The new norms

Global cyber-security protocols face challenges

As 2016 shapes up to be a key year for international efforts to define cyber-security, Tim Maurer examines the likelihood of these diplomatic talks translating into action.

Key points

- Diplomatic efforts intended to define and agree on norms in cyberspace are likely to be tested in 2016, given the increasing frequency and severity of cyber-attacks.
- The Chinese government signed several crucial bilateral and multilateral agreements in 2015 to limit offensive cyber activity, but it is likely to face challenges in implementing them.
- Key states with active cyber programmes, including Iran and North Korea, remain outside the international diplomatic effort.

On 5 January 2016, the Kiev government accused Russia of being behind a major power outage in the west of Ukraine on 23 December 2015. The accusation was based on an investigation conducted by international cyber-security firms, which attributed the cause of the outage to malware that disconnected electrical substations. Moscow denied the accusations, which – if true – would be the first known instance of Russia successfully conducting a cyber-attack using malware of this kind against the critical national infrastructure of another country.

This destructive cyber-attack came at the end of a year during which there were a number of significant data breaches, most notably the theft of data from the US Office of Personnel Management (OPM). However, despite these, 2015 was regarded as a positive year for diplomacy aimed at defining and agreeing international norms regarding cyber activity. The contrast between the progress achieved in the diplomatic arena and the increasingly severe consequences of cyber-attacks globally underlines the fact that the success of diplomatic efforts in 2016 will be judged by the extent to which they materialise into concrete action.

Firm commitments

In September 2015, after Chinese president Xi Jinping visited US president Barack Obama at the White House, China and the United States agreed that neither "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".

Before the agreement, there had been an increasingly active debate in the US about imposing sanctions against China. When US national security adviser Susan Rice travelled to Beijing in August she explicitly mentioned the possibility of punitive measures.

Shortly afterwards, the Chinese government sent Meng Jianzhu, the secretary of the Communist Party of China's Central Political and Legal Affairs Commission and effective head of domestic security, to Washington. His trip came in the context of international news reports in July quoting an unidentified US administration official indicating that the US was seriously considering imposing sanctions against China.

A month after the US-China agreement was announced, Xi also visited the United Kingdom, and the joint statement between China and the UK published on 22 October included very similar language. Bloomberg reported a similar China-Germany agreement on 29 October, and the language contained in these bilateral statements was also repeated in the November G20 communiqué.

International efforts

At the United Nations, a new Group of Governmental Experts (GGE) report proposing norms in international cyber activity was agreed by 20 governments, including China, France, Israel, Russia, the UK, and the US. The new report built on the 2013 landmark report of the previous GGE and provided greater detail, outlining several norms for cyber diplomacy.

These stipulated, "A State should not conduct or knowingly support ICT [Information Communications Technology] 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 [and] 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."

The report also explicitly stated, "States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts."

In addition, a group of 15 international lawyers has been working to advance the discussion on how existing international law applies to cyber incidents. A previous group had already focused on how the existing law of armed conflict applied to cyberspace. This led to the publication of the *Tallinn Manual on the International Law Applicable*

Major cyber-related agreements and meetings since 2010

Date	Agreement or meeting
30 July 2010	2010 United Nations Group of Governmental Experts (GGE) consensus report on cyber-security (10 member states)
17 June 2013	US-Russia heads of state-level meeting with agreement on co-operation on ICT security
24 June 2013	2013 GGE consensus report on cyber-security (15 states)
3 December 2013	Organization for Security and Co-operation in Europe agreement on cyber-security confidence-building measures
9 January 2015	Shanghai Cooperation Organization's draft International Code of Conduct for Information Security
22 July 2015	2015 GGE consensus report on cyber-security (20 states)
25 September 2015	US-China presidential meeting – fact sheets include sections on cyber-security and cyber-enabled theft of intellectual property
22 October 2015	UK-China Joint Statement including section on cyber-enabled theft of intellectual property
16 November 2015	G20 Leaders' Communiqué – Antalya Summit (paragraph 26)

Source: IHS

to Cyber Warfare in January 2013.

The new group is concerned with incidents below the threshold of use of force and armed attack, the category of incidents under which nearly all cyber incidents to date fall. The group is likely to begin to identify the rules and norms that should govern cyber activity and whether any new norms need to be developed.

Implementation challenges

Notwithstanding progress in the diplomatic arena, there are reasons to doubt the extent to which agreements can be implemented. In particular, the willingness of the Chinese government to uphold the terms of its agreement with the US is questionable. Shortly after the presidents' meeting, CrowdStrike, a cyber-security company that tracks Chinese cyber activity, reported that there had been no change in detected activity as of mid-October.

The lack of a visible reduction in this activity led to renewed calls for sanctions, including by the chairman of the US Senate Committee on Armed Services, Senator John McCain, in November. Amid the tense atmosphere of a US presidential election year, this raises the possibility that the US could again attempt to impose sanctions during 2016. Given China's desire to avoid becoming a constant subject of domestic political debate in the US, and the negative signals regarding its economy, it is unlikely that China would risk sanctions by completely failing to stand by the agreement.

It may not be a lack of will that led to this apparent delay in implementing the agreement. Firstly, China is not a monolithic hacking machine. Turning words into action will be a test of Xi's control over the People's Liberation Army (PLA). There are likely to be hackers within the PLA for whom the activity constitutes a profitable side business that they would be unwilling to relinquish. Similarly, there is the risk that deniable or rogue operations would continue despite an order from the PLA leadership to halt certain activities.

If, during 2016, corruption investigations were launched targeting senior PLA commanders believed to be involved in cyber-security, this would be one indicator that Xi was attempting to bring these units under control, given the extent to which previous anti-corruption campaigns have been used to strengthen Chinese presidents' domestic political position.

> **'Ultimately, the effectiveness of these agreements depends on political will'**

Outlook

Similarly, 2016 will be an important year at the UN. The substantial progress achieved by the 2013 and 2015 GGE reports is likely to come under scrutiny if their recommendations are not seen to be implemented. Ultimately, the effectiveness of these various agreements depends on political will, and the norms outlined in the GGE reports are voluntary. However, the deteriorating cyber-security environment has created heightened awareness among senior decision-makers that something needed to be done.

A new GGE will convene in the second half of 2016, when its membership will increase from 20 to 25 member states. The GGE remains divided into two sides. The group led by China and Russia has promoted a draft International Code of Conduct and supports greater control of the internet by individual states. Its opposition, led by the US, has advocated voluntary norms and a multi-stakeholder governance model. The new entrants are likely to be split between these sides, although some could seek to form a third faction calling for a demilitarised internet or the equivalent of unilateral disarmament.

Moreover, all these diplomatic efforts are unlikely to engage with states such as Iran and North Korea, which have been among the most active nations in developing cyber capabilities for political and military purposes. They are likely to ignore any global initiatives to introduce cyber norms, especially given that they lack a seat at the decision-making table. ■

*This article was first published online at **ihs.com/janes** on 5 February 2016.*

On the web

- Efforts made to improve global cyber-security
- China tightens grip on cyberspace

Author

Tim Maurer co-leads the Cyber Policy Initiative at the Carnegie Endowment for International Peace, where he focuses on cyberspace and international affairs.

ihs.com/janes