Fletcher Security Review Vol.2 no.2

Roadmap for a Code of Conduct for Cyberspace

Thomas McCarthy / Alison Russell

1 September 2015

The Fletcher School of Law and Diplomacy continues to mourn the passing of William C. Martel, Associate Professor of International Security Studies, after his battle with cancer ended January 12th, 2015. Professor Martel had been repeatedly recognized by the Fletcher community for showing sincere devotion, kindness and caring towards his students. He has also been recognized for leading the charge to bring cybersecurity studies to the Fletcher School. His pioneering course on Foundations of International Cybersecurity broke the threshold on this critical subject at Fletcher, exposing many students, including myself, to it for the first time. FSR's commitment to promoting new ways of examining security challenges has led us to publish several pieces on cybersecurity, and I have been privileged to serve as editor for this most recent piece by Thomas McCarthy and Alison Russell. The authors, many in the Fletcher community, and myself are forever grateful for the impact Professor Martel had both professionally and personally on our lives, and it is with the utmost respect that we dedicate the following piece in his memory.
– Mark Duarte, Senior Policy Editor, Fletcher Security Review

1 Introduction

> Policy makers also face the truly modern challenge of cyber warfare in the hands of non-state actors. Never before have non-state actors, groups, and movements possessed an instrument capable of inflicting such immense harm. One element of American grand strategy must consider how to deal with groups that could attack the physical and economic infrastructure of American society. Policy makers worry that cyber hackers from an extremist organization might be able to cut off U.S. electric power during the winter or hack into the safety controls of a nuclear reactor. The old grand strategy of containment has become passé in the face of modern foreign and domestic challenges represented by these new and unpredictable sources of disorder.[1] - Professor William C. Martel

Professor Martel, author of *Grand Strategy in Theory and Practice: The Need for an Effective American Foreign Policy*, offers three guiding principles for U.S. grand strategy: rebuilding domestic foundations of power; exercising American leadership to restrain sources of disorder that directly threaten U.S. vital interests; and forging both alliances and partnerships to confront the most pressing threats to global stability.[2] The last of Martel's three principles foreshadows the three cyber security activities at the heart of the newly released U.S. Department of Defense Cyber Strategy.

The three activities around which the new U.S. DoD cyber strategy revolves are: information sharing and interagency coordination; building bridges to the private sector; and building alliances, coalitions, and partnerships abroad.[3] These three coordinating and collaborating activities are the key to building relationships between actors influencing the development of the cyber domain, and are necessary to identify and counter threats. To advance global cyber security, the Cyber Strategy suggests the U.S. must "build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability."[4] As part of this effort, the United States seeks to build security relationships to respond to shifts in the international environment, including sources of disorder. These relationships are built upon trust and cooperation of many actors with varied interests and objectives in cyberspace. Given the wide variety of actors and interests within the cyber domain, establishing relationships of trust based on a shared understanding of acceptable conduct, expected behavior, and governing principles represents a daunting challenge.

2 Cooperation in Cyberspace

Cooperation is a necessary component of growth for any regime. Key aspects of cooperation include trust in the system and the predictability of action among participants. Through consistent and transparent actions, participants in a cooperative environment create a predictable pattern of behavior. This predictable pattern of behavior helps participants learn what to expect from each other and establishes a baseline for future transactions involving greater risk and reward.

The challenge for all actors in cyberspace is to create relationships of trust in the absence of

[1] William C. Martel, *Grand Strategy in Theory and Practice : The Need for an Effective American Foreign Policy* (New York, NY: Cambridge University Press, 2015), 350.
[2] Ibid.
[3] "U.S. Department of Defense Cyber Strategy," (U.S, Department of Defense April 2015), 3-4.
[4] Ibid.

a global authority to impose order on states and institutions. Within cyberspace, as with the development of predictable interactions in other fields of human interaction, codes of conduct can serve to provide a framework from which regime participants will continue to build trust in a systematic way. Codes of conduct, both formal and informal, are developed through repeated transparent interactions. They effectively set expectations of behavior that form a baseline of assessment regarding another participant's consistency and transparency. The goal of formal and informal codes of conduct is to develop a system where actors work with common purpose towards the benefit of all.

3 Why is a Code of Conduct Important?

A code of conduct is defined as the "principles, values, standards, or rules of behavior that guide the decisions, procedures and systems of an organization in a way that (a) contributes to the welfare of its key stakeholders, and (b) respects the rights of all constituents affected by its operations."[5]

These principles and expectations, if widely shared, can transcend geographic, economic, and cultural boundaries and blossom into behavioral norms within the group. While norms themselves are not binding, they are supported and reinforced through socialization and the fear of reputational-loss for transgressions against others. In an environment characterized by repeated interactions, a code of conduct provides the framework for assessing actions, establishing reputations, and demonstrating consistency in behavior.

Although not specifically covered in formalized law or treaty, codes of conduct serve as a universal frame of reference for the promotion of common understanding and the employment of "good judgment" as defined by participants. Standards of behavior spread, and come to functionally define ethical behavior across communities of interest and are even formalized by treaty, widely recognized, and internationally enforced (i.e. the Law of Armed Conflict or the Law of the Sea). Codes of conduct thus serve to regulate and place limits on our actions in the absence of formal enforcement mechanisms and serve as a frame of reference for evaluating the actions of other.

Eventually, well-established codes of conduct lead to self-regulation among the participants and communities of interest, building trust and encouraging frequent interaction. Within the cyber domain, codes of conduct serve to define relationships via the sharing of information, freedom of movement of information along global lines of communication, cooperative enforcement of mutual standards of international law and behavior, and improved communications based on standardized expectations.

4 How Does a Code of Conduct Apply to cyberspace?

Much like cooperation in other domains of human competition and conflict, a cyberspace code of conduct will develop based on informal interaction by parties seeking mutual benefit through repeated interactions. Cyberspace catalyzes cooperation when strategically and creatively applied in the dynamic arena of our increasingly connected world. Success will breed success by establishing norms and rewarding conforming partners. Over time, those seeking to maximize individual benefits will become less desirable partners for interaction, gradually

[5]International Federation of Accountants, "Defining and Developing an Effective Code of Conduct for Organizations," in *International Good Practice Guidance* (2007), 5-6.

forcing them to adapt group norms or endure increased transactional costs. Consistency over time is the key component for development of a code of conduct for cyberspace.

Unfortunately, the pace of innovation, the technological development within cyberspace, and the relative anonymity of actors are likely to hamper development of widely accepted and enduring codes. While there are repeated interactions, it is often difficult to verify the identity of other actors and constant improvements in technology result in an ever-changing variety of interactions requiring thoughtful, and sometimes creative, responses. Thus, unlike other codes of conduct, a code of conduct for cyberspace would demand continual attention, evolution, awareness, and both an ability and a willingness to adapt to new norms of behavior among a wide variety of actors.

Ideally, as a code of conduct becomes widely accepted by leading actors and powerbrokers within the international community, it is formalized and serves as the basis for legal restrictions to behavior. Unfortunately, competing governmental, legal, and cultural norms among cyber actors have thus far prevented and slowed the establishment of common understandings, not to mention formalized agreements. The process of overcoming differences in international norms is underway however; we have already seen the first steps of this process in cyberspace. Legal frameworks such as the European Union's Convention on Cyber Crime have helped establish standards of behavior for its signatories since 2001. Unfortunately, no country in Asia, Africa, or South America has signed it, so its global application is limited. More recently, the Tallinn Manual on International Law Applicable to Cyber Warfare began to extend legal frameworks into cyberspace regarding rules of conduct in cyber conflicts, but there are neither formal international cyber laws nor international agents to enforce compliance.

5 Process of Development

A code of conduct provides a foundation for future cooperation and, because it would be voluntary, it may be able to attract participants that would not be willing or able to commit to a legal agreement. There are a variety of different actors operating in cyberspace with different legal standings and authorities, whether they are individuals, non-state actors, state-sponsored groups, states, or intergovernmental organizations. A code of conduct could provide the framework for defining and measuring behavior of all actors, not just states, and thus be more inclusive and comprehensive even if enforcement is difficult against some groups such as non-state actors. In cyberspace, actors are not assessed by their size, wealth, or capabilities but by their actions. Creating a framework to assess their actions allows for a common understanding of cooperative and professional behavior across actors in cyberspace.

The United States and other countries have engaged in a process of developing a framework for cooperation — or, at least, conflict avoidance — in cyberspace for years. For example, in 2013, the U.S. and Russia signed a pact to create a communications link on cyberspace issues, so that the activities of one state may not be misinterpreted as hostilities against the other.[6] In April 2015, the U.S. and Japan drafted an agreement on bilateral defense rules that will bolster their efforts to defend cyberspace, particularly with regard to information sharing and critical infrastructure protection.[7] South Korea and the United States have also recently vowed to work more closely together on cyber security, especially with regard to

[6]Ellen Nakashima, "U.S. And Russia Sign Pact to Create Communication Link on Cyber Security," *The Washington Post*, June 17, 2013.

[7]Cory Bennett, "U.S., Japan near Cyber Defense Agreement," *The Hill*, April 8, 2015; Franz-Stefan Gady, "Japan and the United States to Deepen Cybersecurity Cooperation " *The Diplomat*, June 2, 2015.

cyber attacks emanating from North Korea.[8] Other types of bilateral cooperative efforts can also take place within the broader landscape of NATO and EU cooperative agreements on cyberspace. The U.S. appears to be building norms in cyberspace through a combined effort of bilateral and multilateral agreements that allow for flexibility in order to make the most progress on a variety of issues with a wide range of partners.

In this context, it is important to note that the private sector is also involved in developing standards of behavior. Microsoft has recently proposed six international cybersecurity norms aimed at limiting conflict in cyberspace through a multi-stakeholder approach. Many of the proposed norms focus on supporting the integrity of private sector information and communications technology companies while protecting civil society from cyber conflict.[9]

From the pure Hobbesian perspective, cooperation among actors seeking to gain advantages over one another will not develop without a central authority to enforce rules of behavior. However, we see cooperation among international actors everywhere. Realists, liberals, and constructivists argue about why cooperation occurs, but all acknowledge it occurs and has an effect on the relationships between actors, even if only because each seeks reciprocity to pursue an individual advantage.

According to R.M. Axelrod, reciprocity is, effectively, cooperation.[10] Within systems of constant and ongoing interaction, it is the expectation of future interaction that overshadows actions in the present, creating a desire to act in accordance with norms, or in some cases codes of conduct. Within the cyber environment, the almost certainty of future interaction can act as a motivating force and is arguably a critical factor in, and incentive for, cooperative behavior. It is in the interest of most, if not all cyber actors to be easily distinguished as non-adversarial by acting in compliance with established norms of behavior, and to develop a reputation for adherence to expectations.

The most important benefits of cooperation and codes of conduct in cyberspace are that they can lead to an advancement of interests and reduce the overall risk of conflict as a result of miscalculation or misunderstanding. The single biggest challenge to cooperation is establishing codes of conduct that provide benefits of compliance to the actor, and are thus mutually beneficial for the parties involved. Over time, increased trust can lead to more permanent and formal cooperation in the cyber domain.

Despite the benefits of cooperation and collective action to regulate or govern cyberspace, not all states and actors are in favor of it. Many states say that they want a regime such as a treaty or a less formal code of conduct for cyberspace, yet differ drastically in what they want and why. Individual states have very different priorities in cyberspace. As such, they have different levels of concerns on a variety of issues making it difficult to reach consensus. Among major cyber powers, including the United States, there are concerns that treaties might reduce flexibility to pursue national interests, while simultaneously enabling other countries to build disruptive cyber capabilities or, worse, gain competitive advantage by ignoring the rules all together. In addition, the cost of organizing a collective effort increases with the size of the group. In large groups, it is difficult to establish and enforce selective incentives to shape interactions. In smaller groups, societal pressure and intense focus helps to provide the incentive for compliance.

Within any large system, it is impossible to have first-hand knowledge of all potential partners; therefore, reputation becomes the key to initial and future interactions with new ac-

[8] Cory Bennett, "U.S. Vows Tighter Cyber Cooperation with South Korea," *The Hill*, May 18, 2015.
[9] Angela MacKay et al., *International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World* (Microsoft, 2014).
[10] R.M. Axelrod, *The Evolution of Cooperation* (Basic Books, 2006).

quaintances. Reputation affects how actors view and react to each other. Successful interactions increase positive reputational aspects and provide mutual benefit, increasing the return for both participants and strengthening them within the operational system. Witnessed by others, success is emulated.

Reciprocity operates both as a reward and a penalty. If a state abides by the rules, then it can reasonably expect others to do that same. In the construct of greater responsibility, states will help each other to insure good treatment for their own interests. However, if a state defects or fails to abide by the norms, then other actors no longer owe them reciprocity in future events. To make sure other nations are forewarned of defectors actions, recently, there has been a greater willingness on the part of some countries, like the United States, to engage in public "naming and shaming" of norm-breakers, such as Chinese hackers or North Korea.

Establishing reputations and transparency of action within the cyber domain is a difficult challenge. The potential for anonymity during interactions leads to risky behavior where actors are not held accountable for failure to comply with norms of behavior. This lack of transparency and accountability among the larger community of actors means that codes of conduct must begin among trusted actors, actors likely to have long standing and trusted relationships based in other domains of diplomacy and commerce. Likewise, willingness to engage in reciprocity when wronged also helps establish a reputation for action and enforces norms.

Attribution is one of the thorniest issues in cyberspace. Because the network was designed to operate with trust and minimal security checks, individuals, non-state actors, and states can mask or fake their identities. Programs, such as The Onion Router (Tor), exist to make cyber attacks or other illicit behavior extremely difficult to trace back to their origins. Even when the physical origin of a cyber attack is known (i.e., the IP address has been successfully traced), the next challenge is to prove who the user was at the time of the attack, and under what authority were they operating (individual hacker, part of a non-state group, or agent of a state). Definitive attribution is often impossible but hybrid approaches, such as those used to track down Ross Ulbricht, the founder and operators of the Silk Road, are increasingly effective.[11] By combining cyber and non-cyber means authorities are developing the means to attribute on-line actors with their real world counterparts. Still, these methods typically take days or weeks, whereas cyber attacks can be instantaneous and the victims may seek to retaliate immediately.

A willingness to act, combined with predictability consistent with established norms, is the key to building a reputation and acting as a role model. The overall system is strengthened when reputation allows even new partners to act in good faith expecting others will act in compliance with the code of conduct. By excluding non-compliant actors, those within the system create pressure that leads to behavioral change. Finally, the reputation of states for compliance can create prestige within the community.

6 Conclusion and Roadmap Ahead

The normative power of codes of conduct provides a basis from which to address the behaviors of the wide variety of actors within the cyberspace domain. Many of the existing codes of conduct, both formal and informal, have emerged through the leadership of the major

[11] For more information on the law enforcement operation capture Ulbricht see: http://www.wired.com/2015/05/silk-road-2/.

actors who set standards and impose costs on those unwilling to act in accordance with these standards. As part of this process, leading actors who stand to benefit from the establishment of widespread and powerful norms of behavior must create transparency as they work to reduce the potential for misinterpretation of actions.

In that tradition, the following roughly outlines a practical guide, or road map, for the creation of a code of conduct for cyberspace. First, epistemic communities should continue developing their own codes of conduct for their specialized areas. It is necessary to begin with small groups because the benefits of cooperation are specific and clear, and the framework for cooperation is likely limited to the issues of greatest importance. As various communities accept established norms, the collection of smaller codes of conduct, when taken together, will begin to provide a framework informing a broader, more comprehensive approach.

In order to reach that more comprehensive code of conduct, there must be consultation between states and communities of experts for the creation of international agreements and domestic laws or policy. Extant treaties or codes of conduct in other domains, such as the 1967 Outer Space Treaty, may provide useful assistance in developing the code of conduct and generating interest. Martha Finnemore, scholar of international cooperation, describes a "grafting" process whereby a new code of conduct can leverage existing frameworks and ideas for support.[12] International agreements can start between any states, but cooperation theory suggests that territoriality and proximity matter: it is easiest and most productive to begin formalizing behavioral expectations with your neighbors.

Proximity in cyberspace however, is hard to define. There are two potential ways for nations to proceed; either with their geographic neighbors or their "cyber neighbors," the nations with whom they interact most often through cyberspace. For the United States, this could mean collaborating with Canada and Mexico, geographic neighbors, or major trading partners such as the United Kingdom, Germany, Japan and China. Once cooperative agreements have been tested and established with neighbors (however defined), participants can open the code of conduct to others and attempt to expand its reach.

Given the rapid advancement of technology, large number and variety of actors, attribution challenges, and competing interests of actors within the domain, creating a cyber code of conduct will likely be a long process. Regardless of how the process unfolds, two things are clear: a successful cyber code of conduct will require a collaborative, multinational effort; and all collaborative efforts need a leader. The United States, by virtue of its influence in the world and its position at the forefront of cyber technology, should lead the way and forge alliances to create a code of conduct in cyberspace that will restrain cyber sources of disorder that threaten U.S. vital interests and global stability.

About the Authors:

Colonel Thomas McCarthy, PhD is a 2012 Fletcher graduate and serves as the Commandant and Dean of the USAF's School of Advanced Air and Space Studies, Maxwell AFB, Alabama. Commissioned in 1990 from the Air Force Academy he is an active duty officer with world wide operational and strategy development experience. Prior

[12]Martha Finnemore, "Cultivating International Cyber Norms," in *America's Cyber Future: Security and Prosperity in the Information Age*, ed. Kristen Lord and Travis Sharp (Center for a New American Security, 2011).

to his current position, Col. McCarthy served as Director for the USAF's Center for Strategy and Technology conducting studies to identify key characteristics of the military operating environment 30 years in the future. The opinions expressed are Col. McCarthy's alone and do not necessarily reflect those of the United States Air Force, the Department of Defense, or the United States Government.

Alison Lawlor Russell, Ph.D., is a 2012 Fletcher graduate as well and serves as an Assistant Professor of Political Science and International Studies at Merrimack College in N. Andover, MA. She has taught course on Cyber Security, International Politics, and American Foreign Policy, among others. Dr. Russell is also a non-resident Research Scientist at the Center for Naval Analyses, where her works includes cyber security, maritime strategy, critical maritime infrastructure protection, and global engagement strategy. Dr. Russell is author of the book *Cyber Blockades*, which was published by Georgetown University Press in 2014.