Idea Entrepreneurs: The Case of the 2020 United Nations OEWG & Cybersecurity

Nanette S. Levinson
Internet Governance Lab
American University

Abstract
The United Nations OEWG (Open Ended Working Group) focused on cybersecurity provides the context for an examination of idea entrepreneurship regarding the role of nonstate actors and the concepts of human rights, gender and sustainable development against the backdrop of a global pandemic and increasing cybersecurity challenges. Crafting a cross-disciplinary conceptual framework based upon a review of relevant literatures, this study uses archival and content analysis to highlight those organizations serving as idea entrepreneurs and those contesting such ideas. Findings include the presence of key divides among idea entrepreneur organizations (including among nation-state organizations themselves). Additionally, mention of the pandemic emerges as a factor catalyzing idea entrepreneurship.

Keywords
Cybersecurity; norms; idea diffusion; nonstate actors; gender; human rights.

1.0 Introduction

Norms, the ideas behind them, and their diffusion constitute a long-standing and prolific research arena in political science and international relations (Finnemore & Sikkink,1998; Katzenstein,1996; Hurwitz, 2014; ten Oever, 2020). There is recent work that points out how norms begin as ideas (Alger & Dauvergne, 2020) as well as the need for more research that examines the pre-norm stage (Rosert, 2019). Additionally, there are six major factors today that set the scene for revisiting idea diffusion (and discussions around norm development) related to cybersecurity; these factors call for a more cross-disciplinary perspective. They are:

- The increasing importance (and interrelationships) of the geopolitical (Nye, 2017), economic, political, and even epidemiological in national, regional, and global contexts, including the role of small states (Adamson, 2019; Corbett et al., 2020) or even rogue states (Wunderlich,2020)
- The continuing growth of internet technologies-with their inherent interconnectedness--and now, especially the challenges of information-related emerging technologies such as artificial intelligence and the interrelationships among these technologies themselves and the policy arena (Musiani, 2020: DeNardis, 2020)
- The changing roles of international institutions with regard to internet/cyber governance (Levinson and Marzouki, 2016)
- The recent and myriad commissions (e.g. Global Commission on the Stability of Cyberspace), panels (e.g. High Level Panel on Digital Cooperation), and initiatives/working groups focused on generating ideas regarding cybersecurity topics and challenges (including the two entities within the United Nations: the

longer standing GGE (Group of Governmental Experts) and the as of December 2018 OEWG). (See Madokoro (2018) for an analysis of commissions' roles with a focus on the norm of the 'responsibility to protect' or Eggenschwiler (2020) on the outcomes of the Global Commission on the Stability of Cyberspace.)

- The presence and ever more vibrant debates surrounding the multi-stakeholder concept, itself dating back to the Working Group on Internet Governance (WGIG) of the 2003-2005 World Summit on the Information Society (Pohle, 2016)
- The advent of new non-state actors in cybersecurity-related fora (e.g. Gorwa & Peez (2018); Hurel & Lobato (2018); or Fairbank (2019) on the role of the private sector),Tanczer et al. (2018) on CSIRTS and their roles, and even new actors from within nation-state governments (Georgieva, 2020) on the role of intelligence agencies in cybersecurity.

This paper provides an *in res* view of the United Nations Open-Ended Working Group (OEWG) on Developments in the Field of Information and Communication Technologies in the Context of International Security with a focus on its March 2020 Report pre- draft through its September 2020 response comments. Due to the COVID pandemic, the Hon. Jorg Lauber, the Chair of the OEWG, announced adjustments to the 'roadmap' for the Group's ultimate report to the General Assembly, now scheduled for 2021, with a goal of completing informal meetings by the end of 2020, formulating a ZERO draft in early 2021, and a final session tentatively scheduled for March 2021. This delay actually provides an opportunity to view carefully the pre-norm stage, answering the call for work on what occurs during the earliest stages of 'norm emergence' as Finnemore and Sikkink (1998) term it in their norm life cycle stages.

Focusing on a subset of ideas related to nonstate actor roles and to inclusion of ideas revolving around human rights, or gender, or sustainable development put forward in response to the original OEWG pre-draft (see https://www.un.org/disarmament/open-ended-working-group/), it examines responses from sixty-six state, region, intergovernmental organizations, and nongovernmental organizations (using the UN classification that includes several industry-related organizations in the NGO category). Several of the comment submissions represent more than one entity (e.g. comments from Non-aligned Members or from Australia and Mexico on behalf of 13 other countries or a joint submission from 12 civil society organizations). Four countries (Bangladesh, Cuba, Finland and Russia) and one private sector organization (Kaspersky) submitted updated comments in June and September 2020. A final idea element in the subset examined is the presence (or not) of any reference to the pandemic and its impact on cyber or cybersecurity issues,

A contribution of the *in res* mini-case study of the OEWG reported here is the view of an idea flow foundation just prior to 'norm emergence' in what can be called the complex, cross-national, cross-sectoral, and cross-organizational cybersecurity ecosystem. (See Ruhl, et al. (2020) for a description of the complex cybersecurity norm-related ecosystem with its new and fragmented processes.) This case study also captures the context of this flow in its focal setting, the OEWG, functioning as a primarily online environment, due to the COVID-19 pandemic. Using work from the field of innovation

diffusion combined with concepts from several disciplines, it examines cross-organizational pathways for possible information flow. It also contributes information regarding organizations themselves as idea entrepreneurs. (See Stone, 2019 for treatment of organizations as transnational policy entrepreneurs as in the case of the International Crisis Group, a human rights nonstate actor.)

In order to trace fully these patterns, this study adopts a transnational and interorganizational perspective. It contributes a distinctive understanding of nonstate actor vis-à-vis state/regional and international institution actors ebb and flow of ideas and influence. Finally, it adds a lens focused on inequalities or divides with regard to human rights, development, gender) with regard to nation-state vis-à-vis other nation states and nation-states vis-a- vis nonstate actors.

2.0 Theory/Conceptual Framework

Hannan and Freeman (1977) argue that the characteristics of a setting actually influence which organizations survive in a given setting over a long period of time. Now, more than forty years later, this paper argues that the characteristics of a setting, combined with power panoplies and idea framing, —and especially an increasingly interconnected and complex one (Ruhl et al., 2020)—influence which ideas survive and shape norm emergence in the context of cybersecurity. Another related characteristic of the setting is what this author terms the culture kaleidoscope: the often interacting, complex cultures of small groups, organizations, occupations, nation-states, diasporas, and even alliances or partnerships. The culture kaleidoscope, of course, includes recognition of 'localization', the way norms are translated and shaped by local cultures (Acharya, 2013).

The six characteristics highlighted in the introduction to this paper set the scene (and the requirements) for a needed conceptual framework. For the most part, other global governance arenas including environmental and health governance share the technological and political uncertainties, the globally complex interconnections (state and nonstate actors as well) and networked risks at different levels. Thus, while there is some sharing of research across these governance arenas, there is much potential for cross-arena learning.

As Galazs et al. (2017) emphasize in the context of the environmental governance setting, the world faces networked risks. So, too, do nation-states today face networked cybersecurity risks. They also operate in complex power equations including needed knowledge and expertise components often residing in nonstate actors. Nonstate actors, too, can pose threats in the cyber realm. Additionally, while not universally accepted, both environmental governance and cybergovernance share the fuzzy concept of multistakeholderism. (For a critical view of multistakeholderism, see Raymond and DeNardis (2015) or Hofmann (2016).) At a minimum, this concept as it plays out in internet related governance involves cross-stakeholder group dialogue such as that which occurs in the Internet Governance Forum, now approaching its fifteenth year. However, this *in res* mini case study provides an opportunity for examining a

different milieu, a multilateral one, the OEWG in the context of the United Nations system and the presence of nonstate actors.

With regard to context, the United Nations system itself is undergoing change. In recent years, the United Nations Secretary-Generals have begun to highlight the roles of the private sector and even used the term 'partnership'. Yet the UN only recognizes certain civil society organizations. As Weiss and Wilkerson (2018) point out, there is not much attention to those who are 'globally governed'. Some parts of the system, such as UNESCO, have a long history of including civil society organizations in dialogue (Levinson & Marzouki,2016). Other parts, for example, the ITU, have a history of work with the private sector but less with civil society. These histories contribute to the culture of the United Nations and the context for the OEWG related to cybersecurity, a working group to which any member state may send a delegate.

What does this mean for the design of a conceptual framework? Such a framework needs to capture the cross-boundary flow of ideas from origination to contestation (Maurer, 2020) or to inclusion (recognizing that an idea can be transformed over time) and, at the same time, to recognize key characteristics of a setting such as power and culture (both organizational and national) and the role and characteristics of actors in such a setting. Recent research also reminds us that we cannot forget about narrative or storytelling or 'framing' as Finnemore and Hollis (2019) call it or even 'vocabularies' as Pantzerhielm et al. (2019) term it. These 'vocabularies' are what travels across (or not) complex, multilayered networks of individuals, organizations, and groups of organizations. They constitute the substance of what 'idea entrepreneurs' proffer whether formally (as studied here) or informally. Indeed, each nation state or nongovernmental organization or subgroups thereof acts as an idea entrepreneur in the OEWG negotiations regarding the crafting of the OEWG's final report to the United Nations.

The term 'Idea entrepreneurs' refers to more than individuals whether diplomats or technical experts or private sector or civil society leaders. Rather an 'idea entrepreneur' can refer to at least three levels of analysis: the individual, an organization, or even a set of organizations. Here the focal levels are the organizational and the interorganizational as represented by their comments on the pre-draft. Additionally, as we have learned from decades of research on innovation transfer or diffusion (Levinson, 2020; Rogers,1962), an idea or innovation undergoes 'shaping' or adaptation as it flows across organizational and national boundaries or vice versa. It can be a top down process or a bottom up process or a combination thereof. There is even the possibility of learning across stakeholder groups as an idea flows (Cashore et al., 2019). At the same time, power dynamics implicitly and explicitly operate (Alger & Dauvergne, 2020; Deitelhoff & Zimmerman, 2020; Morrison et al., 2019). The work reported here serves as a beginning stage for studying the actual OEWG final Report, now scheduled for 2021.

Research from the public administration/public policy field highlights the roles of 'policy entrepreneurs' whether individuals (the focus of most studies) or other states (as in

policy transfer studies) and provides a powerful perspective for examining the work of idea entrepreneurs in the context of cybersecurity. As noted earlier, recent studies outline such roles for commissions, nonstate actors, rogue states, and less developed nations in shaping cybersecurity or other global governance related discourse.

Writings from this field focus on governance in multiple dimensions. Here research streams on governance learning (Challies et al., 2017) and policy learning (Levinson, 2020) shape this conceptual framework. Recent studies of regime complexes (Nye, 2014; Orsini, et al., 2013) provide a reminder that there is a need to trace possible idea entrepreneurship between and among regimes in a regime complex and, indeed, examine the scene for possible governance learning. While the conceptual framework for a regime complex underlines the issue area and overlaps among issue areas in the 'complex', it focuses neither on the setting characteristics nor on the networks of actors and power panoplies present in and across the regimes with a focus on idea flow and governance learning. However, it is useful to consider regime theory when looking at ideas begun in one regime and applied to another regime or more in a complex.

In sum, literature (norms, power, governance) from international relations and public administration/policy combined with knowledge transfer (innovation diffusion) literature from communication sciences, and that of policy transfer and entrepreneurship/policy learning from public administration combine to provide the framework described above and utilized in this mini-case.

3.0. Methods

The primary research methods include content analyses of the literatures identified in the conceptual framework above (international relations/ political science, public administration, communication sciences) with a special focus on idea, norm or policy knowledge transfer/translation (Gerlak et al., 2020; Song et al., 2019) or contestation (Isaacs,2018). With regard to the mini-case study of the OEWG, methods used include content and archival analysis of OEWG documents publicly available through September 2020. The absence of rich data gathered through quasi-ethnographic observation and in-depth interviews constitutes a constraint of this work as well as a pathway for additional research. As the OEWG Chair points out, much of the work moving the group toward some sort of consensus regarding an idea and ultimate norm happens outside of formal meetings; and written submissions and the pandemic makes this more difficult. What future research may identify is how such face-to-face work on the periphery of the formal translates into some type of equivalent in the online arena.

4.0 Results

4.1 Culture Kaleidoscope

While the values embedded in national cultures can shape ideas as the research of Hofstede (1993) highlights, organizational cultures can also shade responses to ideas. The culture of the United Nations as a seventy-five-year-old multilateral type institution with its nation-state diplomatic core combined in kaleidoscopic manner with the national culture of a delegation clearly colors the 'vocabularies' used in the comments to the pre-Draft. The comments studied often use the following type of language: 'My delegation

aligns itself or supports the statement by (insert another nation-state or group of nation-states delegation).

Within this vocabulary type, national cultures (reflecting embedded values including views on privacy and on nation state roles) and historic political ties shape cross-nation state idea entrepreneur support. Thus, developing nations involved in the OEWG tend to include a statement in support of comments from the NAM, the non-aligned movement. For example, Bangladesh notes its support for the statement from Indonesia on behalf of the NAM countries. Turning to a different grouping, Finland expresses its support by "align(ing) with previous interventions by New Zealand" and by supporting a suggestion by the Czech Republic and other delegations to pay special attention to critical infrastructures. Similarly, several countries either note directly their support of the Russia delegation's ideas or restate that delegation's arguments in their own submissions.

Nonstate actor organizations also have their own cultures, often further shaped by occupational cultures such as that of technical experts. There appears to be greater acknowledgement of commission norms in statements by nonstate actor organizations, often reflecting the interlocking directorates (Mizruchi,1996) that connect a commissioner with a nonstate actor organization on which she or he also serves.

4.2 Multistakeholderism/Roles of Nonstate Actors

There is a clear divide in nation state comments regarding multistakeholderism and the role of nonstate actors. The statement from the Russian delegation decries the call for multistakeholderism, noting it is "artificially exaggerated". Further, the Russian comments argue that "the central role of the UN in ensuring IIS (international information security) is eroded by delegating excessive authority in this field to the regional bodies and organizations. The role of multi-stakeholder model is imposed, with special emphasis laid on the contribution of the private sector, business and academia to ensuring responsible States' behavior in information space." Similarly, China argues that the OEWG is an intergovernmental process so "our discussions should focus on the roles played by states and governments". Interestingly, some statements reference regional organizations. (See Dai et al. (2018) or Koff (2016) for analyses of regions in related contexts.)

The ideas expressed here by Russia and China are clearly in contestation to other nation states' comments regarding multistakeholderism or nonstate actor roles. The comments from Finland talk about the "high value in exchange of views" and the "importance of involving all stakeholders in this debate". Canada requests "a stronger reference to the request, made by several States, that nongovernmental stakeholders play as much of a role as possible in the OEWG process." France notes that consultation with stakeholders is essential. Denmark, too, calls for more attention in the Report to multistakeholder input. The number of statements made in strong support of multistakeholder inputs to the OEWG definitely outweighs the statements by China and Russia.

Turning to nonstate organization comments, none oppose a multistakeholder model. Indeed, the Kaspersky comments remind the reader not to overlook the technical community as a stakeholder group and call for additional strengthening of a multistakeholder approach. They also highlight a multistakeholder role in capacity-building, calling for regular consultation with stakeholders in fostering dialogue. In this way, they argue, that inclusion of opportunities for multistakeholder consultation can help build global consensus. As the Internet Society writes in its submission, "threats cannot be solved by states alone." Finally, the joint submission by the twelve civil society organizations emphasizes that any OEWG recommended mechanism for information sharing be sure to "include meaningful opportunities for nongovernment stakeholders and regional bodies to participate." Further, this joint statement underlines the need for nongovernmental organizations to exchange ideas with the OEWG and for states "to support capacity-building efforts to support the implementation of norms".

4.3 Human Rights

The joint submission by twelve civil society organizations recommends that human rights "be mainstreamed in the elaboration and implementation of norms". Global Partners Digital also supports this incorporation of human rights into OEWG norms. Turning to nation state responses that incorporate support for the idea of human rights inclusion in norms, Armenia, Australia, Austria, Brazil, Columbia, Czech Republic, Ecuador, Estonia, and Uruguay are among the delegations especially including human rights or international humanitarian law in their ideas.

Directly opposed to this idea are the comments from China, Cuba, Iran, Russia and Zimbabwe. The statement from Russia details its opposition by arguing that human rights belong elsewhere in the United Nations and not in the OEWG discussion of norms. The Russian delegation submits that "it is absolutely unacceptable that the draft fixes the principle of full and automatic applicability of IHL (International Humanitarian Law) to the ICT environment in peacetime." (They use a similar argument for their opposition to multistakeholderism and to gender.)

4.4 Gender

Here, too, there are clear divides. Australia "welcomes references to gender, including the need to encourage meaningful participation of women" as do OEWG delegations such as Columbia, Ecuador, Estonia, Ireland, Sweden and New Zealand. The United States delegation calls for an inclusive approach. In contrast, China argues that gender equality (and human rights as well as sustainable development) should not be an OEWG priority, arguing these topics are the domain of other UN groups. Similarly, Russia notes that there are "excessive references to sustainable development, in particular to social aspects, human rights, and gender equality."

4.5 Sustainable development/capacity-building

As noted in the sections on multistakeholderism, human rights, and gender, Russia and China see discussions on sustainable development belonging elsewhere in the UN system. In fact, China calls for cutting down the content on human rights and on development.

Contrastingly, Bangladesh calls for the “peaceful, people-centered and development-oriented focus if ICT is to be used as a positive force in reaching the sustainable development goals”. Canada also supports a focus on capacity building. It points out that instead of a recommendation for a new mechanism to coordinate global capacity building, the OEWG Report should note that the Global Forum on Cyber Expertise already does what the pre-Draft Report recommended. In fact, as Canada points out, the recommendation actually calls for what would be a duplicative mechanism. Indeed, the statement from the Global Forum on Cyber Expertise itself highlights its own existing role in global cyber capacity-building.

4.6 The Pandemic

Several nations make note of the pandemic. Bangladesh highlights COVID. Australia also mentions the pandemic and particularly comments on health care infrastructures. As noted earlier in the section on the UN culture, Finland’s remarks echo that of the Czech Republic and other delegations calling for the OEWG final draft to pay special attention to critical infrastructures. Comments from the Netherlands delegation discuss the pandemic and underline the transnational nature of the threats. The NAM comments also include a call for a focus on critical infrastructure.

Focusing on nonstate actor organization comments, Kaspersky submitted comments on the threats the pandemic especially poses. The Kaspersky submission notes its support of the relevant comments by the Czech Republic and other states to focus on critical infrastructures. Additionally, the CyberPeace Institute notes its support for the ICRC (International Committee for the Red Cross) new norm “prohibiting states conducting or knowingly supporting ICT activity that would harm medical services or medical facilities”. Comments from Russia, on the other hand, mention the pandemic in a different light: they criticize the OEWG’s plans to delay and plans for virtual convenings, especially noting their delegation’s view that the United States too stringently shut down New York City.

There are, indeed, two aspects of the discussion stemming from recognition of the immensity and uncertainty of a global pandemic period. First, there is the call to protect critical infrastructures and especially health infrastructures. Here, for example, the Internet Society notes its support for the norm (to protect the public core) proposed by the Global Commission on the Stability of Cyberspace (GCSC). Other nonstate actors also mention and support this norm, using sometimes slightly different wording. The ICT4Peace Foundation expresses its support for the norm of not targeting critical infrastructure. Microsoft mentions that “elements central to the functioning of the Internet should be protected”. The second is a more controversial and related call for the protection of human rights. Here, as noted in Section 4.2, there is direct contestation from Russia and the other nations supporting Russia’s stance.

5.0 Discussion

The above findings highlight the presence of divides, often mirroring cultural, political, social and economic divides that exist outside of the UN system itself. One example

stems from Latin American country comments highlighting the underrepresented needs of developing countries. Another example is the submission by the NAM (the nonaligned movement countries), illustrating how small or less powerful states can band together as an interorganizational idea entrepreneur. As shown in the findings related to the inclusion of sustainable development goals in the OERWG's purview, a number of developed countries as well as developing countries from around the world support inclusion of wording related to the sustainable development goals. At the same time, it is important to note the absence of a number of African countries from the OEWG, even though all member states were invited to participate in the OEWG. This divide reflects the limited time and limited resources of many developing nations with smaller delegations, tighter budgets, and other key priorities. (Note that the OEWG began its work in person in New York City in 2019, before the current pandemic.) It is possible that those delegations not participating at the original call might view a call differently, if it were to participate in a virtual negotiating environment. This is the subject for additional research.

Taken together, what do these findings, focused only on a select subset of ideas, tell us? There is a pattern. Contestation to one of the ideas studied here (human rights, gender, sustainable development) (excluding the pandemic related ideas) tends to correlate with contestation of the other ideas. As research in another governance domain tells us, there may be a 'galaxy' of ideas/pre-norms that hang together (Diggs et al., 2019). Perhaps a focus on the pandemic and its impact on cybersecurity issues and idea generation as a rationale can bring along other nation states, through linking and reframing the other ideas, as work on norm galaxies and norm adoption in other venues indicates. There is clear evidence noted in the findings above of the COVID 19 pandemic's impact on idea flow: there is a sudden and apparent shift in narrative from some nation state and nongovernmental actors, bringing the healthcare infrastructure to the fore and complementing calls for protecting core infrastructure.

Recently, Milhorance (2020) examined a policy network of state and nonstate organizations in Brazil, highlighting how membership in a coalition of nonstate and government actors made diffusion for nonstate actor' ideas to international organizations possible. Milhorance's research focused on a formal coalition; the conceptual framework called for here adds an informal dimension. It poses the question are there any informal connections affording pathways for idea flow. In the findings above, Canada's statement noting that the pre-Draft recommendation for a global mechanism for capacity-building actually duplicates the existing work of the Global Forum on Cyber Expertise. (The Global Forum on Cyber Expertise also put forth its own submission, making the same argument.) Note that the Global Forum on Cyber Expertise is a large multistakeholder organization with a number of developed (including Canada) and developing country members as well as international organizations (such as the World Bank) and private sector companies. (Neither China nor Russia are members.)

6.0 Conclusions

The comparative advantage of this *in res* research allows for an analytic focus on the initial pre-draft and subsequent comments as well as a design for a needed, cross-disciplinary conceptual framework, while a comparative constraint is, of course, an absence of final outcomes for analyses. Yet viewing this mini-case midpoint allows for a close up of idea proffering and idea contestation with a view toward recognizing characteristics of context including the culture kaleidoscope and power panoplies and divides as well as related vocabularies. It also provides a preliminary view of a 'galaxy' of ideas (human rights, gender, sustainable development) that one group of nations include as a part of their OEWG vocabulary whereas a smaller number of nations contest their presence in the OEWG specific purview. The outcome remains to be seen.

Further research needs to focus on all categories of nation-state comments with reference to the pre-Draft ideas, and ultimately to the outcomes as embedded in the Final Report. As Alger and Dauvergne (2020) poignantly point out in a different global governance arena, "Struggles to frame norms never end, nor are norms ever truly consistent across groups and time" (p. 156). What, then, are the implications for cybersecurity diplomacy in the context of the OEWG? (See by way of background Feijoo et al., (2020) for a discussion of artificial intelligence and 'a new technology diplomacy'.) As noted earlier, future research should also probe the informal and online contextual dimensions of idea flow, as it tracks any changes from the positions presented in the initial subset of comments discussed here.

Note: All quotations without attribution come directly from statements posted at: https://www.un.org/disarmament/open-ended-working-group/

Acknowledgements
The author wishes to acknowledge the research assistance of School of International Service Graduate Assistant, Raven Neely.

Funding
The author expresses appreciation to American University's Internet Governance Lab and the Hewlett Foundation for its support of this Project.

References

Acharya, A. (2013). The R2P and norm diffusion: Towards a framework of norm circulation. *Global Responsibility to Protect*, *5*(4), 466–479. https://doi.org/10.1163/1875984X-00504006

Adamson., L. (2019). Let them roar: Small states as cyber norm entrepreneurs. *European Foreign Affairs Review 24*(2), 217-234. https://kluwerlawonline/journalarticle/European+Foreign+Affairs+Review/24.2/EERR2019014

Alger, J., & Dauvergne, P. (2020). The translocal politics of environmental norm diffusion. *Environmental Communication, 14*(2), 155-167. https://doi.org/10.1080/17524032.2019.1665567
Andrews, N. (2019) *Gold mining and the discourses of corporate social responsibility in Ghana.* Palgrave Macmillan.
Azmi, R., Tibben, W., & Win, K.T. (2018). Review of cybersecurity frameworks: Context and shared concepts. *Journal of Cyber Policy, 3*(2), 258-283. https://doi.org/10.1080/23738871.2018.1520271
Baram, G., & Menashri, H. (2019). Why can't we be friends? Challenges to international cyberwarfare cooperation efforts and the way ahead. *Comparative Strategy, 38*(2), 89-97. https://doi.org/10.1080/01495933.2019.1573069
Barrinha, A., & Renard, T. (2020). Power and diplomacy in the post-liberal cyberspace. *International Affairs 96*(3), 749-766. https://doi.org/10.1093/ia/iiz274
Biermann, F., Betsill., M.M., Gupta, J., Kanie, N., Lebel, L., Liverman, D., Schroeder, H., & Sievenhüner, B. (2009). Science and implementation plan of the Earth System Governance Project. *Earth System Governance.* https://www.earthsystemgovernance.org/about
Cashore, B., Bernstein, S., Humphreys, D., Visseren-Hamakers, I., & Rietig, K. (2019). Designing stakeholder learning dialogues for effective global governance. *Policy and Society, 38*(1), 118-147. https://doi.org/10.1080/14494035.2019.1579505
Cavelty, M.D., & Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy, 41*(1), 5-32. https://doi.org/10.1080/13523260.2019.1678855
Challies, E., Newig, J., Kochskämper, E., & Jager, N.W. (2017). Governance change and governance learning in Europe: Stakeholder participation in environmental policy implementation. *Policy and Society 36*(2), 288-303. https://doi.org/10.1080/14494035.2017.1320854
Collier, J. (2018). Cyber security assemblages: A framework for understanding the dynamic and contested nature of security provision. *Politics and Governance, 6*(2), 13-21. https://doi.org/10.17645/pag.v6i2.1324
Dai, C.T., & Gomez, M.A. (2018). Challenges and opportunities for cyber norms in ASEAN. *Journal of Cyber Policy, 3*(2), 217-235. https://doi.org/10.1080/23738871.2018.1487987
Deitelhoff, N. & Zimmerman, L. (2013). Things we lost in the fire: how different types of contestation affect the validity of international norms. PRIF working papers, 18. *Frankfurt am Main: Hessische Stiftung Friedens und Konfliktforschung.* https://nbn-resolving.org/urn:nbn:de:0168-ssoar-455201
DeNardis, L. (2020) *The Internet in Everything.* Yale University Press.

Diggs, E. G., Regan, M., & Parance, B. (2019). Business and human rights as a galaxy of norms. *Georgetown Journal of International Law*, *50*(2), 509+. https://link-gale-com.proxyau.wrlc.org/apps/doc/A633545362/LT?u=wash11212&sid=LT&xid=44f69dc2
Eggenschwiler, J. (2020), Expert commissions and norms of responsible behaviour in cyberspace: a review of the activities of the GCSC. *Digital Policy, Regulation and Governance.* Emerald Publishing.
Fairbank, N.A. (2019). The state of Microsoft?: The role of corporations in international norm creation. *Journal of Cyber Policy 4*(3), pp. 380-403. https://doi.org/10.1080/23738871.2019.1696852.
Feijoo, C., Kwon, Y., Bauer, J.M., Bohlin, E., Howell, B., Jain, R., Potgieter, P., Vu, K., & Whalley, J. (2020). Harnessing artificial intelligence (AI) to increase wellbeing for all: The case for a new technology diplomacy. *Telecommunications Policy.*44, pp. 1-14.
Finnemore, M., & Sikkink, K. (1998). International norm dynamics and political change. *International Organization 52*(4), 887-917. https://doi.org/10.1162/002081898550789
Georgieva, I. (2020) The unexpected norm-setters: Intelligence agencies in cyberspace. *Contemporary Security Policy, 41*(1), pp. 33-54. https://doi.org/10.1080/13523260.2019.1677389
Gerlak, A.K., Heikkila, T., & Newig., J. (2020) Learning in environmental governance: opportunities for translating theory to practice. *Journal of Environmental Policy & Planning.* https://doi.org/10.1080/1523908X.2020.1776100
Gorwa, R. & Peez, A. (2018). Big Tech hits the diplomatic circuit: Norm entrepreneurship, policy advocacy, and Microsoft's cybersecurity tech accord. Paper presented at the Hague Program for Cyber Norms Conference, 07– 09 November.
Hofmann, J. (2016). Multi-stakeholderism and internet governance: Putting a fiction into practice. *Journal of Cyber Policy 1*(1), pp. 29-49. https://doi.org/10.1080/23738871.2016.1158303
Hofstede, Geert (March 1993). Cultures and Organizations: Software of the Mind. *Administrative Science Quarterly*. Johnson Graduate School of Management, Cornell University. 38 (1). pp. 132–134. doi:10.2307/2393257.
Hurel, L.M., & Lobato, L.C. (2018). Unpacking cyber norms: Private companies as norm entrepreneurs. *Journal of Cyber Policy 3*(1), pp. 61-76. https://doi/org/10.1080/23738871.2018.1467942
Hurwitz, R. (2014) The play of states: Norms and security in cyberspace. *American Foreign Policy Interests 36*(5), 322-331. https://doi.org/10.1080/10803920.2014.969180
Isaacs, R. (2018). The micro-politics of norm contestation between the OSCE and Kazakhstan: Square pegs in round holes. *Third World Quarterly 39*(9), pp.1831-1847. https://doi.org/10.1080/01436597.2017.1357144.
Katzenstein P (1996) *The culture of national security: norms and identity in world politics.* Columbia University Press, New York.

Koff, H. (2016). Reconciling competing globalizations through regionalisms? Environmental security in the framework of expanding security norms and narrowing security policies. *Globalizations, 13*(6), pp. 664-682. https://doi.org/10.1080/14747731.2015.1133044
Levinson, N. (2020). Toward future internet governance research and methods in *Researching internet governance: Methods, frameworks, futures.* DeNardis, L., Cogburn, D., Levinson, N. & Musiani, F. (Eds.) Cambridge: MIT Press.
Levinson, N. & Marzouki, M. (2016) International organizations and global internet governance: Interorganizational architecture. In F. Musiani, D.L. Cogburn, L. DeNardis & N.S. Levinson (Eds.), *The Turn to Infrastructure In Internet Governance* (pp. 47-71). Palgrave Macmillan.
Madokoro, D. (2019). International commissions as norm entrepreneurs: Creating the normative idea of the responsibility to protect. *Review of International Studies* 45(1). pp.100-119 https://doi.org/10.1017/S0260210518000219.
Maurer, T. (2020) A Dose of Realism: The Contestation and Politics of Cyber Norms. *Hague J Rule Law* 12, pp. 283–305). https://doi.org/10.1007/s40803-019-00129-8.
Milhorance, C. (2020) Diffusion of Brazil's food policies in international organizations: Assessing the processes of knowledge framing. *Policy and Society 39*(1), pp.36-52. https://doi.org/10.1080/14494035.2020.1724362
Mizruchi, M.S. (1996) What do interlocks do? An analysis, critique, and assessment of research on interlocking directorates. *Annual Review of Sociology 22*(1), pp.271-298. https://doi.org/10.1146/annurev.soc.22.1.271
Morrison, T.H., Adger., W.N., Brown., Lemos, M.C., Huitema, D., Phelps, J., Evans, L., Cohen, P., Song, A.M., Turner, R., Quinn, T., & Hughes, T.P. (2019). The black box of power in polycentric environmental governance. *Global Environmental Change 57*, pp. 1-8. https://doi.org/10.1016/j.gloenvcha.2019.101934
Musiani, F. (2020) Science and technology studies approaches to Internet governance: Controversies and infrastructures as Internet politics. Chapter 4 in *Researching internet governance: Methods, frameworks, futures.* DeNardis, L., Cogburn, D., Levinson, N. & Musiani, F. (eds.) Cambridge: MIT Press.
Nye, J. (2014). The Regime Complex for Managing Global Cyber Activities. The Centre for International Governance; Global Commission on Internet Governance: Paper Series 1. http://nrs.harvard.edu/urn-3:HUL.InstRepos:12308565
Nye, J. (2017). Deterrence and dissuasion in cyberspace. *International Security 41*(3), 44-71. https://doi.org/10.1162/isec_a_00266
Orsini, A., Morin, J.F., & Young, O. (2013). Regime complexes: A buzz, a boom, or a boost for global governance?. *Global Governance 19*(1), pp. 27-39. https://doi.org/10.1163/19426720-01901003
Pantzerhielm, L., Holzscheiter, A., & Bahr., T. (2019). Governing effectively in a complex world? How metagovernance norms and changing repertoires of knowledge

shape international organization discourses on institutional order in global health. *Cambridge Review of International Affairs*.
https://doi.org/10.1080/09557571.2019.1678112
Pohle, J. (2016). Multistakeholder governance processes as production sites: Enhanced cooperation "in the making". *Internet Policy Revie*w, 5(3).
https://doi.org/10.14763/2016.3.432
Rosert, E. (2019) Norm emergence as agenda diffusion: Failure and success in the regulation of cluster munitions. *European Journal of International Relations*. 25(4) pp. 1103–1131. https://doi.org/10.1177/1354066119842644
Ruhl, C., Hollis, D., Hoffman, W., & Maurer, T. (2020). Cyberspace and geopolitics: Assessing global cybersecurity norm processes at a crossroads. Carnegie Endowment for International Peace Working Paper.
Song, A.M., Cohen, P.J., Hanich, Q., Morrison, T.H., Andrew, N. (2019). Multi-scale policy diffusion and translation in Pacific Island coastal fisheries. *Ocean & Coastal Management, 168,* pp.139-149. https://doi.org/10.1016/j.ocecoaman.2018.11.005
Stone, D. (2019). Transnational policy entrepreneurs and the cultivation of influence: Individuals, organizations and their networks. *Globalizations, 16*(7), pp.1128-1144.
https://doi.org/10.1080/14747731.2019.1567976
Tanczer, L.M., Brass, I., & Carr, M. (2018) CSIRTs and global cybersecurity: How technical experts support science diplomacy. *Global Policy* 9 (S3), pp. 60-66.
https://doi.org/10.1111/1758-5899.12625
Weiss,T. G. & Wilkinson, R. (2018). The Globally governed—Everyday global governance. *Global Governance: A Review of Multilateralism and International Organizations* 24 (2).
Wunderlich, Carmen. (202*0). Rogue states as norm entrepreneurs: Black sheep or sheep in wolves' clothing?* Switzerland: Springer Nature AG.