S. RAJARATNAM SCHOOL
OF INTERNATIONAL STUDIES
A Graduate School of Nanyang Technological University

RSIS COMMENTARIES

No. 171/2013 dated 19 September 2013

Enhancing International Cybersecurity: Will the UN Reach a Deal?

By Senol Yilmaz

Synopsis

The 68th session of the United Nations General Assembly has just started. The recent recommendations by the international Group of Governmental Experts may pave the way for enhancing cybersecurity.

Commentary

A WINDOW of opportunity has opened to enhance international regulation of cyberspace, after more than a decade of rather unsuccessful attempts to do so under the roof of the United Nations. The main rivalling powers, namely the United States and Russia, seem to be prepared to make concessions to move the debate forward.

At the heart of the difference between the two powers is the term "information security" - which means different things to them.

Information Security – A term with ambiguity

First, software made up of information in the form of zeros and ones is considered information technology, as is the physical infrastructure of cyberspace consisting of wires, servers, and routers, etc. Malicious software such as Stuxnet that can cause substantial damage is therefore considered an "information weapon".

Second, words that form ideas and knowledge as those that we hear on the news or read in newspapers are also considered "information". The challenge for some states, especially authoritarian ones, is that certain information could potentially serve subversive purposes. Similarly, Internet platforms like Twitter and Facebook can be used for subversive activities such as organising anti-government protests, as well as simply communicating unpleasant ideas and knowledge. Hence, ideas and communication platforms can also fall under the category "information" and "information technology", respectively.

While the United States favours the first, narrower, definition, the Russians treat the term information security as encompassing both, bits and words. This difference made finding common ground difficult.

When Russia suggested a draft resolution to the UN General Assembly as early as 1998, proposing to define and sanction "information weapons", the US did not support the draft resolution, arguing that extant laws regulated the military use of cyberspace sufficiently.

US and Russian fears

The US rejection could be due to three reasons. Firstly, for a long time, Washington considered criminals and terrorists as the main challenge to its national security from cyberspace, rather than cyber warfare waged by state actors. Secondly, restrictions of the freedom of expression that could have potentially ensued are anathema to American values and, at least official, US foreign policy. Thirdly, the US has arguably the most powerful offensive cyber capabilities in the world. Restricting the use of cyberweapons was therefore not in its interest.

This position seemed to change in 2010, when the US, together with Russia and several other countries, sponsored a draft resolution, subsequently adopted by the UN General Assembly without a vote. Despite the limited scale of the resolution, it was a first step towards finding international norms to enhance cybersecurity at a global level.

The reason for the US' policy change is not entirely clear. One could assume that US policymakers realised their country's own vulnerability in cyberspace, and hence changed their stance. Richard Clarke, former cybersecurity advisor to the White House, argues that strong offensive capabilities are merely one of three factors of any nation's overall cyberpower. According to his framework, national cyberpower is also contingent upon defensive capabilities, as well as a given country's dependence on cyberspace.

Clarke makes the argument that while Russia, China and Iran presumably have weaker offensive capabilities than the US, they have stronger defences and that they are less dependent on cyberspace than the US. Considering all three factors holistically, Clarke concludes that the US' overall national cyber power is weaker than its main competitors'.

It is plausible, therefore, that the growing awareness of its own vulnerability led the US to co-sponsor the draft resolution with Russia in 2010 as a basis to move further.

An important aspect of Russia's international cyberpolicy became evident in 2011. Russia, along with China, Tajikistan and Uzbekistan proposed a resolution to sanction the use of "information technology to carry out hostile activities". The draft proposal also suggested to respect the right to search for, acquire, and disseminate information "on the basis of national laws".

The latter point of the draft resolution however was unacceptable to the US and most Western countries, simply because the national laws of the four co-sponsors of the resolution tend to restrict the freedom of expression. According to Freedom House's "Freedom of the Press 2013" report, the four countries belong to the 30 most restrictive states regarding print, broadcast and internet freedom. Therefore, from the Western states' point of view, the proposal would serve to sanction the freedom of expression.

Way forward: Slice it up

After more than a decade of attempts to find a common basis for the regulation of cyberspace at the UN, a glimmer of hope has appeared recently. The international Group of Governmental Experts, representing 15 countries, submitted a report to the Secretary General of the United Nations. The US, China and Russia were represented in the Group. The report could provide a basis for a resolution to further regulate state behaviour in cyberspace at the 68th session of the United Nations General Assembly, which opened this week.

The report of the Group concluded that cyberspace was not the Wild West of the 21st century. Rather, extant international laws were applicable to cyberspace, a claim the US has been making for years. At the same time, it was emphasised that states exert sovereignty and jurisdiction over information and communication technology in their territory, incorporating Russian objectives. It seems that both camps have made some concessions to achieve some of their goals. It remains to be seen if and to what extent the General Assembly considers the Group's recommendations.

To further enhance international cybersecurity, a lesson could be learned from conflict resolution practice. Mediators often use a technique called "slicing": To solve conflicts, they first disentangle the plethora of disputed issues between parties and isolate single issues that are debated, and ideally resolve one issue after another until the entire set of differences is solved.

In a similar manner, cyber warfare could be prioritised and isolated from numerous other issues surrounding cybersecurity, such as cybercrime, cyberespionage, and of course the debate about information security in the wider sense. Hopefully, individual member states will make concessions to realise what is possible and necessary to make cyberspace more secure.

Senol Yilmaz is an Associate Research Fellow at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University.