Standard issues

UN body considers international cyber norms

Following the September meeting of the UN Group of Governmental Experts, Tim Maurer examines the likelihood of major powers agreeing on standards for cyber behaviour.

Key points

- The September 2016 meeting of governmental experts is part of a process to establish cyber norms that has been going on since the late 1990s.
- China, Russia, and the United States all agree in principle that international law, including the UN Charter, should apply to cyberspace.
- Although China and the US have shown they can work together, Russian behaviour suggests a consensus will not be achieved.

The Democratic National Committee (DNC) was hacked and confidential data leaked in July 2016, in a highly publicised event that caused serious concern in the United States and around the world. The deliberate leaking of confidential data in an apparent attempt to influence the US election was unprecedented and targeted the core of the US political system.

This was not the first time an election has been the target of hackers, however. In 2014, Ukrainian officials found and removed malware designed to influence the Ukrainian presidential election. Nevertheless, the possibility that somebody would dare to target the United States in a similar fashion seemed unlikely until the July attack. The highest-ranking Democrat in Congress, House Minority Leader Nancy Pelosi, called it an "electronic Watergate".

The cyber attack against the electrical grid in Western Ukraine in December 2015; the destructive malware targeting Sony Pictures Entertainment in December 2014; Stuxnet manipulating the control systems at the Natanz nuclear facility in Iran, discovered in 2010; and the use of Distributed Denial of Service attacks to disrupt the Georgian government's websites during the Russia-Georgia war in 2008 and to target Estonia in 2007 are all examples of an increasing sophistication of cyber-attack methodology.

The DNC hack was only the latest, albeit a particularly powerful, reminder of how cyberspace can be used for political and military purposes.

Taking stock of cyber security

The international community has been discussing what rules do and should apply to cyberspace since the late 1990s. Through a series of groups of governmental experts meeting under the auspices of the United Nations Group of Governmental Experts (UNGGE), major players such as China, Russia, and the US have agreed that international law, including the UN Charter, applies to cyberspace. They have also developed a set of voluntary norms.

The UN Charter matters because it outlines the right to war and when it is legitimate for states to use force. Another important aspect of this discussion was the application of international humanitarian law and its guidance on the conduct of war. Initially, some states such as China contested this notion, calling for a new law to be developed instead. This agreement paved the way for states to discuss not whether, but how international law applies to cyberspace and how to interpret and translate existing provisions as they affect this new area of activity.

In early September, a new UNGGE convened, which is expected to produce another consensus report by mid-2017. To support this development and the internalisation of norms for cyberspace, states have also tried to increase confidence among themselves and provide positive incentives.

Building on the experience of the Cold War, the 57 states participating in the Organisation for Security and Co-operation in Europe (OSCE) agreed to a first set of confidence-building measures in December 2013, followed by a second set announced in March 2016. The list included the establishment of a crisis-management hotline and a commitment that "participating States will, on a voluntary basis, encourage responsible reporting of vulnerabilities affecting the security of and in the use of ICTs and share associated information on available remedies to such vulnerabilities, including with relevant segments of the ICT business and industry".

The goal of these measures was to increase co-operation and transparency within the OSCE region. Meanwhile, as with all trust-building exercises, the process – in this case discussions leading to agreements – matters as much as, if not more than, the substance of the agreements themselves.

Cyber espionage, for both political and economic purposes, has not been discussed in the context of the UNGGE. Instead, the US

government came to a bilateral agreement with China in September 2015, with both sides agreeing 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." This agreement set the stage for very similar language to be adopted by the G20 group, widening its scope substantially.

What all of these agreements have in common is that they are political agreements and therefore are not legally binding. That is why great effort has gone into widening the number of countries committing to this language by inserting it into head-of-state-level communiqués. The international discussion about the rules for cyberspace really started to make progress in 2015, after a decade of inertia.

However, even as the fifth UNGGE is taking up its work, with the September meeting consisting of 25 instead of 20 member states, there is still no guarantee that the recommendations will be taken forward.

PA: 1685199

In this 5 March 2015 picture, a map of the US shows cyber attacks in real time. The DNC was hacked and confidential data leaked in July 2016, in an attack aimed at the core of the US political system.

Fork in the road

The international community stands at a fork in the road, and with the fifth UNGGE underway, one of the decisions the group will need to find agreement on is whether the work will transition to an open-ended working group, an existing body, or an entirely new mechanism. The expansion of the UNGGE also reflects the group's effort to broaden and deepen the legitimacy of the work developed by its predecessors.

One possibility is that the agreements achieved so far could be taken up by the full UN General Assembly and included in a resolution, although the timeline for this, should it happen, is unknown.

However, the UNGGE system has been criticised. For example, the head of the Israeli National Cyber Bureau, Eviatar Matania, criticised the US Department of State's strategy for developing international cyber-security norms, calling the plans "overly broad." According to Matania, speaking at the Billington Cybersecurity Summit in Washington, DC, "The norm of 'do not attack critical infrastructures' sounds great, but can you define for me what critical infrastructures are ... The definition in every nation is different. Some will define everything as critical."

In other words, the success of the agreements reached so far depends largely on their implementation. The 2015 cyber attack against the electrical grid in western Ukraine, which took its power offline for several hours, was arguably surprising given the agreement earlier that year in which UNGGE states committed to the voluntary norm not to target critical infrastructure in peacetime.

Another hurdle to overcome is information sharing. States can only know if the norms are voluntarily adhered to if they know what kinds of incidents are taking place. If critical infrastructure operators, for example, are unaware of the norm and do not report relevant incidents, it is difficult to assess the norm's effectiveness.

Outlook

Cyber-security company FireEye in June 2016 published a report stating that "since mid-2014, we have observed an overall decrease in successful network compromises by China-based groups against organisations in the United States and 25 other countries". The 2015 agreement may have contributed to this reduction and the change in behaviour by the Chinese government.

Some states are also advancing more far-reaching proposals as part of the norms discussion. The Dutch government, for example, is focusing specifically on the protection of the core and backbone of the internet. This was championed during its hosting of the fourth Global Governance on Cyberspace conference in 2015, which set out to define the internet's key protocols and infrastructure that could be considered a global public good and to address growing state interference.

The latest iteration of the UNGGE is due to publish its report in June 2017. It appears that the Chinese and US governments will be able to work together and come to an agreement, even on sensitive issues, and that the agreement will subsequently be honoured. The Russian government's actions in Ukraine and elsewhere, however, have raised doubts about its intentions and sincerity, which is particularly relevant in the context of the UNGGE, given that the group itself dates back to a Russian initiative. ■

First published online: 24/10/16

On the web

- Global cyber-security norms face challenges
- Asian cyber-security alliance remains distant
- Russia increases use of cyber proxies

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