Global Digital Futures Policy Forum 2016: Issues Brief

Panel 3B: Cyber Conflict: Prevention, Stability and Control

By Jason Healey[1] and Tim Maurer[2]

'Removing the Heat from Cyber Competition and Conflict'

Only a few years ago, there were almost no norms globally accepted by governments on cybersecurity or cyber conflict. Even the United States, which had long pushed such norms, had publicly announced very few. The United States and a few other allies confirmed that laws of armed conflict (otherwise known as International Humanitarian Law or the "Geneva Convention") applied to cyberspace.

This has changed with tremendous progress recently, so much so that 2015 could be called was the Year of Global Cyber Norms.

Norms and Cyber Norms

In the academic literature, norms have been famously defined by Peter Katzenstein as "collective expectations for the proper behavior of actors with a given identity."[3] Norms generally can range from the global level to the nucleus of the family and they can be implicit or explicit. For example, laws can but do not always represent a norm. A law to which people adhere can represent "a collective expectation for the proper behavior of actors with a given identity." On the other hand, a law that's in the books but that nobody adheres is not reflective of an actual norm and collective expectation for the proper behavior.

In the international cybersecurity discussion, "norms" have taken on a slightly different meaning. The 2015 report of the UN Group of Governmental Experts states that "Voluntary, non-binding norms of responsible State behavior can reduce risks to international peace, security and stability. Accordingly, norms do not seek to limit or prohibit action that is otherwise consistent with international law."[4] Cyber "norms" in this sense could be seen as "potentially a precursor to

---

[1] Jason Healey is Senior Research Scholar at Columbia University's School of International and Public Affairs and Senior Fellow at the Atlantic Council.
[2] Tim Maurer co-leads the Cyber Policy Initiative at the Carnegie Endowment for International Peace and serves as a member of the Research Advisory Network of the Global Commission on Internet Governance.
[3] Peter Katzenstein. *The Culture of National Security: Norms and Identity in World Politics* (New York: Columbia University Press: 1996) 5
[4] United Nations, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" (22 July 2015) UN Doc A/70/174

eventual customary international law (through practice) that might eventually (after years) be codified."[5]

The narrative about norms for cyberspace (or alternately, ICTs for Information and Communication Technologies) is rooted in politics, as with most norms. The process started with a Russian proposal in the late 1990s for a legally binding cybersecurity treaty.[6] According to Sergey Ivanov, Russia's Minister of Defense from 2001 to 2007, "Russia wants to develop international law regimes for preventing the use of information technologies for purposes incompatible with missions of ensuring international stability and security."[7] However, the Russian government's proposal was met with skepticism not just by the U.S. government. As Ronald Deibert, professor of political science, explains

> Russia has been pushing for arms control in cyberspace, or information-weapons control. Most people dismiss this as disingenuous, and I tend to agree. Most observers see it as Russia's attempt to constrain U.S. superiority in the cyber domain. Russia is more concerned about color revolutions and mobilization on the Internet by dissident and human rights groups – and trying to eliminate the United States' ability to support that type of social mobilization – than it is about protecting the Internet.[8]

These concerns are complemented by skepticism regarding the enforceability and verifiability of a treaty relating to cybersecurity. The United States pushed its own process, leading to five unanimous UNGA resolutions on "Creating a Culture of Cybersecurity, because "challenges to cybersecurity was better answered by a good defense than by constraining offense (technology), providing a juxtaposition to the Russian argument that security could only be accomplished through arms control."[9]

The norms agenda really started to pick up speed when the Obama administration took office with a marked shift toward more international engagement. This shift included greater engagement in discussions about cybersecurity, with the US starting to actively promote the idea of international norms for cybersecurity after it largely ignored the resolution in the UN General Assembly's First Committee for the first decade.[10]

---

[5] Michele Markoff, Department of State, in email conversation with authors, 7 April 2016.
[6] Tim Maurer, "Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?", Discussion Paper 2011-11, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011
[7] Christopher A. Ford, "The Trouble with Cyber Arms Control," The New Atlantis – A Journal of Technology & Society, Fall 2010, http://www.thenewatlantis.com/publications/the-trouble-with-cyber-arms-control.
[8] Ronald Deibert, "Tracking the emerging arms race in cyberspace," Bulletin of the Atomic Scientists 67.1, January/February 2011, http://thebulletin.org/2011/januaryfebruary/ronald-deibert-tracking-emerging-arms-race-cyberspace.
[9] Michele Markoff, Department of State, in email conversation with authors, 7 April 2016
[10] White House. "U.S. International Strategy for Cyberspace". 16 May 2011;

Over time, the norms agenda evolved, as it was adopted and expanded by other countries and became a concerted effort of the international community. The overarching goal of the diplomatic efforts to date has been to agree to norms guiding behavior in cyberspace. From an academic perspective, these discussions can be broken down into four components: contestation, translation, emergence, and internationalization.[11]

Cyber Norms: Contestation, Translation, and Emergence

Norm contestation: At first, there was disagreement in the international community whether existing international law and norms already apply to cyberspace or if the international community should develop new laws specific to cyberspace. A few countries, China, in particular, contested the idea that existing norms apply and were a proponent and promoter of the latter approach. Conversely, the United States and United Kingdom announced a set of set of norm-like policy goals or "rules of the road" (in the words of then UK Foreign Minister William Hague), as did Dr. Hamadoun Touré, the Secretary General of the International Telecommunications Union.[12]

However, in 2013, the UN Group of Governmental Experts (with representatives from 15 countries including China, Russia and the United States), published a consensus report affirming that "international law and in particular the United Nations Charter, is applicable." This report and the year 2013 can therefore be seen as the end of the norm contestation period, especially regarding the application of international humanitarian law. Though pushback flares up occasionally, the idea of norms in this space has been largely put to rest.

Norm translation: In parallel to these political negotiations, other experts had been investigating how existing norms and laws could be translated to cyberspace. The United States, United Kingdom, Australia and other states had already announced that they believed the laws of armed conflict applied to military cyber operations. However, there was little work describing precisely *how* they applied.

Accordingly, the most important effort of norm translation has been the *Tallinn Manual on the International Law Applicable to Cyber Warfare* developed by a group of international (but all Western) lawyers under the auspices of NATO's Cooperative Cyber Defense Center for Excellence published in 2013.[13] It examines in significant detail how existing international law governing activity above the threshold of use of force and armed attack could apply to

---

U.S. Department of State, International Security Advisory Board. "Report on A Framework for International Cyber Stability". 2 July 2014

[11] This section is based in part on Maurer, Tim. "Cybersecurity and Asia" (September 2015) https://static.newamerica.org/attachments/9847-cybersecurity-and-asia/Cyber-security%20and%20Asia.b7302cdb44324fc38d6c49455429b59e.pdf.

[12] Jason Healey, "Comparing Norms for National Conduct in Cyberspace," Atlantic Council, 20 June 2011, http://www.atlanticcouncil.org/blogs/new-atlanticist/comparing-norms-for-national-conduct-in-cyberspace.

[13] Cooperative Cyber Defense Center of Excellence, "Tallinn Manual," https://ccdcoe.org/tallinn-manual.html.

cyberspace. This area has moved to the center of the cyber-security community's attention. The Tallinn Manual 2.0 expected in 2016 is only one example of an increasing flurry of activity focusing on this issue.

Norm emergence: Just as the year 2013 saw the end of the phase of global discussions on norm contestation, so was 2015 the year of norm emergence and internationalization.

The process started with a speech in May 2015 in Seoul, wherein Secretary of State John Kerry laid out two sets of norms important to the United States; the first set already rooted in international law, the second are proposed norms to create better rules of the road on cyber offense and defense:

> [T]he basic rules of international law apply in cyberspace. Acts of aggression are not permissible. And countries that are hurt by an attack have a right to respond in ways that are appropriate, proportional, and that minimize harm to innocent parties.
>
> We also support a set of additional principles that, if observed, can contribute substantially to conflict prevention and stability in time of peace...
>
> First, no country should conduct or knowingly support online activity that intentionally damages or impedes the use of another country's critical infrastructure.
>
> Second, no country should seek either to prevent emergency teams from responding to a cybersecurity incident, or allow its own teams to cause harm.
>
> Third, no country should conduct or support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information for commercial gain.
>
> Fourth, every country should mitigate malicious cyber activity emanating from its soil, and they should do so in a transparent, accountable and cooperative way.
>
> And fifth, every country should do what it can to help states that are victimized by a cyberattack.[14]

These norms were treated with a bit of caution by many experts. As expressed by General Michael Hayden, former head of the Central Intelligence Agency and National Security Agency, "We only steal stuff to keep you free and to keep you safe. We do not steal stuff to make you rich. I know of four other countries that can say those last two sentences. Everyone else steals for commercial advantage." This complicates the U.S. government's push that national intelligence agencies should not steal commercial secrets for the benefit of local companies, Kerry's third norm.

---

[14] Secretary John Kerry, "An Open and Secure Internet: We Must Have Both," remarks in South Korea, 18 May 2015, http://www.state.gov/secretary/remarks/2015/05/242553.htm.

Yet it turns out, these norms were in fact the beginning of a new era. With the growing number of bilateral and multilateral agreements, norm internationalization is now also starting to take center stage.[15]

Cyber Norms: 2015, the Year of Internationalization

Just a few months after the Secretary Kerry laid out the U.S. perspective on norms, in July 2015, another UN Group of Governmental Experts, this time comprised of representatives from 20 countries, agreed to a new consensus report including the following cyber norms in addition to several others focusing on supply chain integrity and responsible vulnerability disclosure:

- States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;
- States, in ensuring the secure use of ICTs, should respect … the promotion, protection and enjoyment of human rights on the Internet, as well as … the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;
- A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;
- States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts.
- States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;
- States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams … of another State. A State should not use authorized emergency response teams to engage in malicious international activity.[16]

This was a far richer set of norms than most outside experts had expected the UN GGE to be able to agree on; after all, the level of tension between the United States, China and Russia on a range of issues, not just cyber, was already high. The Snowden revelations of US cyber espionage seemed likely to torpedo any significant agreement, yet there was more concordance to come.

---

[15] *See* Tim Maurer, "The new norms." *Jane's Intelligence Review* (March 2016): 52-53

[16] United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," UNGA A/70/174, 22 July 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

During his September 2015 visit to the United States, President Xi Jinping of China and President Barrack Obama welcomed the UN GGE report and agreed to "establish a high-level joint dialogue mechanism on fighting cybercrime and related issues" as well as important norms:

> The United States and China agree that timely responses should be provided to requests for information and assistance concerning malicious cyber activities.
>
> The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.[17]

A month later, when Xi visited London, he struck a similar agreement on theft of trade secrets with Prime Minister Cameron:

> UK and China agree not to conduct or support cyber-enabled theft of intellectual property, trade secrets or confidential business information with the intent of providing competitive advantage.[18]

According to press, when Premier Angela Merkel of Germany was in Beijing, she was able to secure the same promise, so that "China and Germany agreed to work on stopping economic cyber spying between the two nations," however, unlike the US and UK agreements, this has yet to appear in a formal, concluding statement by the leaders.[19] Even so, there was still more norm internationalization to come.

At the Ankara Summit, in November 2015, the leaders of the G20 nations – including from true cyber powers such as Russia, China and the United States but also from Brazil, India and Indonesia – gave their approval to this latest UN GGE report and called out several specific norms:

> We affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.
>
> All states in ensuring the secure use of ICTs, should respect and protect the principles of freedom from unlawful and arbitrary interference of privacy, including in the context of digital communications.

---

[17] The White House, "FACT SHEET: President Xi Jinping's State Visit to the United States," 25 September 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.
[18] UK Government, "UK-China Joint Statement 2015," 22 October 2015, https://www.gov.uk/government/news/uk-china-joint-statement-2015.
[19] Stefan Nicola, "China Working to Halt Commercial Cyberwar in Deal With Germany," Bloomberg Technology, 29 October 2015, http://www.bloomberg.com/news/articles/2015-10-29/china-working-to-halt-commercial-cyberwar-in-deal-with-germany.

> We also … affirm that international law, and in particular the UN Charter, is applicable to state conduct in the use of ICTs and commit ourselves to the view that all states should abide by norms of responsible state behaviour in the use of ICTs.[20]

Secretary Kerry's speech in Seoul has just been in May 2015 and by November of that same year, just six months later, norms went from proposal to agreement at the top levels of global governance.

Private-Sector Norms

In addition to states proposing international cybersecurity norms, non-state actors have also been actively participating in this discussion. In one sense, the Internet was built on norm-like international behavior, from technologists building the network based on "rough consensus" to cooperating across boundaries to limit disruptions to the network. In late 2014, Microsoft took these norms one step further, launching a report proposing six specific norms overlapping with certain norms proposed by states:

1. States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services.
2. States should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.
3. States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.
4. States should commit to nonproliferation activities related to cyber weapons.
5. States should limit their engagement in cyber offensive operations to avoid creating a mass event.
6. States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.[21]

Complementing its substantive proposals, Microsoft also issued a procedural recommendation proposing a G20 + ICT20, the G20 member states meeting with twenty leading ICT providers, to develop an "agreed-upon norms document" which would "allow the 20 most developed economies to hold themselves and others accountable to the agreed-upon behaviors in cyberspace."

---

[20] G20, "G20 Leaders' Communiqué Antalya Summit, 15-16 November 2015," http://www.consilium.europa.eu/en/meetings/international-summit/2015/11/G20-Antalya-Leaders-Summit-Communique-_pdf/.

[21] Angela McKay, Jan Neutze, Paul Nicholas, and Kevin Sullivan, "International Cybersecurity Norms," Microsoft, December 2014, http://aka.ms/cybernorms.

Why Was 2015 the Year of Cyber Norms?

While these norms include certain caveats, for example, what is considered "unlawful" will depend on each country's domestic laws, it appears the remarks by Secretary Kerry lit a spark which took norms from an area of contention toward much greater international appeal, including G20 backing and statements by heads of state. The two most repeated norms include one of the least controversial (that "the basic rules of international law apply in cyberspace" which had been previously agreed to in the 2013 UN GGE report) up to certainly the most controversial (that "no country should conduct or support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information for commercial gain").

There are at least six likely, overlapping reasons why 2015 was a year when so much progress was made on articulating cyber norms.

Rising cyber tensions. Certainly within the United States, but assumedly in other nations as well, government officials and experts were seeking means to counter the rising frequency and violence of cyber attacks. From cyber espionage, to disruptive attacks like Stuxnet or against Sony, each nation seems to feel strategic vulnerability to others in cyberspace. Norms, in part, gained appeal because key states saw stability as being in their national security interest.

Leadership's personal attention. Within the United States, this concern was driven by the personal attention of President Barrack Obama who raised the issue with President Xi Jinping in the Sunnylands summit, mentioning the "deep concerns we have as a government around theft of intellectual property."[22] In China, President Xi named himself chair of an Internet security working group.[23]

Diplomacy and summit politics. Diplomats sometimes need a win for national (or even personal reasons) and may be willing to make tradeoffs they'd otherwise refuse. Likewise, leaders want to have successful summits. China came ready to the United States and the United Kingdom to make deals and ensure the summits would be a success. According to discussion with participants in the earlier 2013 UN GGE report, similar to President Xi having his first summit with President Obama at Sunnylands, the Chinese delegation was willing to compromise at the 2015 UN GGE.

Universality. When the governments selected norms at least some of them were meant to be relatively easy for most states to agree to, as it would be in their long-term interest. Therefore, key criteria were universal appeal and utility to be good for all states' national security.

---

[22] The White House, "Remarks by President Obama and President Xi Jinping of the People's Republic of China After Bilateral Meeting," 8 June 2013, https://www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china-.

[23] Shannon Tiezzi, "Xi Jinping Leads China's New Internet Security Group," The Diplomat, 28 February 2014, http://thediplomat.com/2014/02/xi-jinping-leads-chinas-new-internet-security-group/

Hard diplomacy. Diplomats, especially but not only from the US State Department, put in long hours negotiating and dealing with their counterparts to make progress over the course of 2015. Key international conferences, such as the Global Conference on Cyberspace in The Hague in April 2015, kept this momentum thanks to hard work by the Dutch government.

Low cost to commit to norms. It is also possible nations were willing to commit to norms because there give modest gain at relatively low cost. After all, if attribution continues to afford plausible deniability, then it could be hard for other states to prove that a nation is violating the norms. Many pessimistic experts felt there is little-to-no chance countries would forego cyber espionage. Likewise, other experts doubt states will live to up to the norm that "States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products."

Looking Forward

This last possible reason - a perceived low cost for committing to norms - points to the key factor in whether these new international norms will be effective.

The new, most pressing question will be whether and how states will implement and internalize the norms to which they agreed. According to the lead US diplomat negotiating these norms,

> most states are not in a position to accept new binding concepts in cyberspace. This allows them to initially sign on with no real penalty - that is, until the international community makes it common practice. Then deviations in behavior may be punished by the international community whether the norms are codified or not.[24]

Since the Obama-Xi agreement to limit stealing intellectual property for commercial gain, there has been intense debate within the US cyber community on whether China is living to the letter (or even the spirit) of the norm. But even if it leads to a reduction, but not an elimination, of such cyber espionage, it should still be considered a success. After all, diplomacy isn't binary. It's analog and if the norm leads to "less but not zero" – it is still a win for the United States and other nations facing such thefts.

If norms are in fact "collective expectations for the proper behavior of actors" then actors that fail to live up to those expectations will suffer at least reputational costs, especially if heads of state personally and publicly committed to them. In fact, this can be a central goal of diplomacy, to unveil the hypocrisy of other actors. So if a givens norm is not enacted national leaders who received a face-to-face agreement from President Xi will be in a much stronger position to respond to Beijing over its commercial espionage. The same holds true for other nations who may feel their critical infrastructure has been targeted or attacked by the Russian or

[24] Michele Markoff, Department of State, in email conversation with authors, 7 April 2016.

the US military or intelligence community, despite the explicit commitments by those governments.

Even though the progress on cyber norms over 2015 was sudden, that success had in fact been built on the years of hard work by diplomats, cyber experts, and many others. It is now time for more hard work, to help nations live up to these norms to ensure a more peaceful cyberspace in future.