PIR CENTER ПИР-ЦЕНТР

Alfredo Morelli,
Argentina’s representative in the Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security established pursuant to resolution A/RES/53/70 (2012)

The whole process developed by the GGE is positive in the sense of keeping up this very important issue on the agenda but it will not affect the security-driven political decisions take by individual states. For this to be a matter of real advance, the states should openly declare their desire to start discussing ‘digital restraint’. This is something we don’t really see happening – on the opposite, we witness an arms race dominated by the ICTs as its major component.

Alfredo **Morelli,** Argentina’s representative in the Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security established pursuant to resolution A/RES/53/70 (2012), has shared with *Cyber Pulse* his impressions from the 4th GGE work. Mr Morelli has commented on the GGE report issued in August 2015, which reflects the agreements of the member-states on a number of exact norms of behaviour in cyberspace, which the previous group didn’t manage to put on paper.

What is your overall impression of the work done by the 4th UN GGE as compared to your experience with the previous group? Where do you see the biggest breakthroughs and the most viable agreements?

The results are sufficiently vague so that everyone can make of them what they wish. The Group hasn’t advanced much, in fact the real threats advance much faster than the GGE agreements. That said, given the pace at which risks, threats and incidents increase, the processes which claim to lead us to a more secure, stable, global and free cyberspace should be sped up.

The key conceptual differences in views on information/cyber-security between Russia, China on the one side and western countries on the other are well known. Do you see any of them smoothed out a bit? On the contrary – are there more misunderstandings emerging?

I believe there has been some progress in the differentiation of the network security and the security of network use. Secondly, the international law applicability to cyberspace has been generally accepted. Thirdly, the importance of confidence building measures has been recognized as well as the necessity to preserve global connectivity and information flow, the necessity to refrain from accusations towards the states from whose territory cyberattacks originated, no use of information to influence internal affairs of other states as part of responsible behaviour in cyberspace. In any case, the US seems to be solidifying its hegemony in this area.

How far do you expect technical cooperation among states to go given major distrust at the times of geopolitical shake-ups? Will nations be willing to share vulnerabilities in their critical infrastructures?

Technical cooperation will never reach the level at which information disclosure could threaten state security. Similar to the private sector (banks) which refuse to disclose information when they have suffered an attack, the states will find it hard to share the existing vulnerabilities of their critical information infrastructure. The cooperation should in particular promote capacity building mechanisms in developing countries, taking into account that the same document envisages that the focus of cybersecurity efforts should be global. A country at a low level of cybersecurity development is a threat to all.

It was previously suggested that the Group might find it easier to agree on non-attacking specific types of critical infrastructure rather than go for general commitments – such as banking/finance or nuclear industry. Why do you think this didn't happen?

The point is that each country defines for itself what constitutes its sectors of critical infrastructure in accordance with its economic, social and political structure. Therefore, it seems reasonable to use a more general formula, which says that "the states should abstain from attacking each other's objects of critical infrastructure".

In your view, how important was the reported debate about Article 51 of the UN Charter which Russia didn't want to be singled out in the text of the Group report? Does this truly matter given that Article 5 of the Washington treaty allows for retaliation in cyber to NATO states anyway?

The legitimate self-defense right under Article 51 of the UN Charter is complicated by the attribution challenges. It is impossible to exercise "legitimate defense" if there is no certainty about the attack's origin. Besides there is no definition of what constitutes "an attack", and while the applicability of Article 51 (as well as other norms of international law) is acknowledged, it is not clear how exactly it is to be implemented. The statement that the states can take 'measures' only multiplies uncertainties.

Do you expect the agreed norms to actually work in a meaningful way? Do you believe that these and later developed voluntary norms could actually become binding one day? What would be needed for this to happen?

Strictly speaking, the non-binding norms are recommendations. It seems that political pacts are in trend since the countries are incapable of agreeing on anything. I see it as populism and lack of leadership in some countries. In any case these agreements allow to 'name and shame' those who don't comply but there is a great risk of biased assessment of states' bahaviour. The whole process developed by the GGE is positive in the sense of keeping up this very important issue on the agenda but it will not affect the security-driven political decisions taken by individual states. For this to be a matter of real advances, the states should openly declare their desire to start discussing 'digital restraint'. This is something we don't really see happening – on the opposite, we witness an arms race dominated by the ICTs as a major component.

The agreement on non-use of harmful hidden functions in ICTs runs counter the long disclosed practice of "public private partnership" between certain states and private companies on inserting exploits allowing for electronic surveillance. How do you think these can be reconciled?

It is important to study the role and responsibility of the private sector and the forms of its activities. Since the states use private companies as tools for their security policy, the suggestion to give up the use of 'harmful functionalities" in ICTs is not likely to go beyond mere declarations.

Do you see any immediate "winners' of this agreement?

This discussion is driven by the big countries, for developing countries political uncertainty is bad news since we don't have much resources and we'd rather employ ones we have for developmental ends, than military use. In any case, I believe that the problem doesn't lie with the states, which at the end of the day will agree on a 'modus vivendi', but non-state actors which operate in a highly lucrative market and are hard to control. If we fail to do this, we will all lose.

Questions by A. Kulikova