Military Cyber Affairs

Volume 3 | Issue 1 Article 2

2018

Cyber Futures and the Justice Motive: Avoiding Pyrrhic Victory

Mark Raymond
University of Oklahoma, mraymond@ou.edu

Cyber Futures and the Justice Motive: Avoiding Pyrrhic Victory

Cover Page Footnote

The author acknowledges the support of the Cyber Governance and Policy Center at the University of Oklahoma, as well as the Carnegie Corporation of New York and the School of International and Public Affairs at Columbia University.

Cyber Futures and the Justice Motive: Avoiding Pyrrhic Victory[1]

Mark Raymond[2]

Abstract: Evaluating, and choosing between, possible cyber futures requires making collective decisions about values. Tradeoffs exist in the design of any governance arrangement for information and communications technologies (ICTs). At minimum, policymakers will be required to choose between governance arrangements that optimize for speed and scale on the one hand, and those that optimize for diversity and decentralization on the other. As in any other political domain, every eventual outcome will create winners and losers, at least in relative terms. Actors dissatisfied with outcomes may perceive a discrepancy between entitlements and benefits. In some such cases, they will act on this justice motive. Existing research on justice as a motive for human behavior suggests that cases of conflict where one party is driven primarily by a justice motive may be associated both with intractable conflict, and with conflict characterized by lack of restraint. In the cyber domain, these kinds of conflicts will be most costly to advanced industrial democracies most dependent on ICTs. Pressing the first mover advantage in the digital domain is likely to foster resentment that will have negative consequences for the global cyber regime complex, and perhaps also for the rules and institutions of the international system writ large. Rule-making efforts in the ongoing process of global cyber regime complex formation should proceed in a deliberate manner and accept partial, voluntarist outcomes less likely to create highly dissatisfied parties. The article describes basic value tradeoffs associated with different cyber futures, reviews the literature on justice as a motive for human behavior, and outlines its implications for the future of the cyber domain. It ultimately concludes that the most likely outcome is that the United States will find itself in an increasingly isolated position.

[1] Please cite as: Raymond, Mark, "Cyber Futures and the Justice Motive: Avoiding Pyrrhic Victory," in Demchak, Chris and Benjamin Schechter, eds. *Military Cyber Affairs: Cyber, Economics, and National Security* 3, no. 1 (2018).

[2] Wick Cary Assistant Professor of International Security and Director of Cyber Governance and Policy Center, University of Oklahoma

Evaluating, and choosing between, possible cyber futures requires making collective decisions about values. Tradeoffs exist in the design of any governance arrangement for information and communications technologies (ICTs). At the broadest level, we will often be in the position of choosing between governance arrangements that optimize for speed and scale on the one hand, and those that optimize for diversity and decentralization on the other. This is because governance arrangements most conducive to speed and scale in the cyber domain typically require high levels of standardization and broad jurisdictional scope that can make it difficult to allow the implementation of policies designed to satisfy particularistic values with respect to various kinds of objectionable conduct or divergent expectations about security and privacy.

As in any other political domain, every eventual outcome will create winners and losers, at least in relative terms. Some actors are likely to feel that whatever governance arrangements result do not sufficiently instantiate their values and/or advance their interests. Actors dissatisfied with the outcome may perceive a discrepancy between entitlements and benefits, i.e., a perceived lack of 'justice'. In some such cases, dissatisfied actors will pursue this justice motive, independent of whether their perceptions are accurate. There are good reasons to suspect that cases of conflict where at least one party is driven primarily by a justice motive may be associated both with intractable conflict, and with conflict characterized by lack of restraint. In the cyber domain, these kinds of conflicts will be most costly to advanced industrial democracies that (as early adopters) tend to be most dependent on ICTs. Accordingly, it is vital that governments, firms and citizens of advanced industrial democracies take the long view.

Pressing the first mover advantage in the digital domain is likely to foster resentment that will have negative consequences both for the global cyber regime complex, and perhaps also for the rules and institutions of the international system writ large. Accordingly, rule-making efforts in the ongoing process of global cyber regime complex formation should proceed in a deliberate manner and should accept partial, voluntarist outcomes less likely to create highly dissatisfied parties.

The article proceeds in three parts. The first describes basic value tradeoffs associated with different cyber futures. The second reviews the literature on justice as a motive for human behavior, and assesses the extent to which the justice motive may be present in the cyber domain.

The article concludes by outlining the implications of justice-seeking behavior for the future of the cyber domain.

Cyber Futures and Value Tradeoffs

Cyber futures are a product of technological developments and social responses to such breakthroughs (Ruggie 1975, p. 558). Accordingly, analysis of governance and institutions is essential to projecting the future trajectory of the cyber domain. In this section, I briefly characterize existing governance arrangements as well as three potential cyber futures, and discuss some major value tradeoffs at stake in these various possible alternative futures. Governance arrangements in the cyber domain remain highly privatized, and highly decentralized (Raymond 2013/14; Raymond and DeNardis 2015; Raymond 2016). However, these governance arrangements are also rapidly evolving, and are doing so in ways characterized by considerable political contention (Nye 2014; Bradshaw et al. 2015). The outcome of these processes of institutional evolution is not certain, and such outcomes are in any event only ever provisional (March and Olsen 1998). To cope with these kinds of analytical challenges, political scientists have developed scenario-based forecasting techniques that explicitly contemplate multiple possible outcomes and attempt to identify the critical causal factors most essential to determining which path is ultimately taken (Bernstein et al. 2000; Barma et al. 2016).

One effort to develop scenarios for the future of the cyber domain has proposed three most-likely outcomes: the cyber status quo; cyber Westphalia; and a system of cybered alliances, spheres and independents, or CASI (Demchak 2017, this issue). Continuation of the status quo entails Western leadership and reliance on privatized governance, largely through legacy Internet governance modalities. In this scenario, cyberspace will remain relatively open and insecure. Institutional evolution is likely to be driven by ongoing tensions between privacy, security and profit. The cyber Westphalia scenario is characterized by the increasing determination of states to exert authority and jurisdiction over the digital domain that is becoming vital to every area of human life. In this scenario, states mutually agree that national jurisdiction applies online but, at least for the foreseeable future, generally lack significant enforcement capacity. States are in principle held accountable for actions that violate the sovereignty of other states, but only the most advanced states have any significant ability to impose costs on violators. National cyber policies

are expected to proliferate via emulation, and take forms similar to other kinds of safety regulations. Larger states may be able to require and enforce data localization and supply chain rules on firms as conditions of market access. The final scenario, CASI, adopts the primary expectations of the cyber Westphalia scenario, but additionally expects that states will either immediately or over time arrive at the conclusion that purely national approaches are not viable. In response, the expectation is that states will tend to join blocs led by the largest cyber powers (the US, China and perhaps Russia) on the basis of a combination of similar values, historical ties and geographic contiguity. Blocs will share technological filters and controls, systems for R&D and procurement, and incident response strategies.

These scenarios collectively provide useful guidance in thinking about, and preparing for, future trends in the cyber domain. While it is not my purpose in this article to evaluate the relative plausibility of these scenarios, it is worth nothing that there are important signs that elements of the cyber Westphalian and CASI scenarios are already being incorporated into the status quo. National cyber policies and military cyber commands are already proliferating (Finnemore and Hollis 2016, p. 435). The Group of Governmental Experts (GGE) on cybersecurity sponsored by the First Committee of the United Nations General Assembly has also issued a unanimous report expressing the opinion that existing international law applies to state military use of ICTs (UNGA 2013, A/68/98). This report is noteworthy, as the GGE included representatives from all of the permanent members of the Security Council, and because the report explicitly affirmed the applicability of the UN Charter – and therefore its protections for state sovereignty – in this context. A critical group of states has therefore explicitly endorsed the fundamental pillar of Demchak's second and third scenarios. Finally, efforts by major cyber powers to build multilateral groupings to promote preferred institutional arrangements for cyber governance have been observed in various contexts (Maurer 2011; Tikk-Ringas 2012; Raymond and Smith 2014). However, despite these developments, the legacy Internet governance regime that relies heavily on private and multistakeholder governance modalities is unlikely to vanish in the foreseeable future, if only because of the path-dependent, evolutionary nature of institutional development in the international system (Keohane 1984; March and Olsen 1998; Wendt 2001).

In the short to medium-term, it is likely that no single scenario will predominate and that elements of all three will coexist. Crucially, value tradeoffs are unavoidable no matter the overall future of the cyber domain. In some ways, in fact, the different scenarios Demchak outlines

represent *outcomes* of choices about value tradeoffs, even if such choices about institutional design are rarely made all at once or in a conscious manner (March and Olsen 1998; Wendt 2001). The most fundamental such tradeoff is between social and technological arrangements that optimize for speed and scale, on the one hand, and arrangements that optimize for diversity and decentralization on the other. Both the cyber Westphalia and CASI scenarios are likely to compromise the speed and scale of global connectivity, in order to allow political authorities to exert greater local control over information flows. Different political communities will employ this local control to achieve different substantive ends, reflecting both their distinctive cultures and the relative strengths of various players in domestic and/or bloc politics. Authoritarian regimes that prioritize regime stability will exercise sovereignty in a different manner than genuinely competitive democracies; but distinctive varieties of capitalism (Hall and Soskice 2001) in Europe, Asia and the Anglosphere will also generate different ways of balancing various public goods including national security, individual privacy and other rights, and economic competitiveness. Such differences are already evident in approaches to digital trade issues (Aaronson 2012), competition policy in the digital domain (Haucap and Stühmeier 2016), and issues of privacy such as the 'right to be forgotten' (Newman 2015).

This patchwork landscape will entail opportunity costs in terms of the economic and social benefits of global communication flows, but it is important to remember that these costs are the price of securing other socially valued goods, even if there is no guarantee either that the price paid will be minimized, or that the collective political process of deciding what price to pay for which other values is reasonable or fair. Value tradeoffs are unavoidable even if security is held to be a 'prime value' that must be secured before all others (Baldwin 1997, p. 18-19). This is because security is empty of content without a clear understanding of who, or what, is being secured – and of what kind of security is being provided to a specific valued referent object.

The fundamental question of who gets what must still be answered, and different kinds of stakeholders have very different positions. The technical community, for example, has strenuously sought to make the case that common approaches to ensuring *national* security in a digital world may actually undermine the security of computer *networks* and the data that resides on them (Abelson et al. 2015). Perhaps the most important point is that no actor will get all of what it wants, for the simple reason that achieving some ends (and attaining some values) can *only* be done at the expense of others. Further, it is almost certain that any outcome will result in actors who feel, to

varying extents, that values important to them have been sacrificed on the altar of the values championed by members of other groups.

Every conceivable cyber future will have winners and losers, and will therefore have parties motivated by perceptions of injustice. Such actors are likely to be unresponsive to side-payments, negotiation, and even potentially to deterrence and compellence. They are also likely to fight harder and with less restraint than parties motivated by self-interest. *The extent to which actors are motivated by justice considerations should therefore be seen as a key driver of any potential shift from the cyber status quo to the cyber Westphalia or CASI scenarios.* Minimizing the prevalence and intensity of such motives is therefore essential to preserving governance arrangements that optimize for speed, scale and openness in the cyber domain, and more broadly to minimizing conflict and disruption. Accomplishing these objectives requires obtaining the best possible understanding of the justice motive. I turn to this task in the next section, before expanding on the policy implications of my argument in the final section of the article.

Taking the Justice Motive Seriously

Over the past twenty-five years, scholars of International Relations have significantly expanded their understanding of why actors do what they do, but we are still in the early stages of developing sophisticated and nuanced accounts of agency in world politics. In this section, I argue that taking justice seriously as a motive for human behavior advances the broader IR debate about logics of action by helping to account more fully for the ways actors respond to (real or perceived) violations of applicable standards of appropriateness, and also that there are good prima facie reasons to think that the justice motive plays an important role in the contemporary global politics of Internet governance and of cybersecurity.

The assumption that states could be adequately understood as rational actors motivated by maximization of self-interest was foundational to realist theory (Morgenthau 1948; Waltz 1979), and was later adopted by institutionalists who argued that neorealists exaggerated the difficulties associated with cooperation among rational egoists in conditions of anarchy (Keohane 1984; Oye 1986; Keohane and Martin 2003). This neo-utilitarian position (Ruggie 1998) was challenged by constructivists, who demonstrated that actors sometimes acted in accordance with norms and rules

out of sincere belief in their appropriateness (Wendt 1992; Finnemore and Sikkink 1998; March and Olsen 1998; Hurd 1999).

More recently, constructivists have moved beyond a dichotomy between the logic of consequences and the logic of appropriateness to demonstrate the operation of at least two other behavioral logics (or reasons for action) in world politics: the logic of habit (Hopf 2010) and the logic of practice (Adler and Pouliot 2011). While both are important contributions to understanding agency in world politics, they are of less relevance for understanding how actors that perceive threats to their interests and values from ongoing developments in the cyber domain are likely to react, and for that reason I largely leave them aside in the remainder of this article.

The nature of the relationship between the logics of consequences and appropriateness remains an open question. Some scholars have sought to portray the two as complementary, at least in some cases. Jepperson, Wendt and Katzenstein (1996, p. 68-72) argued that the logics of consequences and appropriateness could be found in various relationships running from competing explanations, to stage complementarity or nesting. Other constructivists have emphasized that actors are often strategic in their use of, and advocacy for, norms (Finnemore and Sikkink 1998), and that rules are crucial power resources (Onuf 1989; Barnett and Duvall 2005).

Constructivists most inclined to see rules and norms as ubiquitous and power-laden have also suggested that rules effectively subsume strategic interaction, since various specific forms of strategic interaction (e.g. bargaining and negotiation, deterrence, power-balancing, etc.) are mutually intelligible to actors only on the basis of intersubjectively-shared understandings of what counts as these behaviors and how they can be performed (Onuf 1989; Müller 2004; Adler and Pouliot 2011). There is no single or simple relationship between the various logics of action, and it is unhelpful to try and demonstrate the correctness or superiority of any particular logic (Barkin 2010, p. 57-58; Kornprobst 2011). Rather, my goal is to build on existing knowledge about the range of reasons for action in world politics, and to demonstrate the practical as well as scholarly value of taking seriously the idea that actors make choices motivated in important part by a desire to change or remedy situations at odds with their values. An outcome at odds with an actor's fundamental values is, by definition, one that contravenes the actor's understanding of applicable standards of appropriateness. Unfortunately, the norms literature provides limited guidance on how actors respond when they believe norms have been violated. One group of studies focused on how

norms are diffused (Finnemore and Sikkink 1998; Keck and Sikkink 1998; Acharya 2004) and changed (Sandholtz 2008), as well as how they decay and disappear (Bailey 2008; Panke and Petersohn 2012). Analytical emphasis has been on the norms themselves as the objects of analysis. Studies examining compliance with international norms have focused on whether, under what conditions, and for what reasons actors comply with norms (Chayes and Chayes 1993; Cortell and Davis 1996; Simmons 1998; Hurd 1999; Krebs and Jackson 2007). Only a smaller number of studies explicitly examine norm violation as a phenomenon. Shannon (2000) and Shannon and Keller (2007) seek to explain norm violation by examining the political psychology of leaders. While important, the study of norm violators' choices does not answer the separate question of how actors react to observed norm violations.

To the extent that we know how actors respond to norm violations by others, or to situations that contravene their ideas about standards of appropriateness more generally, the literature suggests we should see one of two broad kinds of responses. Wendt noted the possibility that predation in benign anarchies might play a role in the emergence of self-help systems, as other actors emulate "bad apples" (1992, p. 408409). This argument associates norm violation with norm decay or disappearance (Bailey 2008; Panke and Petersohn 2012) though it should not be conflated with the realist argument that norms are epiphenomenal (Mearsheimer 1994/95). In such cases, for constructivists, benign rules and norms are eventually replaced by nastier ones. The second possibility is that actors will respond by criticizing the violation to defend the norm. This kind of response is emphasized by scholars focusing on processes of contestation and argumentation in world politics (Crawford 2002; Müller 2004; Brunnée and Toope 2010), as well as by work documenting processes of stigmatization (Adler-Nissen 2014). Such processes are certainly both common and, in many cases, causally important in explaining international political outcomes. However, it is less clear why actors undertake such courses of action, and what else they might choose to do beyond criticizing the behavior or situations they see as inappropriate.

One possible answer to the first question is that actors might criticize inappropriate situations or behavior because it is in their interest to do so. Another is that they might do so because they understand themselves to be engaged in ongoing social practices of international politics (such as diplomacy and international law) that require socially competent performers to criticize inappropriate behavior by other players. These potential explanations correspond respectively to the logic of consequences and the logic of practice. A third possibility is that they

criticize because they believe it is the right, or appropriate, thing to do – that is, because the situation or behavior in question is unjust. To the extent that they do so, they act on what David Welch has called "the justice motive", which he defines as "the desire to correct a perceived discrepancy between entitlements and benefits" (1993, p. 19). As Welch notes, the presence or absence of the justice motive – or any other motive for criticism of norm violations – is an empirical question (2014, p. 413). For now, the key point is that the literatures on norms and on the justice motive have developed somewhat independently. Welch, for example, correctly points out that IR scholars have not fully appreciated the importance of the justice motive; however, his review of the justice motive literature (2014) neglects its clear connection to the constructivist literature on norms and the logic of appropriateness.

This mutual neglect is detrimental, because the literature on the justice motive offers empirical evidence about a range of other behaviors actors in world politics regularly undertake to rectify discrepancies between entitlements and benefits, both for themselves and for others. Welch's original study showed that in a range of a cases, the justice motive was of varying degrees of importance in explaining choices about war initiation (1993). Cecilia Albin has shown that considerations of both substantive and procedural justice are important in explaining the success or failure of international negotiations (2001) – that is, to explaining whether or not actors chose to accept or reject agreements. The empirical literature on justice as a reason for human behavior therefore offers significant value to the norms literature in more fully specifying the range of responses to inappropriate behavior and situations in world politics. Responses to inappropriate behavior or situations may, and often do, take the form of criticism, contestation and even stigmatization; but they may also encompass negotiation and even the use of political violence. Recognizing this contribution invites further research on the conditions under which actors choose various possible responses.

In addition to the more general importance of recognizing the justice motive literature as related to the norms literature, taking the justice motive seriously is of significant practical utility in dealing with contemporary global challenges in the cyber domain. Before addressing these benefits directly in the final section of this article, I first demonstrate that there are empirical grounds to think that the justice motive is present in this case. Doing so requires evidence that considerations of justice do, in fact, motivate actors' choices about issues in the cyber domain. Notably, it does not require showing that any particular conception of justice is correct, or that

actors agree on a conception of justice; this is because, "one need not answer the deeper philosophical questions about what is or is not just to understand the importance people attach to their own answers to these questions" (Welch 2014, p. 414). Evidence that justice considerations matter also need not be definitive, for two reasons. First, my argument is not that justice is the sole or even the predominant motive – only that it is present for some actors in some circumstances, even if alongside other motives. Second, while "it is indeed difficult to have extremely high confidence about motives in many cases," Welch correctly notes that "there are error bars around every interesting and important judgment in the social sciences, and we do not ordinarily – nor should we – give up as a result" (2014, p. 415). For a variety of reasons, when assessing motives, "typically the best we can do is arrive at a balance of plausibilities judgment with rough characterizations of the relative contributions of justice and other motives" (Welch 2014, 417). In doing so, a particularly valuable but underutilized source of evidence can be found in "signs that the unique sense of moral outrage triggered by the sense of injustice is, in fact, in play" (Welch 2014, p. 417).

At least four examples suggest instances in which actors have been motivated in significant part by considerations of justice with respect to prominent issues in the cyber domain. The first is a major 2011 address by Secretary of State Hillary Clinton on Internet freedom. The speech was explicitly framed in response to Internet shutdowns in Iran (2009) and Egypt (2011) intended to handicap political dissent. Clinton asserted that "it is our values that cause these stories to inspire or outrage us – our sense of human dignity, the rights that flow from it, and the principles grounded in it. And it is these values that ought to drive us to think about the road ahead" (Clinton 2011). This passage highlights two important features of the speech: its framing in terms of rights, which suggests the concern with the matching of entitlements and benefits characteristic of the justice motive, and the explicit connection of the question of rights with the future of the cyber domain. The speech expressed a universalist position on online rights, but sought to rebut a potential charge of naïveté by making a case both for the fundamental compatibility of various rights often portrayed as being in tension and for the instrumental value of respecting online rights. Clinton argued that with respect to the balance between liberty and security, "the challenge is finding the proper measure – enough security to enable our freedoms but not so much, or so little, as to endanger them." With respect to the instrumental value of online rights, she argued that imposing limits on online freedoms "entails a variety of costs – moral, political, and economic" (2011).

This expansive accounting method highlights the difficulty of identifying the justice motive, as the notion of 'moral costs' is an ambiguous one. Does such a phrase indicate a logic of consequences, or appropriateness? While acknowledging the complexity of political judgments (Kornprobst 2011), there are good reasons to allow for the possibility that American concern with justice expressed in the speech was both genuine and not entirely self-regarding. Clinton noted, for example, that "monitoring and responding to threats to Internet freedom has become part of the daily work of our diplomats" and that the US government "continues to help people in oppressive Internet environments", including by developing and disseminating multiple means of circumventing Internet controls. It is possible that such efforts are entirely self-serving, but showing that would require substantial empirical evidence. The more empirically likely possibility is that motives are substantially more complex.

The second and third examples of apparent concern with justice in the cyber domain deal with reaction by state and nonstate actors to the Snowden revelations. In a speech to the United Nations General Assembly, Brazilian President Dilma Rousseff called the activities of the American intelligence community "a breach of international law and an affront" to Brazilian sovereignty (Lynch 2013). She went on to argue that "without respect for sovereignty, there is no basis for proper relations among nations" (Lynch 2013). Contemporaneous media accounts indicated that Brazil filed a diplomatic protest with the Obama administration demanding an apology and a "guarantee that such acts will not be repeated" (Lynch 2013). These actions and statements reflect a sense of outrage and injustice, and are especially noteworthy given that few if any reports demonstrated appreciable costs imposed on Brazil by American intelligence collection efforts. Lodging protests they must reasonably have known would prove essentially ineffective in response to American actions that had not yet resulted in demonstrable concrete harm seems unusual from the perspective of rationalist approaches to IR theory, and more consistent with approaches that allow space for concern with justice in explaining human conduct. Even the potential rationalist fallback that Rousseff rationally sought to play to domestic and international audiences requires the heroic assumption that Brazil's leadership was somehow immune from the impulses that nevertheless motivated both Brazilian citizens and international observers. The hypocrisy evident in the Brazilian protests given the (smaller-scale) work of Brazil's own intelligence community does not in itself indicate that Rousseff's reaction was entirely cynical,

since people routinely show bias in evaluating the morality of their own conduct (Goldgeier and Tetlock 2001).

Brazil and other governments were not the only actors to respond with outrage to the Snowden revelations. Many in the Internet technical community were similarly motivated by a deep sense of injustice. These feelings were apparent at the November 2013 meeting of the Internet Engineering Task Force (IETF) in Vancouver. In remarks to the meeting's Technical Plenary session, Stephen Farrell concluded that "the actions of NSA and their partners (nation-state or not, coerced or not) are a multi-faceted form of attack" on the Internet, "or are indistinguishable from that" (Farrell 2013). He argued that "the right response is for the IETF to develop technical mitigations" that would make such attacks "significantly more expensive for a bad actor" (Farrell 2013). The reference to the 'right', as opposed to 'most beneficial' response suggests the presence of the justice motive. This language is notable because despite the fact that Farrell is an Irish citizen, he was speaking to an audience comprised largely of Americans. Farrell's feelings were apparently broadly shared even by the American technology and civil liberties communities. The Chief Technologist for the American Civil Liberties Union (ACLU), Chris Soghoian, noted that "there's a lot of anger out there" and that he had "seen two blog posts by Google engineers in the last three days that contained the words 'fuck you, NSA'" (The Economist 2013).

Finally, a number of authoritarian states have acted cooperatively to promote an illiberal multilateral approach to global Internet governance intended to legitimize domestic restrictions on speech and political dissent understood by democratic states to be incompatible with human rights. These efforts are embodied in a voluntary "Code of Conduct" presented to the United Nations most recently on 13 January 2015 (UNGA 2015, A/69/723). This revised iteration of the Code of Conduct was jointly presented by the representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan – all of which are members of the Shanghai Cooperation Organization (SCO). While the Code of Conduct and other similar proposals are almost certainly rooted in self-interested attempts by these regimes to stay in power, it is worth considering the possibility that the Code is also consistent with understandings of appropriate behavior sincerely held not only by the ruling elites in these states, but also by at least some significant proportion of their populations. To the extent this is the case, these states may also be partially motivated by justice considerations. Indeed, the content of the proposed Code of Conduct suggests the salience of several different kinds of justice concerns; at minimum, it seems clear that

its proponents are aware that their audiences (domestic and international) may be moved by such issues.

The Code of Conduct reflects concern with at least four issues on justice grounds. The most readily apparent is what China and other states have called "cyber sovereignty".[3] The Code requires adherents to pledge that they will "comply with the Charter of the United Nations and universally recognized norms governing international relations" and specifically enumerates "inter alia, respect for the sovereignty, territorial integrity and political independence of all states" (UNGA 2015). This language is in itself relatively uncontroversial, especially given the recognition by the UN GGE that existing international law applies online (UNGA 2013). As such, while it is clear that states understand protection of their sovereignty as a self-interest, it should be equally clear that states and their populations are likely to see violations of sovereignty as injustices.[4] A separate pledge in the Code of Conduct commit adherents to "prevent other States from exploiting their dominant position in information and communications technologies… to undermine States right to independent control of information and communications technology goods and services, or to threaten their political, economic and social security" (UNGA 2015). This provision connects concern for state sovereignty with the issue of the digital divide between developed and developing economies, and seeks to portray the exploitation of first-mover advantages as inappropriate and unjust.

The code later explicitly raises the issue of economic justice more generally, in asserting an obligation "to assist developing countries in their efforts to enhance capacity-building on information security and to close the digital divide" (UNGA 2015). Again, the authors of the code have drawn on existing discourses about international economic justice that have been long-established in the international trade regime and elsewhere. While it is likely that such efforts are, at least in part, attempts to rhetorically coerce (Krebs and Jackson 2007) industrial democracies to support the Code of Conduct or else pay a price in international legitimacy in the eyes of the

[3] In using this term it is important to acknowledge that even in China there is some penumbra of uncertainty about what this concept means in practical application (see Zeng, Stevens and Chen 2017).

[4] More generally, it is worth considering the possibility that a sense of injustice is an important part of the explanation for the contention in prospect theory that actors are likely to be more risk accepting in situations they understand as entailing the avoidance of loss. On prospect theory in international relations, see Levy (1997) and Goldgeier and Tetlock (2001).

developing world, there is no a priori reason to rule out the possibility that this claim is not also sincerely held.

Perhaps the most problematic provision of the code is its treatment of individual rights. The revised version attempted to assuage concerns that it was a vehicle for sharp curtailment of online rights by acknowledging that "the rights of an individual in the offline environment must also be protected in the online environment" (UNGA 2015). However, it asserted that the right to free speech must be implemented in a manner "taking into account the fact that the International Covenant on Civil and Political Rights (article 19) attaches to that right special duties and responsibilities" and that "it may therefore be subject to certain restrictions". Specifically, these restrictions are claimed to allow for "respect of the rights or reputations of others" and "for the protection of national security or of public order (ordre public), or of public health or morals" (UNGA 2015). Many authoritarian states (Hellmeier 2016), and some democracies,[5] exploit these provisions in bad faith to justify repressive practices clearly at odds with the object and purpose of the treaty. In at least some cases, governments clearly take such measures to preserve their hold on power. But instrumental use of rights is not evidence against the possibility that parties may also sincerely believe such rights are appropriate and just. The careful framing of this provision in terms of legitimate existing rules of human rights law suggests, at minimum, that the authors of the Code of Conduct were aware of criticisms of their proposal on justice grounds and that they sought to rebut these.

Finally, the Code of Conduct makes procedural justice claims for change to existing multistakeholder mechanisms for Internet governance. It insists that "all States must play the same role in, and carry equal responsibility for, international governance of the Internet" and that such governance should be accomplished "in a way which promotes the establishment of multilateral, transparent and democratic international Internet governance mechanisms which ensure an equitable distribution of resources, facilitate access for all and ensure the stable and secure functioning of the Internet" (UNGA 2015). These claims echo positions advanced by Russia, China, Iran and other states in recent debates over Internet governance, and portray multistakeholder governance as fundamentally illegitimate in that it allows participation by firms

[5] See, for example, Scott-Railton et al. (2017).

and voluntary sector actors, often on equal terms with sovereign states.[6] Somewhat ironically, this debate has placed authoritarian states in the position of advocating multilateralism, while the Western democracies that pioneered this form of global governance (Ruggie 1992) have come to see it as unfairly limiting participation to governments. In any event, the issues at stake (who is entitled to participate in rulemaking and on what terms) are clearly issues of procedural justice, even if they also implicate the interests of the various parties.

Avoiding Pyrrhic Victory and Other Implications for Global Governance

If, and to the extent that, actors are genuinely motivated by justice concerns in the cyber domain, what does this suggest about the likelihood of the scenarios Demchak identifies? The relative underdevelopment of the empirical literature on the justice motive in world politics suggests the need for a degree of caution, as do to the inherent difficulties in predicting the future in the social world (Bernstein et al. 2000). Despite these challenges, however, two points are noteworthy. Actors motivated by considerations of justice may be particularly unresponsive to side-payments, and perhaps negotiations in general. Negotiation and bargaining are not always thought to be appropriate behaviors, at least for every potential stake. One would not, for example, negotiate to purchase the flower arrangements from a family friend's funeral. Rules and norms determine the bounds within which bargaining and negotiation are socially acceptable (Müller 2004). While there is no single possible response to an inappropriate bargaining overture, the likelihood is that the receiving party may be offended, particularly if the initiating party persists in its efforts – for example, because it does not recognize that the recipient is motivated by considerations of justice. Put simply, actors are not likely to accept being bought off if they believe the stakes are an important matter of justice. Indeed, in such situations they may be particularly willing to employ political violence, as the persistence of national liberation and self-determination movements demonstrates (Kissane and Sitter 2013). *Where parties have mutually exclusive conceptions of what justice requires, conflicts may be intractable short of outright victory by one party, or a major shift in how at least one party frames or understands the stakes.*

[6] For an evaluation of the recent transition to new governance modalities for core Internet naming and addressing functions, see Hill (2016). On multistakeholder governance in contrast with multilateralism, see Raymond and DeNardis (2015).

In the cyber domain, at least two such deadlocks seem possible. The first is the conflict over the proper balance between individual political freedoms and the rights of states to ensure domestic tranquility. Though democracies are increasingly willing to consider restrictions on online expression, they are unlikely to agree to the kinds of broad powers in this domain already exerted by authoritarian states. Recognition that international law, including sovereignty, applies online may resolve many such cases by delegating choices to states; but this kind of outcome would seem to accelerate the transition from the cyber status quo scenario to either a cyber Westphalia or a CASI scenario. It also raises important questions about jurisdictional issues in transnational cases where conduct does not occur entirely within the territory of states with similar approaches to such questions. The second is the preference among many states for multilateral rather than multistakeholder mechanisms for Internet governance. To the extent some states see multistakeholder mechanisms as genuinely illegitimate – either because they inappropriately place firms and civil society groups on an equal footing with states, or because they tend to entrench the dominant positions of first-movers, or both – vital technical bodies for Internet governance will continue to experience legitimacy deficits, and efforts to create new organizations and processes will tend to founder on procedural grounds. Such outcomes will inhibit the effectiveness of the global cyber regime complex and may spill over to other related regimes such as the international trade regime, which is already under significant strain in part over digital issues.

There are also good reasons to believe that, in addition to being intractable, conflicts where parties are motivated by justice may also tend to be characterized by lack of restraint. Parties experiencing conflict over stakes they regard as inappropriate matters for compromise and side-payments may fight harder (Atran, Sheikh and Gómez 2014), investing more resources in securing their preferred outcomes and demonstrating greater willingness to disregard norms of peaceful conflict resolution or specific restraints on particular violent practices such as the targeting of civilians.[7] At this point, fortunately, the use of political violence over cyber issues seems relatively remote; however, prior to the last several years, the prospect of direct interference in domestic elections among permanent members of the Security Council would also have seemed remote. Activities commonly attributed to North Korea and to Russia similarly suggest that at least some

[7] On restraint and the variation in forms of violence employed in civil war, see Stanton (2016). Stanton's analysis, however, treats restraint largely as a strategic choice and does not investigate whether it is affected by considerations of justice.

state actors have expansive and rapidly evolving conceptions about the outer bounds of acceptable behavior in the cyber domain despite what had been encouraging signs in the work of the UN GGE. These trends similarly suggest the evolution of the cyber status quo toward the cyber Westphalian or CASI scenarios.

Taking the justice motive seriously also suggests that seeking to secure rapid, maximalist victories on cyber issues in anticipation of a worsening position in the future may result in a Pyrrhic victory. This is because such an approach may lead authoritarian states to respond in kind and convince 'swing states' (Maurer and Morgus 2014) that their misgivings and concerns will not be considered by advanced industrial democracies and large global technology firms. It will generate a sense of injustice among actors who have very different values, as well as expectations of meaningful autonomy on the basis of long-standing global rules and norms that have been championed by Western states. Exacerbating the extent to which actors are making choices on the basis of disparate understandings of what is required by justice runs the risk of worsening contention over cyber issues, and of accelerating the development of a highly-fragmented Internet ecosystem that entails greater tradeoffs in terms of the speed and scale of global connectivity. It may therefore be more effective for advanced industrial democracies to proceed in a deliberate manner, paying close attention to ensuring procedural legitimacy and demonstrating willingness to accept partial, voluntarist outcomes (Raymond 2016) that are less likely to create dissatisfied parties strongly motivated by considerations of justice. Even if such strategies also entail opportunity costs in speed and scale, and thus in the economic and social benefits of the cyber domain, they may prove worthwhile in bolstering the legitimacy, effectiveness and stability of the global cyber regime complex.

While it is very possible to make justice arguments in favor of an open Internet, the reality is that parties motivated by perceived discrepancies between entitlements and benefits are much more likely to be pursuing closure in the cyber domain to allow decentralization and diversity, if only because the status quo is typically framed as entailing a free and open Internet.[8] If actors make justice arguments in favor of decentralization and diversity in the cyber domain, the likelihood increases that governance arrangements will increasingly approximate the cyber Westphalian or

[8] The extent to which this remains accurate is an open, empirical question that already varies significantly across jurisdictions.

CASI scenarios. Attempts to press first-mover advantages to defend legacy governance arrangements seen as increasingly unjust would likely spark intractable conflict characterized by lack of restraint. This suggests willingness to violate rules and/or exercise costly exit options from the current cyber regime complex. Both kinds of outcomes would have significant negative effects for the speed and scale of global connectivity, and potentially also for stability in the cyber domain. In the long run, such scenarios may also have destabilizing spillover effects for other facets of the international system, as more dimensions of human life are dependent on the cyber domain, and as actors become less committed to the existing system of rule-based global order.

Accordingly, strategies of self-restraint on the part of industrial democracies are advisable in order to minimize the salience of the justice motive to the governance of the cyber domain. Unfortunately, a posture of empathetic self-restraint is deeply inconsistent with the worldview of the current American administration. This reality means that further movement in the direction of the cyber Westphalian or CASI scenarios is the most likely outcome. In particular, the analysis presented here suggests that the United States will struggle to solidify its own cyber alliance, leaving it in a cyber Westphalian position. Capitalizing on the predisposition of NATO and other allies toward institutionalized cooperation with the United States requires a degree of empathy and understanding entirely lacking in the administration's actions to date. To the extent that a likely "America first" stance is perceived by American allies as an unjust violation of the basic norms and rules not only of the cyber domain but of the post-1945 rule-based global order more generally, these allies are themselves likely to be increasingly motivated by considerations of justice in their dealings with the United States, and therefore unwilling to make concessions over issues they perceive in terms of basic value differences. To the extent that other major cyber powers such as Russia and China are able to avoid such pitfalls in solidifying their own cyber alliances, they will likely exert increased influence on future governance arrangements in the cyber domain.

REFERENCES

Aaronson, Susan Ariel. "Trade and the Internet," *The International Economy* (Winter 2012): 75-77.

Abelson, Harold, et al. *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, Computer Science and Artificial Intelligence Laboratory Technical Report MIT-CSAIL-TR-2015-026. Cambridge MA: MIT, 2015.

Acharya, Amitav. "How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism," *International Organization* 58.2 (2004): 239275.

Adler, Emanuel, and Vincent Pouliot. "International Practices," *International Theory* 3.1 (2011): 1-36.

Adler-Nissen, Rebecca. "Stigma Management in International Relations: Transgressive Identities, Norms, and Order in International Society," *International Organization* 68.1 (2014): 143-176.

Albin, Cecilia. *Justice and Fairness in International Negotiation*. Cambridge UK: Cambridge University Press, 2001.

Atran, Scott, Hammad Sheikh, and Ángel Gómez, "For Cause and Comrade: Devoted Actors and Willingness to Fight," *Cliodynamics: The Journal of Quantitative History and Cultural Evolution* 5.1 (2014): 41-57.

Bailey, Jennifer L. "Arrested Development: The Fight to End Commercial Whaling as a Case of Failed Norm Change," *European Journal of International Relations* 14.2 (2008): 289-318.

Baldwin, David A. "The Concept of Security," *Review of International Studies* 23.1 (1997): 5-26.

Barma, Naazneen H., Brent Durbin, Eric Lorber, and Rachel E. Whitlark. "'Imagine a World in Which': Using Scenarios in Political Science," *International Studies Perspectives* 17.2 (2016): 117-135.

Barkin, Samuel J. *Realist Constructivism*. Cambridge UK: Cambridge University Press, 2010.

Barnett, Michael, and Raymond Duvall. "Power in International Politics," *International Organization* 59.1 (2005): 39-75.

Bernstein, Steven, Richard Ned Lebow, Janice Gross Stein, and Steven Weber. "God Gave Physics the Easy Problems: Adapting Social Science to an Unpredictable World," *European Journal of International Relations* 6.1 (2000): 43-76.

Bradshaw, Samantha, Laura DeNardis, Fen Osler Hampson, Eric Jardine, and Mark Raymond. "The Emergence of Contention in Global Internet Governance," Global Commission on Internet Governance Paper Series, No. 17. Waterloo: Centre for International Governance Innovation, 2015.

Brunnée, Jutta, and Stephen J. Toope. *Legitimacy and Legality in International Law: An Interactional Account*. Cambridge UK: Cambridge University Press, 2010.

Chayes, Abram, and Antonia Handler Chayes. "On Compliance," *International Organization* 47.2 (1993): 175-205.

Clinton, Hillary Rodham. "Remarks on Internet Freedom," speech delivered at George Washington University, Washington DC, 15 February 2011. Accessed at https://www.eff.org/files/filenode/clinton_internet_rights_wrongs_20110215.pdf.

Cortell, Andrew P., and James W. Davis Jr. "How Do International Institutions Matter? The Domestic Impact of International Rules and Norms," *International Studies Quarterly* 40.4 (1996): 451-478.

Crawford, Neta C. *Argument and Change in World Politics: Ethics, Decolonization, and Humanitarian Intervention*. Cambridge UK: Cambridge University Press, 2002.

Demchak (2017) – this issue.

The Economist. "Internet Security: Besieged." *The Economist* 9 November 2013. Accessed at https://www.economist.com/news/science-and-technology/21589383stung-revelations-ubiquitous-surveillance-and-compromised-software.

Farrell, Stephen. "IETF Response to Pervasisve Monitoring," speech delivered at IETF 88 Technical Plenary, 7 November 2013, Vancouver, Canada. Accessed at https://www.ietf.org/proceedings/88/slides/slides-88-iab-techplenary-8.pdf.

Finnemore, Martha, and Duncan B. Hollis. "Constructing Norms for Global Cybersecurity," *American Journal of International Law* 110.3 (2016): 425-479.

Finnemore, Martha, and Kathryn Sikkink. "International Norm Dynamics and Political Change," *International Organization* 52.4 (1998): 887-917.

Goldgeier, J.M., and P.E. Tetlock. "Psychology in International Relations Theory," *Annual Review of Political Science* 4 (2001): 67-92.

Haucap, Justus, and Torben Stühmeier. "Competition and Antitrust in Internet Markets," DICE Discussion Paper, No. 199 (2015). Accessed at https://www.econstor.eu/handle/10419/121420.

Hellmeier, Sebastian. "The Dictator's Digital Toolkit: Explaining Variation in Internet Filtering in Authoritarian Regimes," *Politics & Policy* 44.6 (2016): 1158-1191.

Hill, Richard. "Internet Governance, Multi-stakeholder Models, and the IANA Transition: Shining Example or Dark Side?" *Journal of Cyber Policy* 1.2 (2016): 176-197.

Hopf, Ted. "The Logic of Habit in International Relations," *European Journal of International Relations* 16.4 (2010): 539-561.

Hurd, Ian. "Legitimacy and Authority in International Politics," *International Organization* 53.2 (1999): 379-408.

Jepperson, Ronald L., Alexander Wendt, and Peter J. Katzenstein. "Norms, Identity, and Culture in National Security," in Peter J. Katzenstein, ed., *The Culture of National Security*. New York: Columbia University Press, 1996.

Keck, Margaret E., and Kathryn Sikkink. *Activists Beyond Borders: Advocacy Networks in International Politics*. Ithaca: Cornell University Press, 1998.

Keohane, Robert O. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press, 1984.

Keohane, Robert O., and Lisa L. Martin. "Institutional Theory as a Research Program," in Colin Elman and Miriam Fendius Elman, eds., *Progress in International Relations Theory: Appraising the Field*. Cambridge MA: MIT Press, 2003.

Kissane, Bill, and Nick Sitter. "Ideas in Conflict: The Nationalism Literature and the Comparative Study of Civil War," *Nationalism and Ethnic Politics* 19.1 (2013): 38-57.

Kornprobst, Markus. "The *Agent's* Logics of Action: Defining and Mapping Political Judgement," *International Theory* 3.1 (2011): 70-104.

Krebs, Ronald R., and Patrick Thaddeus Jackson. "Twisting Tongues and Twisting Arms: The Power of Political Rhetoric," *European Journal of International Relations* 13.1 (2007): 35-66.

Levy, Jack S. "Prospect Theory, Rational Choice, and International Relations," *International Studies Quarterly* 41.1 (1997): 87-112.

Lynch, Colum. "Brazil's President Condemns NSA Spying." *The Washington Post*, 24 September 2013. Accessed at https://www.washingtonpost.com/world/nationalsecurity/brazils-president-condemns-nsa-spying/2013/09/24/fe1f78ee-2525-11e3-b75d5b7f66349852_story.html?utm_term=.61ff684705fd.

March, James G., and Johan P. Olsen. "The Institutional Dynamics of International Political Orders," *International Organization* 52.4 (1998): 943-969.

Maurer, Tim. "Cyber Norm Emergence at the United Nations: An Analysis of the Activites at the UN Regarding Cyber-Security," Discussion Paper 2011-11. Cambridge MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2011.

Maurer, Tim, and Robert Morgus. "Tipping the Scale: An Analysis of Swing States in the Internet Governance Debate," in Mark Raymond and Gordon Smith, eds., *Organized Chaos: Reimagining the Internet*. Waterloo: Centre for International Governance Innovation, 2014.

Mearsheimer, John J. "The False Promise of International Institutions," *International Security* 19.3 (1994/95): 5-49.

Müller, Harald. "Arguing, Bargaining and All That: Communicative Action, Rationalist Theory and the Logic of Appropriateness in International Relations," *European Journal of International Relations* 10.3 (2004): 395-435.

Newman, Abraham L. "What the 'Right to be Forgotten' Means for Privacy in a Digital Age," *Science* 347.6221 (30 January 2015): 507-508.

Nye Jr., Joseph S. "The Regime Complex for Managing Global Cyber Activities," Global Commission on Internet Governance Paper Series, No. 1. Waterloo: Centre for International Governance Innovation, 2014.

Onuf, Nicholas Greenwood. *World of Our Making: Rules and Rule in Social Theory and International Relations*. Columbia: University of South Carolina Press, 1989.

Oye, Kenneth A. *Cooperation Under Anarchy*. Princeton: Princeton University Press, 1986.

Panke, Diana, and Ulrich Petersohn. "Why International Norms Disappear Sometimes," *European Journal of International Relations* 18.4 (2012): 719-742.

Raymond, Mark. "Puncturing the Myth of the Internet as a Commons," *Georgetown Journal of International Affairs* International Engagement on Cyber III (2013/14): 53-64.

Raymond, Mark. "Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot," *Strategic Studies Quarterly* 10.4 (2016): 123-149.

Raymond, Mark, and Gordon Smith. "Reimagining the Internet: The Need for a HighLevel Strategic Vision for Internet Governance," in Mark Raymond and Gordon Smith, eds., *Organized Chaos: Reimagining the Internet*. Waterloo: Centre for International Governance Innovation, 2014.

Raymond, Mark, and Laura DeNardis. "Multistakeholderism: Anatomy of an Inchoate Global Institution," *International Theory* 7.3 (2015): 572-616.

Ruggie, John Gerard. "International Responses to Technology: Concepts and Trends," *International Organization* 29.3 (1975): 557-583.

Ruggie, John Gerard. "Multilateralism: The Anatomy of an Institution," *International Organization* 46.3 (1992): 561-598.

Ruggie, John Gerard. "What Makes the World Hang Together? Neo-utilitarianism and the Social Constructivist Challenge," *International Organization* 52.4 (1998): 855-885.

Sandholtz, Wayne. "Dynamics of International Norm Change: Rules Against Wartime Plunder," *European Journal of International Relations* 14.1 (2008): 101-131.

Scott-Railton, John, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert. *Reckless IV: Lawyers for Murdered Mexican Women's Families Targeted with NSO Spyware* (Toronto: CitizenLab, 2017). Accessed at https://citizenlab.ca/2017/08/lawyers-murdered-women-nso-group/.

Shannon, Vaughn P. "Norms Are What States Make of Them: The Political Psychology of Norm Violation," *International Studies Quarterly* 44.2 (2000): 293-316.

Shannon, Vaughn P., and Jonathan W. Keller. "Leadership Style and International Norm Violation: The Case of the Iraq War," *Foreign Policy Analysis* 3.1 (2007): 79-104.

Simmons, Beth A. "Compliance with International Agreements," *Annual Review of Political Science* 1 (1998): 75-93.

Soskice, David, and Peter A. Hall, eds. *Varieties of Capitalism: The Institutional Foundations of Comparative Advantage*. Oxford: Oxford University Press, 2001.

Stanton, Jessica A. *Violence and Restraint in Civil War: Civilian Targeting in the Shadow of International Law*. Cambridge: Cambridge University Press, 2016.

Tikk-Ringas, Eneken. "Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012." Geneva: ICT4Peace Publishing.

United Nations General Assembly. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/69/98, 24 June 2013.

United Nations General Assembly. "Letter Dated 9 January 2014 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General," A/69/723, 13 January 2015.

Welch, David A. *Justice and the Genesis of War*. Cambridge UK: Cambridge University Press, 1993.

Welch, David A. "The Justice Motive in International Relations: Past, Present, and Future," *International Negotiation* 19.2 (2014): 410-425.

Wendt, Alexander. "Anarchy is What States Make of It: The Social Construction of Power Politics," *International Organization* 46.2 (1992): 391-425.

Wendt, Alexander. "Driving with the Rearview Mirror: On the Rational Science of Institutional Design," *International Organization* 55.4 (2001): 1019-1049.

Zeng, Jinghan, Tim Stevens, and Yaru Chen. "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty'," *Politics & Policy* 45.3 (2017): 432-464.