Social Practices of Rule-Making for International Law in the Cyber Domain

Mark Raymond

University of Oklahoma

Abstract

In 2013, despite deteriorating relations between Russia and the United States and increased global contention over cybersecurity issues, participating states in the First Committee of the United Nations General Assembly agreed on a landmark report endorsing the applicability of existing international law to state military use of information technology. Given these conditions, the timing of this agreement was surprising. In this article I argue that state representatives engaged in a rule-governed social practice of applying old rules to new cases, and that the procedural rules governing this practice help to explain the existence, timing, and form of the agreement. They also help to explain further agreements expressed in a follow-on report issued in 2015. The findings of the case study presented here demonstrate that social practices of rule-making are simultaneously rule-governed and politically contested, and that outcomes of these processes have been shaped by specialized rules for making, interpreting, and applying rules. The effectiveness of procedural rules in shaping the outcome of a contentious, complex global security issue suggests that such rules are likely to matter even more in simpler cases dealing with less contentious issues.

Keywords: Internet governance, cybersecurity, constructivism, international law, norms, global governance

Efforts to govern the effects of information and communication technologies (ICTs) for international security date to at least 1998, when the Russian Federation introduced a draft resolution entitled Developments in the Field of Information and Telecommunications in the Context of International Security (Maurer 2011; Tikk-Ringas 2012). This draft became the basis for a concerted diplomatic effort in the First Committee of the United Nations General Assembly (UNGA), later joined by a significant number of other states, to create a new international legal instrument governing state use of ICTs for military purposes. The work process in the First Committee has centered on several iterations of an expert working group, the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (hereinafter, the GGE). The third GGE report, issued in 2013, contained an important advance in state thinking about these issues. It asserted that “international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment” (UNGA 2013a, 8). Beyond the UN Charter, it specifically enumerated state sovereignty, human rights, and the law of state responsibility as among the applicable bodies of international law governing state use of ICTs (UNGA 2013a, 8).

The 2015 GGE report indicates further progress. It contains a direct discussion of the applicability of international law in this area, explicitly building on the 2013 report by invoking core legal obligations, including the settlement of disputes by peaceful means, the obligation to refrain from the threat and use of force against the territorial integrity or political independence of states,
and even the obligation of nonintervention in the internal affairs of other states. Finally, the document “notes the established legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction” (UNGA 2015b, 12–13). While this language may be interpreted as falling short of clearly affirming the applicability of the law of armed conflict in the cyber domain, and is in any event not legally binding, it is clear that the GGE has made considerable important progress in a relatively short period of time.

Remarkably, this rapid progress on norms for state conduct in the cyber domain has come despite conditions hostile to norm development: (1) a precipitous decline in diplomatic relations between the Russian Federation and the majority of the advanced industrial democracies, largely over Russia’s behavior in Ukraine; and (2) increased contention over Internet governance and cybersecurity issues at the global level (Bradshaw et al. 2015). Accordingly, I seek to explain a puzzling but welcome shift toward agreement on cyber norms for the state use of ICTs. While revelations about Russian interference in domestic elections make this case extremely timely, these events come mainly after the period under examination and are therefore addressed primarily in the conclusion.

The central argument of the article is that state representatives to the GGE engaged in a rule-governed social practice of applying old rules to new cases, and that the procedural rules governing this practice are a necessary component of an explanation both of the substantive outcome and the form of the associated process. Participants drew on existing procedural rules of diplomacy and international law in order to advance their positions on the most desirable and appropriate rules to govern state use of ICTs. These rules simultaneously empowered and constrained state representatives in advancing their positions and in evaluating proposals made by their counterparts. They can therefore be understood as partial explanations for the outcome.1

Social practices of rule-making, structured by procedural rules, are a necessary part of a satisfactory explanation for an important and puzzling outcome—relatively rapid progress on developing potential norms for state use of ICTs at a time when conditions should not lead us to expect this result. The available evidence, drawn from analysis of UN documents, is often suggestive of ways that these procedural rules shaped individual state decisions, especially about the forms and manners in which these states articulated their positions and reacted to other states’ positions. The evidence also indicates that states with greater procedural competence were more able to secure their preferred outcomes. The empirical analysis identifies ways that procedural rules and social practices of rule-making shaped specific state choices and helped account for the ability of states to secure outcomes consistent with their preferences; however, the recency and relative opacity of the process precludes strong causal claims about specific actor choices. Accordingly, my focus is on accounting more broadly for an important part of the larger outcome—a shift from stalemate to international agreement on a set of candidate norms addressing major questions about the legality of state military use of ICTs, in conditions that made such an outcome unlikely. This outcome cannot be explained without accounting for the ways that procedural rules and social practices of rule-making prefigured the ongoing social process in which states sought to deal with questions about the legality of state military use of ICTs.

At present, this ongoing social process has provisionally resulted in agreement by significant groups of states (including the permanent members of the UN Security Council) that the proposal for a multilateral treaty should be eschewed in favor of continued efforts to govern any resulting disputes about state use of ICTs by means of the decentralized legal process fundamental to the contemporary international legal system (including the provisions of the UN Charter, the law of armed conflict, and the customary law of state responsibility), and that the state use of ICTs is governed by existing bodies of international law that impose substantial restrictions on the military use of ICTs. The rejection of the Russian proposal for a new international treaty in favor of this alternative approach is the result of a concerted effort (led by the United States) to apply old rules to a new case. The relatively rapid embrace of this position by a diverse group of countries with divergent positions on Internet governance issues and different interests and capabilities in the cyber domain, during a period in which cyber issues have become increasingly contentious, indicates that relevant procedural rules have relatively strong effects on state behavior. That the reports essentially endorsing the American position were issued on a consensus basis by a group that included many of the states contesting the issue is a further indicator of the strength of these procedural rules.

These outcomes depended fundamentally on the particular set of procedural rules accepted by the actors. If the procedural rules had differed, it is unlikely that states would have made the same choices about how to address concerns pertaining to state military use of ICTs.

---

1 On the notion of reasons as causes in international relations, see Hurd (1999, 391). On constructivist approaches to causation, see Wendt (2001).
For example, without procedural rules about both the modalities for negotiating multilateral treaties and the appropriateness of doing so on issues of international security, it is unlikely that Russia would have raised the issue in the First Committee, or that states such as Spain and Japan would have expressed openness to these ideas in spite of opposition from close allies. Similarly, without informal rules about the appropriateness of relying on expert advice, states might well have chosen a means of negotiation other than the creation of the GGE. Without established professional communities of diplomats and international lawyers accustomed to interpreting and applying bodies of existing international law to novel cases, both in international courts and in advisory settings such as the International Law Commission, it is unlikely that GGE participants could have agreed that existing international law applies online despite evident and abiding disagreements over a range of substantive issues pertaining to Internet governance and digital policy in general, and the state military use of ICTs in particular. At one level, this argument is simply an acknowledgement that path dependence matters in international politics (March and Olsen 1998) and that processes of international law (Brunnée and Toope 2010; Diehl and Ku 2010) and international organization (Johnson 2014) can take on lives of their own. However, it makes an important contribution in demonstrating the relevance of procedural rules for rule-making, interpretation, and application to producing these path-dependent effects of specific international legal and institutional settings.

Even more fundamentally, the outcome in this case depended on the existence of agreement among the parties on appropriate procedural rules, independent of their substantive positions. Put another way, if parties had disagreed about procedural rules, it is extremely unlikely that the GGE would have been created, or that it could have issued either its 2013 or 2015 report. The documentary record is remarkable in part for the absence of disagreement about procedural issues, in sharp contrast to other comparable international processes dealing with Internet-related issues (Bradshaw et al. 2013; Hill 2015, 2016). The 2012 attempt to update the International Telecommunication Regulations ended in a split outcome that resulted in fragmentation of the regime into two operative treaties with different sets of parties, and the 2016 Internet Assigned Numbers Authority (IANA) transition process resulted in a new arrangement for governing Internet naming and addressing functions, but one that left many parties dissatisfied. In both cases, conflict surrounding procedural rules complicated attempts to reach agreement (Bradshaw et al. 2015; Raymond and DeNardis 2015).

These findings have broad relevance for International Relations (IR) theory. They demonstrate that actors are goal-oriented and even strategic in contesting applicable norms and rules, illustrating the complex interplay between the logic of consequences and other behavioral logics more often associated with social construction (such as logics of appropriateness, habit, and practice). They further establish that the settings in which actors contest applicable norms and rules are prefigured by existing social practices of rule-making, interpretation, and application that are themselves constituted by procedural rules. These procedural rules function as meta-rules, or rules about rule-making, that simultaneously enable and constrain different actors and different forms of social action. Finally, the findings from this case lend support to constructivist arguments that treat such social processes as explicitly power-laden (Barnett and Duvall 2005; Krebs and Jackson 2007). The article therefore builds on several constructivist literatures, furnishing additional empirical support for their key claims and extending the literature by conceptualizing the generic social practice of international rule-making.

In highlighting the role of procedural rules for rule-making, interpretation, and application in explaining the apparent failure of Russian attempts to secure a multilateral treaty governing state use of ICTs for military purposes and the success of American attempts to extend existing rules of international law to this new domain, the article’s major contribution lies in connecting these rule systems to the outcome of high-profile, contested cases in the international security realm. The efficacy of these rules in shaping state behavior (including that of the great powers), in what should be a hard case for constructivist arguments, sheds light on the nature and potency of established international rule-making practices. The evidence suggests that, even in the realm of high politics, state representatives understand themselves as engaged in established and ongoing practices of social construction. This finding extends and builds on constructivist work that re-examines the importance of diplomacy and diplomatic practices to IR theory (Neumann 2002; Adler-Nissen 2009; Pouliot 2016). It does so in part by demonstrating
the utility of a focus on procedural rules in realizing potential gains from practice-turn constructivism.⁴

The article proceeds in three parts. The first part briefly develops the empirical puzzle introduced above and introduces the theoretical argument. The second part presents a case study of the attempt to establish cyber norms in the First Committee of UNGA. The third part discusses the findings of the case study and their importance for IR theory.

Social Practices of Rule-Making

The 2013 GGE report is an important milestone in clarifying norms for state behavior in the cyber domain. The GGE was reasonably representative: it included all permanent members of the UN Security Council; major emerging markets such as India and Indonesia; and middle powers Australia and Canada. Member states were selected according to accepted UN practices for ensuring regional balance. While it is an exaggeration to say that the GGE process produced global norms, since the GGE has no definitive competence to do so under the procedural rules of international law and diplomacy, the GGE is part of a class of established advisory mechanisms on international rules and norms that includes the International Law Commission, the advisory function of the International Court of Justice, and various ad hoc global commissions or high-level panels. As such, its reports have a degree of normative force, especially to the extent that they publicly commit key states to particular positions from which any derogations can be criticized and that can be held up as examples of prevailing best practice.⁵ The group made important substantive progress, reaching the first multilateral consensus report declaring the official view of a group of major states that international law is applicable in its entirety to the cyber domain. Notably, this consensus represents a departure from Russian efforts (later co-sponsored by China and other states) to pursue a formal multilateral treaty governing state use of ICTs. The GGE continued its work by issuing another consensus report in 2015 that built on the 2013 report, and by recommending another iteration of the process in 2016–2017. Russia and China have continued to pursue their interests in strong versions of Internet sovereignty in the First Committee despite conclusion of the most recent GGE without a consensus report. In doing so, however, they have altered their procedural approach to accord more closely with the procedural rules and practices utilized by Western states, suggesting the influence of these rules on both processes and outcomes.

Beyond the general reluctance of some IR scholars to accept the causal relevance of norms, rules, and institutions (especially in security cases),⁶ there are two more specific reasons that the agreement and its timing might be regarded as puzzling. First, it occurred rather suddenly despite a substantial worsening of diplomatic relations between Russia and the United States. Russia’s claim to annexation of Crimea and its involvement in the Syrian conflict have caused deep disagreements with the United States and its allies, as well as the imposition of economic sanctions; yet, despite these differences, work on cyber norms was extremely successful in 2012–2015. While it is true that Russia and the United States were also able to work together on negotiations pertaining to the Iranian nuclear program in this time period, that case is less puzzling given the great powers’ long-standing agreement on maintaining nuclear oligopoly. The Iranian case also involves a structured diplomatic and legal framework that draws on many of the same procedural rules that have proven influential in the cyber case examined here. It is possible that cooperation in these two cases is partially explained by this common factor.

Second, agreement on norms of responsible state behavior for the use of ICTs is puzzling because it occurred alongside continuing contention over related issues of global Internet governance (Bradshaw et al. 2015). If anything, agreement on security norms should have been more difficult than agreement on lower politics issues pertaining to the institutional modalities for governing Internet naming and numbering, and the development of Internet technical protocols. These problems involve coordination rather than cooperation problems, and while important distributional consequences flow from the selection of particular equilibria rather than others, these kinds of problems are generally thought to be less problematic for international cooperation (Martin and Simmons 1998). Yet the evidence shows the opposite. Russia and the United States have agreed that international law applies to the state use of ICTs while continuing to advance starkly different proposals for Internet governance. This is partly because Internet governance

⁴ On the relationship between the practice-turn and constructivism, see McCourt (2016).

⁵ More fundamentally, to the extent that any international norm becomes accepted or even internalized, it is important to remember that norms remain provisional and that they depend on continued acceptance and various forms of practice for their continued existence (Sandholtz 2008).

⁶ Constructivists (e.g., Wendt 1995, 77) have sometimes accepted the claim that security cases are “hard cases” for their theories, though it is not always clear whether this is sincere, or a tactical move driven by a desire to gain acceptance from nonconstructivists.
has been politicized in a manner that invokes issues of procedural legitimacy in addition to issues of substantive fairness associated with distributional questions. In contrast, discussions of cybersecurity in the UNGA First Committee have been notable for the absence of procedural conflict, reflecting the presence of greater agreement among the parties on relevant procedural rules.

In the remainder of this article, I present an explanation of the puzzling, rapid emergence of agreement on the applicability of international law to the state use of ICTs. Since this puzzle is a question of explaining the emergence of (at least tentative) international norms, I draw primarily on the constructivist literature. Constructivists have done a great deal of work attempting to explain the emergence of new international norms. This literature contains a large number of proposed theoretical mechanisms, including strategic social construction (Finnemore and Sikkink 1998), learning (Checkel 2001), socialization (Johnston 2001), argumentation (Crawford 2002), norm localization (Acharya 2004), norm contestation (Weiner 2004), rhetorical coercion (Krebs and Jackson 2007), and norm change (Sandholtz 2008). Each of these is a mechanism for creating or altering intersubjective knowledge. However, it is not yet clear whether these mechanisms are competing or complementary. That is, what are the scope conditions? When will actors employ socialization versus persuasion versus strategic social construction versus norm contestation versus norm localization? Are each of these truly distinct mechanisms? Do actors employ these mechanisms simultaneously, or are they, at least to some degree, mutually exclusive choices?

Further, the constructivist literature has not yet engaged two more basic questions: (1) how do actors know how to engage in each of these different kinds of social mechanisms for creating or altering intersubjective knowledge?; and (2) how do they know how to do so in particular contexts? Put differently, why does what counts as persuasive in one context (a courtroom, for example) differ from what counts as persuasive in another context (a romantic relationship, for example)?

Answering these more basic questions can contribute to consolidating and integrating the gains made from constructivist research on social dynamics. I draw on rule-oriented constructivism, practice-turn constructivism, and scholarship dealing with the dynamics of the international legal system to show that actors’ choices about how to present and respond to proposals about making, interpreting, and applying rules were shaped in important part by pre-existing and mutually agreed-upon procedural rules for international rule-making. This finding fills an important gap in the constructivist literature by providing evidence about how actors know how and when to engage in particular forms of social construction. It shows that the various causal mechanisms identified by constructivists should be distinguished inductively, by examining the understandings of the relevant actors in a particular social setting about how to create or alter intersubjective knowledge such as rules or norms. The relevant stock of understandings that tell actors how to accomplish such objectives is provided by the procedural rules that constitute applicable practices of rule-making, interpretation, and application. While this argument is not a complete answer to the questions raised above, it provides an important step forward in constructivist research.

Practice-turn scholars have demonstrated the utility of analyzing international politics through the lens of social practices. Adler and Pouliot (2011, 4) define practices as “socially meaningful patterns of action which, in being performed more or less competently, simultaneously embody, act out and possibly reify background knowledge and discourse in and on the material world.” They further suggest that “practice rests on background knowledge, which it embodies, enacts, and reifies all at once” (Adler and Pouliot 2011, 4). The practice turn is an important advance in IR theory; however, I argue that its conception of background knowledge is overly expansive, and that it would provide a superior guide for empirical research if it were specified more narrowly in terms of procedural rules.

Procedural rules are a subset of rules that deal with establishing legitimate processes for taking certain actions. Despite the lack of focus on this subset of rules, both in practice-turn scholarship and in constructivism more broadly, procedural rules are a vital part of social interactions. For example, practice-turn scholarship rightly emphasizes the evaluation of competence by audiences according to shared standards (Adler and Pouliot 2011, 6–7) and norms scholars have highlighted the role of audiences in adjudicating among multiple possible interpretations of how a norm applies to a particular case (Sandholtz 2008; Winston 2018). Such collective evaluations are impossible without formal and/or informal procedural rules against which to determine the degree to which a particular performance is socially competent or an interpretation is appropriate.

Hart (1994) famously referred to procedural rules for rule-making as secondary rules, in contrast to what he called primary rules of behavior or substantive rules. I prefer to treat procedural rules as a subset of rules rather than a distinct type, since they still govern behavior—simply behavior of a specific kind. I also depart from Hart in believing that secondary rules (i.e., procedural rules for making, interpreting, and applying rules) are
identifiable in the international system, not only within the international legal system but also beyond it. In the contemporary international system, written and unwritten procedural rules are found primarily in the closely related domains of diplomacy and international law. These rules, and the practices they constitute, are in substantial part concerned with a fundamental social activity: making, interpreting, and applying rules. That is, in addition to allowing states (and increasingly other agents) to play the game of international politics, they also provide procedures for amending and altering the rules of that game. This rule-making meta-game has particular procedural rules that structure it.

An example of the difference between a rule and a related procedural rule is the substantive requirement in the UN Charter, Article 2(4), that UN members “shall refrain...from the threat or use of force against the territorial integrity or political independence of any state,” and the related Article 43 provision that authorizes the Security Council to “determine the existence of any threat to the peace, breach of the peace, or act of aggression” and to “make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security” (United Nations 1945). The latter rule deals with how to determine whether the former has been violated, and is therefore a related procedural rule for rule-making, interpretation, and application. It is not, however, the only relevant procedural rule connected to Article 2(4). For example, Article 51 (in addition to customary international law) authorizes states to undertake self-defense measures in the event they are subject to armed attack; however, it requires that the defending state notify the Security Council of such measures (United Nations 1945). As this example makes clear, rules exist in practice as parts of dense, interconnected sets of simultaneously valid rules that are never complete, are often internally inconsistent, and are almost always indeterminate about the manner in which they should collectively be applied to concrete cases. These features of rule systems (Sandholtz 2008) provide space for agency, in that they differentially empower and authorize actors to advance certain kinds of interpretations for evaluation by other actors. But this space for agency is not infinite, and therefore the procedural rules are relevant to explaining the behavior of all the parties involved in such disputes. Even where actors knowingly violate such rules, for example, the rule may explain why (and how) audience members react to that violation and the ways they use related rules to respond, for example by criticizing and otherwise sanctioning the violator in particular ways.

Two distinct literatures help to further illuminate the written and unwritten procedural rules for rule-making, interpretation, and application in international politics. The first examines the dynamics of the international legal system. Rational choice scholarship on legalization in world politics provided important advances in understanding the interplay between international law and international politics. Scholars distinguished between forms of legalization according to their degrees of obligation, precision, and delegation (Abbott et al. 2000), and emphasized the importance of soft law (Abbott and Snidal 2000). However, these approaches were also criticized by constructivists for their truncated understandings of international law. Finnemore and Toope (2001, 743) argued that international law must be understood as “more than the formal, treaty-based law” emphasized by rationalists and that “law is a broad social phenomenon deeply embedded in the practices, beliefs, and traditions of societies, and shaped by interaction among societies.” Finnemore (2005, 187) employed such an understanding of international law in arguing that disputes over the Bush administration’s interpretations of international law pertaining to the use of force “look less like a fight between unilateralism and multilateralism than a fight over what exactly multilateralism means and what the shared rules that govern use of force are (or should be).” This formulation foregrounds the importance of rule-governed interpretation and application of general rules to particular cases. Brunnée and Toope (2010) have correctly pointed out that these processes take place over extended periods of time and require the work of large numbers of experts trained in social practices of international legality, or what they aptly call “the hard work of international law.” Diehl and Ku (2010), drawing on Hart’s work, point out that such practices of interpreting and applying rules draw on a procedural “operating system” as well as a substantive “normative system” of international law, and that the operational law is rule-based.

The second is the literature examining international diplomatic practices. Adler-Nissen (2009) examines what she calls “late sovereign diplomacy” in the European Union, arguing that processes of European integration have fundamentally changed member states’ understandings of their national interests. Adler-Nissen and Pouliot (2014) argue that differences in diplomats’ competences or skills in performing within the broad context set by the rules of the game help to explain the outcome of multilateral diplomacy in the case of international intervention in Libya. Pouliot has expanded on this argument about how differences in players’ abilities to creatively improvise using accepted rules of the game help to explain outcomes in world politics. He argues that “a key consequence of
the multilateralization of international security” has been “the production, reproduction, and contestation of local diplomatic hierarchies that practitioners often call ‘international pecking orders’” (Pouliot 2016). In his view, “the multilateral diplomatic process does something to the politics of international security: it generates a distinctive set of endogenous opportunities and constraints in the making and remaking of international hierarchies” (Pouliot 2016, 6). But these opportunities and constraints are, at least in large part, the product of written and unwritten rules that constitute the specific game of multilateral diplomacy. These rules are well known in the literature on multilateralism (Ruggie 1992; Reus-Smit 1999). Pouliot adds important social texture to understandings of multilateralism, which has typically been understood as having a benevolent and leveling effect in the international system, by showing that multilateralism sometimes instantiates hierarchy. His account also notes the importance of “local codes and rules, which competent diplomats know how to use.” Development of these local codes is fostered by high social density and iterated interaction in institutional contexts such as the UN Security Council (Pouliot 2016, 17).

Each of these literatures adds a great deal to identifying the procedural rules relevant to understanding contemporary practices for making, interpreting, and applying rules in the international system, but neither explicitly theorizes procedural rules or focuses on the ways such rules shape outcomes. Diplomacy and international law are both essential to a more generic rule-governed social practice of rule-making, interpretation, and application. Adopting this view makes clear the relevance of global governance for systemic IR theory. Processes of making, interpreting, and applying rules are central to (and possibly constitutive of) global governance. Accordingly, global governance is a key process whereby the rules and institutions central to constructivist understandings of the international system’s ontology are continually reproduced and altered.

This article makes two major claims. First, that actors in the international system are, inter alia, engaged in a rule-governed social practice of making, interpreting, and applying social rules. Second, that these procedural rules partially determine important outcomes in the international system. They do so by shaping the substance, form, and timing of actors’ proposals for making, interpreting, and applying rules, as well as the way that actors respond to such proposals by others.7

7 For a deeper theoretical discussion of social practices of rule-making, interpretation, and application, see Raymond (2019).

If I am correct, we should see particular kinds of evidence. Actors should present and evaluate proposed rules or interpretations of rules in a manner consistent with relevant procedural rules. That is, they should engage in both critical and justificatory behavior, and should do so in ways consistent with legitimate procedures for rule-making and interpretation. To the extent that procedural rules are causally effective, more procedurally competent proposals and interpretations should be more likely to generate agreement than less procedurally competent proposals and interpretations. It is worth noting that this argument does not require that actors engage in this practice sincerely. Actors can comply with rules for a variety of reasons, and often do so with mixed motives (Hurd 1999). What matters is that the rules shape behavior—simultaneously empowering and constraining actors as they pursue their values and their interests.

Applying Old Rules to New Cases: International Law in the Cyber Domain

Existing studies have documented the work of UNGA’s First Committee on cyber issues from the initial discussions in 1998 through the 2010 GGE process (Maurer 2011; Tikk-Ringas 2012). From 1998 to 2004, the Russian resolution on ICTs in the context of international security was adopted in the First Committee without a vote. However, this did not indicate substantive agreement. While Russia insisted in 1999 that “contemporary international law has virtually no means of regulating the development and application” of a cyber-weapon and called for a multilateral treaty, the United States maintained that “it would be premature to formulate overarching principles pertaining to information security in all its aspects” and that “the international community needs to do a substantial amount of systematic thinking before going further” (UNGA 1999, 8, 13). The American position likely reflected a Bush administration preference to preserve a strategic advantage; however, the crucial point is that, rather than simply refuse to engage the Russian proposal or plainly indicate a preference based on a perceived national interest, the United States chose to proceed by interpreting the Russian proposal in light of procedural rules of great power diplomacy and international law. In particular, the American response relies on procedural rules about the need to engage rule-making proposals advanced by other powers in (at least apparent) good faith to preserve common practices of managing the international system, and about the value of prudence and patience in altering international rules and institutions.

By 2004, the United States had concluded that “an international convention is completely unnecessary.” Its
rationale was that “the law of armed conflict and its principles of necessity, proportionality and limitation of collateral damage already govern the use of such technologies” (UNGA 2004, 4). Thus, the United States replied to the Russian proposal for a new treaty by arguing that new rules were not needed because existing rules already covered this novel case. This is a clear example of interpreting and applying global rules, and of employing the broader procedural frameworks of diplomacy and international law to evaluate (and in this case oppose) a rule-making proposal made by another actor. Specifically, the amended American argument had moved in a more legal vein, relying on established rules and practices for interpreting existing treaties such as the UN Charter and the Geneva Convention, as well as for applying rules of customary international law such as the law of armed conflict and the law of state responsibility. The argument was effectively that these bodies of law were technologically neutral, and thus governed all state military conduct whether accomplished by means of ICTs or not.

This dispute over how to correctly interpret and apply existing rules of international law to a novel, complex, and important case prevented the first iteration of the GGE from issuing a consensus report. Crucially, this view has been expressed publicly by some of the participants. The chair, Russian diplomat A.V. Krushtikik, explicitly attributed this failure in part to “differing interpretations of current international law in the area of international information security” (quoted in Tikk-Ringas 2012, 7). Another member of the Russian delegation, A.A. Streltssov, called this issue “the main stumbling block” (quoted in Maurer 2011, 33). From 2005 to 2008, the United States voted against the Russian resolution. It was the only state to do so. By 2008, Russia had attracted thirty co-sponsors for its resolution in favor of a multilateral cyber arms-control treaty (Tikk-Ringas 2012, 7). Over its first decade, the Russian effort to promote new rules for state use of ICTs thus appeared to have gained greater traction among the members of the UN than the competing interpretation proposed by the United States.

A complete explanation of the apparent reversal in state positions by 2013 would include a number of factors. These include reputation damage suffered by Russia as a result of its alleged orchestration of cyberattacks against Estonia and Georgia (Tikk-Ringas 2012, 7); change in the composition of the GGE membership; and state learning about ICTs and their policy implications.

Ebert and Maurer (2013) suggest that regime type is an important intervening variable affecting state positions on cyber issues. They make a convincing case that regime type is important in accounting for intra-BRICS

in light of continued rapid technological evolution and diffusion over the period from 2008 to 2013. I do not discount any of these factors in explaining the emergence of a consensus that international law applies in its entirety in cyberspace. Rather, I argue that these other factors do not account for the actual social process of rule-making that took place in the First Committee, or for the way in which procedural rules of diplomacy and international law differentially empowered states in making and evaluating competing proposals.

Accordingly, I focus on the GGE processes culminating in the 2013 and 2015 consensus reports. Participants in the UN GGE process and UNGA’s First Committee were engaged in a rule-governed social practice of making, interpreting, and applying rules—in this case, for state conduct in the cyber domain. In doing so, they explicitly drew on agreed-upon procedural rules both in presenting their arguments and in evaluating those made by other participants. There was clear variation in actors’ competences in performing this social practice. These competences are essentially functions of actors’ respective expertise in employing the procedural rules that structure them. Such procedural rules exerted sufficient influence on the outcome to create consensus on the American proposal despite countervailing conditions that seem clearly to work against the emergence of such an agreement—worsening of US-Russia relations on the one hand and a global increase in contention over cyber issues on the other. Note that this argument allows for state action on the basis of logics of appropriateness but does not require it. At least some of the states pursuing a multilateral treaty-based regime for Internet issues do not seem to have abandoned their position; available evidence does not suggest that they have internalized the American position. However, in endorsing the reports by allowing them to be issued on a consensus basis, they have nevertheless conceded important ground that will structure the playing field in future iterations of this game of global cyber rule-making.

The Third Group of Governmental Experts

The third GGE met in three sessions during the period from August 2012 through June 2013. Its consensus (Brazil, Russia, India, China, and South Africa) policy differences on cyber issues, but I would add two points. First, this effect unfolded over time, as states learned about the technology and received input from civil society stakeholders. Second, democracies have nevertheless proven quite willing to contemplate extensive cyber monitoring programs that might be regarded as inconsistent with democratic values and human rights.
The report was issued on June 24, 2013. The report couched its conclusions as extensions of the previous GGE process, noting that the 2010 report had “recommended further dialogue among States on norms pertaining to State use of ICTs” (UNGA 2013a, 6). It broke new ground in affirming that “the application of norms derived from existing international law relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security and stability” (UNGA 2013a, 8). This is a direct affirmation by the GGE members that they understood themselves to be involved in a collective process of applying legal rules to a novel case. However, the 2013 report also noted that the application of such norms could not be settled in a single interpretive act. Rather, it acknowledged that “common understandings on how such norms shall apply to State behavior and the use of ICTs by States requires further study” (UNGA 2013a, 8).

The report makes clear that member states had already begun this interpretive process. It made the explicit claim that “international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.” This is a clear shift toward the American position that existing international legal rules already governed state use of ICTs, especially as the 2013 GGE included both Russia and China. By allowing production of a consensus report, these states were now on the record in supporting the American position. The report also made further progress in identifying particularly relevant bodies of international law in this context. It indicated the view of the GGE that “state sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.” Further, it found that “State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments.” Finally, it concluded that “States must meet their international obligations regarding internationally wrongful acts.” This last finding connects the state use of ICTs specifically to the law of state responsibility, which governs the limits on self-help in the event of a state being injured by another state’s breach of an international legal obligation. In particular, the GGE identified two potential circumstances in which the law of state responsibility might be applicable. The report asserted that “States must not use proxies to commit internationally wrongful acts” and that “States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs” (UNGA 2013a, 8).

As part of the First Committee’s work on cyber issues, the UN Secretary-General receives national submissions. These submissions provide information about state positions on relevant issues, the development of national cybersecurity efforts, and “possible measures that could be taken by the international community to strengthen information security at the global level” (UNGA 2013b, 1). Voluntary submissions were made by a variety of states—including members of the GGE as well as nonmembers, states at varying levels of development, and states with different regime types. Despite this variety, the data are too partial to create generalizations about variables that explain state positions. In any event, the theoretical approach taken here emphasizes that state positions are at least partially endogenous to the social process of rule-making and interpretation undertaken in the First Committee. To the extent that this is true, it is impossible to either explain or predict outcomes simply by examining state characteristics. Instead, the national submissions are useful as evidence of state positions on the interpretive work being undertaken by the GGE and in the First Committee, which constituted the immediate audience for the GGE report. The submissions included in the 2013 report by the Secretary-General range from May through September 2013. All were therefore made after the GGE had begun its work, and the majority were made prior to the production of the consensus report.

The United States did not make a submission to the UN Secretary-General; however, several of its close allies did. These submissions generally adopted similar positions to the American perspective that international law already governed state use of ICTs. Britain, in a May 2013 submission made prior to the GGE report, indicated its view that the “paramount concept” applicable to improving international security in the cyber domain is “that of the application of international law and the existing norms of behaviour that govern relations between and among states.” It asserted that “the United Kingdom firmly believes that these principles apply with equal force to cyberspace and an unambiguous affirmation by States that their activities in cyberspace will be governed by these laws and norms would lay the foundations for a more peaceful, predictable and secure cyberspace.” Britain also explicitly addressed the question of the appropriateness of an international treaty. It made clear that “the United Kingdom does not believe that attempts to conclude comprehensive multilateral treaties, codes of conduct or similar instruments would make a positive contribution to enhanced cybersecurity for the foreseeable future.” Its rationale was that “the complex and comprehensive nature of any binding agreement across the entirety of a cyberspace that is evolving at ‘net speed’ means that it could not be effective or
command widespread support without many years, possibly decades, of painstaking work on norms of behaviour and confidence-building measures to build up the necessary understanding and trust among signatories and to ensure that they can be reliably held to account for their adherence to their commitments.” The pragmatic nature of this rationale was reinforced by the claim that “experience in these agreements on other subjects shows that they can be meaningful and effective only as the culmination of diplomatic attempts to develop shared understandings and approaches, not as their starting point” (UNGA 2013b, 18–19).

The British position entails two central claims. The first is that existing international law already applies to state use of ICTs and thus to state conduct in the cyber domain. The second is that a multilateral treaty is unworkable and undesirable. With respect to the first claim, the British position draws on existing procedural rules that empower states to determine individually whether other states have breached international legal obligations owed to them. This kind of decentralized adjudication is essential to the customary international law on state responsibility (International Law Commission 2001) and also to international legal doctrines on self-defense. The argument on this ground is therefore that the cyber domain presents a straightforward example of applying existing rules to a novel case, in a way that states are explicitly authorized to do by the procedural rules of international law, subject to limits set out mainly in the law of self-defense and the law of state responsibility. Like the earlier American response to the Russian proposal for a multilateral treaty, this position likely reflects Britain’s substantive preferences, but the British government made the argument with reference to specific, identifiable standards for interpreting and applying existing international law. Thus, procedural rules for rule-making provide analytical leverage both on the substance of the British position and on the manner in which it was communicated.

On its second claim, the British submission appears to adopt a much more pragmatic tone that relies on diplomatic experience rather than international legal rules. This is likely because this claim was on weaker legal ground in opposing the idea of a multilateral arms-control treaty in the cyber domain. After all, the Russian position could be grounded in prior state practice erecting arms-control regimes for both nuclear and conventional weapons. It would be hard to sustain the argument that such a decision would be procedurally inappropriate, and even if existing rules of international law applied online, this would not procedurally preclude a multilateral treaty codifying or extending existing legal rules. This basic consistency of the Russian position with past state practice and accepted procedures for governing security problems arising from new technologies likely helps to explain the willingness of many states to co-sponsor the Russian resolution and to endorse a multilateral treaty on cybersecurity. However, the British submission also rejected the terminology of “information security” employed by the Russian government and others sympathetic to it. It indicated that “the United Kingdom does not recognize the validity of the term ‘information security’ when it is used in this context, since it could be employed in attempts to legitimize further controls on freedom of expression beyond those agreed in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights” (UNGA 2013b, 15). Thus, the British submission also argued against the appropriateness of the specific kind of cybersecurity treaty preferred by a number of governments on the grounds that such a treaty would be inconsistent with other international legal obligations. This kind of critical evaluation of another player’s rule-making proposal is consistent with my argument that states understood themselves as engaged in a rule-governed social practice of making, interpreting, and applying international rules. The British objection was clearly based in a substantive preference that reflected support for the protection of civil and political rights, but was expressed in terms of procedural rules that require consideration of the effect of proposed rules on states’ existing international legal obligations. It demonstrates that, when evaluating proposed global rules, states explicitly consider the compatibility of multiple simultaneously valid rulesets, and that they take into account secondary rules governing the interaction of these sets.

In enumerating threats to international peace and security emanating from cyberspace, the German submission (lodged the day after the GGE report) noted that “prevailing ambiguity about what norms apply in cyberspace creates additional unpredictability” (UNGA 2013c, 5). Accordingly, the submission noted that “Germany advocates developing broad, non-contentious, politically binding norms of State behaviour in cyberspace.” It expressed the view that such norms “should be acceptable to a large part of the international community and should include measures to build trust and increase security.” The framing of the submission in terms of “politically binding norms” rather than binding international legal obligations is somewhat puzzling. It may reflect a desire to avoid giving the appearance of endorsing a multilateral treaty-based approach in light of the long-standing Russian diplomatic effort for such a legal instrument. However, the German reply provided a clear endorsement of the GGE report. It indicated that
Germany “strongly welcome[s] the recommendations of the Experts on norms, rules or principles of responsible behaviour of States.” The German submission also affirms the relevance of many of the same bodies of international law deemed relevant by the GGE report. For example, it notes “the necessity to start a debate on international cooperation in the framework of attribution of cyber attacks...State responsibility for cyber attacks launched from their territory when States do nothing to end such attacks, despite being informed about them, and the responsibility of States not to facilitate areas of lawlessness in cyberspace, for example, by knowingly tolerating the storage of illegally collected personal data on their territory” (UNGA 2013c, 8–9). These observations make clear that Germany endorsed the application of the law of armed conflict, the law of state responsibility, and of international human rights law in the cyber domain. Just as the United States and Britain had done, Germany expressed its preferences in a manner simultaneously enabled and constrained by procedural rules for interpreting and applying existing rules of international law. It accepted the argument that existing bodies of international law were applicable, and also indicated that this finding required an ongoing process of interpretation to clarify how these rules applied in this substantive domain.

Like Germany, Canada and the Netherlands made national submissions after the production of the GGE report. The Canadian submission was less detailed in addressing questions of international law than those made by Britain and Germany. Nevertheless, it clearly endorsed the GGE report’s conclusion. Canada asserted that “existing treaty and customary law is applicable to the use of information and communications technologies by States, and is essential to maintaining peace and stability, and promoting an open, secure, peaceful and accessible information and communications technology environment.” Like the German submission, the Canadian response specifically enumerated the UN Charter, as well as international human rights law and international humanitarian law as bodies of international law relevant to the state use of ICTs (UNGA 2013c, 4). The Dutch response indicated that “the Netherlands is of the opinion that the development of norms for State conduct does not require a reinvention of international law, but rather needs the development of norms for State conduct does not require a reinvention of international law, but rather needs...stakeholders must comply with the particular values and principles that each country seeks to uphold.” Oman also articulated a variation of the Russian preference also cannot explain either the positions articulated by states with different declared preferences, or the existence of different procedural interpretations by other NATO members or close allies that expressed support for a free and open Internet, most notably including Spain and Japan.

Armenia and Turkey provided national submissions that did not address the question of the applicability of existing international law to cyberspace or the question of the appropriateness of a multilateral treaty. Each of these replies focused more on elucidating their national cybersecurity efforts (UNGA 2013c, 2–3, 21–4). It is possible that this gap indicates a relative lack of competence in applying international legal rules to this novel and complex technological domain, but it is also impossible (on the basis of available data) to rule out explanations based in domestic politics or in conceptions of national interest, though it is hard to imagine why a state might conclude that it lacks a national interest in participating in global rule-making.

Oman’s national submission, filed two days after the GGE report, proposed “regulating e-transactions and information and inter-State cybersecurity by establishing an international organization under the auspices of the United Nations.” Given that international organizations are typically constituted by a multilateral treaty, this position can be read as supporting the Russian proposal for such a legal instrument. However, the Omani submission illustrates the potential for broad state agreement on the applicability of international law to the cyber domain. It endorses a clear sovereigntist position asserting state authority over non-state actors in declaring that “stakeholders must comply with the particular values and principles that each country seeks to uphold.” Oman also articulated a variation of the Russian justification for an international instrument in contending that “States must join forces and cooperate to combat information security threats” (UNGA 2013c, 19–20). Adoption of this terminology indicates a particular interpretation of state authority vis-à-vis societal actors, and of the appropriate way to handle violations of human rights law in light of state sovereignty. But it is notable that these preferences were articulated in international legal terms that displayed awareness of international
legal rules of sovereignty having to do not only with the state’s substantive right to autonomy, but also with its superior position relative to non-state actors in questions of rule-making, interpretation, and application, as well as its equal position with respect to other states in these matters.

Ukraine, under the pro-Russian Yanukovych government, likewise expressed support for the Russian position. It defined information security as “the degree to which national interests in the field of information are shielded from external and domestic threats” and explicitly indicated that this definition included the “use of information infrastructure to disseminate information that incites animosity and hatred, in general or in a specific country” as well as the “use of cyberspace to destabilize society and undermine the economic, political and social system of another State or to spread misinformation designed to distort cultural, ethical and aesthetic values” (UNGA 2013b, 9–10). In service of these interests in maintaining regime stability, the Ukrainian submission expressed the view that “it may be time to draft a set of international principles to strengthen information and telecommunications network security and international security policy overall.” According to the Yanukovych government, “an important aspect of this would be to determine the international legal status of cyberspace and to enshrine, in regulatory and legal instruments, States’ jurisdictions with regard to the national components of this space (comparable to States’ air space and territorial waters) and the further regulation of issues related to cyberwar, cyberaggression, and so on” (UNGA 2013b, 14).

Like Oman, Ukraine was able to express its support for Russian positions on information security and a multilateral treaty in a manner consistent with existing procedural rules, and evidently saw value in doing so. Submissions discussed thus far have generally conformed with regime type: democracies (Britain, Germany, Canada, the Netherlands) opposed a multilateral treaty and accepted the argument that existing international law is applicable to cyberspace, while more authoritarian regimes (Oman, Ukraine) supported a multilateral treaty to deal with perceived gaps in international law. The irony of more authoritarian regimes promoting a multilateral legal instrument is indicative of the broad legitimacy of the procedural rules of the contemporary international system. This point is worth emphasizing. Despite illiberal preferences inconsistent with prevailing notions of thick multilateralism (Ruggie 1992; Reus-Smit 1999), authoritarian states have regularly and consistently adopted the vernacular of multilateralism and of contractual international law to advance their agendas. Far from making the claim that participation in the post-1945 rule-based global order has transformed the identity of these states or that these states have internalized the norms and rules underpinning that order, I am arguing instead that, to varying degrees, these rules: (1) constrain illiberal states, requiring them to take pains to express their positions in terms at least ostensibly consistent with these rules; and (2) enable them to advance such interpretations, albeit in ways that are subject to limits and constraints. Three national submissions are noteworthy in illustrating how procedural rules and the social practices they constitute can sometimes create strange bedfellows.

Unlike other American allies, Japan was skeptical about the applicability of existing international law to the cyber domain. Its national submission, made after the 2013 GGE report, expressed the view that “we must with urgency start developing realistic and feasible norms of behaviour to address current issues in a non-legally binding form.” The Japanese government based this proposal on its conclusion that “there are no international norms that regulate cyber attacks or cyber espionage in security, economic and social arenas. In addition, the validity of legally binding norms in cyberspace remains unclear at this stage” (UNGA 2013c, 14–15). That Japan would voice this view despite being a member of the GGE (and thus having endorsed its consensus report) is unusual. The expressed desire for norms rather than legal rules may reflect opposition to a multilateral treaty specific to cybersecurity issues, but this reading still places the Japanese position at odds with the conclusion of the GGE that the broader corpus of international law (treaty and custom) was already applicable. The internal inconsistency in the Japanese endorsement of the 2013 GGE report and its submission of a national position contradicting that report highlights the importance of distinguishing between applicable procedural rules for global rule-making and specific performances of that practice, which may be more or less socially competent. Japan effectively made contradictory assessments about whether there were rules or norms applicable to cyberspace without seeming to notice or justify this inconsistency, indicating a less skillful performance of the social practice of global rule-making. Skillful performances should generally be internally consistent, and should also anticipate and preempt such obvious potential criticisms. Nevertheless, the Japanese submission also demonstrates both the plasticity of procedural rules for international rule-making, as well as the apparent consistency of the Russian position with at least some such procedural rules, even in the eyes of an established democracy.

In its May 2013 national submission, prior to the GGE report, Spain similarly asserted that “the protection of an international legal framework to meet
cybersecurity threats is lacking.” It concluded that “there is a need for multilateral cooperation agreements in this area (analogous or similar to the International Convention for the Safety of Life at Sea (SOLAS)) whereby States would undertake to harmonize their legislation with a view to the prosecution of Internet crimes while attempting to ensure, to the extent possible, that anonymity, the absence of legislation and economic interests do not make the Internet the ideal breeding ground for crime and terrorism.” The submission also endorsed the view that “the international community should adopt whatever protection measures are deemed necessary, basing its action on an integrated global vision and, if possible, creating a single authority to lay down rules and standards common to all countries” (UNGA 2013b, 8–9). The Spanish position is clear about the appropriateness of governing the issue according to international law, and potentially also through an international intergovernmental organization; however, it does not display an appreciation of the implications of the Russian proposal for international human rights law, nor does it address the crucial question of whether existing international law applies in cyberspace.

Finally, Iran made a creative national submission indicative of its efforts to employ international legal rules to meet its policy objectives. Its submission emphasized access to ICTs in the developing world, opposing “the adoption of any measure to deny or restrict the transfer for advanced information and telecommunications know-how, technologies and means, as well as the provision of information and telecommunications services, to developing countries.” This line of argumentation was likely intended as an attempt to delegitimize sanctions in this industrial sector by invoking accepted rules from other domains of international law that establish the appropriateness of flexibility and differential treatment for postcolonial, low-income states. It leverages informal analogues to legal precedent in the international system that grant ideas accepted in other issue-areas a prima facie claim to acceptance, in this context to oppose the legal and political legitimacy of sanctions and export controls. While unlikely to sway industrial democracies, it is likely that this kind of claim would be well received by members of the Group of 77 (G77).

Iran also expressed its “view that the most appropriate international mechanism for consideration of the developments in the field of information and telecommunications in the context of international security is to launch a process within the United Nations with the equal participation of all States.” This procedural argument effectively endorses a formal multilateral conference on the basis that it is consistent with the fundamental rule of juridical equality among states. In so doing, Iran explicitly tied the argument for a multilateral process to fundamental rules of international holding that states are formally equal in establishing international legal obligations. The submission went on to suggest that “the main purpose of that process should be to develop a common understanding between States about the importance of enhancing security of information and telecommunications.” It further recommended that this process be conducted “in the format of international conferences every five years to produce political outcomes ranging from declarations to codes of conduct,” with “the ultimate goal” of “the progressive development of solid international legal foundations for strengthening and ensuring the security of global information and telecommunications.” Here, Iran called for the utilization of commonly accepted procedures of periodic review, adopting a procedural norm used in the Non-Proliferation Treaty and other arms-control agreements, as well as in other high-profile areas like climate governance and ICT-related processes such as the International Telecommunication Regulations and the World Summit on the Information Society. Further, in referring to the progressive development of legal foundations, Iran referred explicitly to the mandate of the International Law Commission (UNGA 2013c, 11–13). This reference indicates awareness, and signals acceptance, of prevailing procedural rules for clarifying international legal disputes.

Despite support for a diplomatic process leading to a multilateral treaty, Iran also acknowledged that “as a general principle, international law is applicable and therefore should be applied to the use of information and telecommunications technologies and means by States.” It went on to indicate its interpretation of this claim as entailing states’ legal obligations to respect UN Charter provisions in the cyber domain. In this respect, Iran specifically enumerated Article 2 (paras. 3–4) obligations to settle disputes by peaceful means and to refrain from the threat or use of force (UNGA 2013c, 11–13). This latter interpretive argument is perhaps unsurprising given the injury suffered by the Iranian government as a result of Stuxnet, but it demonstrates that at least some authoritarian regimes were able to employ the accepted interpretive rules of international law and diplomacy to advance their values and interests in light of the American response to the Russian proposal for a multilateral treaty.

This conclusion clearly reflected Iran’s recognition that the Charter accorded it valuable entitlements both to set its internal policies on Internet-related matters and to object to American violations of its sovereignty.
But it is equally noteworthy that Iran understood the importance of registering these claims in the GGE process even as it still sought to advance a multilateral (as opposed to multistakeholder) process for creating, interpreting, and applying such rules in the future. Iran thus sought to recast the American position that existing international law applied in cyberspace as consistent with the Russian proposal for a multilateral treaty. This interpretation had been available since the 2004 American claim that existing international law applied online. It is not clear why the gap had not been bridged prior to 2013, but it does appear that this emerging understanding—arrived at via an international process of interpreting and applying rules—at least partially explains the puzzling outcome, form, and timing of agreement in the 2013 GGE despite inhospitable conditions.

The 2013 GGE report and related national submissions demonstrate the continued existence of a diversity of state positions on the appropriateness of a multilateral cyber treaty. But, more fundamentally, they demonstrate virtually universal agreement on the legitimacy of the basic procedural frameworks of international law and diplomacy for dealing with these issues. Even Britain, a staunch supporter of the multistakeholder model of Internet governance, expressed the view that “it is for Governments to lead international efforts to improve understandings over acceptable State behaviour and in tackling cybercrime” (UNGA 2013b, 16). Similarly, states adopting revisionist positions sought to do so by virtue of a multilateral treaty and a new international organization within the broader UN system. States as diverse as Germany and Iran, with respect to both their basic attitudes toward the international system and toward Internet freedom and state military use of ICTs, nevertheless agreed on the applicability of the UN Charter and other fundamental provisions of international law. No doubt, this agreement on relevant procedural rules was a product, in part, of increasing realization by authoritarian regimes that the American interpretation provided discursive resources for them to advance their Internet policy agendas both at the domestic and international levels, as Iran did in its national submission. But if that is the case, it is puzzling that authoritarian states were unwilling to accept the American claim over the period from 2004 to 2013. Thus, substantive preferences alone are insufficient to account for the form and timing of the outcomes in this case, as well as for the process by which states arrived at these outcomes. Likewise, the near-unanimous expression of support for further interpretive work shows that states simultaneously regarded this rule-governed social practice as legitimate, that they regarded its implications for policy as unclear (to varying extents), and that they saw it as a way to advance their values and interests.

The Fourth Group of Governmental Experts

The fourth GGE began its work in July 2014. It met four times prior to issuing its June 2015 report. The group was enlarged, growing from fifteen states to twenty. It also became more culturally diverse; Argentina, Australia, Canada and India were dropped while Brazil, Colombia, Ghana, Israel, Kenya, Malaysia, Pakistan, and the Republic of Korea were added. Despite this larger, more diverse membership, the GGE made important gains in interpreting and applying existing rules of international law to the cyber domain. Its success also came in spite of considerable international controversy over electronic espionage practices and over institutional modalities for governance of core Internet technical functions.

The GGE endorsed the view that “the adherence by States to international law, in particular their Charter obligations, is an essential framework for their actions in their use of ICTs” and that “these obligations are central to the examination of the application of international law to the use of ICTs by States.” Beyond a broad endorsement of the UN Charter, the GGE also enumerated several other core principles: “sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other states” (UNGA 2015b, 12).

The report also provided consensus views on several other critical matters. First, it stated clearly that “States have jurisdiction over the ICT infrastructure located within their territory.” Questions pertaining to jurisdiction are important to resolving a variety of international legal disputes over cyber issues, including potential trade disputes and law enforcement cooperation on criminal matters. Second, the report “notes the established legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction.” These principles are central to the law of armed conflict, in particular to jus in bello governing state conduct in armed conflict. While the GGE did not reach consensus on inclusion of the law of armed conflict as a body of law clearly applicable in the cyber domain, the inclusion of its central principles in a consensus
report encompassing the entirety of the permanent membership of the Security Council is an important step in the development of international law. Finally, the GGE reached agreement with respect to some important implications of the application of the law of state responsibility to the cyber domain. It affirmed that “States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts” (UNGA 2015b, 12–13). This conclusion is important to dealing effectively with cybercrime and also to ensuring that states do not exploit attribution difficulties in the cyber realm (Nye 2016/17) in order to circumvent their legal obligations under the Charter. Finally, while affirming that “States must meet their international obligations regarding internationally wrongful acts attributable to them under international law,” the GGE noted that “the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State” (UNGA 2015b, 13). This is important, both because prevailing interpretations of customary international law apply a high standard to the attribution of an activity to a state (International Law Commission 2001), and also because of the possibility that various kinds of parties (including increasingly sophisticated non-state actors) may attempt to conceal their involvement in a cyberattack by launching it from a third-party state or by employing technical measures to make it appear that they have done so.

In addition to its interpretive work applying existing international law to the cyber domain, the GGE also proposed several candidate norms for responsible state conduct. While it presented these as “voluntary, non-binding norms of responsible State behaviour” and commended them as useful ways to “reduce risks to international peace, security and stability,” many of the candidate norms are themselves closely related to the interpretations of existing international law promoted by the GGE. In framing the proposed candidate norms, the GGE gave a definition of norms that very closely approximates constructivist scholarship. It declared that “norms reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States.” The GGE also affirmed its own status as a norm entrepreneur, in claiming that “the task before the present Group was to continue to study, with a view to promoting common understandings, norms of responsible State behaviour, determine where existing norms may be formulated for application to the ICT environment, encourage greater acceptance of norms and identify where additional norms that take into account the complexity and unique attributes of ICTs may need to be developed” (UNGA 2015b, 7). The GGE thus clearly understood its work as entailing a structured, rule-governed process of rule interpretation and application.

These norms include the obligation to cooperate in improving cybersecurity and in preventing harmful ICT practices capable of undermining international security. They also include a cautionary norm for state conduct in responding to cyberattacks. This candidate norm calls on states to “consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences” before engaging in self-help measures (UNGA 2015b, 7). This norm explicitly contemplates, and specifies appropriate procedures for, ongoing attempts to apply existing rules to novel cases. These procedures closely resemble the provisions of the Vienna Convention on the Law of Treaties pertaining to treaty interpretation. This demonstrates that the GGE, as state representatives, saw secondary rules and resulting practices of global rule-making and interpretation as essential to international security. Participants also drew on well-established rule-making procedures in novel empirical terrain.

Several of the proposed norms can be grouped under the heading of requiring states to govern their own territories in a responsible manner—i.e., to carry out their international duties qua states. These norms include: the obligation of states to police their own territory and to ensure it is not employed to carry out attacks on other states; an obligation to consider effective practices for law enforcement cooperation; and an obligation to respect human rights in the digital realm. These norms also address the state’s role in the ICT market. In this regard, they assign states the responsibility to try to ensure supply chain integrity in hardware and software and the obligation to encourage reporting of ICT vulnerabilities. Finally, the norms proposed by the GGE deal with state obligations to assist other states requesting assistance with ICT attacks, and to refrain from interference with or exploitation of computer emergency response teams (CERTs) (UNGA 2015b, 7–8). Like past GGE reports, the 2015 report also consolidated global progress on confidence-building and capacity-building measures pertinent to international security (UNGA 2015b, 9–12).

As in the 2013 GGE process, the United States, China and Russia refrained from making public submissions of their national views to the UN Secretary-General. However, the United States opted to publish its private submission in a State Department legal digest. The document supports the view that the United States understood
itself as engaged in an ongoing process of interpreting and applying international legal rules to particular cases. Writing about the 2013 GGE, the document noted the consensus regarding the applicability of existing international law to the cyber domain and reminded the participants that “the Experts also noted the need to further study how international law applies, and recommended that States should further consider how best to cooperate in implementing norms and principles of responsible behavior in the ICT environment” (de Guymon 2014, 733).

The American contribution to the 2015 GGE also addressed the procedural challenges inherent in applying existing international law to a fast-moving technological environment. It pointed out that this kind of challenge is “not unusual” and that “similar challenges have been confronted when applying existing international law to other new technologies and situations.” The proper approach to such cases, it argued, “is providing decision-makers with considerations that may be taken into account when determining how existing law applies to cyberspace.” As a result, it concluded that “this UNGGE needs not reach consensus on exactly how existing principles of international law apply to all conceivable cyber situations.” This argument amounted to a recognition of the problem of incomplete contracting—that rule sets can never specify ex ante every possible future situation. Rather, “it would suffice to identify the basic legal principles that apply and then reach a consensus on some of the relevant considerations States should take into account when they confront real-world situations.” It reminded GGE members that “we need not spell out how international law applies to all hypothetical scenarios” and that states “have not done so with respect to other types of operations, and in any case there will undoubtedly be situations that arise that we are unable to predict given the speed of change in ICTs.” Adopting a framework for modalities of interpretation “will assist all States in meeting the challenge of applying, and abiding by, existing international law when real-world situations involving the use of ICTs present themselves” (de Guymon 2014, 733–4). The submission thus recognized the existence of rules providing for the decentralized, ongoing practice of interpreting how international law applies in cyberspace, and indicated the American government’s willingness to participate in such a practice alongside its fellow states.

The American submission focused on principles pertaining to the law of armed conflict and its application in the cyber domain. In doing so, it advanced claims about how to apply existing rules of international law, albeit claims rooted in American interpretations of those rules. It asserted that “cyber activities may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the UN Charter and customary international law.” Accordingly, the State Department analysis concluded that “a State’s inherent right of self-defense...may in certain circumstances be triggered by cyber activities that amount to an actual or imminent armed attack.” It asserted that “this inherent right of self-defense...applies whether the attacker is a State actor or a non-State actor.” This claim was accompanied by interpretive guidance that emphasized considering the nature and extent of the attack (e.g., whether it caused injury or loss of life, or the physical destruction of property), the nature of the attacker, the nature of the target, “and the intent of the actor” (de Guymon 2014, 734).

Additionally, the American submission advanced the argument that states may, at least in some circumstances, use cyber means to respond to kinetic attacks and vice versa. This argument amounts to the normalization of cyber weapons as a military means under international law, in direct response to earlier Russian attempts to regulate or perhaps even prohibit them. In its accompanying interpretive guidance, the submission indicated that “a State facing an imminent or actual armed attack by a non-State actor in or through cyberspace generally must make a reasonable, good faith effort to seek the territorial State’s consent before using force on its territory against the non-State actor to prevent or end the armed attack.” It further suggested that “the requesting State should give the territorial State a reasonable opportunity to respond, recognizing that the reasonableness of a timeframe in a particular context may be determined in relation to the nature of the actual or imminent armed attack.” Notwithstanding this general obligation to seek consent, the submission is clear in expressing the American view that “a State may act without consent...if the territorial State is unwilling or unable to stop or prevent the actual or imminent armed attack launched in or through cyberspace.” However, if it does so, it “must take reasonable measures to ensure that its defensive actions are directed exclusively at the non-State actors when the territorial State is not also responsible for the armed attack” (de Guymon 2014, 735).

These arguments represent far-reaching interpretations of the applicability of the law of armed conflict to the cyber domain that potentially enable states to undertake cyberattacks in a wide range of circumstances. The wisdom of these interpretations, and whether they are genuinely consistent with American national interests given the potential of such a regime to destabilize the Internet, are beyond the scope of my analysis here. The key point is that the American government clearly engaged in a process of applying existing legal rules to a novel case.
It did not do so in a random fashion, but rather in a way shaped by procedural rules governing how to legitimately interpret and apply international law. The section of the submission dealing with the application of retorsion and other non-forcible countermeasures (de Guymon 2014, 738–9) was clearly shaped, for example, by deep understanding of the customary international law pertaining to state responsibility. At the same time, it clearly exercised discretion and judgment in these interpretive activities, conducting them in a way designed to shape prevailing global interpretations of international law in a manner consistent with American values and interests. The segments of the submission dealing with sovereignty and jurisdiction, for example, noted that “the exercise of jurisdiction by the territorial State, however, is not unlimited; it must be consistent with applicable international law, including human rights obligations” that protect freedom of speech independent of the medium and without regard to national frontiers (de Guymon 2014, 737–8). Similarly, the submission’s approach to jurs ad bellum issues, discussed above, seems clearly intended to exploit continuing American military dominance in the cyber domain as a means to project force at low cost should the need arise. The key point is that, just as these interpretations reflected official understandings of American interests, they were also both enabled and constrained by American understandings of the appropriate ways to interpret and apply existing international law, even when this imposed limits on the exercise of a significant asset of national power.

Russia, in conjunction with China and other members of the Shanghai Cooperation Organization (SCO), also made clear efforts to construct persuasive interpretations of how international law should be applied in the cyber domain. In this regard, the most notable development was the presentation of an updated version of a proposed International Code of Conduct for Information Security. Originally advanced in 2011, the code of conduct prioritized state sovereignty and appeared to give lip-service to human rights obligations while emphasizing the rights of states to control dissemination of information within and across their borders (Ebert and Maurer 2013, 1067). These proposals were consistent with long-standing Russian efforts to create a multilateral cyber treaty. However, the shift from a formal treaty to a soft-law code of conduct reflects an increasingly sophisticated understanding on the part of these governments about the growing reliance of the contemporary system of global governance on a variety of soft-law mechanisms, as well as of the opportunities to assert sovereignty afforded by acceptance of the idea that international law applied to state use of ICTs. This evolving understanding of contemporary procedural rules pertaining to the use of soft law instruments is thus a contributing factor in the willingness of Russia and its like-minded states to accept the applicability of existing international law. It also demonstrates the potential for practices of rule-making to generate outcomes unintended by the original proponent of a particular proposal. I address this point in greater detail in the conclusion, where I examine proposals made in the 2018 work of the First Committee, in which Russia and China have sought to advance their substantive agendas in ways consistent with these evolving procedural rules.

In January 2015, an updated version of the code of conduct was submitted to UNGA by China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan (UNGA 2015c). An initial analysis of the differences between the 2011 and 2015 versions found that the 2015 version had been altered with a view to broadening its international support. For example, the reference to an international norm against using “information weapons” had been dropped, presumably out of recognition that many states were concerned about the effect of this language on international human rights. In another attempt to make the code of conduct palatable to states emphasizing online rights, the 2015 code of conduct explicitly endorsed the notion of parity for human rights regardless of medium. However, the section also prominently included the exceptions to the right of freedom of expression enumerated in Article 19 of the International Covenant on Civil and Political Rights.

Beyond these efforts to make the code of conduct compliant with the letter (if not the spirit) of international human rights law, the updated version contained two notable changes. First, it added a norm calling on states to refrain from acting to “take advantage of” a “dominant position in the sphere of information technology.” While this language was likely intended to blunt Western dominance, it might also be read as an attempt to reassure developing states that China would act with restraint in exerting its own technological influence. Second, the updated version of the code of conduct addressed institutional modalities for Internet governance. In this regard, it asserted that “all States must play the same role in, and carry equal responsibility for, international governance of the Internet” (Rõigas n.d.). This phrase was likely intended to capitalize on support for multilateral institutions and suspicion of multistakeholder processes throughout much of the developing world that are based in part on these states’ relatively greater familiarity with (and acceptance of) the procedural rules of multilateralism than multistakeholderism, and also to further undermine the legitimacy of multistakeholder Internet governance.
Despite the apparent success of the American interpretation that existing international law applies to cyberspace and the shift in SCO strategy toward a soft-law code of conduct (at least as an initial step), the process of interpreting and applying international law in the cyber domain will continue. Available procedural rules conditioned state choices about the nature of their proposals and the ways in which they presented them, but they have not yet fundamentally altered the identity or perceived interests of Russian or Chinese policymakers.

As in the 2013 GGE process, procedural rules for making, interpreting, and applying international rules also shaped the efforts of other states to evaluate the proposals advanced by leading states (UNGA 2014a,b, also shaped the efforts of other states to evaluate the policymakers. them, but they have not yet fundamentally altered the

interpretation that existing international law applies to cyberspace and the shift in SCO strategy toward a soft-law code of conduct (at least as an initial step), the formal social process of interpreting and applying specific rules of international law, and thus in ways enabled and constrained by accepted procedures for interpreting and applying these rules.

France noted its efforts “to establish an international normative framework based on current international law, as well as confidence-building measures and specific standards of conduct in cyberspace” (UNGA 2014b, 3–4). It thus signaled its acceptance of the American interpretation of the applicability of existing international law to cyberspace. The Republic of Korea, another first-time participant in the GGE, expressed its view that “agreeing on a set of international norms and confidence-building measures, building the capacity of developing countries and promoting cooperation among computer emergency response teams are key areas for international cooperation.” Coming on June 30, 2014, prior to the initial meeting of the GGE, the Republic of Korea’s declaration serves as another indication that a novice participant was prepared to engage in the work of the GGE and understood both the substantive nature of its work as well as the relevant process for participating in a socially competent manner.

Spain’s submissions to the Secretary-General during the 2015 GGE process are especially noteworthy, as they illustrate the clearest evolution of a national position in response to social practices of rule-making and interpretation. In its 2013 submission, Spain had expressed interest in “multilateral cooperation agreements” and in the creation of “a single authority to lay down rules and standards common to all countries” (UNGA 2013b, 8–9). In contrast, by June 30, 2014 (prior to the first meeting of the 2015 GGE), Spain had altered its position. While it made clear its view that “the United Nations has a very important role to play in building international consensus in this area” and its support for “institutional dialogue within the framework of the United Nations in order to guarantee peaceful and secure use of information technologies,” the Spanish government now also indicated that it “supports the recommendations of the 2013 report of the United Nations Group of Governmental Experts” (UNGA 2014b, 5). The submission omitted any reference to the creation of further multilateral treaty instruments or to the creation of a global authority to make rules pertaining to cybersecurity. Spain also committed to the notion that “States should continue reflecting on how the principles and norms of international law should be interpreted and applied in cyberspace; especially those relating to the threat or use of force, to humanitarian law and to the protection of the fundamental rights and freedoms of the individual” (UNGA 2015a, 13). This position is couched explicitly in terms of a decentralized, informal social process of interpreting and applying specific
bodies of existing international law, in line with those enumerated by the GGE in its work.

Participation in a rule-governed process of deliberation about how to interpret and apply existing rules of international law to state military use of ICTs thus coincides with a clear change in the Spanish position on the applicability of existing international law. That position converged with those of other states participating in the 2015 GGE. While available evidence does not permit strong causal claims about the effect of procedural rules relative to other factors in explaining the change in Spain’s position, it is notable that there was no identifiable change over this same period in Spain’s broader Internet policy, and thus no reason to expect that Spanish interests explain the change of position. It is also notable that the Spanish position converged with those of the other participants—despite the continued existence of varying preferences among those states on a range of crucial questions pertaining to Internet governance, digital human rights, and cybersecurity, including the desirability of a multilateral approach.

National submissions to the Secretary-General pertaining to the 2015 GGE were not unanimous in their endorsement of the American approach. The Qatari submission, in particular, clearly preferred the multilateral approach. The June 24, 2015 submission indicated that “the State of Qatar believes that information security is crucial for national and global security.” It thus endorsed the SCO terminology explicitly meant to communicate a concern with societal and regime stability. It further noted that “the State of Qatar believes that the international community can contribute to information security by continuing to work towards a binding international instrument to safeguard information security” (UNGA 2015a, 11–12). Finally, none of the states presenting the updated version of the code of conduct for information security provided national submissions to the Secretary-General. Though Russia and China endorsed the consensus report of the 2015 GGE, they opted not to provide further interpretive clarification, at least through this mechanism, on their formal positions. Their modification of the proposed international code of conduct indicates growing familiarity with soft-law mechanisms for making and applying international rules but does not likely signal a shift in their underlying preferences for cyber governance modalities.

Conclusion

Participants in the work of the First Committee and the GGE shared common understandings about the nature of their work. They understood themselves to be engaged in a common rule-making effort that required the interpretation and application of general rules in the context not only of particular cases, but also of adjacent rule sets such as the law of armed conflict and the law of state responsibility. Procedural rules shaped the proposals and the evaluative acts of all the participants. These rules, for example, influenced the terms in which the United States presented its opposition to the initial Russian proposal for a multilateral treaty. They also affected the American national submission to the 2015 GGE, which explicitly presented the GGE’s work in terms of rule application and engaged in detailed interpretive discussion of various bodies of international law and their application to the cyber domain.

Similarly, procedural rules shaped Russian actions. The initial Russian decision to pursue the question of information security via the First Committee of UNGA itself reflected a core degree of procedural competence. This competence is no doubt partially responsible for the early success enjoyed by the resolution; it was regarded as procedurally competent by other states. However, the Russian claim that there was no applicable international law was rejected by all GGE participants, in favor of the argument that the core rules of international law are technologically agnostic. That Russia, China and Iran, among others, accepted this interpretation first offered by the United States reflects both the inability of these states to offer a procedurally valid counterargument, as well as their eventual recognition that sovereignty and various UN Charter provisions offered powerful protections for their interests in regime survival.

Russia and China have also shown the ability to update their respective procedural knowledge. After gaining experience and comfort with soft-law instruments, they shifted toward pursuit of an international code of conduct rather than (or at least as a prelude to) a multilateral treaty. They further updated this proposed code of conduct in 2015 to address the interpretive objections lodged by other states about the implications of their positions for adjacent bodies of international law—in particular, for human rights law. It is also noteworthy that, after 2013, there was almost no contestation of the idea that existing international law applies in cyberspace. Instead, states sought to determine which specific bodies of international law were relevant and the ways in which they applied.

The influence of procedural rules can also be identified in other states’ submissions to the Secretary-General. These documents collectively demonstrate that all participating states had a baseline understanding of appropriate procedures. This is an important point. Despite their considerable substantive differences on various areas of
cyber policy, states were not at all confused about the appropriate venue and most of the appropriate procedures in which to pursue agreement. Nevertheless, the national submissions establish significant variance among states in terms of their social competence in performing specialized tasks for interpreting and applying rules. The most procedurally competent proposals were generally made by large, wealthy states that tended to accept the applicability of existing international law and that tended to oppose the creation of a multilateral cybersecurity treaty. This group of states is distinguished by its greater propensity to accept the legitimacy of soft-law modalities for global governance. At least some of the states that gave procedurally less competent performances in the early phases of the interpretive process also showed improvement over time, adopting substantive positions and procedural understandings consistent with those adopted by the most competent performers. While it is difficult to separate the relative effects of procedural rules from the effects of common interests and values in explaining these patterns, it seems reasonable to conclude (at minimum) that the procedural rules served as a focal point for reducing transaction costs—a broadly accepted mechanism for explaining cooperation in IR theory. Shared ideas about appropriate procedures do seem to make reaching agreement easier and condition the nature of the agreements that states reach, and states with greater procedural competence are more likely to realize their preferred outcomes in rule-making processes.

Most fundamentally, agreement among states on legitimate rules for making, interpreting, and applying rules can help to account for the emergence of a consensus that existing international law applies in the cyber domain at a time when relations between the United States and Russia were deteriorating, and when cyber issues had become more contentious at the global level. Ironically, it may turn out that the supposed hard case of cooperation in international security is more amenable to international agreement on legitimate rules and norms than the formerly purely technical functions of Internet governance. Part of the explanation for this difference seems to be relatively greater agreement among states in the First Committee on legitimate procedural rules, as compared with the diverse array of state and non-state actors involved in less institutionalized settings for Internet governance (Raymond and DeNardis 2015).

While the fifth iteration of the GGE process, which concluded in June 2017, was unable to agree on a consensus report, this does not diminish the progress made in the 2013 and 2015 reports. It would be incorrect to claim that short-term prospects for further development of cyber norms are good or that states will fully comply with the norms articulated by the GGE, especially given apparent Russian interference in foreign elections. However, the chair of the 2017 GGE indicated substantial areas of agreement among participants and held open some degree of hope that interpretive work on applying international law to the cyber domain would continue (Geneva Internet Platform 2017). This indicates commitment to the broader process, which is an important consideration in the evaluation of norms processes (Finnemore and Hollis 2016). Regardless of the GGE’s future, its previous reports remain valid and have not been repudiated. They will therefore comprise part of the normative environment in which all relevant state conduct occurs (Sandholtz 2008). Most important, the lack of a consensus report in 2017 does not undermine the explanation advanced here for the form, timing, process, and outcomes observed in 2013 and 2015.

Social practices of rule-making remain highly relevant to explaining and understanding the First Committee’s ongoing efforts on cybersecurity. In the seventy-third UNGA, the committee adopted two competing resolutions. The first, led by Russia and China, was adopted by a vote of 109 to forty-five, with sixteen abstentions. The second, led by the United States, was adopted by a vote of 139 to eleven, with eighteen abstentions (United Nations 2018). The fact that the resolutions were adopted by vote, rather than by consensus, is itself an example of states employing procedural rules strategically to achieve their preferred objectives. The requirement to vote on the competing resolutions rather than reconciling them into a consensus document was noted with regret by representatives (United Nations 2018).

The resolutions were also crafted to try to employ procedural rules to secure support. The Russian resolution specifies a selection of rules from previous GGE reports for further development and negotiation by an “open-ended working group acting on a consensus basis” (UNGA 2018a, 5). In selectively endorsing specific findings from the 2013 and 2015 GGE reports, the Russian resolution is an attempt to shift the referential baseline for agreed-upon candidate norms in the First Committee’s work process. In doing so, it relies on procedural rules that afford weight to previous agreements. This move was explicitly noted and criticized by the American representative on the First Committee, who argued that the Russian resolution “imposes a list of unacceptable norms and language that is broadly unacceptable to many States” and noted that the competing American resolution “mirrors previous consensus draft resolutions” (United Nations 2018).
The Russian resolution also departed from past First Committee practice by calling for a negotiating group rather than a study group. In doing so, it sought to upgrade the process and put it in a position to create more binding, higher-status outcomes. By making the working group open to all UN members, Russia sought to portray the prior GGE process as procedurally illegitimate, or at least inferior to its proposed process, which it portrayed as “more democratic, inclusive and transparent” (UNGA 2018a, 5). Treating this difference as consequential enough to split the resolution makes sense only if Russia understood the procedural change as socially meaningful. In contrast, the American resolution called for a new iteration of the GGE study group. It also endorsed prior GGE reports in their entirety, rather than specifying particular recommendations as worthy of further discussion. However, the American resolution implicitly addressed Russian criticisms of the procedural legitimacy of the GGE. First, it called for the GGE to be composed “on the basis of equitable geographical distribution,” in line with UN practice of representing various regional groupings (UNGA 2018b), thereby highlighting the consistency of the GGE process with established UN practice. Second, it tasked the Office for Disarmament Affairs with convening consultations with various regional intergovernmental organizations prior to the GGE process. Third, it tasked the GGE chair with arranging a pair of two-day consultative meetings open to all UN member states to add a universal component to the GGE’s deliberations (UNGA 2018b).

These ongoing efforts make clear that states continue to have deep disagreements about state military use of ICTs and about global cybersecurity governance more broadly. The agreement that international law applies online, embodied in the 2013 and 2015 GGE reports, was not a panacea. However, the GGE reports also demonstrate that leading states understand procedural rules to be vital tools in achieving outcomes in line with their values and interests. The reports suggest that appeals rooted in procedural justice are regarded as valuable ways to secure approval for preferred proposals and to undermine undesirable ones, and that procedural criticisms require rebuttal. They also suggest that authoritarian states are increasingly skillful in deploying legitimate practices of rule-making in creative ways that align with illiberal objectives, and that we may see the emergence of authoritarian multilateralism.

One possible objection to the argument advanced here is that any outcome would have been shaped by procedural rules for rule-making, and that there is no way to gauge the causal effect of these procedural rules since they are always present. Another related objection is that any particular set of procedural rules permits all kinds of substantive claims to be made, and that procedural rules therefore do not impose meaningful restrictions on actors. Both objections miss crucial facets of how social practices of rule-making work. While it is true that procedural rules shape any conceivable outcome in a situation where the relevant actors are able to jointly engage in collective rule-making and interpretation, their effects are not binary in nature. Compliance (or not) is only one of several choices actors face about what to do to, with, or about a particular rule. Actors also face choices about precisely how to comply (or not), and about whether and how to interpret a rule, justify behavior in light of a rule, and so on. And rules exist in complex sets, such that what the same actor feels is acceptable or appropriate to do about an individual rule in one situation, subject to additional rules A, B, and C, may be different than the perceived range of acceptable responses to the same rule in a different situation, subject to additional rules B, D, F, and K. Other variables, like the subject matter, the stakes involved, actors’ skills with procedural rules, and the identity of the other involved parties, will also affect this calculus.

In this case of cybersecurity, the most obvious such counterfactual would be one in which the parties accepted the Russian call for a multilateral treaty. This outcome was possible, and would have been shaped by (among other factors) the participants’ views about applicable practices of rule-making. However, these same practices of rule-making, and the procedural rules that constitute and regulate them, made this outcome less likely. While the Russian call for a multilateral treaty was consistent with a range of international security governance arrangements, the claim that existing international law did not apply was deeply flawed. In fact, international law is held to apply to all state conduct. The technological means by which such action takes place is virtually never held to affect whether international law applies; at most, it may affect how it applies. In breaking so clearly from accepted international legal procedure, Russia left itself open to the reply that a treaty was either unnecessary or premature.

Such a reply did not fully determine the actual outcome of the case. The parties could have concluded—and may yet conclude—that a multilateral treaty is desirable. However, the recognition in the 2013 GGE report that existing international law applied to state military use of ICTs was a crucial branching point, as it both: (1) raised a host of questions about precisely how these multiple bodies of law apply (individually and in combination); and (2) suggested a clear process of international legal and diplomatic rule-making and interpretation as the
contextually appropriate way to resolve these questions. While it is true that further success in reaching common ground has thus far proved elusive, it is important to note that, even in the twentieth century during which a great deal of international law was codified, such efforts often spanned decades and did not all succeed. Further, ongoing Russian and American efforts to use explicitly procedural gambits to advance their interests on these questions demonstrate that great powers are clearly aware of these rules and that they regard them as consequential.

If rule-governed social practices for making, interpreting, and applying global rules matter in explaining the success or failure of particular attempts to change international rules and institutions even in a complex, novel, and contentious security case, there is a good basis to expect that these rules and practices are of considerable general importance across the contemporary system of global governance. These procedural rules are central to providing actors with the social resources they require to participate in a mutually intelligible practice of global governance that is a major means for the reproduction and transformation of the social structure of the international system. Accordingly, these procedural rules also shape—in tandem with actors’ identities, interests, and capabilities—the substantive rules that constitute and govern the other practices, beyond rule-making and interpretation, that collectively define international relations in a particular social context.

Acknowledgements
Thanks to the editors and the anonymous reviewers for their helpful comments, as well as to David Welch, Emanuel Adler, Steven Bernstein, Jon Lindsay, and other participants in a seminar at the University of Toronto; Peter Haas, Paul Musgrave, and other participants in a seminar at the University of Massachusetts, Amherst; Niels Nagelhus Schia, Lilly Pijnenburg Muller, and the other participants in a seminar at the Norwegian Institute of International Affairs (NUPI); and Chris McIntosh, Aaron Brantly, and Samantha Bradshaw. Research assistance was provided by Stefanie Neumeier and Josie Davis. Financial support was provided by the Norwegian Research Council’s IKTPLUSS Program and Policy Center at the University of Oklahoma, and by financial support was provided by the Cyber Governance Project at the University of Toronto; Pe- ter Nagelhus Schia, Lilly Pijnenburg Muller, and the other participants in a seminar at the Norwegian Institute of International Affairs (NUPI); and Chris McIntosh, Aaron Brantly, and Samantha Bradshaw. Research assistance was provided by Stefanie Neumeier and Josie Davis. Financial support was provided by the Cyber Governance Project at the University of Oklahoma, and by the Norwegian Research Council’s IKTPLUSS Program under grant number 288744, “Digital Vulnerability and National Autonomy.”

References
Abbott, Kenneth W., Robert O. Keohane, Andrew Moravcsik, Anne-Marie Slaughter, and Duncan Snidal. 2000. “The Concept of Legalization.” *International Organization* 54 (3): 401–19.
Abbott, Kenneth W., and Duncan Snidal. 2000. “Hard and Soft Law in International Governance.” *International Organization* 54 (3): 421–56.
Acharya, Amitav. 2004. “How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism.” *International Organization* 58 (2): 239–75.
Adler, Emanuel, and Vincent Pouliot. 2011. “International Practices.” *International Practice* 3 (1): 1–36.
Adler-Nissen, Rebecca. 2009. “Late Sovereign Diplomacy.” *Hague Journal of Diplomacy* 4 (2): 121–41.
Adler-Nissen, Rebecca, and Vincent Pouliot. 2014. “Power in Practice: Negotiating the International Intervention in Libya.” *European Journal of International Relations* 20 (4): 1–23.
Barnett, Michael, and Raymond Duvall. 2005. “Power in International Politics.” *International Organization* 59 (1): 39–75.
Bradshaw, Samantha, Laura DeNardis, Fen Osler Hampson, Eric Jardine, and Mark Raymond. 2015. “The Emergence of Convention in Global Internet Governance.” Global Commission on Internet Governance Paper Series, No. 17. Waterloo: CIGI.
Brunnée, Jutta, and Stephen J. Toope. 2010. *Legitimacy and Legality in International Law: An Interactional Account*. Cambridge: Cambridge University Press.
Checkel, Jeffrey. 2001. “Why Comply? Social Learning and European Identity Change.” *International Organization* 55 (3): 533–88.
Crawford, Neta C. 2002. *Argument and Change in World Politics: Ethics, Decolonization, and Humanitarian Intervention*. Cambridge: Cambridge University Press.
de Guymon, CarrieLyn, ed. 2014. *Digest of United States Practice in International Law* 2014. Washington, DC: Office of the Legal Advisor, United States Department of State.
Diehl, Paul F., and Charlotte Ku. 2010. *The Dynamics of International Law*. Cambridge: Cambridge University Press.
Ebert, Hannes, and Tim Maurer. 2013. “Contested Cyberspace and Rising Powers.” *Third World Quarterly* 34 (6): 1054–74.
Finnemore, Martha. 2005. “Fights About Rules: The Role of Efficacy and Power in Changing Multilateralism.” *Review of International Studies* 31 (S1): 187–206.
Finnemore, Martha, and Duncan B. Hollis. 2016. “Constructing Norms for Global Cybersecurity.” *American Journal of International Law* 110 (3): 425–79.
Finnemore, Martha, and Kathryn Sikkink. 1998. “International Norm Dynamics and Political Change.” *International Organization* 52 (4): 887–917.
Finnemore, Martha, and Stephen J. Toope. 2001. “Alternatives to ‘Legalization’: Richer Views of Law and Politics.” *International Organization* 55 (3): 743–58.
Geneva Internet Platform. 2017. “UN GGE: Quo Vadis?” *Digital Watch Newsletter* 22. https://dig.watch/DWnewsletter22#UNGGE.
Hart, H.L.A. 1994. *The Concept of Law*. Oxford: Clarendon Press.
Hill, Richard. 2015. “Dealing with Cyber Security Threats: International Cooperation, ITU, and WCIT,” in *7th International
Security: Report of the Secretary-General (Addendum).” A/69/112/Add.1.
—. 2015a. “Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General.” A/70/172.
—. 2015b. “Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” A/70/174.
—. 2015c. “Letter Dated 9 January 2015 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.
—. 2018a. “Developments in the Field of Information and Telecommunications in the Context of International Security.” A/C.1/73/L.27/Rev.1.
—. 2018b. “Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.” A/C.1/73/L.37.
Weiner, Antje. 2004. “Contested Compliance: Interventions on the Normative Structure of World Politics.” European Journal of International Relations 10 (2): 189–234.
Wendt, Alexander. 1995. “Constructing International Politics.” International Security 20 (1): 71–81.
—. 2001. “Driving with the Rearview Mirror: On the Rational Science of Institutional Design.” International Organization 55 (4): 1019–49.
Winston, Carla. 2018. “Norm Structure, Diffusion, and Evolution: A Conceptual Approach.” European Journal of International Relations 24 (3): 638–61.