Global Cybersecurity Governance Is Fragmented – Get over It

https://www.e-ir.info/2021/04/10/global-cybersecurity-governance-is-fragmented-get-over-it/

EMMA SANDVIK LING, APR 10 2021

During the 14th annual meeting of the Internet Governance Forum (IGF) in November 2019, UN Secretary-General Antonio Guterres posted a 'Tweet' of encouragement: "Access to a free and open Internet is at risk. We aren't working together across siloed social, economic and political divides. But that can change" (Guterres 2019). With this, Guterres summed up a central debate in contemporary cybersecurity. Efforts to implement substantial global cybersecurity norms and regulations have so far seen limited success. However, Guterres, and many more, remain hopeful that more coherent global cyber governance is possible. This essay will discuss the fragmentation of global cybersecurity governance.

To this end, I first reflect on the nature of global governance in general. With reference to Ian Hurd (2017) I argue that traditional global governance, beyond cybersecurity considerations, is not synonymous with unity. There is in fact evidence of fragmentation in global governance beyond cybersecurity. I then quickly explore a definition for the terms 'cybersecurity' and 'cyber governance,' highlighting how the concepts are highly political. Moving on, I reflect on current trends in global cybersecurity governance, finding that the tendencies of fragmentation in global governance do indeed extend to cybersecurity. I highlight evidence of increased collaborative efforts among states with established traditions of cooperation, while the issue is more complicated between adversarial actors. Having identified fragmentation, I ask how the fragmentation should best be addressed. I first consider values-based approaches to uniting cybersecurity governance using work from Mihr (2014) and Fliegauf (2016). Finding that these approaches fail to consider broader security dynamics, I look to Brechbühl et al. (2010) to suggest that cybersecurity governance is based on a network of collaboration, meaning that even local or regional efforts of collaboration can potentially contribute towards global stability. To round out, I point to confidence building measures and the Responsibility to Troubleshoot (R2T) as examples of low-threshold initiatives which could stabilise the cybersecurity landscape without leaning on an unrealistic expectation of a unified global approach. In this essay I argue that fragmentation in global governance in general, and cybersecurity in particular is normal, and indeed inevitable. Rather than aspiring for unified global cybersecurity governance, the focus should shift to finding means of increasing and ensuring stability in cyberspace.

Before exploring the potential for global cybersecurity governance, it is necessary to reflect on the nature of global governance in general. Global governance refers to the system by which sovereign states, relevant non-state actors, and civil society regulate and organise international affairs (Dodds 2016, 98). Indeed, even traditional conceptions of global governance are fragmented to a certain extent. Practices vary depending on region, and states are bound by international laws only to the extent that they have explicitly or tacitly consented to them (ibid. 99). Without an overarching global authority, global governance can best be understood as a network of structures, rather than one unified establishment. With this in mind, Ian Hurd (2017) attempts to counter skepticism regarding the utility of global governance structures. Hurd suggests that one must set aside conventional expectations based on domestic governance in order to fully appreciate the utility of global governance structures, with specific reference to law. Domestically, Hurd holds that law should be governed by certain rules which apply equally and dispassionately to all. This, he suggests cannot be expected of international law. In its very nature, international law applies differently to different actors depending on the treaties they have ratified. The landscape is further complicated by looking to non-state actors (ibid. 26-28). Furthermore, expecting adherence to international law would completely ignore the political dynamics which motivate or discourage states to act in accordance with international legal structures. Importantly, this is not to suggest that international law and other institutions regulating actor's behaviours internationally are without value. Rather, Hurd encourages his readers to set aside expectations of strict adherence to international institutions (ibid. 44). It is unproductive to assume that global governance is domestic governance on a larger scale. Any constructive debate about global governance should first appreciate its scope and recognise its limitations with regards to governing sovereign states. Observers should abandon expectations for complete compliance and unity as indicative of successful global governance as these preconceptions will hinder a nuanced analysis of the merits of current structures. The essay will now move to examine the terms 'cyber security' and 'cyber governance.'

According to Greiman, "cyberspace includes, but is not coextensive with, the Internet" (Greiman 2018, 149). Cyberspace is often described as borderless (Mihr 2014, 24), but this assumption should not be accepted without critical consideration. This essay will soon argue that though cyberspace is not divided by traditional borders, it is occupied by actors with particular interests and motives. This truism forms the basis for cybersecurity considerations. Cybersecurity and interests in cyberspace are reflective and productive of security interests more broadly. Global cyber governance, in the context of this essay understood as synonymous with internet governance, deals with the development and management of the technologies on which the internet depends, as well as the production of policies needed for the regulation of cyberspace (DeNardis 2014, 6). The structures governing cyberspace are still very much developing, but it is clear that cyber governance in general, and cybersecurity governance in particular, are multifaceted issues which encompass technical, administrative, legal and political considerations (Orji 2015, 107). Following DeNardis and Orji, the government of cyberspace includes political and technical components. Going back to Hurd, observers should not have the same expectations of global cybersecurity governance as a traditional domestic context. Due to the structure of cyberspace, which is very much still unfolding, the scope and nature of governance structures will inevitably look different compared to traditional conceptualisations of governance.

Importantly, the politics of cyberspace depends on cooperation between a diverse set of stakeholders. Rather than relying on a strictly state-centred approach, state and non-state actors must be considered to helpfully develop governing structures (DeNardis 2014, 14). This idea of multistakeholderism is reflected in discussions from the World Summit on the Information Society (WSIS) in 2003 and 2005. Sponsored by the United Nations, the two-part summit produced a coherent definition of internet governance: "Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures and programmes that shape the evolution and use of the Internet" (WGIG 2005, 4). Inherent in this is the aforementioned multistakeholderism, with an acknowledgement that the responsibility of cyber governance stretches beyond the sovereign state. Carr (2015) finds that this approach has many benefits: it recognises the uneven landscape of actors in cyberspace and encourages participation from a multitude of actors in policy making and enforcement (Carr 2015, 549). However, as Carr points out, the approach does have significant weaknesses. Multistakeholderism, as it stands, risks reinforcing and reproducing existing power dynamics where the US, and her western allies, dominate the playing field (Carr 2015, 658). Cattaruzza et al. (2016) expand this, pointing to a dynamic with the United States and her allies celebrating multi-stakeholder governance and others, most notably Russia and China, defending 'cyber sovereignty' with a state-focused approach (ibid. 7). This is an important consideration which will soon be discussed further: the idea that the core principles of current understandings of internet governance are in themselves a manifestation of broader power dynamics. Accepting this would mean that fragmentation is in fact inevitable in the current approach to global cybersecurity governance.

With a solid understanding of what global cybersecurity governance is, this essay now moves to examine current trends in cybersecurity governance. The essay will in particular point to evidence of fragmentation in contemporary global cybersecurity governance. Analysing ten national cybersecurity strategies as well as the approaches adopted by multiple international organisations, Sabillon et al. (2016) find that though many countries have developed national cybersecurity strategies, there is little effort spent on the international standardization of cybersecurity policies. The topic of international consideration is largely neglected in national cybersecurity strategies. Written at the height of the fight against the Islamic State, the article suggests that the ability states have demonstrated to cooperate in that case can be transferred to the fight against cybercrime. The authors also do highlight efforts – mainly by the US, UK and the Netherlands – to increase international cooperation on matters of cybersecurity (ibid, 79). It is important to be mindful here that the article was written in 2016 and there have been many important developments since then.

Using the EU to illustrate this point, the Union implemented the standardised European Data Protection Regulation in May 2018 (Laybats and Davies 2018, 81). There has also been an increased focus on the development of national cybersecurity strategies within the EU in general over the last decade, with emphasis on knowledge sharing and collaboration (ENISA 2020). There does seem to be tendencies for states with well-established political and economic relationships to work together to coordinate cybersecurity practices. However, the tendencies still point to an overemphasis on national considerations in a domain which is often considered "borderless." Furthermore, the issue becomes even more complicated when considering states with weaker cooperative traditions, as was previously discussed with reference how the Western and American approaches to cybersecurity governance differ from Chinese and Russian strategies.

So far, the essay has examined the current trends in global cybersecurity governance to find that there is indeed a great deal of fragmentation, and that the fragmentation can be traced back to the very basic understanding of what cyber governance is. Accepting that the fragmentation is present in global cybersecurity governance, considerations should turn to how the fragmentation can best be managed to avoid significant disruptions. What should global cybersecurity governance look like? Is fragmentation really such a bad thing? Identifying the fragmentation in global cybersecurity governance, some scholars suggest value-based remedies. Anja Mihr (2014) calls for more unity in cyber governance and advocates for a human rights-based approach. She argues that more accountability, transparency and stakeholder participation is needed and looks to universal human rights norms as benchmark guidance for establishing norms in cyberspace, thus creating a foundation for good cyber governance (ibid. 25). In a similar vein, Mark Fliegauf (2016) urges the international community to establish norms and shared codes of conduct in cyberspace to avoid a downward spiral of militarisation and distrust which ultimately compromises the foundational integrity of cyberspace. He highlights the conflicting behaviour of states working to protect national infrastructures while at the same time seeking to exploit vulnerabilities abroad (ibid. 79). Fliegauf acknowledges that establishing global cyber governance structures will be difficult and even goes to the extent of calling the task "Herculean" (ibid. 80). However, he stresses that the success of the project will depend on the credible commitment of all relevant parties, and proposes that the project should be overseen by "smart American leadership" (ibid. 81), arguing that the US already has a leading role by pointing to their efforts within the UN Group of Governmental Experts (GGE).

For Mihr and Fliegauf, the absence of coherent values is a hindrance to cyber governance. They reason that more coherent values would therefore lead to greater unity in global cyber governance. There are certainly many examples of institutions and countries who vow to govern cyberspace with certain values in mind. For example, the 2018 US National Cyber Strategy is "anchored by enduring American values, such as the belief in the power of individual liberty, free expression, free markets, and privacy" (White House 2018, 12). However, the idea that the fragmentation of global cyber governance can be remedied through a common adherence to certain norms and values fails to acknowledge how larger power dynamics are reflected in cyber security considerations. This can be exemplified with reference to the GGE, which Fliegauf interestingly highlighted as a prime example of good American leadership in cyber governance. The GGE was a group of governmental experts set up by the UN Secretary-General to study security and cyber technology (Henriksen 2018, 2). Determining the application of international law to cybersecurity sets out the legitimate scope of state activity in cyberspace. These debates are therefore strategically significant. In 2017, one year after Fliegauf's article was published, negotiations broke down during the GGE's fifth session. Discussions broke down when Cuban, Russian, and Chinese representatives objected to the application of international humanitarian law to cybersecurity due to fundamental differences in ideology and political interests (ibid. 3). For China in particular, the term "cyber sovereignty" is key and is often used in contrast to the western focus on a free and open internet (Cuihong 2018, 65). The key Chinese concern was centred around the potential for national cyber sovereignty to be compromised on order to protect the integrity of international humanitarian law in cyberspace. Grigsby contextualises this discussion by pointing out that Russia and China on the one hand and the US on the other have fundamentally different understandings of cyber conflict. While the US understands cybersecurity as "the protection of bits," meaning software and hardware, from unauthorised access, China and Russia focus on information security, with emphasis on state control and sovereignty (Grigsby 2017, 114). The fragmentation of cybersecurity governance relies on differences in deeply held political beliefs and practices. Therefore, the hypothetical success of a values-based approach to global cyber governance would necessarily rely on fundamental ideological shifts in international politics overall. This is unlikely to happen in the foreseeable future.

It is not realistic to expect that a values-based approach will successfully remedy the fragmentation in global cybersecurity governance as it fails to appreciate the role of broader power dynamics in cyber security considerations. As was discussed with Hurd, however, global governance should not necessarily be understood as synonymous with global unity. In other words, fragmentation does not necessarily mean that any attempt at global cybersecurity governance will be dead on arrival. Brechbühl et al. (2010) insist that productive cybersecurity depends on a network of cooperation. Therefore, local or regional policy development does not exclude international efforts to develop cybersecurity policy. The authors find that a robust global cybersecurity approach will depend on a network of shared responsibility between and among all relevant stakeholders. It is challenging to assign responsibilities and rights within a diverse and evolving group of stakeholders, which again complicates the creation of public policies on the matter (ibid. 84). To counteract this, the authors suggest that stakeholders must communicate with each other regarding shared responsibilities and interests, thus forming networks of ties from which a structure of governance can emerge (ibid. 85). Cybersecurity is not an individual endeavour but relies on a sense of collective responsibility (ibid. 87). In this sense, seemingly fragmented approaches to organise cyberspace can indeed contribute to a network of global governance.

Moving away from value-based aspirations of unity in cybersecurity governance, then, it is helpful to look briefly to alternative, low threshold strategies which encourage cooperation among relevant actors. Raymond acknowledges that "Even the most optimistic projection for the nascent cyber-regime complex must acknowledge that, for the foreseeable future, most governance will remain decentralized" (Raymond 2016, 124). Raymond actually echoes Mihr and Fliegauf in identifying that the main obstacle to united cyber policy is the difference in values and interests. Crucially however, he turns to pragmatics to remedy this challenge, with the Responsibility to Troubleshoot (R2T) as an alternative or supplement to more substantial international legal norms on cybersecurity. Raymond points out that the negative consequences of cyber activity are rarely intentional and determining intention can often be tricky. Furthermore, the diversity of actors in cyberspace further complicates the security landscape (ibid. 134). With this in mind the R2T, inspired by the Responsibility to Protect (R2P), would be a responsibility for relevant actors to troubleshoot when something does go wrong in an effort to mitigate undesirable disruptions in cyberspace. This, Raymond reasons, is more likely to gather broad support than more substantive laws or norms. Likewise, Grigsby (2017) also encourages his readers to move away from expectations of unifying cybersecurity governance. In lieu of international norms, Grigsby turns to confidence-building measures (CBMs). Though he does not completely rule out the establishment of broader norms, he sees CBMs as a feasible temporary fix which could help to establish a certain level of trust between actors in cyberspace. A more thorough evaluation of Raymond and Grigsby's approaches, or indeed an exploration of alternative suggestions more broadly, goes beyond the scope of this essay. However, they helpfully illustrate that thinking differently about what can feasibly be expected by global cybersecurity governance reveals potential for more accessible, low threshold collaborative efforts. Rather than seeing fragmentation as an indication that efforts towards global cybersecurity governance is futile, alternative approaches can focus on ensuring greater stability in cyberspace.

In this essay I argued that fragmentation in global governance in general, and cybersecurity in particular is normal, and indeed inevitable. Rather than aspiring for unified global cybersecurity governance, the focus should shift to finding means of increasing and ensuring stability in cyberspace. Supporting this argument, I began by exploring traditional conceptions of global governance before exploring the scope of cyber governance. I then moved to discuss current trends in global cybersecurity governance, finding that there is indeed evidence of fragmentation along traditional strategic lines. Moving on, I briefly considered values-based approaches to remedying the aforementioned fragmentation, focusing on contributions from Mihr and Fliegauf. I found that these approaches fail to fully appreciate how cybersecurity interests fit into broader political and strategic interests. Leaving the values-based approaches behind, I argued that global cyber governance should not be expected to manifest in a united, coherent approach. Indeed, abandoning this expectation allows for useful low-threshold pragmatic approaches which can helpfully contribute to a more stable cybersecurity landscape overall. Fragmentation is to be expected in global governance in general, and in global cybersecurity governance in particular. Scholars, policy makers and lawyers alike should therefore 'get over it,' and then 'get on with it.'

References

Brechbühl, H., Bruce, R., Dynes, S., Johnson, M. (2010) “Protecting Critical Information Infrastructure: Developing Cybersecurity Policy,” in *Information technology for development*, Vol.16(1), pp.83-91.

Carr, M. (2015) “Power Plays in Global Internet Governance,” in *Millennium Journal of International Studies*, Vol. 43(2), 640-659.

Cattaruzza, A., Danet, D., Taillat, S., Laudrain, A., (2016) “Sovereignty in Cyberspace: Balkanization or Democratization,” in *International Conference on Cyber Conflict (CyCon U.S.)*, pp.1-9.

Cuihong, C. (2018) “Global Cyber Governance: China’s Contribution and Approach,” in *China Quarterly of International Strategic Studies*, Vol. 4(1), 55-76.

DeNardis, L. (2014) *The Global War for Internet Governance*. Connecticut: Yale university press.

Dodds, K. (2016) “Global governance,” in *Teaching Geography*, Vol. 41(3), 98-102.

European Union Agency for Cyber Security (ENISA) (2020), *National Cybersecurity Strategies,* available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies (Accessed 15.12.2020).

Fliegauf, M., (2016) “In Cyber (Governance) We Trust,” in *Global Policy,* Vol 7(1), pp 78-81.

Greiman, V. (2018) “Reflecting on Cyber Governance for a new World Order: An Ontological Approach,” in *Academic Conferences International Limited European Conference on Research Methodology for Business and Management Studies*, pp.148-155.

Grigsby, A., (2017), “The End of Cyber Norms,” in *Survival (London)*, Vol.59(6), pp.109-122.

Guterres Antonio (@antonioguterres) (2019), “Access to a free and open Internet is at risk. We aren’t working together across siloed social, economic and political divides. But that can change. #IGF2019 shows how we can share a digital future that works better for and protects all of us.” 26 Nov. 2019, 2.38 PM. Tweet.

Henriksen, A. (2018), “The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace,” in *Journal of Cybersecurity,* pp. 1-9.

Hurd, I. (2017), *How to do Things with International Law,* New Jersey: Princeton University Press.

Laybats C, Davies J. (2018) “GDPR: Implementing the regulations,” in *Business Information Review*, vol. 35(2), pp. 81-83.

Mihr, A. (2014) “Good Cyber Governance: The Human Rights and Multi-Stakeholder Approach,” in*Georgetown Journal of International Affairs International Engagement on Cyber IV*, pp. 24-34.

Orji, U (2015) “Multilateral legal responses to cyber security in Africa: Any hope for effective international cooperation?” in *7th International Conference on Cyber Conflict: Architectures in Cyberspace (CyCon)*, pp 105-118.

Raymond, M. (2016) “Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot,” in*Strategic Studies Quarterly,* Vol. 10(4), pp. 123-149.

Sabillon, R., Cavaller, V., Cano, J., (2016) “National Cyber Security Strategies: Global Trends in Cyberspace,” in *International Journal of Computer Science and Software Engineering*, Vol. 5(5), pp. 67-81.

White House (2018), *National Cyber Strategy of the United States of America, September 2018,* pp. 1-40. Available

at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (accessed 10.12.2020).
Working Group on Internet Governance (WGIG) (2005) *Report of the Working Group on Internet Governance, Château de Bossey*, available at: http://www.wgig.org/docs/WGIGREPORT.pdf (accessed 15.12.20).

Written at: King's College London
Written for: War Studies Department
Date written: December 2020