Norms, Epistemic Communities and the Global Cyber Security Assemblage

https://www.e-ir.info/2012/03/27/norms-epistemic-communities-and-the-global-cyber-security-assemblage/

TIM STEVENS, MAR 27 2012

Even as norms begin to pervade national and international discourse on cybersecurity, they remain poorly understood. States and multilateral institutions are seeking to mitigate the problems deriving from the use of information communication technologies for a wide range of purposes, many of which are antithetical to their own ends. As they do so, they are looking to develop normative regimes that promote their own strategic ends and those of transnational political communities. Given the relative novelty of cybersecurity as an identifiable form of security governance, it is evident that although norms most certainly exist within this field, their formalisation and contingent analysis are at a very early stage.

Norms are the expectations held in common by a community of actors, which serve to direct social behaviours within acceptable bounds.[1] Constitutive norms help to create and maintain the identity and interests of a given actor or group of actors.[2] Regulative norms serve as 'rules of the road', which order and constrain the actions of individuals or groups.[3] Norms, therefore, shape the means of social actions and the ends to which those actions are aligned. In the policy discourse on cybersecurity, little distinction is made between constitutive or regulative norms. Nonetheless, we can begin to trace, tentatively at least, the relationships and mutual contingency of these two forms.

Since at least 2008, for example, the U.S. government has held the development of norms as integral to its policy for international cybersecurity engagement. In its latest iteration, this finds expression principally in the understanding of norms as 'the broad expectations of peaceful and just interstate conduct' in cyberspace, in order to create 'stability' as exists in 'other spheres of international relations'.[4] In this context, norms are regulative norms that constrain actors in order to avoid interstate conflict, whilst also preserving states' right to self-defence consistent with the UN Charter. On numerous occasions, this process has been described as establishing 'rules of the road' for interstate behaviour in global cyberspace.

If we characterise regulative norms crudely as a 'top-down' approach to effecting amenable behavioural change, it is evident that the US and its allies will not achieve this overnight, nor would they suggest otherwise. There is a long process of consultation and diplomatic negotiation ahead, which may yet founder on the inability to persuade non-'like-minded' nations that the U.S.-led vision of global cybersecurity is more attractive than the alternatives.[5] There is also an equally important process occurring in which the constitutive norms of cybersecurity are being developed, at the level of individual actors networked in communities of practice.

Frank Webster has observed that analyses of the 'information society' tend to either assert its continuity with the past or stress its novelty.[6] As ever, the sensible analytical course lies somewhere between the two, and the same can be said of our interrogations of 'cybersecurity'. We can, indeed, trace its origins in disparate strands of process and practice back to the pre-WWII era. On the other hand, it is only in the last ten years that even computer science professionals have self-identified as cybersecurity experts.[7] Over that period what we might describe as an epistemic community has emerged, in which individuals are enlisted in networks on the basis of their expertise in cybersecurity, and who may reproduce policy-relevant knowledge from within that field.[8]

Cybersecurity is a heterogeneous process, encompassing aspects of critical infrastructure protection, policing,

intelligence, information security, counterterrorism and military operations, to name but a few, and governments are fully aware that cybersecurity expertise is not located in any single organisation, sector or discipline. Most of the current proliferation of cybersecurity conferences, workshops, summits and symposia pride themselves on the diversity of backgrounds from which their delegates hail. What professionals in these various fields do share, however, is a set of structuring beliefs and assumptions regarding the necessity to pursue cybersecurity as a matter of national and economic concern.

Although the details of how to achieve positive cybersecurity outcomes are often hotly disputed, the aims in themselves are not. Most professionals, for example, will agree on the need to tackle 'cyber-crime' and 'cyber-espionage', to prevent acts of 'cyber-terrorism', and to develop means to counter the threat of 'cyber-war', or the importance of being able to effectively prosecute all of these, if necessary. On the basis of their professional expertise, and shared sets of values and goals, the growing cybersecurity epistemic community is in a strong position to influence national and international cybersecurity agendas and subsequent policy formulation. Indeed, governments and supranational bodies directly appeal to this community for assistance in information gathering, and the development of policy and legislation. In this way, the constitutive norms of practice communities interact with the regulative norms of policy communities in an iterative and often mutually reinforcing dynamic.

Of course, this is oversimplifying a highly complex set of processes, the analysis of which is currently underdeveloped. Closer examination of this nascent cybersecurity epistemic community would reveal tensions between the normative commitments of, for example, privacy advocates on the one hand, and the police and intelligence communities on the other. Conversely, it would also reveal normative affinities between militaries and industry in what has been dubbed a 'cyber military-industrial complex'.[9] Similarly, policy communities are not reducible to sets of regulative norms alone, and they themselves demonstrate complex webs of institutional dynamics in which constitutive norms are crucial to their identities and actions.

The elaboration of how the local and global interact in cybersecurity remains a research project of substantial scale and difficulty. We can begin to describe the contours and outlines of cybersecurity as a 'global security assemblage', in which traditional boundaries between the public and private and global and local are increasingly diffuse and dynamic within the field of transnational and globalised cybersecurity.[10] Norms and actors within a global security assemblage 'interact, cooperate and compete' to produce new agents, practices and forms of security governance.[11] As all parties to the development of global cyber security governance recognise, this process is at an early and—somewhat paradoxically—highly visible, stage.

We can, however, suggest that norms will play a highly important role in determining how cybersecurity governance is both implemented and received, as they do in all security regimes. Although the picture presented here relies almost solely on cybersecurity as viewed by Western governments and industry, we might also stop to consider how their norms differ from those of the many other communities vying for influence and control in cyberspace, not least of which are networked cultures like Anonymous whose stated objectives are entirely antithetical to most forms of governance and government. How these power struggles play out will also be immensely important for the future of global cyberspace.

—

Tim Stevens *is a PhD candidate in the Department of War Studies, King's College London, and an Associate of the Centre for Science & Security Studies. He is the co-author (with David J. Betz) of* Cyberspace and the State *(London: Routledge, 2011). You can follow him on Twitter @Cyberassemblage.*

[1] Finnemore M (1996) *National Interests in International Society.*Ithaca, NY: Cornell University Press, 22.

[2] Wendt A (1999) *Social Theory of International Politics.*Cambridge: Cambridge University Press, 92-138.

[3] Raymond GA (1997) Problems and prospects in the study of international norms.*Mershon International Studies Review* 41(2): 205-245.

[4] *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*.Washington,DC: White House, 2011, 9.

[5] Stevens T (2012) A cyberwar of ideas? Deterrence and norms in cyberspace. *Contemporary Security Policy* 33(1): 148-170.

[6] Webster F (1995) *Theories of the Information Society*.London: Routledge.

[7] Denning PJ & Frailey DJ (2011) Who are we—now? *Communications of the ACM* 54(6): 25-27.

[8] Haas PM (1992) Introduction: Epistemic communities and international policy coordination. *International Organization* 46(1): 1-35.

[9] Interview: Ronald Deibert: Tracking the Emerging Arms Race in Cyberspace. *Bulletin of the Atomic Scientists* 67(1): 1-8.

[10] Abrahamsen R & Williams MC (2011) *Security Beyond the State: Private Security in International Politics*.Cambridge: Cambridge University Press.

[11] *Ibid.*, 90.

About the author:

Tim Stevens is a Teaching Fellow in the Department of Politics and International Relations, Royal Holloway, University of London. His newest book is *Cyber Security and the Politics of Time* (Cambridge University Press, 2016). He has published articles on the politics of security in*Security Dialogue*, *International Political Sociology* and *Contemporary Security Issues*.