RESEARCH IN FOCUS

The politics of cyber norms: Beyond norm construction towards strategic narrative contestation

Xymena Kurowska
Central European University and Aberystwyth University
March 2019

EU CYBER DIRECT
Supporting EU Cyber Diplomacy

This project is funded by the European Union.

Contents

Abstract

This paper interprets the current efforts towards norm development in cyberspace through the lens of scholarship on norms in international politics. It has two aims: First, it brings a wide range of norm research traditions to debates in cyber diplomacy. It shows that despite the relative uniqueness of cyberspace, many of the dilemmas at the core of current discussions have been debated before. Analogies will not work perfectly, yet it is useful to consider research and policy around previous attempts at building normative regimes. There is, however, also a need to bring research and advocacy in sync with the actualities of cyber diplomacy; that is this paper's second objective. Primary among those actualities are incommensurable normative differences among emerging cybernorms. Against propositions of socialisation into universal cybernorms, this paper argues that the politics of norm contestation cannot, and should not, be erased by apparent consensus or ostensibly effective implementation. Such political desires no longer reflect the reality of the global world order. They fuel resistance which adds to the backlash against liberal norms. But contestedness of norms in an environment in which good faith, and therefore parameters of dialogue, cannot be assumed presents a formidable challenge. That said, regressing to crude geopolitics or 'good' liberal norms that the west should diffuse and the rest should learn is hardly a productive answer. As an alternative, this paper suggests strategic narrative contestation as a way of engaging in the politics of cybernorms, which is both normative and purposeful. In strategic narrative contestation, all can tell their stories. But some stories are better than others and can also be better told.

Key points

- There is agreement in the international community that some form of 'governance through norms' is important for maintaining stability in cyberspace.
- Yet normative developments in cyberspace are mired by a curious contradiction: Long established, and long-evolving norms, are recurrently presented as 'new' or 'to be created'.
- Simultaneously, the old strategy of norm construction and diffusion sees its revival in the world order which no longer lends itself to such approach.
- Strategic norm construction does not take into consideration the realities of cybernorms politics. Its emphasis on socialisation and compliance may increase the likelihood of norm backlash.
- EU cyber diplomacy could, instead, engage in strategic narrative contestation in order to shape the process of Internet governance more meaningfully and contemporaneously. There are formidable challenges to this task, however.

Acknowledgements

Many thanks to Patryk Pawlak for the extensive exchange over this paper and François Delerue for his consultations on international law. The usual disclaimer applies. The paper reflects personal views.

1. Introduction

The efforts towards cybernorms development in international politics are robust and wide-ranging. There is agreement that some form of 'governance through norms' is needed where international law may apply in principle but is contested in practice. Norms serve to interpret international law and regulate state behaviour when traditionally binding instruments are absent. But cybernorms development unfolds in a taxing environment: Much of contemporary geopolitical friction plays out in cyberspace, even as all bona fide stakeholders pledge their commitment to its stability and safety. The focus on norms as a regulatory tool is a tempting fallback but may ultimately be a false promise. Such failure is likely if we stick to the fallacy that either law or norms can erase interpretation and contestation - and thus politics.[1]

The dominant approach in the political and scholarly accounts of cybernorms development is "strategic norm construction".[2] It sees political actors as strategists manipulating shared normative frames for their political ends.[3] This quest is not simply utilitarian. Actors in international politics are motivated as much by what they interpret as appropriate behaviour as by cost-benefit calculation. They make political calculations, yet they do so within a dense normative social environment that constitutes their preferences and choices.[4] The calculations are made out of normative material in the sense that they include ideas about appropriateness. Norms are then more than a means to coordinate and collaborate in order to maximise utilities.[5] They link to actors' identities. All actors, whether those promoting liberal or illiberal norms, are subject to this condition which can be called "the normative saturation of strategic action".[6]

"

Much of contemporary geopolitical friction plays out in cyberspace, even as all bona fide stakeholders pledge their commitment to its stability and safety. The focus on norms as a regulatory tool is a tempting fallback but may ultimately be a false promise.

Seen from such perspective, the process of cybernorms development has unfolded in a fairly standard manner. Typical dilemmas of other norm regimes, e.g. nuclear, environmental, or humanitarian, recur. Two are worth highlighting: First, contrasting norms can collide with each other in any given situation. The norm of non-interference clashes with the norm of civilian protection in humanitarian emergencies, for example. So does the norm of self-determination and sovereign integrity whenever the question of independence or annexation comes up. In cyberspace, similarly, there are numerous clashing norms and actors weigh which of them should prevail given their identity and interests. There is no automaticity to their judgement. Second, norms do not have a single stable meaning, nor do they mean the same thing to all actors involved. It is a common misconception, or an exercise of normative dominance, to interpret such difference as sabotage or normative backwardness. It is more useful to see it in terms of partly overlapping but also contrasting and dynamic normative commitments. In short, while all stakeholders may agree on a norm in abstract (sovereign equality is formally a fundamental norm of the international system), they will disagree on its meaning and the conditions of its application.

[1] For an alternative concept of international law as defined by politics, see Martti Koskenniemi, *From Apology to Utopia: The Structure of International Legal Argument*, (Cambridge: Cambridge University Press, 2006).
[2] Martha Finnemore & Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization,* 52 (1998): 887–917.
[3] Roger Payne, "Persuasion, Frames and Norm Construction," *European Journal of International Relations,* 7 (2001): 37–61.
[4] Jelena Subotic, "Narrative, Ontological Security, and Foreign Policy Change," *Foreign Policy Analysis,* 12 (2016): 610–627.
[5] George Goertz & Paul Diehl, "Toward a Theory of International Norms," *Journal of Conflict Resolution,* 36 (1998): 634-664, p. 640.
[6] Xymena Kurowska, "Multipolarity as Resistance to Liberal Norms: Russia's Position on Responsibility to Protect," *Conflict, Security & Development*, 14 (2014): 489-508.

This paper makes sense of such contestation by probing entrenched myths about norms in order to engage in the politics of cybernorms on more realistic terms. Many questions about international norms have already been pondered, including, for example, whether non-binding normative standards are more advantageous than codification through international treaties, what makes norm entrepreneurs more likely to succeed, or how state and non-state actors differ in their advocacy of norms. The issue of contestation remains, however, a thorny one. Primarily, we persist in the fantasy that regulation through law or norms eliminates politics. Such fantasy ignores the fact that law and norms are a matter of continuous interpretation. We also disregard the fact that, if conducted from a position of advantage, norm advocacy is a form of dominance. The latter effect of norm promotion is increasingly resisted and it also plays into the hands of those actors who instrumentalise such resistance for their purposes. Politically, contestation is awkward: It levels the field where many build their credibility by recourse to moral superiority. The contesting party is presented as a spoiler, or in need of upgrading their capacity to see right.

Cyberspace is increasingly a playground for norm backlash when actors double down or intensify violations in the context of transnational advocacy. The field is populated at least in equal measure by norm entrepreneurs and antipreneurs who resist normative change in world politics.

Yet norm contestation is a constitutive practice of international politics; it presses on normative developments in cyberspace. These developments are replete with different forms of resistance to, or even defiance of, liberal norms, defined by Rochelle Terman as "the commitment to norm offending behaviour as a reaction to norm sanctioning."[7] Cyberspace is increasingly a playground for norm backlash when actors double down or intensify violations in the context of transnational advocacy. The field is populated at least in equal measure by norm entrepreneurs and antipreneurs who resist normative change in world politics.[8] Legitimacy is built no longer exclusively on a greater fit into the liberal world order. Some leaders engage in transforming stigma of resistance to international norms into an emblem of domestic and, increasingly, international pride.[9] In such constellation, merely mounting transnational pressure will be counterproductive. Falling back on the rhetoric of spoilers and forging ahead with the promotion of universal cybernorms despite such constellation may backfire. A better story is needed. This paper suggests strategic narrative contestation as a productive way of engaging in cybernorms politics to foster the EU's cyber diplomacy. To concretise this proposition, I first lay out the understanding of norms as social facts and bring a range of insights about norms from diverse scholarly perspectives.

2. Norms in international politics – definitions and interpretations

The dominant definition of a norm in international politics is "a collective expectation for the proper behaviour of actors with a given identity".[10] As formulated in the UN Group of Governmental Experts on Information Security on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) 2015 report, "Norms reflect the expectations of the

[7] Rochelle Terman, 'Rewarding Resistance: Theorizing Defiance to International Norms,' August 2017, p. 1. Accessed 21 February 2019. http://rochelleterman.com/wp-content/uploads/2014/08/4b_Defiance.pdf.

[8] Alan Bloomfield, "Norm Antipreneurs and Theorising Resistance to Normative Change," *Review of International Studies*, 42 (2016): 310–33.

[9] Rebecca Adler-Nissen, "Stigma Management in International Relations: Transgressive Identities, Norms, and Order in International Society," *International Organization,* 68 (2014): 143–176.

[10] Peter Katzenstein, ed., *The Culture of National Security: Norms and Identity in World Politics* (New York: Columbia University Press, 1996), p. 5.

international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States."[11] Norms regulate behaviour and are constitutive of actors' identities and interests.[12] Regulative norms describe obligations, prohibitions, etc. Constitutive norms create institutional facts and modify normative systems. To give an example from ordinary life, the rules of polite table behaviour regulate eating, but social eating exists independently of these rules. Similarly, the institutions of marriage, money and promise are systems of constitutive norms[13] that establish such phenomena as social facts. More specifically to international politics, the norm of sovereignty is constitutive of the contemporary international (normative) system. It also comes with distinct obligations and prohibitions which regulate its functioning. Yet the norm of sovereignty and, consequently, the normative constitution of the international system have not been fixed. For example, the shift towards 'sovereignty as responsibility' has developed alongside the new norms of human security, which also shows interconnections with different norms.

"

Falling back on the rhetoric of spoilers and forging ahead with the promotion of universal cybernorms despite such constellation may backfire. A better story is needed.

Fundamentally, norms assume a degree of collective identification, expressed in the UNGGE 2015 report by reference to the international community. Traditionally, collective identification has been explained by 'resonance': A norm cannot be arbitrarily imposed but needs to resonate within a community to take root. It is not immediately obvious what the relevant community in Internet governance is, whether it is the international community as a whole or some of its islands which claim the core status. The process is acknowledged as a 'multi-stakeholder' one and comprises diverse communities. Many experts call for inclusivity, broad societal dialogue and confidence-building measures if the process is to be legitimate and sustainable. Advocacy for the group of "the like-minded"[14] facilitates community building but it does so along the lines of a security community or even traditional alliances. They may integrate as units but also grow antagonistic towards one another. Such processes risk turning norms into instruments of coercion, undermining the social logic of how norms work.

Resonance also denotes that specifying and formally adopting substantive normative prescriptions does not automatically create a norm or even ensure its relevance. It may be an element of normative leadership and help in the process of normative development. But it is neither a necessary nor sufficient condition for establishing a norm. Relevant actors comply because they see norms as defining who they are, what they want and how they view international politics.[15] Thus, adopting a norm reflects broader normative commitments. It is debatable to what extent specific norms, even neatly written ones, can immediately become part of a recognised responsible behaviour in cyberspace if a sense of community and allegiance are absent. 'Grafting', that is inserting, cybernorms into broader normative commitments, in contrast to the idea that cybernorms have to be specified and formalised as a separate regime, could be a useful practice towards creating an international cybersociety.[16] Fragmentation, in turn, that is the proliferation of autonomous fora for cybernorm development, does not need to be an obstacle for establishing 'governance through norms'. If there is productive interaction between such fora, it can

[11] United Nations, General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", para. 13(c), UN Doc. A/70/174 (22 July 2015).
[12] Ronald Jepperson, Alexander Wendt, and Peter Katzenstein, "Norms, Identity, and Culture in National Security," in *The Culture of National Security*, edited by Peter Katzenstein (New York: Columbia University Press, 1996), pp. 33-78, p. 54.
[13] John Searle, *Speech Acts: An Essay in the Philosophy of Language* (Cambridge: Cambridge University Press, 1969), p. 131.
[14] "Like-minded" initiatives were suggested by some states in lieu of an agreement at the UN level after the UNGGE failure to agree on a consensus report in 2017, see Joseph Nye, "Normative Constraints on Cyber Arms," in *Getting Beyond Norms, New Approaches to International Cyber Security Challenges*, edited by Fen O. Hampson & Michael Sulmeyer, Special Report 2017, Centre for International Governance Innovation, p. 21.
[15] Martha Finnemore & Kathryn Sikkink "International Norm Dynamics and Political Change."
[16] Martha Finnemore and Duncan B. Hollis "Constructing Norms for Global Cybersecurity," *The American Journal of International Law* 110 (2016): 425-479.

give rise to the incremental emergence of constitutionalising principles, even in the absence of a formal effort to create a 'global cyberconstitution'.

Norms have diverse aspects which all are subject to differences in interpretation. The range of contestation includes disputes of the validity, the meaning and the application of norms.[17] For instance, the validity of the norm that states should not allow the use of their territory for malicious cyberattacks on other countries may be undisputed, but what the use of territory means in a digital environment and what exceptions to this norm may exist may well be contested. Because a single norm has multiple components, actors may agree on the general purpose of the norm but contest specific prescriptions or parameters.[18] A norm's prescription guides actors in what is considered to represent appropriate behaviour. A norm's parameters instruct actors in which situations the norm's prescription applies.[19] Simply put, an actor with a given identity should (not) do X in situations A, B or C. A responsible stakeholder should not 'hack back' unless there are specific circumstances that justify this. Possible justifications are likely to be contentious. Specification of parameters can also be a way of contesting a norm. In the recent Russia-sponsored resolution[20], the application of UN Charter for maintaining peace and security in cyberspace is linked to, illustratively, respect for the diversity of history, culture and social systems of all countries.

Incidents of norm breaches are important for understanding how norms work. Norms are counterfactually valid: Behaviour that violates norms does not necessarily undermine them. In fact, it may strengthen their validity by defining the scope of application.[21] So the establishment of a norm is often most visible at an instance acknowledged as constituting a breach. Because norms embody the quality of 'oughtness' and commonality in moral assessment, they leave an extensive trail of communication.[22] An actor in breach will go to great lengths to explain an action which is recognised as a failure to act on a norm. Soul-searching over non-action in humanitarian atrocities by the international community shows at least two things: the existence of a norm against the arbitrary killing of civilians and the fact that this norm shall not determine any one type of behaviour. As social phenomena, norms guide but do not govern behaviour. They constitute a normative environment in which states weigh contrasting norms that prescribe different courses of action.[23]

Instances of norm violation or non-application therefore have a role to play in both consolidating a community and crystallising the parameters of a norm. The Russian intervention in Georgia in 2008, partly justified by the Russian authorities on humanitarian grounds, was widely recognised as not in sync with the provisions of Responsibility to Protect (R2P), which helped clarify the doctrine.[24] The Burma-Myanmar cyclone in 2008, after which the military regime did not initially allow international assistance, was not deemed to be an R2P case, despite the advocacy of then-French Foreign Minister

[17] Jonas Wolff & Lisbeth Zimmermann, "Between Banyans and Battle Scenes: Liberal Norms, Contestation, and the Limits of Critique," *Review of International Studies* 42 (2016): 513-534, p. 518.

[18] Contestation over the type of situation to which the norm applies and how it needs to be applied has, for instance, been described as applicatory contestation, see Nicole Deitelhoff & Lisbeth Zimmermann "Things we lost in the fire: how different types of contestation affect the validity of international norms," PRIF Working Paper No. 18 (2013): 1–17.

[19] Vaughn Shannon, "Norms Are What States Make of Them: the Political Psychology of Norm Violation," *International Studies Quarterly* 44 (2000): 293–316, p. 295.

[20] Presented by Russia in the 1st First Committee of the UN General Assembly 73rd session in October 2018 and adopted by the UN General Assembly in December 2018, United Nations, General Assembly, "Developments in the field of information and telecommunications in the context of international security." UN Doc. A/C.1/73/L.27/Rev 1 (29 October 2018). Accessed 8 March 2019. https://undocs.org/A/C.1/73/L.27/Rev.1

[21] Friedrich Kratochwil and John G. Ruggie, "International Organization: a State of the Art on an Art of the State," *International Organization*, 40 (1986): 753-775, p. 767.

[22] Martha Finnemore & Kathryn Sikkink "International Norm Dynamics and Political Change," p. 982.

[23] Friedrich Kratochwil, *Rules, Norms, and Decisions. On the Conditions of Practical and Legal Reasoning in International Relations and Domestic Affairs* (Cambridge: Cambridge University Press, 1989).

[24] Cristina Badescu and Thomas Weiss, "Misrepresenting R2P and Advancing Norms: An Alternative Spiral?" *International Studies Perspectives* 11 (2010): 354–374.

Bernard Kouchner. But it could have become one if the generals' behaviour had continued long enough so as to constitute a situation of indifference to human suffering.[25]

A closer look at different logics of norm development will help design contextually appropriate scenarios for cyber diplomacy.

3. Perspectives on norm development

There are four main perspectives on norm development in academic literature.

3.1. Regulatory function of norms

This is a 'popular' understanding of norms as instruments of bestowing obligations and deciding on prohibitions. In this context, norms are often understood as a preliminary, legally non-binding step towards a legally binding arrangement. They can be part of an internationally recognised custom, however. As such, they belong to customary international law which is formally recognised as a source of international law. The assumption remains, however, that legally codified norms in the form of law are superior because of the embedded sanction mechanisms and the presumed elimination of contestation.[26] The superiority of legal codification, however, is debatable. There are plenty of examples of treaties that have remained 'dead provisions', such as in the environmental regime. Norms can also gain new status in other ways. The Russia-sponsored resolution of the UN General Assembly, adopted in December 2018, reuses and enshrines for the first time several cybernorms formulated by UNGGE reports. Thus far, the UNGGE reports were only notified to the UN General Assembly, so such re-use in a resolution introduces an upgrade in status. While the resolution itself is contested by the "like-minded" group as disrupting the consensus around cybernorms, it does formalise the status of some of the norms they co-authored and have been promoting.

Formal regulation seems to be the most transparent and consequential, but it does not automatically provide for the normative pull for compliance. Neither specificity nor coherence nor careful elaboration will secure the standing of a norm if the relevant community (or communities) does not identify with it. The perspective of norms as outcomes of regulatory processes creates a semblance of control but reverses the order in which norms take social effect, possibly leading to a waste of time and resources. The call for a comprehensive treaty on cyberspace should take this aspect into consideration. Arguably, it is flexibility and adaptability, as well as the possibility to form clubs or smaller groupings of "like-minded states", that can pioneer norms to be extended globally at a later stage.[27] This proposition, however, has become a major bone of contention as it represents exclusionary practices which monopolise the process of norm development and thus reproduce existing inequalities.

There are many examples of regulatory function of norms in cyberspace. The Budapest Convention on Cybercrime, drawn up by the Council of Europe in 2001, is the first international treaty to address Internet and computer crime. It has been promoted by the group of the "like-minded" and has been successful in gathering signatories. But the Budapest convention raises criticism of transposing one western model on all regions. Such perception creates ideological obstacles for some actors to sign the treaty even if many of its provisions become part of national frameworks as a result of domestic legislation. The most controversial part of the treaty remains paragraph 32b, which allows for transborder access to data among the parties without prior consent. Some interpret this provision as infringing on national sovereignty. Another example of regulatory function of norms is the International

[25] Roberta Cohen, "The Burma Cyclone and the Responsibility to Protect," *Global Responsibility to Protect* 1 (2009): 253-257.
[26] For an alternative view see Martha Finnemore and Stephen J Toope, "Alternatives to 'Legalization': Richer Views of Law and Politics," *International Organization,* 55 (2001): 743–58.
[27] This is the main premise of the argument about regime complexity, e.g. Joseph Nye, *The Regime Complex for Managing Global Cyber Activities,* Centre for International Governance Innovation and the Royal Institute for International Affairs, 2014. Accessed 21 February 2019. https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

Code of Conduct for Information Security, sponsored by Russia and China. Widely discredited in the west as a geopolitical initiative that challenges human rights and online freedoms, it does enshrine a distinct vision of regulating cyberspace vis-à-vis the control of information by the state. The treaty has become part of cybersecurity policy regulation in Russia and China and is likely to be emulated among states that subscribe to similar normative visions. The Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, adopted 16 June 2009, is an international treaty which serves a similar function.

> **Formal regulation seems to be the most transparent and consequential, but it does not automatically provide for the normative pull for compliance.**

The UNGGE process has a para-regulatory character: Its aim is to create a global framework that would guide states' conduct in cyberspace, particularly by building consensus on the applicability of international law in cyberspace. The UNGGE produced three reports: in 2010, 2013 and 2015. In the global context informed by cyber insecurities and a frantic search for solutions, the reports have been consequential: They streamlined the discussion on international law and norms in cyberspace and became a reference point in global cyber matters. In April 2017, the G7 adopted a declaration of responsible state behaviour norms in cyberspace which draws on the UNGGE's 2013 and 2015 reports. The EU referred to them in its Council Conclusions on response to malicious cyber activities in April 2018. In October 2018, the ASEAN Ministerial Conference on Cybersecurity agreed in principle to certain voluntary norms of behaviour in cyberspace as promulgated in UNGGE reports. We may be witnessing a paralegal 'cascading constitutionalisation.' However, this development is unfolding as multilateral coordination gives way to bilateral dynamics[28] of state agreements on cyberspace. These do not have to be contradictory phenomena as long as the bilateral dynamics use the vocabulary lifted from the UN process.

3.2. Strategic construction of norms[29]

This perspective envisages the mechanism of normative change as strategic action by norm entrepreneurs, i.e. states, individuals with social capital, transnational advocacy networks, epistemic communities or expert groups with a high standing, such as international commissions. These entities share a normative repertoire or a body of knowledge and act purposefully to spread new norms and alter policies in accordance with those new norms. The main strategies of proliferation they employ are framing and persuasion. The classic model of normative change in this tradition is described as "norm cycle/cascade"[30]: Strategic action by norm entrepreneurs may lead to "a tipping point", which is the moment when enough actors in a group characterise the norm as central to their identity. After this moment, a norm becomes part of relevant actors' identity and therefore triggers the normative pull to comply. "Socialisation" is a mechanism which enables this update of identity: It operates through: (1) the emulation of other, successful states; (2) praise by states and other actors for conformity; (3) ridicule for deviation; and (4) diplomatic and economic pressure to "induce norm breakers to become norm followers."[31]

The cycle/cascade model of normative change is solidly established but has been subject to significant criticism. Despite the acknowledgement of norm dynamics, its aim of the greatest possible

[28] White House Homeland Security Adviser Tom Bossert stated in June 2017 that the American approach to cybernorms under the Trump administration will shift from multilateral to bilateral engagement. This reflects a practical judgment that addressing specific relationships or aspects of cybersecurity will be more fruitful than pursuing a grand bargain approach for norms, see White House, "Remarks by Homeland Security Advisor Thomas P. Bossert at Cyber Week 2017,"26 June 2017. Accessed 21 February 2019. https://www.whitehouse.gov/briefings-statements/remarks-homeland-security-advisor-thomas-p-bossert-cyber-week-2017/.

[29] Martha Finnemore & Kathryn Sikkink, "International Norm Dynamics and Political Change."

[30] Ibid.

[31] Ibid, pp. 902-4.

dissemination means that norms are implicitly viewed as being relatively stable. Contestation is to be eliminated through socialisation for better results on compliance. Such focus on the strategies of diffusion downplays the continuous negotiation of normative meaning. Norms are either taken over or rejected, yet this fails to capture the reciprocal exchange between actors that negotiate the validity, meaning and application of norms. Instead, the model presents a unidirectional causal story "from socialiser to socialisee".[32] It also takes for granted the normative predispositions behind the norms that are to be diffused: It sees as inherently 'good' the normative substance promoted by norm entrepreneurs. Socialisation envisages progressive improvement of other actors by morally superior leaders. As experience shows, however, strategies of dissemination are generally combined with conditionality, sanctions, praising and shaming and other pressures that have more to do with coercion than persuasion.[33]

The strategic construction of norms is most useful in cases of normative change with an element of unidirectional 'learning', a strong moral component linked to claims of universal validity and the social capital of norms entrepreneurs which increases their power of persuasion. This is how the anti-slavery norm became established and how the prohibition of nuclear, chemical, and biological weapons has been developed. The strategic construction of norms in cyberspace will accordingly depend on framing cybernorms as universal and on the emergence of legitimate norm entrepreneurs with capital, which facilitates persuasion.

"

The strategic construction of norms is most useful in cases of normative change with an element of unidirectional 'learning', a strong moral component linked to claims of universal validity and the social capital of norms entrepreneurs which increases their power of persuasion.

There are several applicants to such role at the moment: The Global Commission on the Stability of Cyberspace, which released its Singapore Norm Package in November 2018, and the private actor Microsoft, which promoted the failed Digital Geneva Convention. In contrast to the UNGGE, the Global Commission engages in dynamic advocacy and actively promotes its norms as universal. Individual members of the Global Commission become entrepreneurs in their own right and disseminate the Global Commission norm catalogue to other institutional venues. For instance, Marietje Schaake, one of the commissioners on the Global Commission, has also been a member of the European Parliament where she endorses a digital agenda in line with the work of the Global Commission.[34]

Microsoft put forward the proposal for the Digital Geneva Convention in the aftermath of the Petya and WannaCry cyberattacks in May and June 2017, which both exploited the same vulnerability in the legacy Microsoft operating system Windows XP and Windows Server 2003. The Digital Geneva Convention envisaged states refraining from launching cyberattacks against the private sector, critical infrastructure or intellectual property. It called on the tech sector to agree on shared principles and behaviours, such as conducting "100 percent defence and zero percent offence" and operating as a "neutral Digital Switzerland", ensuring protection for all customers regardless of nationality or location. The draft convention aimed to create an independent non-governmental organisation that would investigate and publicly attribute cyberattacks to specific states.[35] Due to a strong pushback from states, Microsoft moved on to proposing a more technology-focused

[32] Charlotte Epstein, "Stop Telling Us How to Behave: Socialization or Infantilization?" *International Studies Perspectives,* 13 (2012): 135–145, p. 140.
[33] Thomas Risse & Stephen Ropp, "Introduction and Overview" in *The Persistent Power of Human Rights. From Commitment to Compliance* edited by Thomas Risse, Stephen Ropp & Kathryn Sikkink (Cambridge: Cambridge University Press, 1999), 3–25.
[34] "Digital Agenda." Marietje Schaake. Accessed 21 February 2019. https://marietjeschaake.eu/en/tag/digital-agenda-1.
[35] Tim Maurer & Kathryn Taylor, "Outlook on International Cyber Norms: Three Avenues for Future Progress," Carnegie Endowment for International Peace, 2 March 2018. Accessed 21 February 2019. https://carnegieendowment.org/2018/03/02/outlook-on-international-cyber-norms-three-avenues-for-future-progress-pub-75704.

Cybersecurity Tech Accord, defined as "a public commitment among global companies to protect and empower civilians online and to improve the security, stability and resilience of cyberspace".[36] They have also launched the Digital Peace initiative aimed at fostering the stability of digital global society "from below" through the engagement of digital citizens.

The entrepreneurship of both the Global Commission and Microsoft has been reflected in the Paris Call for Trust and Security in Cyberspace sponsored by the French government. While the Call has only attracted select followers, it envisages a distinct agenda that will continue to develop and consolidate.

3.3. Norm contestation framework[37]

If strategic construction of norms seeks progressive convergence of interests and identities under normative leadership, the contestation framework both assumes - and works with – differences and, potentially, conflict. Norms are seen as being in constant 'flux' or 'motion', that is to say, always in the midst of processes of interpretation, interrogation, endorsement, rejection and, ultimately, change.[38] They are not objects with stable and universal meaning to be diffused. They are social, produced as they are through practical activity[39] and their meaning is in their use.[40] Norms may therefore be ambiguous, with the content subject to different interpretations of how actors should behave. Strategic norm construction looks for compliance with a priori norms and focuses on action *in response to* a norm. Contestation is interested in action *in relation to* a norm.[41]

An important aspect of contestation is that much normative meaning relates to the local context. Actors rely on local understandings and situational factors to establish what the appropriate behaviour in relation to a given norm is. Because norm entrepreneurs and norm "receivers" may not share the same context, their interpretations of what constitutes compliance may differ.[42] This generates disagreements on specific elements of a norm's contents and, therefore, norm contestation; however, it does not necessarily affect general agreement on the norm itself.[43] For example, everybody agrees on the norm which prescribes non-interference, but there will be differences about what exactly constitutes non-interference and what exceptions should be considered.

Contestation plays a key role in legitimising norms. It constitutes a legitimate exercise of an actor's rights to interrogate the norms according to which they are judged. Arguably, a norm that cannot be contested cannot be legitimate.[44] As Wiener argues: "*The principle of contestedness reflects the global agreement that, in principle, the norms, rules and principles of governance are contested and that they therefore require regular contestation in order to work. For the legitimacy gap between fundamental norms and standardised procedures to be filled, therefore, access to regular contestation (as opposed to ad-hoc contestation) needs to be facilitated, in principle, for all involved stakeholders."*[45]

[36] See "Cybersecurity Tech Accord." Accessed 21 February 2019. https://cybertechaccord.org/
[37] Antje Wiener, *A Theory of Contestation*, (Heidelberg: Springer, 2014).
[38] Holger Niemann & Henrik Schillinger, "Contestation 'All the Way Down?' The Grammar of Contestation in Norm Research," *Review of International Studies*, 43 (2017): 29-49.
[39] Mark Laffey and Jutta Weldes, "Beyond Belief: Ideas and Symbolic Technologies in the Study of International Relations," *European Journal of International Relations* 3 (1997): 193–237.
[40] Antje Wiener, "Enacting Meaning-in-use: Qualitative Research on Norms and International Relations," *Review of International Studies* 35 (2009): 175–193.
[41] Xymena Kurowska, "Practicality by Judgement: Transnational Interpreters of Local Ownership in the Polish-Ukrainian Border Reform Encounter," *Journal of International Relations and Development*, 17 (2014): 545–565.
[42] Betsy Jose, *Norm Contestation Insights into Non-Conformity with Armed Conflict Norms,* (Heidelberg: Springer, 2018).
[43] Audie Klotz, "Norms Reconstituting Interests: Global Racial Equality and US Sanctions against South Africa," *International Organization,* 49 (1995):451–78.
[44] Maria Rost Rublee & Avner Cohen, "Nuclear Norms in Global Governance: A Progressive Research Agenda," *Contemporary Security Policy*, 39 (2018): 317-340, 325.
[45] Antje Wiener, *A Theory of Contestation,* p. 3.

In sum, norms are legitimately constructed in a process of meaningful exchange. They offer a platform to debate contending ideas of what is considered appropriate behaviour. Access to contestation will therefore increase legitimacy of a norm and produce stronger and more precise norms.

“

Contestation plays a key role in legitimising norms. It constitutes a legitimate exercise of an actor's rights to interrogate the norms according to which they are judged. Arguably, a norm that cannot be contested cannot be legitimate.

The contestation framework is most productive in cases with a lack of agreement about any component of a norm which is otherwise agreed upon. Intense contestation has shaped debates over humanitarian intervention, for instance: most recently with the Responsibility to Protect (R2P). The most contested, third pillar of R2P advocates international remedial responsibility to act when a state, either due to a lack of ability or willingness, fails to protect its population from the crimes of genocide, war crimes, ethnic cleansing and crimes against humanity.[46] R2P reflects a larger normative shift from state to human security, in which the latter is valued higher than state sovereignty. Contestation here stems in part from norm conflict. Humanitarian intervention trumps one norm (sovereignty) in favour of another (prohibition of atrocity against civilians). However, no credible actor would present arguments anymore against the prohibition of atrocities exclusively based on the supremacy of sovereignty. What is most contested are the parameters of the prohibition of atrocities, including what constitutes the threshold for intervention and who can intervene legitimately.

Cyberspace has similarly become a field of norm contestation: While there is a general commitment to fostering the stability of cyberspace and responsible behaviour of both state and non-state actors, the stakeholders have different understandings of how such stability comes about. Contestation accommodates the focus on the multi-stakeholder character of the process in which actors 'learn from each other' rather than 'being socialised into good norms' by 'superior normative leaders'. Norms can thus be developed in a participatory and inclusive manner, which helps bolster their legitimacy and sustainability.

Such premises reflect a traditional perspective on contestation which relies on democratic deliberation inherent to liberal approaches to global governance. The deliberation assumes bona fide involvement of all parties who have agreed on the rules of the dialogue among them. But contemporary norm contestation exceeds such parameters. The politics of contestation increasingly challenge the monopoly over the application and interpretation of liberal principles. It also mobilises alternative non-liberal normative frameworks. This form of contestation came to sharp relief in the recent dispute about the norm of representativeness in the UNGGE. Although the group of governmental experts has increased from 15 to 25 members, it does not formally reflect the UN membership. The Russian delegation characteristically radicalised this charge in its statement in the UN General Assembly First Committee: *"The practice of some club agreements should be sent into the annals of history. All states, irrespective of their technological development, have the full right to directly participate in negotiation on International Information Security within the UN and thus influence decision-making."*[47]

[46] The first pillar includes the responsibility of the state to protect its own citizens. The second pillar envisages a state turning to the international community when it cannot fulfil its obligations. Arguably, future development of cybernorms may include the parameter of capacities, where the lack of cybersecurity capacities by one state can constitute a case for an intervention by the international community on behalf of international security.

[47] In introducing the Russia-sponsored resolution, "Developments in the field of information and telecommunications in the context of international security," during First Committee (Disarmament and International Security Committee), 31st meeting in the 73rd session of the General Assembly on 8 Nov 2018, see video United Nations Web TV, "First Committee, 31st meeting - General Assembly, 73rd session." (8 November 2018). Accessed 6 March 2019. http://webtv.un.org/meetings-events/general-assembly/main-committees/1st-committee/watch/first-committee-31st-meeting-general-assembly-73rd-session/5859574011001.

Such sentiment is supported by a range of actors, including China and India, and at least acknowledged by some members of the "like-minded" group.[48] The Russia-sponsored resolution from December 2018 includes a provision about the equal role and responsibility of all UN Member States in the international governance of the Internet. It initiates an Open-Ended Working Group (OEWG) for 2019-2020, calling for the entire UN membership to participate. It will run in parallel to the new UNGGE, which also has an extended consultative mechanism as suggested by the concomitantly adopted US-sponsored resolution "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security".

This situation is illustrative of cybernorms politics. Russia is accused of undermining consensus around the UNGGE reports and distorting its normative contents by introducing provisions which increase state control over the Internet.[49] It does so by exploiting the sentiment that the design of international governance of the Internet has been monopolised by western powers. Herein lies a genuine dilemma. The UNGGE process has admittedly been selective. Justification of its organisation, in terms of expertise and efficiency, can only go thus far when the legitimacy of global governance is at stake. Russian diplomacy made use of UN institutional tools to contest this process on substantive grounds. Such rule-based contestation cannot be easily dismissed. Its normative contents are certainly disputed, but the advocacy for democratising the rule-making around global Internet governance is gaining momentum. The exploitation of such momentum is a diplomatic feat which affects the process of contestation. Russia has captured the dispute over the arbitrary normative leadership for its interest of staying on geopolitical par with the west. Still, although the effects of resisting liberal norms can resemble the outcomes of strategic manoeuvring, they cannot be reduced to such. The substance of such resistance is not contrived. It builds on resonating normative commitments which should not be dismissed by any player in the politics of cybernorms.

"

Strategic construction of norms by the group of the 'like-minded' under western leadership is not seen as legitimate. It reflects political reasoning which belongs to the past of the liberal world order. Increasing pressure for norm adoption and compliance in such a context is likely to increase defiance and norm backlash. Norm contestation that allows for participatory norm shaping, and thus their sustainability, is intuitively appealing as an alternative.

The dilemma brings to sharp relief the impasse at which we find ourselves today: Strategic construction of norms by the group of the 'like-minded' under western leadership is not seen as legitimate. It reflects political reasoning which belongs to the past of the liberal world order. Increasing pressure for norm adoption and compliance in such a context is likely to increase defiance and norm backlash. Norm contestation that allows for participatory norm shaping, and thus their sustainability, is intuitively appealing as an alternative. Yet there are inherent challenges. As illustrated above, the classical notion of contestation relies on good faith underpinned by a fundamental harmony of interests. Such harmony is an illusion. Despite declarations, the politics of cybernorms entrench differences and no one ultimately seeks open-ended contestation. To move on, we should reclaim the kind of contestation which, to use Bonnie Honig's formulation, "affirm[s] the reality of perpetual contest".[50]

Alister Miskimmon *et al.* introduce the useful notion of strategic narrative contestation[51] which calls for telling compelling stories in a purposeful way. The authors point to a twofold power effect of strategic narrative: the classical A getting B to do what B otherwise would not do and shaping

[48] See the statements by the delegations of Canada and Australia in the same session as above.
[49] See the same session.
[50] Bonnie Honig, *Political Theory and the Displacement of Politics*, (Cornell University Press, Ithaca and London, 1993), p. 15.
[51] Alister Miskimmon, Ben O'Loughlin, & Laura Roselle, *Strategic Narratives. Communication Power and the New World Order*, (Routledge: New York and London, 2013).

the experience of international affairs, which aims at transforming identity. Such definition still harks back to strategic construction of norms in the sense that A's objective is to alter B in its own image. Yet change also comes out of exchange in contestation, which transforms both parties. Just 'projecting' a narrative without engaging with others, and potentially making their stories part of one's own narrative, will remain a shot in the dark.

3.4. Decolonial approach to international norms

This approach considers norms as a form of hierarchical ordering. This tradition reveals to what extent global norm construction and diffusion are pervaded by idealised west-centred interpretations that project the western liberal experience as universal.[52] That is, norms that are widely accepted in the west are perceived and acknowledged as global norms. This sentiment pervades the politics of cybernorms. The insights of this perspective have important implications for normative developments in cyberspace. First, the claim about universality, coherence and common understanding of cybernorms is interpreted as imposition. Any talk of consensus will smack of exclusion. Second, conflict and the politics of dominance are inherent to normative change, especially when it is modelled on unidirectional learning and socialisation.[53] Normative change does not necessarily bring progress. By default, it engrains one set of rules against another. Third, the naturalisation of western norms impedes norm contestation. Such naturalisation both halts a norm in preferred prescriptions and parameters and leads to a perception that any resistance against that norm is illegitimate and immoral. This raises the question about the inclusivity of cybernorms development, specifically the role of the Global South in terms of substantive input and access to negotiation.

The decolonisation approach to international norms is present in debates on cyberspace in several forms: as a traditional element of foreign policy of some crucial actors, such as India or Brazil; as a growing assertion that cyberspace be used for development purposes and well-being of citizens against the expropriation by the global powerful; and as normative material for building a strategic coalition against the liberal western dominance. The protestations of India, China, the African countries or Russia against digital inequality and insistence on genuine cyber multilateralism within the UN should take all these considerations meaningfully into account. Stressing the role of established power relations in norm change should not, however, lead to essentialising the west and local tradition as enclosed spaces. It is productive to focus on translations between the Global South and the Global North, which pluralise value systems.[54]

4. Towards strategic narrative contestation in the EU's cyber diplomacy

If we see norm development as a platform for conversation or negotiation rather than as a means of indirect coercion, persuasion becomes a primary concern. Each of the perspectives on norms presented above contains a take on persuasion. The regulatory approach focuses on formal adoption and sanction mechanisms in case of a norm breach. Strategic norm construction relies on the process of socialisation by normative leaders. Their legitimacy and structural advantage are what make their story so persuasive. Contestation introduces an element of continuous difference, mutual learning and co-creation of norms. It shows how interactions can alter actors' preferences and identities, which allows for a more meaningful sense of persuasion to be achieved. The decolonial approach reveals structural hierarchies in the very process of persuasion. It retrieves side-lined understandings of norms and highlights the

[52] Amitav Acharya, "How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism," *International Organization*, 58 (2004): 239–275.
[53] Stephan Engelkamp, Katharina Glaab & Judith Renner, "Office Hours: How (Critical) Norm Research Can Regain its Voice," *World Political Science Review*, 10 (2014): 33–62.
[54] Nicole Deitelhoff & Lisbeth Zimmermann, "Things We Lost in the Fire."

generative aspect of resistance against alleged consensus. Normative processes in cyberspace benefit from conclusions drawn within all these approaches. The regulatory perspective and strategic construction of norms have dominated the debate thus far and given much meaning to the story of cybernorms development. Yet as argued throughout this paper, they are not in sync with the current politics of cybernorms. Contestation which integrates the reality of the decolonial claim, in contrast to exploiting such a claim, needs to feed into the EU's story about cybernorms.

What would the EU's strategy of contestation be about and what should it avoid? Principally, the EU should not abdicate and cede the ground for projecting their narratives to others, but actively engage in contestation. This includes a proactive contribution to shaping the meaning of fundamental concepts such as peace, equality or even the need for a new cyber-specific treaty so that no single actor nor a group of actors can claim it as their flagship. There are two stumbling blocks along the way, however. Norm contestation is taboo. It is perceived as self-defeating, resembling concession, appeasement, or giving the other the benefit of the doubt in a duplicitous situation. Furthermore, bona fide contestation is indeed under threat in the communication ecology in which involvement risks ultimately "feeding the troll": That is, arguments presented in good faith by one side may be used by political opponents to bolster their own positions.

Russia's exploitation of the decolonial claim, for example, pushes the EU to positions where it becomes defensive about the structural inequality of the international system. The 8 November 2018 session of the UN General Assembly First Committee, mentioned above, illustrates this well. In the general statements, the Russian delegation depicted the UNGGE process as exclusionary and OEWG as a way forward which democratises cybernorms development. In its own statement, the EU only recognised the role of OEWG in disseminating knowledge and expertise and fostering, rather than shaping, understanding about fundamental rules and their application in cyberspace. In recognition that all UN Member States should be able to contribute to the process of cybernorms development, the EU brought up its investment into capacity building in the area of cybersecurity and cybercrime.[55] This fairly standard framing from the old repertoire of "the normative power Europe"[56] may have a limited advantage in the politics of cybernorms. It is advisable that the EU as a collective take up a proactive role in the space of OEWG for strategic narrative contestation, including focusing on multilateralism and cyber capacity building. Otherwise it risks being trolled and accused of contributing to what Russian diplomats like to call "maintaining digital inequality between various members of the international community".[57]

Principally, the EU should not abdicate and cede the ground for projecting their narratives to others, but actively engage in contestation. This includes a proactive contribution to shaping the meaning of fundamental concepts such as peace, equality or even the need for a new cyber-specific treaty so that no single actor nor a group of actors can claim it as their flagship.

Cyber capacity-building as a form of development assistance will be at the core of strategic narrative contestation. There is an across-the-board agreement that such assistance is needed both in order to close the 'digital divide' between countries and to build national resilience in third countries as a means of increasing the level of cybersecurity globally. Naturally, approaches differ how to go about it. They

[55] See the recording from 48:30, United Nations Web TV, "First Committee, 31st meeting" (8 November 2018). Accessed 6 March 2019. http://webtv.un.org/meetings-events/general-assembly/main-committees/1st-committee/watch/first-committee-31st-meeting-general-assembly-73rd-session/5859574011001.

[56] The term was initially introduced by Ian Manners in his seminal article from 2002, "Normative Power Europe: A Contradiction in Terms?" *Journal of Common Market Studies*, 40(2): 235-258.

[57] Press release on the UN General Assembly adoption of a Russian-proposed resolution on combating cybercrime, The Ministry of Foreign Affairs of the Russian Federation, "Press release on the UN General Assembly adoption of a Russian-proposed resolution on combating cyber crime," 18 December 2018. Accessed 16 March 2019. http://www.mid.ru/en_GB/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3449030

range from an allegedly unconditional assistance for 'recipients' of aid to a model based on merging values, interests and principles that seeks to work with other parties as partners.[58] The standing dilemma of development assistance will affect strategic narrative contestation as well: Such assistance implies both an economic benefit for and the transfer of values from donor countries[59] and a desire to decrease inequalities and further human development. The choice of strategy is not binary, however, as these components cannot be easily disentangled. The parties involved, local and international, are well aware of this 'double-use' of development assistance. Creating a narrative that makes sense of such conditions could bring a strategic dividend in times of hypocrisy fatigue.

This narrative may involve more nuanced thinking about consensus. Consensus, as Chantal Mouffe aptly explains, is an illusion. It is naïve to think that people can just leave aside their particular interests and think as rational beings. But consensus is also a form of imposition as it is always based on some exclusion and de facto renunciation of pluralism.[60] Pluralism remains an awkward challenge in cybernorms development. But strategic narrative contestation offers some clue: Conflict and divisions are inherent to politics and we must cultivate political arenas in which differences can be meaningfully confronted. A good story will go a long way in such confrontations.

[58] For the latter see, Patryk Pawlak, "Operational Guidance for the EU's International Cooperation on Cyber Capacity Building," European Commission, 31 August 2018. Accessed 22 February 2019. https://www.iss.europa.eu/content/operational-guidance-eu%E2%80%99s-international-cooperation-cyber-capacity-building.

[59] Zine Homburger, "The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace," *Global Society*, 2019, DOI: 10.1080/13600826.2019.1569502

[60] Chantal Mouffe, *The Democratic Paradox,* (London and New York: Verso, 2000).

About the author

Xymena Kurowska is an IR theorist interested in interpretive policy analysis. She received her doctorate from European University Institute in Florence, Italy. She works within International Political Sociology and at the intersection of psychoanalysis and politics, with particular focus on security theory and practice, border politics, subjectivity, and interpretive methodologies. She was a grantee of the European Foreign and Security Policy Studies Programme to research border policies in Eastern Europe. She also served as the CEU principal investigator in Global Norm Evolution and Responsibility to Protect, chair of International Political Sociology section at International Studies Association, co-editor of Palgrave book series 'Central and Eastern European Perspectives on International Relations', and academic rapporteur on norms for EU Cyber Direct. Currently, she is a Marie Skłodowska-Curie fellow at the Department of International Politics at Aberystwyth University.

About EU CyberDirect

The **EU Cyber Direct** project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through extensive dialogues with strategic partner countries and regional/international organisations. The **EU Cyber Direct** is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

RESEARCH IN FOCUS

is a series of research papers aimed at supporting the EU's cyber-related policies by providing a timely and policy-relevant analysis.

EU CYBER DIRECT

This project is funded by the European Union.