Realism of Niebuhr, Morgenthau, and Waltz* (New York: Columbia University Press, 2003) and 'The Nuclear Revolution as Theory,' in *International Relations Theory Today,* 2nd ed., eds. Ken Booth and Toni Erskine (Cambridge: Polity Press, 2016). Prominent neo-realist contributions are the following: Robert Jervis, *The Illogic of American Nuclear Strategy* (Ithaca: Cornell University Press, 1985) and *The Meaning of the Nuclear Revolution: Statecraft and Prospects for Armageddon* (Ithaca: Cornell University Press, 1990); and Kenneth N. Waltz, 'Nuclear Myths and Political Realities', *American Political Science Review,* 84: 3 (Sept. 1990), 730-745. Influential precursors to normative IR theory on this topic are Paul Ramsey, *The Just War: Force and Political Responsibility* (Oxford; New York: Rowman and Littlefield, 1968 and 2002), Part III, and Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (New York: Basic Books, 1977 and 2nd ed. 1992), chapter 17. For a prominent constructivist study, see Nina Tannenwald, *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons since 1945* (New York: Cambridge University Press, 2007).

6 'Constructivism' within IR has various, multifaceted strands and we realise that a distinction such as that between 'mainstream' or 'empirical' constructivism on the one hand and 'critical' or 'language-based' constructivism on the other oversimplifies a sophisticated and diverse body of work. Our aim here is simply to make clear that our intended focus is the work of those empirically-minded constructivists, with firm roots in American IR, whose social scientific commitments have been amenable to mainstream IR, and who, collectively, have produced a significant body of work on norm development in international relations.

related, key characteristics: 1) it has prescriptive and evaluative force; and 2) it is widely-accepted and internalised by those within a particular community.

Norms as phenomena studied in IR are principles that embody established codes of what actors *should* do, or refrain from doing, in certain circumstances. Thus conceived, they possess prescriptive force. By extension, norms also entail an evaluative dimension: norms are invoked to variously condemn or condone behaviour in world politics, and even to support proposals for sanctions when they have been violated. In short, they embody powerful expectations that can both constrain and compel actors in world politics. As guides to what is required, permitted, or prohibited, they are widely understood to have moral weight.[7] To highlight this important feature of norms, they have been referred to as 'moral norms' within both mainstream constructivism and normative IR theory.[8] This label highlights their important prescriptive and evaluative dimension. Moreover, it distinguishes this conception of a norm both from its more colloquial counterpart, which simply connotes habitual behaviour ('it is the norm to break for coffee at 10am'), and from the broader category of 'social norms' which, Nina Tannenwald usefully notes, encompasses 'moral norms', but also includes 'more mundane kinds of norms or rules for social interaction, such as diplomatic protocol'.[9] Throughout this chapter, when we talk about 'norms' in cyberspace, or in international relations more generally, we will be referring to norms that can be thus labelled.

Both broadly communitarian positions within normative IR theory and IR's constructivism see norms as social facts that are intersubjectively defined.[10] Simply, shared understandings regarding right and wrong conduct are established over time by those who participate in particular practices. (We understand practices as sustained interactions between purposive actors that both rely on and establish rules, customs, and common meanings.) Norms are principles that represent these collective expectations and are both widely accepted and internalised by the members of the community within which they evolve. Importantly, the community in question need not be territorially defined, but can emerge in the context of geographically dispersed and often transnational practices.[11] Norms might be codified in law, or

7 Erskine, 'Normative International Relations Theory,' 246-247.

8 See, for example, Richard Price, 'The Ethics of Constructivism,' in *The Oxford Handbook of International Relations,* eds. Reus-Smit and Snidal, 317-326 and Erskine, 'Normative International Relations Theory.'

9 Tannenwald, *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons since 1945,* 58. Notably, we do not agree with Tannenwald's account that 'moral norms' are necessarily 'rooted in impartiality' and are 'universalisable' in the Kantian sense. Moral norms as we understand them can also boast a particularist moral starting point and be circumscribed in scope.

10 For an account of the common ground between communitarian normative IR theory and IR's constructivism, see Erskine, 'Whose Progress, Which Morals?' 462-463. Emmanuel Adler provides and incisive account of intersubjectivity in Emanuel Adler, 'Seizing the Middle Ground: Constructivism in World Politics,' *European Journal of International Relations* 3 (1997): 327-328. The seminal work in establishing a broad analytical distinction between 'communitarianism' and 'cosmopolitanism' in normative IR theory is Chris Brown, *International Relations Theory Today: New Normative Approaches* (New York: Columbia University Press, 1992). The broadly 'communitarian' theorists central to work in normative IR theory whose understanding of norms we are relying on here are Michael Walzer and Mervyn Frost, both of whom will be addressed below.

11 For a detailed account of this conception of 'dislocated community' (that addresses 'morally constitutive communities' but also applies to communities of shared understandings and emerging norms), see Toni Erskine, *Embedded Cosmopolitanism: Duties to Strangers and Enemies in a World of Dislocated Communities* (New York: Oxford University Press, 2008), 173-174; 218-227. This understanding of community as not necessarily territorially defined is important when we are talking about norms in cyberspace.

they might be internalised *without* being formally institutionalised. Either way, their defining feature is that they are widely accepted by, and inform the behaviour of, those who participate in the relevant practice. By this account, it is conceivable that a law might *not* constitute a norm if it is neither internalised by, nor informs the behaviour of, those to whom it is meant to apply.[12] Indeed, while a principle might be widely accepted and internalised within a community (in other words, achieve the status of a norm) *before* being codified in law, it is also the case that formally institutionalising a principle in law may contribute to its eventual (but not inevitable) acceptance as a norm. Our point here is simply that laws and norms are often overlapping categories, but they are not equivalent. In sum, norms embody a community's widely accepted and internalised customs, mores and perceived rules regarding right and wrong conduct in relation to particular practices.

The norms that are subjects of study in IR are typically those associated with international practices, by which we mean, simply, practices whose participants – whether individual human beings or corporate agents – are not restricted to those within the borders of any one state. The category of *international* norm that we associate with such practices might elicit scepticism. It suggests the possibility of agreement on expectations and standards of conduct in a realm that is generally characterised more by division and dispute than by consensus. The sceptic might protest that international norms are nothing more than wishful thinking. After all, our sceptic might observe, even the most prominent ostensible examples of international norms, such as the prohibition against intentionally targeting non-combatants in war, are regularly transgressed or evaded. Moreover, he or she might add, it would be difficult to argue that there is unanimous agreement on the source of authority for such principles. The sceptic might conclude that international moral norms are not even conceivable. In response, Mervyn Frost's careful account of what he calls 'settled norms' in international politics is extremely useful.

Frost has been a pioneering figure in normative IR theory. In a book first published in 1986, he defines 'settled norms' in international politics not as principles that are universally observed, or even uniformly grounded, but, rather, as principles for which there is a perceived need either to keep their infringement clandestine, or to provide special justification for any attempt to override or deny them.[13] In short, such principles are not openly transgressed without pointed justifications and excuses. They are tacitly respected, even in their breach. According to this understanding, 'settled norms' in international politics profoundly affect agents' behaviour, and specifically how they variously describe and defend, justify and judge, carry out and sometimes conceal acts and omissions.

12 As we will elaborate on below, by 'inform the behaviour' of an agent, we do not mean that a norm necessarily engenders compliance. Rather, a norm might inform the behaviour of an agent, and thus be discernible, by prompting attempts to justify, excuse, or hide its violation.

13 The first edition of Frost's book is *Towards a Normative Theory of International Relations* (Cambridge: Cambridge University Press, 1986). Page references in this chapter will be to the second edition: Frost, *Ethics in International Relations: A Constitutive Theory* (Cambridge: Cambridge University Press, 1996), 105-106.

Despite Frost's label of 'settled' norms, it is important to emphasise that international norms are not static. This point is highlighted in an important contribution to the mainstream constructivist literature on norms. In an influential article published in 1997, Martha Finnemore and Kathryn Sikkink propose that norms have a three-stage life-cycle: norm emergence; norm cascade (or broad norm acceptance) and internalisation.[14] In addition to usefully demonstrating the dynamic nature of international norms, their depiction of a process of normative change also reinforces both defining features of norms outlined above: their prescriptive and evaluative force,[15] and their broad acceptance and internalisation by the members of a specific community.[16] However, there are a few points that we suggest warrant attention before attempts are made to apply this concept without qualification to norms in cyberspace.

First, the focus of this particular article by Finnemore and Sikkink is on norms that are deliberately established by what they call 'norm entrepreneurs'. In one sense, this is especially relevant to the exploration of norms in cyberspace, where there has been a tendency (as noted above) to talk about cultivating, promoting and developing norms. However, we understand norms also to be the result of organic processes of emergence and change alongside conscious, concerted efforts to institutionalise them in particular forms. Indeed, one of our aims in this chapter is to highlight the need to acknowledge the significance and the consequences of the former before embarking on the latter. Second, the lifecycle of a norm, as presented by Finnemore and Sikkink, is something that strikes us as only possible to map with any accuracy retrospectively, which is not something that can yet be done in relation to expectations of right and wrong conduct in the context of the relatively new practices that currently define cyberspace. Our focus later in this chapter will be on identifying norms that at least begin to display features of what Frost has called a 'settled [international] norm' without analysing what stage they might be in a lifecycle that, we suggest, is still on-going in relation to Finnemore and Sikkink's proposed stages. Finally, there is a sense that the image of the lifecycle – through which expectations and codes of conduct evolve and gain progressively wider acceptance – does not allow for the regression or erosion of norms once they are established or widely accepted. We want to highlight that the dynamic process of normative change in cyberspace (like in any other realm) need not be, and is unlikely to be, linear according to some preconceived notion of an ideal endpoint.

14 Martha Finnemore and Kathryn Sikkink, 'International Norm Dynamics and Political Change', *International Organisation* 52:4 (1998), 887-1061 (895-905).

15 Finnemore and Sikkink emphasise that 'it is precisely the prescriptive (or evaluative) quality of 'oughtness' that sets norms apart from other kinds of rules'. Ibid, 891.

16 Note, however, that our conception of 'internalisation' differs from that of Finnemore and Sikkink in an important respect. They maintain that 'internalisation' entails 'a 'taken-for-granted' quality that makes conformance with the norm almost automatic'. Ibid, 904. For us, following Frost, what is taken for granted is the perceived need to justify, rationalise, excuse, deny or hide deviation from norm. Conformance need not be 'automatic' for a norm to be internalised. Its prescriptive and evaluative force is what is internalised.

2. A Fundamental Task: Interpreting Norms

A norm, we have argued, qualifies as such if it both displays prescriptive and evaluative force and is widely accepted and internalised by the members of a particular community. Cyberspace is a realm of principles, customs and codes of conduct that meet these two key criteria to various degrees. *Interpreting* these existing norms is the first crucial step before attempting to revise them, or to cultivate new norms. We need to explain what we mean when we claim the norms are things to be interpreted.

Interpretation is a process that we understand in terms of reading and deciphering the values, standards, and codes of conduct within a community in relation to a particular practice.[17] Importantly, this conception does not reduce norms to mere reflections of the *status quo*. Indeed, norms represent a rough consensus at a particular point in time on what *should* be done in a particular context. As such, norms are variously invoked to prescribe actions, tacitly acknowledged by agents in attempts to justify their infringement (as we learned from Frost), and appealed to in the censure of perceived violations. All of this means that interpreting norms demands more than a superficial reading of what is actually *done*. In other words, the objects of interpretation are not merely espoused principles or prevailing policies. Rather, they include the underlying values and shared understandings of the community in question, in relation to a particular practice, as revealed through agents' accounts of their own actions and the actions of others.

Frost's cogent definition of a 'settled norm', relayed above, helps to explain how international norms can be interpreted and studied. What is crucial in identifying a norm, according to Frost, is the perceived need to justify, excuse, rationalise, hide or deny any deviation from it. Any study of norms seeks to uncover our collective understandings of standards of right and wrong conduct. These are not revealed straightforwardly in what we do or refrain from doing, but rather in how we justify and judge acts and omissions. On this fundamental point, we might also turn to Michael Walzer's seminal 1977 book, *Just and Unjust Wars* – another key influence on normative IR theory. In this work, Walzer examines norms in the conduct of war, which he relabels 'the war convention'.[18] He argues that, in discerning these norms:

> '[i]t is important to stress that it is our judgments that are at issue here, not conduct itself. We cannot get at the substance of the convention by studying combat behaviour, any more than we can understand the norms of friendship by studying the way friends actually treat one another. The norms are apparent, instead, in the expectations friends have, the complaints they make, the

17 Our understanding of interpretation owes much to Michael Walzer's account in *Interpretation and Social Criticism* (Cambridge, Massachusetts: Harvard University Press, 1987).

18 Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, 125-222. Like our understanding of interpretation more generally, our reading of *Just and Unjust Wars* is influenced by Walzer's later book *Interpretation and Social Criticism*.

hypocrisies they adopt. So it is with war: relations between combatants have a normative structure in what they say (and what the rest of us say) rather than in what they do – though, no doubt what they do, as with friends, is affected by what they say.' [19]

Although working in a very different scholarly tradition, Finnemore and Sikkink make a similar assumption of how norms can be identified. They explain that 'because norms by definition embody a quality of 'oughtness' and shared moral assessment, norms prompt justifications for action and leave an extensive trail of communication among actors that we can study'. The illustration that they offer in support of this statement is useful, and reveals a means of deciphering norms similar to that proposed, respectively, by Walzer and Frost: '[f]or example, the US' explanations about why it feels compelled to continue using land mines in South Korea reveal that it recognizes the emerging norm against the use of such mines'. They conclude that '[i]f not for the norm, there would be no need to mention, explain, or justify the use of mines in Korea at all'.[20] As Walzer, Frost, Finnemore and Sikkink emphasise, in deciphering norms, it is necessary to pay attention to what agents say about their own and others' deviations from them.

Interpreting norms requires recognition of the broader systems of meaning and value within which they are situated, negotiated, and debated. Significantly, this means that even espoused principles and prevailing policies within a given community can be (internally) evaluated and criticised in relation to the community's norms, which must be carefully extracted from a complex context of contestation.[21] It also explains why, when interpreting norms, an appeal to a single source of espoused principles or even their codification in law is not enough. In relation to norms in the conduct of war, for example, Walzer emphasises the variety of sources that must be appealed to in the process of interpretation: 'we look to lawyers for general formulas, but to historical cases and actual debates for those particular judgments that both reflect the war convention and constitute its vital force'. He goes on to clarify that 'I don't mean to suggest that our judgements, even over time, have an unambiguous collective form. Nor, however, are they idiosyncratic and private in character'. Rather, '[t]hey are socially patterned, and the patterning is religious, cultural, and political, as well as legal'.[22] Tannenwald, writing almost thirty years later in the mainstream constructivist tradition (and citing the influence of

19 Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, 44.

20 Finnemore and Sikkink, 'International Norm Dynamics,' 892.

21 For accounts of an interpretive approach thus understood, which we associate with a critical stream of communitarianism, see the following: Walzer, *Interpretation and Social Criticism*; Walzer, *Spheres of Justice: A Defense of Pluralism and Equality* (New York: Basic Books, 1983); Walzer, '"Spheres of Justice": An Exchange,' *New York Review of Books* 30 (1983): 43-46; and Erskine, 'Whose Progress, Which Morals?' 463-464. According to such an approach, it is possible to challenge espoused principles and prevailing policies within a particular community by exposing their inconsistencies and tension with underlying values and social meanings. Walzer, for example, talks about the process of distinguishing 'deep and inclusive accounts of our social life from shallow and partisan accounts' in '"Spheres of Justice": An Exchange,' 43. For an assessment of the advantages and shortcomings of this critical communitarianism, see Toni Erskine, 'Qualifying Cosmopolitanism? Solidarity, Criticism, and Michael Walzer's 'View from the Cave,' *International Politics* 44 (2007): 135-36.

22 Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations,* 45.

Walzer's approach in *Just and Unjust Wars),* describes norms not as 'governmental constructs' but rather as 'fundamentally cultural, religious and political phenomena' that, over time, 'emerge through a process of contestation and legitimation'.[23] Borrowing the words of James Turner Johnson, another central figure in normative IR theory in relation to work on the just war tradition, Tannenwald observes that 'in a given historical context, a great deal of work may be needed to define the content of a value that has begun to be seen dimly.'[24]

3. Three Challenges of the Cyber Domain

This task of interpreting norms is demanding in any domain, but there are reasons why it is particularly challenging, at this point in history, in the context of cyberspace. Namely, cyberspace is a realm of new practices, contested values, and often ambiguous agents. While we believe that these characteristics of cyberspace are well understood, their implications for addressing norms in this domain are not. In what follows, we will focus on these characteristics of cyberspace in relation to how they render the interpretation of norms – and, by extension, their promotion and revision – particularly difficult.

3.1 New Practices

Especially challenging contexts within which to interpret international norms are practices that are new, as yet not well understood, and quickly changing, such as those in the cyber domain. The rapidly advancing technology that defines cyberspace means that its constitutive practices are necessarily in flux. Referring specifically to the US military, Deputy Secretary of Defense William Lynn pointed out in 2010 that 'in less than a generation, information technology in the military has evolved from a tool for enhancing office productivity to a national strategic asset in its own right'.[25] Norms, as we have described them in the sections above, are necessarily the result of argument and negotiation within a community in relation to particular practices. They take time to evolve. As Walzer observed in relation to norms in the conduct of war, '[t]he war convention as we know it today has been expounded, debated, criticised, and revised over a period of many centuries'.[26]

New practices that have been emerging alongside the rapid development of cyberspace include those related to, for example, governing the global domain name system,

23 Tannenwald, *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons since 1945,* 58.

24 Tannenwald, *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons since 1945,* 58. For the original articulation, see James Turner Johnson, *Just War Tradition and the Restraint of War: A Moral and Historical Inquiry* (Princeton: Princeton University Press, 1981), 167.

25 William J. Lynn III, 'Defending a New Domain: The Pentagon's Cyberstrategy,' *Foreign Affairs* 89 (2010).

26 Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations,* 45.

negotiating what is considered allowable content, individual network management, social media communication, coordination of on-line financial transaction protocols, and the anticipation of, protection against, and response to cyber attacks. It would be unreasonable to assume that the host of nascent and quickly changing transnational practices that are emerging in these areas have each already produced clear expectations regarding right and wrong conduct that are widely shared amongst, and inform the behaviour of, their participants. As we will demonstrate below, there *are* some principles that have begun to display the qualifying characteristics of norms in cyberspace. Nevertheless, the novelty and the relative instability of practices in cyberspace mean that there are likely to be fewer settled norms than in more established practices. It also, separately, renders more difficult the task of identifying those norms that have begun to emerge. Admiral Rogers' astute response to the charge of an apparent lack of progress in establishing norms in cyberspace is worth repeating. In the context of the discussion cited above, and drawing a comparison with what he described as the now-established norms relating to nuclear weapons, he noted simply that *'all of this has taken time,* and cyber is no different'.[27]

3.2 Competing Value Systems

A second complicating factor in attempting to identify norms in cyberspace arises not from the novel and dynamic nature of the evolving practices themselves, but rather from the tensions and even blatant contradictions between the various value systems that these globalised practices bring together. For example, competing understandings of the relationship between privacy, transparency and anonymity generate tension around differing perceptions of 'security' in cyberspace. For many western states premised upon notions of individual rights, anonymity is fundamentally linked to privacy and, from a civil liberties perspective, is therefore regarded as essential for a sense of personal security.[28] Although anonymity can be problematic for national security and law enforcement, these states are faced with the difficult task of trying to balance the necessity of identifying some individuals online with the protection of personal privacy, a task that requires some transparency of government and law enforcement practices. In states like China that adhere to more collectivist principles, anonymity can be seen to lead to a lack of accountability, which can be understood as a *threat* to the inextricably bound notions of personal and collective security.[29] Anonymity in this context is regarded as facilitating anti-social

27 Rogers, 'A Conversation with Mike Rogers.'

28 As President of Brazil, Dilma Rousseff pointed out, 'In the absence of the right to privacy, there can be no true freedom of expression and opinion, and therefore no effective 'democracy'. 'Speech by H. E. Dilma Rousseff, President of the Federative Republic of Brazil, at the Opening of the General Debate of the 68th Session of the United Nations General Assembly' (United Nations, The 68th Session of the United Nations General Assembly, New York 24 September 2013), http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf.

29 Although some sectors of Chinese civil society reject government control over Internet content and activity, others express a sense of concern about the implications of Internet technology for social cohesion. A recent Pew poll found that 75% of people polled in China regard the Internet as having a negative effect on morality, 62% feel it has a negative effect on politics and 57% feel it has a negative effect on personal relationships. Pew Research Center, *Internet Seen as Positive Influence on Education but Negative on Morality in Emerging and Developing Nations* (March 19, 2015), http://www.pewglobal.org/2015/03/19/3-influence-of-internet-in-emerging-and-developing-nations/.

behaviour such as trolling, and it is seen to undermine the transparency necessary for harmonious social interaction. Even if we can clearly identify and fully comprehend a particular cyber practice, the norms that begin to emerge in relation to it will necessarily be contested when the *underlying values* to which its participants appeal are radically different and sometimes incompatible.[30]

Yet another feature of this landscape of competing values is the diversity of actors and interests involved in cyberspace's emerging practices. It is important, for example, to remain alert to the significant role that the private sector plays in governing, developing and moderating Internet access, services and infrastructure. These actors are engaged in a delicate balancing act of trying to adhere to state demands and laws while also catering to the demands of their customers. The expectations of the two are not always in concert. Significantly, the underlying values of the private sector are oriented around the need to maximise profits. Inevitably, this shapes the practices that this sector engages in, and the interests that it brings to various negotiations about expectations and codes of conduct within them.[31]

Such clashes of values are deeply consequential when we are talking about norms. This is because, as we have argued, norms are necessarily embedded within broader systems of meaning and value. Interpreting norms in cyberspace requires that we pay attention to the types of competing values that we have just outlined. Importantly, currently conflicting values may change and even become more compatible over time as a result of prolonged interaction (between participants in particular transnational practices, for example), persuasion, negotiation, converging interests, the desire for reciprocity, shared goals or threats, and the perceived benefits of cooperation. Yet, an eventual convergence of values cannot be assumed. Practices in cyberspace whose participants are influenced by markedly different value systems may also experience the emergence of *competing* norms. Understanding norms in cyberspace demands attention to the complexities of their underlying values, as does any attempt to promote new norms or revise existing ones.

3.3 Ambiguous Agency

If we think of norms as widely-accepted expectations regarding conduct, then we also must consider to whom, or to what, these expectations can attach. Norms embody guidelines regarding what purposive actors should do and refrain from doing in certain contexts. In other words, these norms set out responsibilities which, to be met, must be attached to agents capable of understanding and discharging them. If norms in cyberspace outline expectations as to what is permissible, prohibited and required, to which agents do they apply? If one is to speak meaningfully about norms in cyberspace, it is necessary to identify the relevant *moral agents,* or bearers of duties, that are expected to adhere to the injunctions, imperatives and

30 Madeline Carr, *US Power and the Internet in International Relations: The Irony of the Information Age,* (London: Palgrave Macmillan, 2016); Madeline Carr, 'Public Private Partnerships in National Cyber Security Strategies', *International Affairs* 92 (2016), 43-62.

31 Madeline Carr, 'Public Private Partnerships in National Cyber Security Strategies.'

codes of conduct that we might variously interpret, negotiate, seek to shape, and strive to codify.[32]

Our starting-point here is that, alongside individual human beings, formal organisations such as states, non-governmental organisations (NGOs), multinational corporations (MNCs) and intergovernmental organisations are moral agents in world politics and crucial, and powerful, bearers of responsibilities in the cyber domain.[33] Yet, while the importance of identifying agents to which norms in cyberspace can be attached seems fairly straightforward, the often ambiguous nature of agency in cyberspace makes realising this endeavour difficult. This ambiguous agency is, in some instances, an inevitable result of what are, as yet, nascent practices. In others, it is a consciously-created feature of cyberspace resulting from values of privacy and anonymity.

Within the relatively new practices of cyberspace, the roles and responsibilities of particular agents are often ill-defined and poorly understood.[34] Moreover, and separately, this is a space of both human and non-human actors and, consequently, understanding 'machine-to-machine' agency in the context of the expanding 'Internet of Things' will be increasingly important to discussions of norms, specifically with respect to questions of attribution and perceptions of responsibility. Can semi-autonomous, and perhaps even autonomous, decision-making on the part of computers, for example, create the impression of mitigating responsibility on the part of more traditional purposive agents in world politics? The possibility that such 'machines' might be moral agents (or qualify as such in the future as their decision-making capacities become more sophisticated), and, separately, the *perception* that they carry this status, even in some attenuated form, both have far-reaching implications for how we understand assigning duties and apportioning blame in cyberspace. Although attempting to solve these specific puzzles is beyond the scope of this chapter, it is important to note that they contribute to the challenge of ambiguous agency in cyberspace and deserve further attention.[35]

With regard to the separate consideration of consciously-created ambiguous agency in cyberspace, individuals, states, and non-state actors can, in many cases, take actions with some expectation of anonymity. The challenges of attribution leave open opportunities for 'plausible deniability'. Actors responsible for illicit activities

32 To clarify, the label 'moral agent' does not describe good or somehow commendable actors (although they might, of course, be both); rather, it refers to those actors of whom we can reasonably have certain expectations. In very general terms, moral agents have capacities for deliberating over possible courses of action and their consequences and acting on the basis of this deliberation. These capacities render them vulnerable to the ascription of duties and the apportioning of moral praise and blame in the context of specific actions or omissions. See Toni Erskine, 'Making Sense of "Responsibility" in International Relations – Key Questions and Concepts,' in *Can Institutions Have Responsibilities? Collective Moral Agency and International Relations,* ed. Toni Erskine (New York: Palgrave Macmillan, 2003), 6-7.

33 See Toni Erskine, 'Assigning Responsibilities to Institutional Moral Agents: The Case of States and Quasi-States,' *Ethics & International Affairs* 15 (2001): 67-85 and 'Locating Responsibility: The Problem of Moral Agency in International Relations,' in *The Oxford Handbook of International Relations,* eds. Reus-Smit and Snidal.

34 A recent article by Mark Raymond and Laura DeNardis illustrates how the complex array of actors and practices involved in Internet governance is not well understood. Mark Raymond and Laura DeNardis, 'Multistakeholderism: Anatomy of an Inchoate Global Institution,' *International Theory* 7 (2015): 1-45.

35 See Erskine, 'Moral Responsibility, Artificial Agency and Dehumanized War' (Paper presented at the Oceanic Conference on International Studies, Melbourne, Victoria, 1 July 2014).

in cyberspace may maintain a posture of denial either when they believe they have successfully masked their identity or when they realise that for a prosecuting actor to present compelling evidence it would be necessary to reveal more about its own forensic capabilities than would be prudent. The motivations behind cyber attacks can be difficult to discern and state responses to belligerent behaviour (crime, terrorism or state use of force) fundamentally rely upon the identity and motivation of the perpetrator. Although many cyber attacks are blamed on governments, and despite many media and technical reports that suggest conclusive evidence, it actually remains unclear (at least, in the public domain) who was behind incidents like the 2014 Sony Pictures hack which prompted President Obama to impose further sanctions on North Korea as a form of retribution.

Given that identifying the relevant agents in the cyber domain that can discharge espoused responsibilities is fundamental to speaking coherently about how particular norms can be realised, both the fact that a clear understanding of relevant agents and their roles is often lacking in the context of particular practices and the capacity for actors to remain anonymous in cyberspace can be seen as significant impediments.[36] Nevertheless, in relation to the first problem, it is important to point out that defining responsibilities that accompany particular roles is part of the process of evolving norms within relatively new practices. With respect to the second concern of consciously-created ambiguous agency, responsibilities *can* be assigned (prospectively) and powerful expectations of right behaviour can be fostered in the context of cyber practices, even if the possibility of (retrospectively) apportioning blame and responding to delinquency is often made exceedingly difficult. Moreover, if we go back to Frost's account of 'settled norms' as principles for which there is a perceived need either to keep their infringement clandestine, or to provide special justification for any attempt to override or deny them, careful attempts to maintain anonymity and plausible deniability in cases of transgression can actually provide evidence of tacit acknowledgment of the norm itself.

36 Interestingly, if one adopts the definition of a norm cited frequently in mainstream constructivist work – namely, 'a standard of appropriate behaviour *for actors with a given identity*' – then the challenge of ambiguous agency would arguably impede the emergence of norms themselves and not just pose a challenge to how they are deciphered and applied in particular cases. This is the definition provided by Finnemore and Sikkink in 'Norm Dynamics and Political Change,' 891 (emphasis added), who, in turn, cite Peter J. Katzenstein's definition in 'Introduction: Alternatives Perspective on National Security,' in *The Culture of National Security: Norms and Identity in World Politics*, ed. by Peter J. Katzenstein, (New York: Columbia University Press, 1996), 5: 'The authors [in this volume] use the concept of *norm* to describe collective expectations for the proper behaviour of actors with a given identity'. However, our definition of a norm (influenced by work in political philosophy and normative IR theory and, we maintain, compatible with key assumptions underlying mainstream constructivist definitions), does not include this qualification. Indeed, we are not convinced this is a defining feature of all norms. After all, many norms, such as those associated with the conduct of war, are *general* prohibitions or prescriptions which relate to a particular practice rather than being tied to the identities of specific agents. Of course, some norms do define what we would call 'role responsibilities' or 'obligations'. (For an excellent account of this concept, see Michael O. Hardimon, 'Role Obligations,' *Journal of Philosophy* 91 (1994): 333–363). Such role-defining norms are important, but they do not exhaust the category of norm.

4. The Temptation of 'Quasi-Norms'

Attempts to address norms in the challenging context of cyberspace often fall into the trap of espousing *quasi-norms*. 'Quasi-norm' is a term that we have coined for the purpose of this chapter to refer to principles and codes of conduct that have been labelled 'norms', but that lack the key qualifying features of norms that we have identified above: namely, prescriptive and evaluative force, and wide acceptance and internalisation by the members of a particular community.[37] There are at least two common avenues along which those who espouse these merely purported norms seem to travel when it comes to discussions of cyberspace. The first is traversed by those who seek to 'create', 'implement' or 'impose' norms in this realm; the second by those who see their task as importing settled norms from distinct, but arguably comparable, realms.

4.1 'Quasi-Norms' as Normative Aspirations

It is not at all surprising to think that agents with particular interests or values will seek to impose rules and codes of conduct on practices that further these interests or values. This is a common, and often laudable, occurrence in discussions of cyberspace. Our very simple point is that these preferred principles and proposed rules *are not norms.* They are normative aspirations. Norms by definition are widely accepted and internalised by the members of a particular community. As such, they cannot be simply implemented or imposed. Rules might be imposed, norms cannot be. This is more than a mere semantic objection. The assumption that norms are things that can be imposed misses the crucial point that their power lies in the way they inform behaviour because agents have internalised their prescriptive and evaluative force. This conflation of norms with what are merely proposed rules and normative aspirations also overlooks potentially valuable strategies that might be adopted in fostering or cultivating norms, a point that we will return to in the conclusion.

4.2 'Quasi-Norms' as Imported Rules and Principles

Another context in which quasi-norms frequently appear in discussions of cyberspace is when attempts are made to import settled norms *from other realms* (in other words, norms that have evolved in the context of distinct practices) based on comparisons of the two realms. Our position here is that the comparisons themselves are understandable, and sometimes valuable, but that norms are not things that can logically be imported in this way.

It is often the case that analogies are drawn between relatively new and unfamiliar practices in cyberspace and those practices with which we are more acquainted. Indeed, a common, and frequently useful way to conceptualise a new phenomenon is through metaphor, invoking something that is already known in

37 We discovered subsequently that this is also a term used to describe a completely different phenomenon in algebra. Our focus, of course, is on ostensible 'norms' in international relations that do not, in fact, possess what we have argued are their defining characteristics.

order to come to grips with novelty. There are many examples of this strategy in relation to how cyberspace is represented and analysed. In the late 1980s, metaphors of transport infrastructure were common (the 'information superhighway', 'online traffic'). Metaphors from the health sector still shape the way we talk about cyber security ('viruses', 'infections', 'computer hygiene'). And, of course, some look for ways that language generally used to describe kinetic conflict can be invoked to help explain the daunting new reality of global cyber insecurity ('cyber war',[38] 'cyber deterrence',[39] 'cyber arms race'[40]). Yet, there is a danger to this strategy if we extend it to the attempt to uncover norms for cyberspace.

Practices in cyberspace do not simply map onto the very different practices from which these often-useful metaphors are drawn. This might seem a fairly straightforward point, yet the temptation to equate cyber practices with practices in other realms in the attempt to appropriate already-established, well-understood and influential standards of right and wrong conduct is strong enough to make it worth emphasising. For example, in some cases in which tropes and images from conventional warfare are borrowed in the attempt to make sense of cyber as an offensive tool, the logical next step is seen to be to appropriate the established (and often institutionalised) principles and codes of conduct from this purportedly analogous realm and transfer them to the cyber domain. A prominent example of this can be found in proposals to take principles from the just war tradition – principles which have evolved over centuries, if not millennia, in the context of practices that are very different to those of the cyber domain – and apply them to so-called cyber warfare.[41]

Attempts to relate a particular cyber practice under scrutiny to another, ostensibly similar, practice for which norms are already 'settled' are potentially valuable in terms of employing metaphors as heuristic tools to illustrate and interrogate specific features of the practice – and necessarily risky if the practices are conflated in the hope of thereby 'discovering' cyber-norms. If norms in international relations are understood to emerge, evolve, and be interpreted in the context of particular practices, they cannot be imported from one practice to another without risking significant loss of meaning and moral force.[42]

38 Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010); John Arquilla and David F. Rondfeldt, eds., *Networks and Netwars: The Future of Terror, Crime and Militancy* (Santa Monica, CA: RAND Corporation, 2001). Thomas Rid critiques the term in *Cyber War Will Not Take Place*, 1st edn (Oxford University Press, 2013).

39 Gary F. Wheatley and Richard E. Hayes, *Information Warfare and Deterrence* (Washington D.C.: National Defense University Press, 1996). Also Jason Ma, 'Information Operations to Play a Major Role in Deterrence Posture,' *Inside Missile Defense*, December 10, 2003.

40 Quote from US Cyber Command Director of Intelligence Samuel Cox, 'From our perspective, what we're looking at is a global cyber arms race [that] is not proceeding as a leisurely or even linear fashion but is, in fact, accelerating.' Cheryl Pellerin, 'DOD Expands International Cyber Cooperation, Official Says,' *American Forces Press Service*, April 10, 2012, http://archive.defense.gov/news/newsarticle.aspx?id=67889.

41 For such proposals to import just war norms and apply them to cyberspace, see, for example: Mariarosaria Taddeo, 'An Analysis For A Just Cyber Warfare,' in *2012 4th International Conference on Cyber Conflict,* ed. Christian Czosseck, et al. (Tallinn: NATO CCD COE Publications, 2012) and Luciano Floridi and Mariarosaria Taddeo, eds., *The Ethics of Information Warfare* (Switzerland: Springer, 2014).

42 Our criticism of attempts to 'import' norms from one practice to another – and thereby uproot them from the value systems in which they are embedded and the context in which they have been negotiated over time – is not directed at the process of 'grafting' that some mainstream constructivists, such as Richard Price, describe as a potentially effective means of norm promotion. See Richard Price, 'Reversing the Gun Sights: Transnational Civil Society Targets Land Mines,' *International Organization,* 52 (1998): 627-631. Understood as *part of the process of persuasion* undertaken by so-called norm entrepreneurs (which is how Price presents it), rather than as an attempt to simply implement or impose norms based on their acceptance in other realms, 'grafting' need not lead to quasi-norms.

In sum, unlike what we have labelled 'quasi-norms', norms evolve over time through necessarily complex and messy processes of contestation and negotiation in the context of the practices to which they are understood to apply. They can neither be imposed on a particular practice nor imported from one to another – although both moves might become tempting in the face of the obstacles outlined in the previous section and an accompanying impatience with the current stage of norm development in cyberspace. Nevertheless, despite the obstacles to both their emergence and interpretation, and what we have identified as the trap of appealing to 'quasi-norms', it *is* possible to uncover principles that have begun to qualify as norms. This can be done through the process of interpretation set out above.

5. Beyond Quasi-Norms in Cyberspace: The Norm of De-Territorialised Data

There are a number of frequently propounded principles and emerging codes of conduct in cyberspace that have at least begun to display the defining features of norms as we have identified them in this chapter. These include respective prohibitions against attacking critical infrastructure and against exerting sovereign control over digital information. The challenges that we articulated in section 3 render the process of these principles being established as norms extremely complex and multifaceted, and, relatedly, the task of attempting to interpret them as such particularly demanding. These principles are, after all, each articulated in relation to a new and rapidly-changing practice, each embedded in a system of values that is necessarily in flux and encounters challenges, and each associated with a fluid and often difficult-to-define constituency of agents. Determining whether each is a 'quasi-norm', proposed by particular agents, but lacking the defining features of norms, or, alternatively, has begun to display these defining features, is an important and daunting undertaking. We have suggested that such a problem might be addressed through a careful process of analysing explanations and evaluations of the principle's contravention by a broad cross-section of the agents who participate in the relevant practices. Although a comprehensive study of either one of these two principles would take us well beyond the scope of this chapter, in this section we will highlight examples of the types of judgements and justifications that would contribute to identifying a norm in such a study. Specifically, we will focus on the second of the two principles: namely, the prohibition against exerting sovereign control over digital information.

5.1 Underlying Values, Organic Processes of Evolving 'Shared Understandings', and 'Norm Entrepreneurs'

The expectation that data should be 'de-territorialised' emerged quite early in the development of Internet technology. It came about as a consequence of both conscious promotion by what Finnemore and Sikkink call 'norm entrepreneurs' (in this case, the US government) and the unintended, organic process (which we highlighted in section 1) of customs, mores and shared understandings being established over time between participants in a common practice. During the formative years of the development of Internet technology, an ideal of the world as open and connected through trade and the promotion of democracy and human rights was articulated by the Clinton-Gore administration. They framed these ideas as not only 'America's core values' but values with universal appeal.[43] Indeed, in a 1994 speech to the UN, US Vice President Al Gore described the Internet as 'a metaphor for democracy itself',[44] and suggested that '… as members of the same … vast, increasingly interconnected human family … we will derive robust and sustainable economic progress, strong democracies, … and, ultimately, a greater sense of shared stewardship of our small planet'.[45] In short, the free movement of data was explicitly associated with a proposed cosmopolitan ethos.

This approach was premised on an understanding of the universal nature of specific values including freedom of speech and freedom to access information. Importantly, this resonated strongly with the values of the technical community that was at the forefront of developing Internet technology.[46] This community placed a high premium on inter-operability, consensus-based decision making, and freedom to innovate exemplified in John Perry Barlow's 1996 *Declaration of the Independence of Cyberspace*.[47] The values of openness, freedom of information and minimal regulation over information flows became embedded in a broad global approach to Internet technology that passionately rejected the imposition of sovereign control over digital information.

These values have been reflected in statements by prominent political leaders. Indeed, the view of the global benefits of 'de-territorialised' digital information is routinely reinforced, often through the use of quite striking images. In one of her landmark speeches about Internet Freedom, Hillary Clinton referred to the Internet as 'a new nervous system for our planet' which implied indivisibility, interdependence and a united purpose.[48] She also made reference to the geopolitics of the Cold

43 Anthony Lake, 'From Containment to Enlargement' (Speech before the Johns Hopkins University School of Advanced International Studies, Washington, D.C., 21 September 1993, https://www.mtholyoke.edu/acad/intrel/lakedoc.html); and Warren Christopher, 'Building Peace in the Middle East' (Speech at Columbia University, 20 September 1993).

44 He uses the term 'global information infrastructure' at this point. Albert Gore Jr., 'Information Superhighways' (Speech before the International Telecommunications Union, 21 March 1994), http://vlib.iue.it/history/internet/algorespeech.htm.

45 Ibid.

46 Madeline Carr, *US Power and the Internet in International Relations: The Irony of the Information Age*.

47 John Perry Barlow, 'A Declaration of the Independence of Cyberspace' (Davos, Switzerland, 8 February 1996), https://projects.eff.org/~barlow/Declaration-Final.html.

48 Hillary Rodham Clinton, U.S. Department of State, *Remarks on Internet Freedom* (Washington D.C., 2010), http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

War by suggesting that 'a new information curtain is descending across much of the world' and '[s]ome countries have erected electronic barriers that prevent their people from accessing portions of the world's networks'.[49] The perceived imperative to prevent sovereign control over digital information is also framed as a global struggle in which each actor, state or non-state, must play a part. Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda, urged delegates at the 2014 United Nations Internet Governance Forum to 'deliver what is needed to keep the internet open, unfragmented, and reliable. The time is now to ensure it develops further as a global source of empowerment, innovation and creativity for all'.[50] Kroes evoked arguably universal values by suggesting that the Internet is not 'just a technology' but also 'the new frontier of freedom and a new tool to exercise this freedom'.[51]

Interestingly, similar positive affirmations have issued from China despite that state's preference for a sovereign conception of cyberspace. President Xi Jinping delivered the keynote address to the second World Internet Conference in December 2015. In his speech, he emphasised that 'the Internet is a common space for mankind, and all countries should jointly build a community of shared destiny in cyberspace'.[52] He also called for all states to 'jointly foster a peaceful, secure, open and cooperative cyberspace and build a multilateral, democratic and transparent global Internet governance system'. [53]

Of course, even a principle that meshes with existing, underlying values, is actively backed by 'norm entrepreneurs', and also appears to have evolved organically through shared understandings between participants in transnational practices need not constitute a norm. At the very least, it represents a quasi-norm, or a normative aspiration. More work is required to establish that it meets the criteria to qualify as a norm.

5.2 Evidence of a Norm? Justifications and Judgements of Its Violation

In what follows, we will draw on the insights that we have taken from IR regarding both the nature of norms and the process of interpreting them in order to present evidence of what we call *the norm of de-territorialised data*. According to this principle, data in cyberspace should not be differentiated according to sovereign borders, but should, rather, be presented as a universal experience regardless of geography. In providing a preliminary case for the existence of this norm, we will demonstrate that this principle meets the two defining criteria outlined above; namely, it is: 1) understood to have prescriptive and evaluative force; and

49 Ibid.
50 Neelie Kroes, 'Defending the Open Internet' (European Commission, Opening ceremony of the Internet Governance Forum, Istanbul, 2 September 2014), http://europa.eu/rapid/press-release_SPEECH-14-576_en.htm.
51 Neelie Kroes, 'Protecting a Free Media in Azerbaijan' (European Commission, Speech at the Internet Governance Forum, Baku, 7 November 2012), http://europa.eu/rapid/press-release_SPEECH-12-784_en.htm.
52 Xi Jinping, Keynote Speech (Opening Ceremony of Second World Internet Conference, Wuzhen, 16 December 2015). Summary in English on the Chinese Embassy of the UK website, http://www.chinese-embassy.org.uk/eng/zgyw/t1325603.htm.
53 Ibid.

2) widely accepted and internalised by the members of the community of state and non-state actors who participate in a range of practices related to the flow of digital information. Specifically, we will suggest that a perceived prohibition against exerting sovereign control over digital information is discernible in actors' justifications and judgements of practices such as controlling online content (censorship), limiting access to certain online services, and, increasingly, seeking to exercise sovereign control over the physical location of stored data and the physical infrastructure of the Internet.

In 2011, the response to the introduction of the *International Code of Conduct for Information Security* put forward to the UN by China, Russia, Tajikistan and Uzbekistan, revealed a strong perception that any violation of the principle that digital information is borderless demands a justification. The Code called for compliance in cyberspace with 'universally recognised norms [including] the sovereignty, territorial integrity and political independence of all states'.[54] This was necessary, the document suggested, in part as a consequence of the extent to which online data 'undermines other nations' political, economic and social stability, as well as their spiritual and cultural environment'. This was met with approbation in the US with Jason Healey referring to this passage specifically as 'standard boiler plate from autocratic countries to limit freedom of expression'.[55] Michele Markoff, the US State Department's Senior Policy Adviser on Cyber Affairs, also described the Code as an attempt by the proposing states to 'justify the establishment of sovereign government control over Internet resources and over freedom of expression in order to maintain the security of their state'.[56]

This perceived need to justify sovereign control is significant. With reference to Frost's work, we have argued that establishing the existence of a norm does not require demonstrating that a principle is universally adhered to. (Indeed, if this were the qualifying criterion, it would be impossible to defend the existence of *any* international norms.) Rather, a principle is tacitly acknowledged as a norm when there is a perceived imperative to justify or deny its violation. Or, as Richard Price, a mainstream constructivist scholar, argues following a similar logic, 'one can say that a norm exists when the dominant discourse shifts in such a way that puts opponents on the defensive'.[57]

China recently demonstrated this perceived need to account for deviating from the principle of de-territorialised data. In the same speech before the World Internet Conference in which he commended the concept of a global commons in

54 United Nations, General Assembly, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, A/66/359 (14 September 2011), https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf.

55 Jason Healey was the Director for Cyber Infrastructure Protection at the White House under President George W. Bush. At the time of these comments, he was Director of the Cyber Statecraft Initiative at the Atlantic Council. Jason Healey, 'Breakthrough or Just Broken? China and Russia's UNGA Proposal on Cyber Norms,' *The Atlantic Council Blog*, September 21, 2011, http://www.atlanticcouncil.org/blogs/new-atlanticist/breakthrough-or-just-broken-china-and-russia-s-unga-proposal-on-cyber-norms.

56 Gerry Smith, 'State Department Official Accuses Russia and China of Seeking Greater Internet Control,' *Huffington Post*, September 28, 2011, http://www.huffingtonpost.com/2011/09/27/russia-china-internet-control_n_984223.html.

57 Price, 'Reversing the Gun Sights: Transnational Civil Society Targets Land Mines,' 631.

cyberspace, President Xi engaged with a different conception of freedom to that used by Neelie Kroes. He linked freedom to order by saying that 'order is the guarantee of freedom' and therefore, it is necessary to respect sovereign law in cyberspace 'as it will help protect the legitimate rights and interests of all internet users'.[58] In a similar effort to justify exercising domestic law (and thereby infringing the norm of de-territorialised data), US Senator Patrick Leahy made the following comments when introducing a bill designed to prevent 'foreign-owned and operated' websites from facilitating intellectual property theft: 'We cannot excuse the behaviour because it happens online and the owners operate overseas. The Internet needs to be free – not lawless'.[59] This tension between the desire to apply domestic law to digital information that does not remain tethered by geography and the promotion of an online experience that transcends territorial borders is a common framework within which justifications for imposing sovereign control are put forward. What is important here is not exactly *how* these actors account for their failure to adhere to the principle of de-territorialised data, but the perceived need to do so.

National security is increasingly provided as justification for imposing sovereign control on digital information. Again, the perceived imperative to justify this action is revealing. In November 2015, days after the terrorist attacks in Paris (and making explicit reference to them), UK Chancellor George Osborne defended the passage of the Investigatory Powers Bill (otherwise known in the UK as the 'Snoopers' Charter') by arguing that 'when the internet was first created, it was built on trust. That trust, appropriate inside a community of scholars, is not merited in a world with hostile powers, criminals and terrorists'. In other words, the prohibition against exerting sovereign control over data is tacitly acknowledged in the argument that it must be overridden due to what is presented as an extreme, dangerous security situation. (This is analogous to 'supreme emergency' arguments in Walzer's account of the war convention.)[60] Indeed, Osborne goes on to link the vulnerabilities of UK critical infrastructure with concerns that 'ISIL's murderous brutality has a strong digital element'. Consequently, he argues, '[o]nly government can defend against the most sophisticated threats, using its sovereign capability. And that's exactly what we will do'.[61] Extreme threats to security are invoked as rationales for violating the prohibition against sovereign control over digital information.

The Snowden revelations in 2013 have also been employed as justification by many states for bringing digital information more firmly under sovereign control.[62]

58 Xi, keynote speech at the Second World Internet Conference, 2015.

59 Patrick Leahy, 'Senate Judiciary Committee Advances Bipartisan Bill to Combat Copyright Infringement and Counterfeits,' November 18, 2010, http://www.leahy.senate.gov/press/senate-judiciary-committee-advances-bipartisan-bill-to-combat-copyright-infringement-and-counterfeits.

60 See the discussion of tacitly acknowledging norms through such 'supreme emergency' justifications of their violation in Erskine, *Embedded Cosmopolitanism*, 189, 194. For Walzer's original 'supreme emergency' argument, see Walzer, *Just and Unjust Wars,* 251-268.

61 George Osborne, 'Chancellor's Speech to GCHQ on Cyber Security' (Delivered at Government Communications Headquarters, Cheltenham, 17 November 2015), https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.

62 Jonah Force Hill, 'The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders,' *The Hague Institute for Global Justice, Conference on the Future of Cyber Governance*, May 1, 2014, http://ssrn.com/abstract=2430275.105.

In 2015, citing the potential for human rights abuses, the EU revoked the Safe Harbour Act which had allowed the personal data of EU citizens to be stored in the US.[63] The EU Commissioner responsible for data protection, Věra Jourová, pointed out that this was not simply a matter for the US, but that it applied to 'the conditions to transfer data to third countries, whatever they may be'.[64] This 're-territorialisation' of digital information has also been extended to the physical infrastructure across which data travels. Having previously called the Internet a 'CIA project' and following what he regarded as biased reporting in the western media of the conflict in Crimea, Russian President Vladimir Putin announced plans to develop the capacity to segregate Russian cyberspace in case of '*emergencies*'. The proposal would potentially bring the .ru domain under state control, which Russian newspapers reported would strengthen Russia's sovereignty in cyberspace.[65] Presidential aide and former Minister of Communications and Mass Media, Igor Shchegolev, explained that this had become necessary due to the unpredictability of western politicians and businesses.[66] He linked the Russian state's concerns to the Internet outage experienced by Syria in 2012, which some attribute to the US. Again, what is particularly noteworthy in these cases of statements by both the EU and Russian political leaders is the perceived imperative to explain any deviation from the principle of de-territorialised data.

This brief analysis does a number of important things. First, it demonstrates that the prohibition against exerting sovereign control over digital information at least begins to meet our two qualifying criteria of a norm. The norm of de-territorialised data is not without challenges, but both its prescriptive force and wide acceptance and internalisation amongst participants in transnational practices related to the digital flow of information are evident in the pervasive perceived need to justify its violation. Second, in providing evidence for this norm of de-territorialised data, this case illustrates how norms might be interpreted in cyberspace through detailed attention to the way that states and other agents variously justify and rationalise their own actions and judge the actions of others. The task of interpreting cyberspace's normative terrain cannot rely on superficial observations of agents' conduct. Third, this analysis reiterates significant features of our account of norms, inspired by prominent positions in IR: that norms are firmly embedded in broader systems of values; that both deliberate attempts to foster, shape and institutionalise principles in particular forms *and* organic, unplanned processes of negotiation and contestation in the context of evolving, shared practices contribute to the emergence of norms; and that norms, carefully interpreted, are distinct from, and can be invoked

63 This was initiated through a court case brought by Max Schrems who highlighted the flaws in the Safe Harbour Act with respect to Facebook. Europe v Facebook, http://europe-v-facebook.org/EN/en.html.

64 Věra Jourová, 'Commissioner Jourová's Remarks on Safe Harbour EU Court of Justice Judgement before the Committee on Civil Liberties, Justice and Home Affairs' (European Commission, Speech before the Committee on Civil Liberties, Justice and Home Affairs, Strasbourg, 26 October 2015), http://europa.eu/rapid/press-release_SPEECH-15-5916_en.htm.

65 Luke Harding, 'Putin Considers Plan to Unplug Russia from the Internet "in an emergency"', *The Guardian*, September 19, 2014, http://www.theguardian.com/world/2014/sep/19/vladimir-putin-plan-unplug-russia-internet-emergency-kremlin-moscow.

66 '"Unpredictable West" Could Isolate Russian Internet, Putin's Aide Warns,' *RT*, October 17, 2014, https://www.rt.com/politics/196848-russia-internet-west-plan/.

to challenge, espoused principles and prevailing policies when these are at odds with a community's deeper commitments and tacitly acknowledged values.

6. Conclusion

Three quite different lessons can be drawn from our preliminary analysis, each of which points to areas of further study.

First, and at the level of *how* one might go about studying cyberspace's rapidly changing normative landscape, two areas of scholarship within the discipline of IR – normative IR theory and mainstream constructivism – have produced rich and diverse bodies of work on the nature of norms in international relations that together provide an invaluable starting-point. The combined insights of both approaches offer a nuanced conceptual understanding of norms and an account of how they might be deciphered in a challenging context such as cyberspace. Notably, these two approaches to norms have developed largely independently of each other (a curious and all-too-common occurrence when it comes to different 'camps' within the discipline of IR).[67] Further work on the points of commonality and divergence between normative IR theory and mainstream constructivist approaches to norms in international relations has the potential to refine and bolster the arguments of each – and to contribute to sophisticated analyses of emerging norms in cyberspace.

Second, and related to the ambitious attempts to 'cultivate' and 'promote' norms in cyberspace noted above, the chapter repeatedly gestures towards a crucial caveat. For norm promotion to be effective it is not only proposed principles or codes of conduct that must be the objects of such efforts. Rather, the broader systems of underlying values in which norms necessarily emerge and are embedded must also be the focus of analysis, and possibly persuasion, negotiation and concerted attempts at revision over time. Neglect of the complex context in which international norms must be situated leads to the promotion of quasi-norms, which may be clear statements of preferred principles on the part of certain actors, but lack the prescriptive force and collective acceptance that make norms so powerful in international relations. Attempts might be made to cultivate or revise norms, but the success of such endeavours depends on whether they are consistent with (and cognisant of) the broader systems of meaning and values already accepted – and always contested and open to re-negotiation – by the members of a particular community.

Third, the chapter suggests that interpreting existing norms in cyberspace – such as the proposed norm of de-territorialised data – might yield results that are,

67 For accounts of the costs of the discipline's division into competing theoretical and methodological 'camps' see David A. Lake, 'Why "Isms" Are Evil: Theory, Epistemology, and Academic Sects as Impediments to Understanding Progress', *International Studies Quarterly* 55 (2011): 465-80 and Erskine, 'Whose Progress? Which morals?', 449.

perhaps surprisingly, out of step with normative change in other realms of international relations. Our brief analysis above uncovers an established cosmopolitan norm in cyberspace that eschews sovereign jurisdiction and political borders. The study also suggests that this norm of de-territorialised data is facing a new emerging norm in cyberspace: one that we might call the *norm of sovereign control over data.* In other words, the norm of de-territorialised data is already in the process of being challenged, and perhaps eclipsed, by a competing norm.[68] Notably, this apparently emerging opposing norm is, in fact, one that seems to map closely onto the long-established norms in international relations of state sovereignty and territorial integrity – norms that have recently been challenged by the emerging cosmopolitan norm of humanitarian intervention in response to mass atrocity. In short, the normative change that we have begun to uncover in cyberspace seems to be the reverse of what has been occurring in the context of the recent endorsement and institutionalisation of the proposed 'responsibility to protect' and its accompanying claim of contingent sovereignty. These very different patterns of normative change warrant further attention – as does the fascinating case of competing norms regarding the jurisdiction of data in cyberspace.

International norms in cyberspace are the product of, *inter alia*, negotiation and contestation over time in the context of evolving transnational practices, accompanying shifts in dynamic, underlying value systems that variously conflict and overlap, political compromise between multiple national and private interests, pragmatic agreements, serendipitous convergences, attempts at carrot-and-stick persuasion by the most powerful actors, and the socialisation of these same powerful agents. In short, they are the product of both chance and design, cooperation and conflict, emerging collective identities and changing conceptions of self-interest. The important point that we have tried to highlight is that we need to understand where we currently are in terms of expectations, values and perceived constraints in cyberspace in order to navigate – and perhaps even attempt to shape or radically revise – the complex normative terrain. This, in turn, requires a sophisticated understanding of both the concept of norms and how they operate in cyberspace.

68 The changing constitution of the community within which norms regarding the jurisdiction of data have been negotiated seems relevant to us – and demands further attention. There was certainly a concerted effort by the US government to promote values of free movement of data, but there had also been a more organic process on the part of the (transnational) technical community, for whom these values had been firmly established and informed the early development of the Internet. The values of the technical community happened to synergise with US policy in the context of the norm of de-territorialised data and served to reinforce it. However, as this issue of data jurisdiction has shifted from the transnational technical community to state leaders in international political negotiations, arguably competing value systems have become more prominent.