International Cyber Norms Dialogue as an Exercise of Normative Power
Eneken Tikk-Ringas

“[t]o have power is to be taken into account in others’ acts (policies).”

Introduction

The fourth session of the UN Group of Governmental Experts (UN GGE) on International Information Security concluded with an excellent testament of the interaction between law and politics. Leaving legal positivists frustrated with the lack of progress in restating seemingly obvious international legal provisions, the report of Experts offers a treasure chest for analysis of how great cyber powers make use of norms as an instrument of power.

The intersection of law, policy and strategy in the international cyber security dialogue is at the core of this inquiry, putting special emphasis on the systematic and structured use of normative instruments in support of national interests pertaining to the development and use of ICTs. Evident in this dialogue are competing narratives on the benefits and threats embedded in widespread uses of ICTs as views derive from diverging priorities and evidence a gulf of capacity and capabilities.

The increasingly structured and systematic use of normative instruments in support of national interests invites attention to the normative strategies of leading cyber powers. Aspirations to shape legal thought target the current balance of power and speak to diverging visions of what ought to be. Norms, as technology itself, serve calculated and purposeful aspirations to shape the perception of the ‘new normal’ that Manners refers to as the greatest power of all. In Wolfers’ terms, States are up to shaping the milieu in which they are going to operate. Given the diametrically different visions of ‘open, resilient, stable, secure and peaceful cyberspace’ materializing such visions requires global subscription to what is to become the leading narrative.

The discourse of normative power has been extensively developed under the ‘normative power Europe’ agenda. Manners and Tocci derive their normative power framework from’ Carr’s distinction between economic power, military power
and power over opinion; Duchêne’s idée force and Galtung’s ‘ideological power as the power of ideas.’ Diez aligns EU normative power with hegemony implicitly recognizes the power-interest nexus within normative power, yet stays loyal to the established EU discourse Manners has set.

This article deliberately decouples the discourse of normative power from the liberalist-ethical considerations attached to it in the ‘normative power Europe’ discourse. Leaving aside handles of ‘unprecedented political forms’, ‘no gain’ as well as overly loaded terms such as ‘hegemony’, this article views the exercise of normative power as the use, by States, of normative instruments for shaping how things ought to be within the normative space. This approach helps to observe what States are making of international law, thereby adding dimensions to the discussion of the development of international law, both in the context of international cyber security specifically and technological advances more broadly.

Examination of the UN GGE as an exercise of State power follows the discourse of ‘normative power’, constellated in the first part of the article. The author then turns to reviewing the progress made in the three consecutive GGEs, mapping the outcomes of this process to the positions of the three leading powers – the US, China and Russia. The article discusses the potential of the UN GGE as a normative tool and platform for countries to further promote their national interests related to development and uses of ICTs. Finally, the article will draw from these discourses some recommendations on adding the dimension of normative power in the exercise and analysis of modern statecraft.

**Normative Power**

The following is a contribution to what Berenskoetter refers to as the ‘third dimension’ of power: shaping normality. It builds on Keohane’s and Nye’s analysis of international rules, norms and procedures as an intervening factor in the interdependence of States. It acknowledges the relationship between national interests and norms, addressed by Finnemore. It treats norms as an objective of State interests of its own right. It furthers Finnemore’s and Sikkink’s analysis on how norms come to being and how they create political change by emphasizing how states push for standards of behavior to achieve their goals.

Normative power, therefore, is about serving national interests by normative instruments, and, by Rosecrance, ‘setting world standards in normative terms.’ It features Therborn’s ‘telling other parts of the world what political, economic and social institutions they should have.’ It also includes what Manners refers to ‘normalising’ rules and values in international affairs through non-coercive means, with the intention to redefine ‘normal’ in international relations.

At the core of normative power is the goal of attracting others to join in one’s vision of what the ‘norm’ is. Attached to it is a calculated and purposeful aspiration to influence the world order by shaping the normative conscience of the international
community. Underlying this agenda is the idea of the *civilizing* potential of treaties, rules, and norms. Viewing international law as providing justifications to relatively new international cyber security issues invites and allows (re-)determining applicable norms, (re-)offering own interpretations and suggesting new norms to be adopted as baseline of law’s objectivity.xix

The normative space goes beyond the ‘internal’ and ‘external’ distinction as bilateral, multilateral (including regional and sub-regional) and universal aspirations can be identified in the interest areas of States acting as norm entrepreneursxx or norm externalizers.xxxi However, especially in the context of globalization and increasing technology-dependence of world affairs, the milieu in which nations seek to operatexxii is global.

Normative frameworks provide a grid for legitimating and illegitimating the exercise of State power. At the time where violence and force of arms is replaced with the ‘more gentle constraint of uninterrupted visibility’,xxxii legal checks and balances of low-profile power projection become subject to extra scrutiny. Therefore, open issues on ‘norms’ are far from trivial. National positions on the legal status of norms, modalities of their application and further development are elementarily attached to more fundamental aspirations and, especially in the context of ICTs, to widely differing national capacity and capabilities.

‘Cyber’ is, of course, not the first or the only arena where the emergence and utility of normative power can be witnessed. Case studies in Tocci’s comparison of the EU normative power posture to those of the US, Russia, India and China offer a variety of examples,xxiv as do Ingebritsen’s take on Scandinavia’s role in world politics,xxv Furthermore the emergence of ‘rules or rule-complexes, legal institutions and spheres of legal practice’ (referred to as fragmentation of international law),xxvi as well as the so called regime complexxxvii both can be seen as functions of the growing normative interests, inputs and outputs in international politics.

Changes in international affairs are the enabling, if not inviting the emergence of normative power. As the sensitivity to disruption and disturbances has increased, existing legal frameworks and thinking dating to the era of great wars and survival do not necessarily match the expectations of today. As a result, international law no longer offers a refuge for states, itself becoming an arena of great power ambitions and contestation. Resulting from this are openings for restating international law and the existing normative concepts in new, previously uncontested contexts.

Normative instruments of power can serve other instruments of State power – military, economic, informational and technological. The quest for cyber norms ranges from the considerations of development and uses of military cyber capabilities to broader issues of trust and confidence in the information society the same technologies helped build and sustain. The convergence of computing and communication technologies changes the nature of government and accelerates the diffusion of power.xxxviii
It is essential to remember the weight attached to norms, and especially international law, in the eyes of some key actors. Chinese contemporary international legal thought views the international legal order seeded by Grotius, Vattel and the Peace of Westphalia as a tool to sustain Western dominance.xxx The United States’ entry into the formation of international law in the late nineteenth century added to the instrumental view of international law in great politics. This reality highlights the interrelationship between world politics and the development of both domestic and international norms.

Norms

‘Normative’ is to be regarded broadly for the purposes of examining the nexus between norms and State interests. Following Merriam-Webster, normative refers to what is (to be) considered to be the usual or correct way of doing something.xxx

The pursuit of norms does not stop at legally binding ‘hard norms.’ While there are strong views among legal scholars about the existence and value of ‘soft law,’ relevant norms play an increasingly prominent role in contemporary international relations and their influence is likely to increase in the future. xxxi It is therefore necessary to address issues that attach to the ambivalence in the concept of the norm.

A comprehensive normative approach acknowledges international law’s many origins but expands the scope of accepted and appropriate mechanisms to soft law and other legally non-binding instruments. This broadened approach is outlined below, and comes from Terpan, who argues for soft law’s impact in both legally binding and non-binding norms.xxxii

Applying a broad approach to rules and normative instruments corresponds to the emerging understanding of feasible and functional remedies. For example, were studies of general principles of law or national and corporate approaches to reveal significantly diverging practices, this would signal for a possible call for unification of views in those areas. Should examination of domestic practices evidence predominant unity in any given question, that unity as a common nominator could be usefully turned into the next international consensus development platform and utilized as treaty or custom base. Were one to discover countries lack any substantially new views on matters, this would seriously indicate no need for new law. In line with this, where countries cannot agree on modalities of implementation of international law, non-binding norms, rules and principles offer a parallel track.

UN GGE as an exercise of normative power

The UN GGE is instrumental to the UN level discussions of the threats to international information security. While perhaps not the Hague Peace Conferences for cyber security, the UN GGE is the venue for addressing the future of norms in the
context of advances in ICTs. First proposed by the Russian Federation in 2001, the group of governmental experts was first established in 2004 to help the UN Secretary-General ‘consider existing and potential threats in the sphere of information security and possible cooperative measures to address them,’ and to conduct a study ‘on international concepts aimed at strengthening the security of global information and telecommunications systems.’

Four GGEs have convened since 2004. The first GGE (2004/2005) did not produce a consensus report. The second GGE (2009/2010), called to ‘continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them,’ recommended steps for confidence-building and other measures to reduce the risk of misperception over ICT disruptions. In particular, the second GGE invited further dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructure and recommended confidence-building, stability and risk reduction measures to address the implications of State use of ICTs.

The third GGE (2012/2013) continued the discussion of confidence-building measures and broadened the discussion on norms, rules and principles of responsible behavior by States into two separate threads: applicability of international law and norms of responsible State behavior. Accordingly, the 2014/2015 GGE report addressed norms, rules and principles for the responsible behavior of States (chapter III) separately from how international law applies to the use of ICTs (chapter VI), framing the former as ‘voluntary, non-binding norms’ that do not seek to limit or prohibit action that is otherwise consistent with international law.

The three leading themes of the UN GGE are closely related and often difficult to distinguish in practice. In their essence, international law, non-binding norms of behavior and CBMs are all normative instruments. However, following the reasoning of the Group, the norms discussion is aimed at further developing voluntary mechanisms that turn into measurable and verifiable actions once implemented.

The tripartite agenda of the UN GGE embraced a critical review of existing international law, potential areas of norms development, as well as concrete short-term remedies against the most urgent cyber threats. As such, the GGE operates within broadest margins of ‘the normative,’ understood as standards of behavior, obligations, responsibilities, rights and duties of States.

While the first GGE failed to produce a consensus report, it was an important milestone in growing Russian normative power. When the United States and other like-minded states refused to discuss international law in the context of ICTs, Russia still found a way to shape international cyber behavior. Russian success demonstrates the equalizing power of the UN where, in an expert level working
group, Russia is *en par* with the US, discussing matters of technological development where its own leadership and cyber capabilities are modest.

Out of many standards of behavior under discussion at the UN GGE, three merit special attention due to their intertwinenement with conflicting State interests. These are the applicability of International Humanitarian Law to conflict in cyberspace, the free flow of information and State responsibility for malicious and hostile activities in cyberspace.

1. **The applicability of International Humanitarian Law**

Washington used the 2015 GGE to confirm existing principles of international law serve as the appropriate framework to identify and analyze rules and norms of behavior that should govern the use of cyberspace. Although the report does not mention the Law of Armed Conflict, it contains language referring to the inherent right of self-defence under Article 51 of the UN Charter and affirms the IHL principles of humanity, necessity, proportionality and distinction.

The United States refuses to accept any restriction on current norms of Law of Armed Conflict. US policy seeks to dissuade and deter malicious actors, making clear Washington reserves the right to defend their vital national assets as deemed necessary and appropriate. The uncertainty from the lack of consensus would be anxiety inducing for the country with uncontestably superior cyber capabilities. The integrity of existing international law, including LOAC, supports the US stand for a broader culture of responsibility and accountability to sustain stability online as well as off. Protecting civilian targets is a core US security policy objective, and LOAC provides guarantees against assault the US perceives herself most targeted and vulnerable to.

That the GGE affirmed the applicability of LOAC in cyberspace confirms this issue was not settled in the previous GGE (although emphasized by the US as one of the key outcomes of the 2013 GGE). For Russia and China there is little loss in meeting the West in their aspirations to prove LOAC is a useful legal regime to deal with cyber issues. Failure to compromise could have meant normative defeat with advancements at all. Moreover, the Chinese objective – cyberspace as peaceful space – is underscored in the same paragraph from which the applicability of LOAC is inferred. The report prominently highlights the principles of sovereign equality, the settlement of international disputes by peaceful means, obligation to refrain from threat or use of force and non-intervention in internal affairs that all flow from the Sino-Russo language. In particular, China and Russia have joined forces to promote an alternative norms agenda in the UN. The Code of Conduct on International Information Security forwards Sino-Russo interpretations of international law.

2. **Free flow of information**
One of the main disagreements between states is the conditions of free flow of information. The GGEs have been unable to make progress on the issue of human rights, where the US anchored its freedom of information plea. The status quo, whereby Washington reads Article 19 of the ICCPR as consisting of two paragraphs, while Moscow focuses on the third, illustrates the gulf between the two camps. This perfect normative problem, however, will hardly lend itself to resolution. The US position since signing the ICCPR in 1992 is that States Party to the Covenant should wherever possible refrain from imposing any restrictions or limitations on the exercise of the rights recognized and protected by the Covenant, even when such restrictions and limitations are permissible under the terms of the Covenant. For the US, this statement follows from the First Amendment in force since 1791. In contrast, Russia frequently compares ICTs to weapons of mass destruction, and views decentralized and uncontrolled information flows dangerous to internal stability. The ‘information security’ doctrine emphasizes information as part, if not core, of the problem.

Deliberations at the GGE merge into the broader issue of Internet Governance. Russia has called for a state-centric model of Internet governance, whereas the US is advocating for a decentralized ‘multi-stakeholder model.’ The split between these two camps became evident in the 2012 vote on International Telecommunication Regulations, where, 89:55, a significant minority, voted against ITU’s (and therefore government-centric) approach to Internet Governance. The US protested the explicit inclusion of Internet and Internet Governance in the treaty, as well as ITUs’ claim of authority in cybersecurity.

More broadly, both freedom of information and the issue of Internet Governance flow into the question of national sovereignty in cyberspace. When it comes to the fundamental principle of sovereignty, there is little doubt of its applicability, as the very exercise of the UN GGE negotiations testifies to countries making use of their statehood. However, the modalities of exercise of national sovereignty depend on what will be the accepted protection area of ‘freedom of information’ and ‘privacy’ or who ends up making decisions about the administration of the Internet infrastructure. This contextualizes the Sino-Russo position that respect for freedoms in information space are subject to restrictions provided by (national) law.

3. Rhetoric of Responsibility

Another semi-transparent normative agenda in the UN GGE is that of accountability. From the US perspective, the question is both on responsibilities of States in assuring cybersecurity as well as deterrence against asymmetric attacks. Ability to defend against cybersecurity threats would reduce the likelihood of malicious activities routed through the ‘responsible actors’ territories, reduce the load on law enforcement and result in trust and confidence that supports both economic growth and social stability.
These instruments socialize the US position that effective cybersecurity is not merely a matter of government or law enforcement practices, but must be addressed through prevention and supported throughout society. For the US, the discourse of norms at the UN GGE is another vehicle for promoting their long-standing efforts to ‘advance norms for individual and State behavior in the interest of cybersecurity.’xlix The 2015 GGE cemented the global culture of cybersecurity, a 2001 US initiative.¹

As expected, States were not in unanimous agreement on the premises and extent of State responsibility, a legal concept with contested status.¹i Experts decided to note the accusations of organizing and implementing wrongful acts brought against States should be substantiated.¹ii Commenting on the issue, the Russian expert explained: “The charges of the organization and implementation of cyber attacks must be proven. This eliminates the possibility of indiscriminately holding a state responsible for the attack it had allegedly committed in the information space, as it was in the case of the sanctions which the United States introduced against North Korea in response to hacking the servers of the film company Sony Pictures.”¹iii

State responsibility clauses have also been inserted into the chapter of (non-binding) norms, rules and principles rather than international law.¹iv What follows from this practice is the conclusion that State consensus is absent on the scope and essence of these normative constructs at this time. This leads back to the ‘bottom lines’ of the current discourse.

**Considerations of Normative Power Beyond GGE**

States’ determination to use norms to support their international aspirations goes well beyond the GGE. ‘Stability through norms’ is a chapter in the US international cyber security strategy.¹v Then-State Department Legal Advisor Koh explained ‘compliance with international law frees us to do more, and do more legitimately, in cyberspace, in a way that more fully promotes our national interests.’¹vi The White House has publicly promoted international regulatory cooperation as reducing, eliminating, or preventing unnecessary differences in regulatory requirements.¹vii

On the other hand, the US has maintained for years that countries need to improve their ability to categorize and remedy malicious and hostile uses of ICTs. For a legally strategic and cognizant country the authority of the international legal order creates a level of predictability and stability. A law-abiding international community would mean more responsible State behavior and predefined ramifications for operations in and through cyberspace – where the US enjoys a dominant role.

Normative arguments have become a tool for the reformulation of Russia’s messages to the world, while being embedded in Russia’s understanding of its international power. Makarychev argues President Putin is not only eager to get involved in the global norms debate, but tries to use it to reassert Russia’s leadership.¹viii Referring to a set of norms Russia considers universally accepted
deprives Russia of any responsibility for their articulation. In addition, Putin accepts
the responsibility of transforming and adapting these norms to support universal applicability.\textsuperscript{lx}

During the 15-year GGE process, Russia has remained skeptical about the efficacy of international law in cyberspace, taking the view that not all legal norms ‘automatically’ extend to interstate relations in the field of ICTs and relevant criteria need to be specified.\textsuperscript{lx} Moscow’s signature on the GGE reports have not made it change its position on the need to adapt international law to ICTs. Such a position is logical for an underdog in the technological race but also consistent with Kremlin’s ambition to keep the world alert of the military potential of ICTs. Russia and China have reason to distrust the US use of cyber capabilities, due to Washington’s military superiority as well as the US’ considerable expertise in operating in the cyber domain and the global Internet.

Other governments and organizations have taken up the role of norms in pursuit of their cyber security interests. Kenya sees ‘increased incentives to participate in the formation of international rules,’ as one of benefits of improved cybersecurity.\textsuperscript{lxii} An Estonian GGE expert, addressing the European Dialogue on Internet Governance, echoed the conclusion of the 2013 GGE, adding: “We have all agreed that international law applies to the cyber sphere…We do not need new international treaties, but rather a consensus on how existing international law applies to cyberspace.”\textsuperscript{lxii}

The Global Conference on Cyberspace (GCCS) Chairman’s Statement stressed the need for broad and inclusive engagement to enhance shared understandings of how international law applies to State activities in cyberspace. In particular, the Statement pointed out the ability of States to settle their international disputes peacefully would benefit from developing shared understandings of what might constitute a threat or use of force in cyberspace for the purposes of article 2 (4) of the UN Charter.\textsuperscript{lxiii} Similarly, the Asian-African Legal Consultative Organization conference, running parallel to the GCCS, examined ‘how the existing norms of IHL apply, and whether there is a need for new rules or principles in order to comprehensively address cyber warfare.’\textsuperscript{lxiv}

Conclusion

Countries don’t just promote their interpretations of existing international law, also utilize non-binding norms to shape new expectations of behavior. They are pushing new normality and making use of regimes as an instrument of their normative aspirations, utilizing both bilateral and multilateral platforms to support the international norms agenda.

The exercise of normative power by States merits closer analysis, as it will help develop narratives that socialize one’s own normative aspirations and help dissolve undesired normative initiatives. It is essential to apply academic research and
analysis to normative strategies of States, as this will support identifying potential allies and consensus camps for norm entrepreneurship.

After all, positions tabled at the UN GGE and other international venues are not simply legal positions, they are declarations of fundamental values and interests States are determined to guard and promote. As such, these positions reflect more than ‘State understanding of international law’ – they reflect the potential and future of international law, as the latter can only be what States make of it. This emphasizes the value of ‘soft’ norms designed to overcome acute issues or a temporary lack of codified international legal consensus. At the same time, the effort that States put into making clear their dissent regarding existing international norms, demonstrates their determination to keep international law ‘flexible enough.’ One should therefore not expect quick solutions to difficult cyber security questions.

---


xi At the same time not dismissing Condliffe: Power, involving the possible use of force, is not necessarily evil but may be used to achieve moral purposes. J. B. Condliffe, “Economic Power as an Instrument of National Policy,” *The American Economic Review* 34, no. 1, part 2, Supplement, Papers and Proceedings of the Fifty-sixth Annual Meeting of the American Economic Association (March


xxiv Tocci, Who Is a Normative Foreign Policy Actor.


Everyone shall have the right to hold opinions without interference. 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (order public), or of public health or morals.

3ii Koskenniemi, From Apology to Utopia, 25.
insofar as they contain ‘unsupported restrictions on the use of countermeasures’. See “Draft Articles


US Constitution Amendment I (1789, coming into force 1791): “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.” There are numerous state and federal statutes that seek to ensure the full extent of the guarantee of the First Amendment, such as the Freedom of Information Act and the Privacy Act.


The US, in particular, has taken the view that ILC Draft Articles do not represent customary law insofar as they contain ‘unsupported restrictions on the use of countermeasures’. See “Draft Articles


United Nations Secretary-General and United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note / by the Secretary-General (A/70/174), paras 13 (c) and (e).

The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior – in times of peace and conflict – also apply in cyberspace. Nonetheless, unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them. We will continue to work internationally to forge consensus regarding how norms of behavior apply to cyberspace, with the understanding that an important first step in such efforts is applying the broad expectations of peaceful and just interstate conduct to cyberspace.


Ibid., 203.


