What it’ll take to forge peace in cyberspace

The international community has finally started a serious conversation about norms in cyberspace. But reaching a global consensus still needs the world’s attention.

By Jason Healey and Tim Maurer

Only a few years ago, there were almost no public commitments globally accepted by governments on norms for cybersecurity or
cyberconflict. Even the US had publicly announced very few. Yet, within a relatively short period of time, the international community agreed to several, including personal commitments by the US and Chinese presidents and a consensus report adopted by 20 states under the auspices of the United Nations.

In fact, there was so much recent progress that 2015 could be called the Year of Global Cyber Norms. That is why the outcome of the US election also raises particularly important questions for the future of this process and the hardening of the aspirational norms that now form part of political yet not legally binding agreements.

This article starts with a discussion of cyber norms, a short history of norms with focus on the leaps taken in 2015, and some of the causes of that progress.

**Cyber Norms: Contestation, Translation, and Emergence**

At first, there was international disagreement whether existing international law and norms already apply to cyberspace or if new laws specific to cyberspace were needed. A few countries, China, in particular, contested the idea that existing laws apply and was a proponent and promoter of the latter approach. 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 evolution of the international discussion can be broken down into four components: contestation, translation, emergence, and internalization.

**Norm contestation:** The narrative about norms for cyberspace (or alternately, ICTs for Information and Communication Technologies) is rooted in politics. The process started with a Russian proposal in the late 1990s for a legally binding cybersecurity treaty. However, the Russian government’s proposal was widely seen in the West as disingenuous, an attempt to limit US cyber superiority and concern over “color revolutions and mobilization on the Internet by dissident and human rights groups.”

These concerns are complemented by US skepticism regarding the negotiability, enforceability, and verifiability of a treaty relating to
cybersecurity and favoring existing treaties, such as the Geneva Convention. The US accordingly pushed its own process, leading to five unanimous UN General Assembly resolutions on “Creating a Culture of Cybersecurity” since challenges to cybersecurity were “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.”

Conversely, the US and Britain announced a set of aspirational norms or “rules of the road” (in the words of then British Foreign Minister William Hague), as did Dr. Hamadoun Touré, the Secretary General of the International Telecommunications Union.

The norms discussion accelerated with a shift toward more international engagement with the Obama administration. The US pushed greater engagement in discussions about cybersecurity, actively promoting the idea of international cybersecurity agreements after it largely ignored the resolution in the UN General Assembly's First Committee for the first decade. The centerpiece of these US efforts was the International Strategy for Cyberspace, to push “the norms of responsible, just, and peaceful” conduct.

In 2013, the UN Group of Governmental Experts (the UNGGE), with representatives from 15 countries including China, Russia, and the US, published a consensus report affirming that “international law and in particular the United Nations Charter, is applicable.” This was an important achievement because, at first, a few countries contested the idea that existing international law applies and argued that new laws specific to cyberspace were needed. This report and the year 2013 can therefore be seen as the end of the norm contestation period further cemented with the 2015 UNGGE report.

This report also found that “[v]oluntary, nonbinding 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.” Cyber “norms” in this sense could be seen as “potentially a precursor to eventual customary international law (through practice) that might eventually (after years) be codified.” Norms in this context are essentially aspirational norms and therefore differ from how the term
is used in the academic literature as existing and usually adhered to rather than aspirational standards of appropriate behavior.

**Norm translation:** In parallel to these political negotiations, legal experts had been investigating how existing norms expressed through international customary law and codified treaties could be translated to cyberspace. The US, Britain, 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 and could be interpreted.

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. It examines in significant detail how existing international law governing activity above the threshold of use of force and armed attack could apply to cyberspace with a Tallinn Manual 2.0 recently released to look at an even wider set of questions.

**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. The process started with a speech in May 2015 in Seoul, wherein Secretary of State John Kerry laid out the aspirational norms important to the United States:

> [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.

These proposals were treated with a bit of caution by many experts. Why, after all, would other nations abide by such norms, an issue Harvard Law School professor Jack Goldsmith, for example, discussed in the context of the US-China agreement. Moreover, what, given the difficulties of attack attribution, could the United States do to prove if nations transgressed them, or punish those transgressors? And it was clear that proposed norms pushing against commercial espionage would face strong headwinds.

Yet it turns out, these norm proposals were in fact the beginning of a new era with the growing number of bilateral and multilateral agreements. To what extent and how states will now implement these agreements, the process of norm internalization, is now moving to take center stage.

**Cyber Norms: 2015, the Year of Internationalization**

Just a few months after then-Secretary Kerry laid out the US 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
agreements 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…;

- A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure…;

- 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.

This was a far richer set of agreed upon voluntary norms than most outside experts had expected the UN GGE to be able to agree on given the high tensions between the US, China, and Russia.

The Edward Snowden revelations of US cyberespionage seemed likely to torpedo any significant agreement, yet there was more concordance to come (after an implicit threat of sanctions). During his September 2015 visit to the US, President Xi Jinping of China and President 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 that:

> The US and China agree that timely responses should be provided to requests for information and assistance concerning malicious cyberactivities.
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.

A month later, when President Xi visited London, he struck a similar agreement on theft of trade secrets with then-British Prime Minister Cameron. According to press, “China and Germany agreed to work on stopping economic cyber spying between the two nations,” however, unlike the US and British agreements, this has yet to appear in a formal, concluding statement by the leaders. At the Ankara Summit, in November 2015, the leaders of the G20 nations—including from major cyber powers such as Russia, China, and the US but also from Brazil, India, and Indonesia—approved this latest UN GGE report and called out several specific norms, including most surprisingly the prohibition on commercial espionage.

Mr. Kerry’s speech in Seoul had just been given in May 2015 and by November of that same year, just six months later, the proposed language for norms went from proposal to agreement at the top levels of global governance. These norms are still largely only backed by the agreement of political leaders. None yet have been codified by treaty and it still too early to consider any to be customary international law (other than, of course, the agreement by the UN GGE that previous international laws do in fact apply to cyberspace).

In addition to states proposing international cybersecurity norms, nonstate actors have also been actively participating in this discussion. In late 2014, Microsoft launched a report proposing six specific norms overlapping with certain norms proposed by states. 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” that would “allow the 20 most developed economies to hold themselves and others accountable to the agreed-upon behaviors in cyberspace.” Given the outsized role technology companies play in cyberspace, such non-state approaches to norm development require even more attention than in discussion on the land, sea, air or space.

Why Was 2015 the Year of Cyber Norms?

While these aspirational norms include certain caveats, for example, what is considered “unlawful” will depend on each country’s domestic laws, it appears the remarks by Kerry lit a spark which took the norms discussion from an area of contention toward much greater international appeal. There are at least six likely, overlapping reasons why 2015 was a year when so much diplomatic progress was made on articulating cyber norms.

Escalation of dangerous cyber activities. Norms, in part, gained appeal because key states saw stability as being in their national security interest. Certainly within the US, but assumedly in other nations as well, government officials and experts were seeking means to counter the rising frequency and violence of cyberattacks.

Leadership’s personal attention. Within the US, this concern was driven by the personal attention of President Obama who raised the issue with Mr. Xi in the Sunnylands summit, mentioning the “deep concerns we have as a government around theft of intellectual property.” In China, Xi named himself chair of an Internet security working group.

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 US and Britain to make deals and ensure the summits would be a success.

Universality. When the governments selected norms at least some of them were meant to be relatively easy for most states to agree with, as it would be in their long-term interest. Universal appeal and utility were key to aligning with many states’ national security.

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 these agreements 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.

Will Cyber Norms Matter?

This last possible reason—a perceived low cost for committing to these agreements—points to the key factor in whether these new international norms will be effective. If states can just sign up to these agreements with no internal commitment, are they all just hot, diplomatic air with no relation to what activities states are actually conducting in the network? According to the lead US diplomat negotiating these agreements, there is some truth here but it is not the whole story:

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.

Perhaps the most critical case here is that the Obama-Xi agreement to limit stealing intellectual property for commercial gain was subsequently also incorporated in the G20 communiqué. Since that agreement in September 2015, 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.

After some initial mixed evidence, a report by cybersecurity firm FireEye showed a staggering decline. According to the company, they saw a steady rate of compromises by Chinese-linked groups, about 65 compromises per month until the middle of 2014, following the US indictment of Chinese military hackers. After that action by the US to enforce its preferred norm, the Chinese operations began to significantly drop.

In July 2015, just after the Obama administration finalized sanction authority to use against China and in the run-up for President Xi’s visit, the number of observed Chinese operations did not just
decrease, but rapidly plummeted. Instead of 65 per month a few years before, by late 2015 there were less than five. Analysis by FireEye and others seems to indicate that China has not stopped, but rather appears to have shifted from using proxy and nonstate spies in favor of state-run professional intelligence teams, in line (but not fully complicit) with the agreed-to norms.

But even if it leads to a reduction, and not an elimination, of such cyber espionage, the agreement supporting the norm should still be considered a success. After all, diplomacy isn’t binary. It’s a spectrum and if the norm leads to “less but not zero”—it is still a win for the US and other nations that have suffered Chinese commercially-motivated cyber espionage.

Moreover, 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.

Political agreements, voluntary norms, and threats of punishments, unfortunately, are perhaps more useful to tackle a pattern of activity than any specific act. Attributing what nation, if any, is responsible for a cyberattack is getting far more accurate and timely, but may depend on classified evidence a victim nation (or its allies) may be unwilling to share, especially quickly enough to influence the news cycle and public opinion. The public policy dilemma is simplified somewhat when the offending activity goes on for years, allowing the victim nation to cherry pick the most glaring cases. This is useful to reduce the intensity of espionage but less so for conflict de-escalation when one side is hiding behind proxies to conduct just-deniable-enough cyber or hybrid attacks.

Looking back, 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 agreements to ensure a more peaceful cyberspace in the future.

Jason Healey is senior research scholar at Columbia University’s School of International and Public Affairs and a senior fellow at the Atlantic Council.
Tim Maurer coleads 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.