Purpose, Power, and Problems: The Pursuit of Norms for Cybersecurity

https://www.e-ir.info/2016/01/17/purpose-power-and-problems-the-pursuit-of-norms-for-cybersecurity/

NAM KHOA NGUYEN, JAN 17 2016

To find out more about E-IR essay awards, click here.

—

Since the Stuxnet worm attacked Iranian centrifuges in 2010, the possibilities of cyber war – or at least the spectrum to which cyber space can be used for malicious purposes – have captured the imagination of policy-makers, practitioners and academics. Regulating new technologies is always difficult to achieve and often lags behind common practice in both legal and policy areas. Cyberspace, and its uses in conflict, is no exception to this. Some academics and policy makers argue that norms are the best methods of developing some consensus within cyberspace at this point in time but, like other areas of significant debate within the international system, a way forward may not be as easy as it would appear.

This paper will explore the norm development process and how it applies to cyberspace within the context of an armed conflict. It contends that norms are just the first steps to regulating cyberspace and provides utility for understanding future uses of cyber in armed conflict scenarios. First, it is important to understand how norms can

influence events on the global stage. Secondly, careful consideration must be given as to how cyberspace is a different domain to other domains or areas of political debates and why norm development is facing its challenges within the context of cyberspace. Finally, a way ahead is presented for consideration within the debate of cyberspace regulation beyond existing themes by addressing issues. Whilst this paper explores norm development within cyberspace, the focus of the issues being presented are more concerned with how cyberspace is used as a tool of government within armed conflicts.

Norm Development in Cyberspace

Norms within international relations are an ongoing process that occurs through direct involvement by states. Norms can also sometimes evolve around states even if the states involved did not intend for such norms to develop in the way that they had. Unlike a social setting, however, norms within international relations can have a further moral dimension that seeks to govern behaviour for the 'group'. Toni Erskine, an ethics professor at the University of New South Wales, states that 'established norms are involved to variously condemn or condone behaviour in world politics, and even to support proposals for sanctions when they have been violated.'[1] On this point, March and Olsen expand further:

'Human actors are imagined to follow rules that associate particular identities to particular situations, approaching individual opportunities for action by assessing similarities between current identities and choice dilemmas and more general concepts of self and situation. Action involves evoking an identity or role and matching the obligations of that identity or role to a specific situation.'[2]

So why would states pursue norm development as a means of regulating behaviour? As War studies professor Mervyn Frost suggests, the pursuit of 'settled norms' means that there is a general consensus to maintain adherence to them, or at least keep any infringement of these norms as a clandestine event.[3] Norms provide consistency, predictability and a means of infringing those who transgress them. Within international relations it is important, therefore, to understand which norms will become law, both hard and soft law, and how exactly compliance with these laws will come about. This is essential as a topic of inquiry as laws developed as a result of norms will be used to determine political actors' behaviour.

Within the cyberspace debate, norm development is particularly important to consider given that the majority of states within the international system are not middle powers, let alone 'great' powers. For 'smaller' states there is a great deal of interest in trying to achieve norm regulation within the international political domain. In terms of the ability to influence smaller states do not necessarily have the physical capacity to enforce norms without the assistance of other states to achieve the intended outcome. In this case there is some merit in trying to pursue norm development as a policy tool on the international sphere. But the emphasis remains, however, that it is norm development and requires critical mass in order to reach a level of codification of accepted norms.

Why Cyberspace is Different

How the norm development process translates into cyberspace is less simple. Information communication technologies, enabled by cyberspace, have progressed beyond the exclusivity of the engineer or programmer; soldiers, diplomats, politicians and everyday users now must have a higher awareness of cyberspace and the security impact.[4] Even though norms can have a positive effect by creating expectations and understanding, cybersecurity presents new challenges unlike other domains as it binds states more closely together.

By virtue of the 'connectivity' it provides, the perceptions of 'transnational risk' increases.[5] Tim Maurer, an analyst on strategic technologies, explains that there are three points that states will need to contend with in order to understand the changing norms concerning cyber security. Firstly, the threat of cyber warfare is no longer science fiction. This includes cyber actions in isolation, as demonstrated by Stuxnet, and cyber capabilities in support of conventional action, such as the Russian cyber attacks observed during the Russian-Georgian conflict in 2008. Secondly, the debate regarding current and future norms is already in full swing so there needs to be shaping in both desired outcomes and an understanding that today's actions will have an impact on what norms will persist. The third

and final consideration is that perceptions of what constitutes national interests will be informed by the discussions on how to use new technologies for warfare.[6]

In terms of warfare the entire cyber domain makes traditional fighting 'difficult'. Traditionally, strategists consider how best to attack an adversary, and normally it is at the weakest point. In cyberspace, however, the foundation of hardware is common across many states and users. Thus the vulnerabilities one would find in an adversary can also be found in one's own networks and systems. A more realistic assessment of how cyber attack capabilities can be classified is provided by James Lewis:

'We can regard cyber attack capabilities as just another mode attack, which like a missile or an aircraft can strike the enemy from a great distance. And like aircraft or long-range missiles, cyber attack can serve both tactical and strategic purposes. Cyber attack will not be decisive; cyber attack by itself will not win a conflict, particularly against a large and powerful opponent. But it does provide military advantage and therefore will be used.'[7]

Furthermore, because of its many uses across many countries and organisations, a policy solution is difficult to define because the same dilemmas exist in seemingly benign uses of cyberspace.

Perhaps some of the difficulties in the early stages of norm development that is being observed in the cyber security debate is that there remain divergent views on how to best address these problems. The East West Institute, an American think tank neatly summarises this clash:

'…the United States focuses on a law enforcement approach at the domestic level with voluntary international collaboration, while Russia focuses on developing binding international regimes. There are also quite different philosophies at work: Russia favors [sic] social control of the Internet as a medium, while the United States, for the most part, does not.'[8]

The report, however, does continue to explain that there are significant efforts being made by both states to strengthen internet security and limiting the use of cyberspace for military purposes. Whilst this example focuses heavily on the US view on cyber security, it is useful in demonstrating that there is in fact very little consensus on the way ahead.

Some Areas of Consensus

Even if an agreement is reached, ultimately leading to a codified norm or international law, there remains the question of how to enforce the codified manifestations of accepted norms. As Stevens suggests:

'It may be that states can be persuaded to comply with international normative frameworks through a mix of inducement, coercion and moral pressure. So too might industry and civil society be persuaded to do their part through a gradual process of cultural learning, and all parties work together to achieve the "global culture of cyber security" …'[9]

How this is achieved is an entire area of inquiry in its own right but it is an important element to consider when moving forward in the norms debate.

Perhaps what is required is to compare cyberspace, and associated security and deterrence issues, to other forms of governance debates. Roger Hurwitz posits that cyberspace, and thus the way to regulate it, is 'more like a social system based on a commons that can be sustained but also depleted' – in essence it would be more useful to characterise cyberspace as a common pool resource.[10] Therefore governing cyberspace and associated security and warfare concerns becomes a collective action problem particularly as the cyber commons is comparable to the high seas or international airspace where the primary concern is the right of innocent passage.[11]Even these areas had significant lead times in developing international law and in the immediate future, broad-sweeping agreements or codes of conduct might be difficult to achieve because of the reasons outlined earlier in this paper.

Comparatively 'smaller' issues may be more effective in establishing norms or incite confidence-building between states. Cooperation between Japan, China and South Korea on the Conficker worm, for example, demonstrates a shared commitment between experts from each country to address an emerging problem. Such actions serve to create professional commitment and experience with those from another state/organisation. This style of global governance is what international relations scholar Joseph Nye refers to as 'regimes'. Regimes, as subset of norms, may provide a way ahead in governing cyberspace.

Strictly speaking, regimes are essentially shared expectations about appropriate behaviour.[12] According to Nye it is more useful to compare cyber issues in terms of four dimensions: depth, breadth, fabric and compliance. Depth refers to the hierarchical coherence of a set of rules or norms. Breadth refers to the scope of the numbers of state and non-state actors that accepted a set of norms. "Fabric" refers to the mix of state and non-state actors in an issue area. A fourth dimension for comparison is compliance: how widespread is the behavioural adherence to a set of norms?[13]

The problem of coordination, and thus compliance, in cyberspace is likely to remain for some time. On initial inspection it can be inferred that the cyber war component of norm development is comparable to those issues seen in climate change debates. As Keohane and Victor argue it is

'…actually many different cooperation problems, implying different tasks and structures. Three forces – the distribution of interest, the gains from linkages, and the management of uncertainty – help to account for the variation in the institutional outcomes, from integration to fragmentation.'[14]

The Way Ahead

Before making any critical arguments against certain expert's views on cyber security governance it is important to remember how new cyberspace actually is. From a modest US Defense Department-sponsored

'…connection of a few computers called ARPANET in 1969… it has only been in the last decade and a half that the number of websites burgeoned, and business begin to use this new technology to shift production and procurement in complex global supply chains.'[15]

It is clear from the views presented by many scholars and practitioners that a single overarching scheme may not be achievable, at least in the near future. Different sub-issues may develop at different rates due to the level of common interest between states at varying points. Issues such as cybercrime, for example, may have more success than debates concerning intellectual property or offensive cyber operations due to divergent views on how to use the domain. Rather than reaching for global agreements, perhaps confidence-building measures and 'rules of the road' between like-minded states will be the first, and most successful, steps to avoid destabilising behaviour that can lead to more formal agreements in future.

It is important to consider the threshold in which cyber attacks or weapons can actually change the strategic balance. Many scholars have submitted that the problem regarding cyber war debate is that the technology is still new and the full extent of its military application is highly classified. As such the prospects for a 'cyber Pearl Harbour' or 'cyber 9-11' are being postulated as possibilities if not properly regulated. Even then, however, it should be noted that neither of these two historical events resulted in national meltdown that some of the 'doomsday' analysts are suggesting.[16]

Conclusion

Whilst the military application of cyber may not be the most pressing problem for the international community, after all the chance of a major armed conflict as a result of cyberspace is still yet to be seen, it does offer an 'easy' approach to agreement due to the application of precedents developed through consensus to other aspects of international security.[17] The many problems in trying to achieve an overarching, single document on cyberspace include managing treaty compliance, an inability to define 'information weapons' – let alone 'cyber weapons' – and the

overwhelming consensus that the majority of cyberspace is used for commercial purposes.[18]

A norms-based approach to achieving cyber security has its merits but there are significant hurdles to overcome to make developing norms lasting. This is further complicated by a wide disparity of views on how to address problems of cyber security. Furthermore, the debate between purposes and technologies that make a cyber attack achievable is still yet to provide adequate boundaries for international agreements. After all, is it the technology or the intents and actions of a cyber attack that should be regulated in conflict? In any case the near future will continue to see more case studies as states continue to explore ways to use cyber in support of security goals and whether the international can come together to regulate future actions will determine to what extent precedents and norms develop.

Bibliography

Arquilla, J., *Worst Enemy: The Reluctant Transformation of the American Military,* Ivan R. Dee, Chicago, 2008.

Betz, D., 'The More You Know, The Less You Understand: The Problem with Information Warfare,' *Journal of Strategic Studies,* Vol. 29, No. 3, 2006, pp. 505-533.

Denmark, A. and Mulvenon, J.(eds.), *Contested Commons: The Future of American Power in a Multipolar World,* Center for a New American Security, Washington DC, 2010.

Erskine, Toni, 'Interpreting norms and assigning responsibilities in cyberspace,' Summary circulated to delegates in advance of presentation at workshop on "Cyber Norms & International Relations", sponsored by the NATO Cooperative Cyber Defence Centre of Excellence, 28-29 April 2014, Stockholm at the Swedish National Defence College.

Finnemore, M., *National Interests in International Society*, Cornell University Press, New York, 1996.

Frost, M., E*thics in International Relations: A Constitutive Theory,* Cambridge, Cambridge University Press, 1996.

Gady, F.S. and Austin, G., 'Russia, the United States, and Cyber Diplomacy: Opening the Doors', New York, EastWest Institute, 2009.

Hurwitz, R., 'Depleted Trust in the Cyber Commons', *Strategic Studies Quarterly,* Vol. 6, No. 3, Fall 2012, pp. 20-45.

Jian, Shen, 'An International Code of Conduct for Information Security: China's perspective on building a peaceful, secure, open and cooperative cyberspace', paper presented at the Cyber Stability Seminar 2014: Preventing Cyber Conflict, February 10, 2014, Geneva, Switzerland.

Jiao, W. & Zhao, S., 'Nations call on UN to discuss cyber security', *China Daily*, September 9, 2011, accessed 30 September 2015, <http://www.chinadailyasia.com/news/2011-09/14/content_106967.html>

Keohane, R. &Victor, D., 'The Regime Complex for Climate Change', *Perspectives on Politics,* Vol. 9, No. 1, 2011, pp. 7-23.

Lawson, S., 'Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History', *Working Paper 11-01,* Mercatus Center, Georgia Mason University, 2011.

Lewis, J., 'Confidence-building and international agreement in cybersecurity', in Kerstin Vignard, McCrae, R. & Powers, J. (eds.), *Confronting Cyber Conflict,* UNIDIR Disarmament Forum, Geneva, 2011.

Libicki, Martin C., *Cyberdeterrence and Cyberwar,* RAND Corporation, Santa Monica, 2009.

Maurer, Tim, 'Cyber Norm Emergence at the United Nations — An Analysis of the UN's Activities Regarding Cybersecurity', Discussion Paper 2011-11, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011.

Nye, J., 'The Regime Complex for Managing Global Cyber Activities,' Global Commission on Internet Governance, Paper Series No. 1, 2014.

Stevens, T., 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace,' *Contemporary Security Policy,* Vol. 33, No. 1, 2012, pp. 148-170.

The White House, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World,* White House, Washington DC, 2011, pp. 9-12.

Endnotes

[1]Toni Erskine, Interpreting norms and assigning responsibilities in cyberspace, Summary circulated to delegates in advance of presentation at workshop on "Cyber Norms & International Relations", sponsored by the NATO Cooperative Cyber Defence Centre of Excellence, 28-29 April 2014, Stockholm at the Swedish National Defence College.

[2]James March and Johan Olsen, 'The Institutional Dynamics of International Political Orders,' *International Organization,* Vol. 54, No. 2, 1998, pp. 943-969.

[3] Mervyn Frost, *Ethics in International Relations: A Constitutive Theory,* Cambridge, Cambridge University Press, 1996, pp. 105-106.

[4]Tim Stevens, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace,' *Contemporary Security Policy,* Vol. 33, No. 1, 2012, p. 148.

[5]James Lewis, 'Confidence-building and international agreement in cybersecurity', in Kerstin Vignard, Ross McCrae & Jason Powers (eds.), *Confronting Cyber Conflict,* UNIDIR Disarmament Forum, Geneva, 2011, p. 53.

[6] Tim Maurer, 'Cyber Norm Emergence at the United Nations—An Analysis of the UN's Activities Regarding Cybersecurity', Discussion Paper 2011-11, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011, p. 3.

[7] Lewis, 'Confidence-building and international agreement in cybersecurity', pp. 51-59.

[8]Franz-Stefan Gady and Greg Austin, 'Russia, The United States, and Cyber Diplomacy: Opening the Doors', New York, EastWest Institute, 2009, p. i.

[9] Stevens, 'Deterrence and Norms in Cyberspace', p. 165.

[10] Roger Hurwitz, 'Depleted Trust in the Cyber Commons', *Strategic Studies Quarterly,* Vol. 6, No. 3, Fall 2012, pp. 21-22.

[11] Abraham Denmark & James Mulvenon, eds., *Contested Commons: The Future of American Power in a Multipolar World,* Center for a New American Security, Washington DC, 2010.

[12]Joseph Nye, 'The Regime Complex for Managing Global Cyber Activities,' Global Commission on Internet Governance, Paper Series No. 1, 2014, p. 7.

[13]*Ibid.*, p. 9.

[14] Robert Keohane & David Victor, 'The Regime Complex for Climate Change', *Perspectives on Politics,* Vol. 9, No. 1, 2011, p. 8.

[15]Nye, 'The Regime Complex,' p. 5.

[16] Sean Lawson, 'Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History', *Working Paper 11-01,* Mercatus Center, Georgia Mason University, 2011.

[17] Lewis, 'Confidence-building and international agreement', p. 52.

[18]*Ibid.*, pp. 52-53.

Written by: Nam Khoa Nguyen
Written at: University of New South Wales
Written for: Paula Keating
Date written: October 2015