Committee: United Nations General Assembly

Topic: Advancing Responsible State Behaviour in Cyberspace in the Context of International Security

Country: The Russian Federation

Cybersecurity is one of the most complex, challenging issues. The difficulty of attribution in cyberspace; the plethora of nonstate cybercriminals; the rapid development of increasingly sophisticated cyber tools; the uncertainty surrounding the consequences of their use; and the hyper secrecy of countries around their cyber capabilities all militate against the development of a code of conduct in cyberspace. These issues include some provisions which should excite no controversy in any part of the world, such as avoidance of breaches of rights and freedoms, or “criminalisation of use of information resources for illegal purposes”. On December 27, by majority vote, the UN General Assembly in New York adopted the resolution “Countering the use of information and communications technologies for criminal purposes,” sponsored by the Russian Federation.

The Russian Federation is a secular country which maintains one of the world's most liberal immigration policies. It officially recognizes Orthodox Christianity, Islam, Judaism, and Buddhism as the country's traditional religions. Russia is a member of the Commonwealth of Independent States (CIS), Union of Russia and Belarus, Organization for Security and Cooperation in Europe (OSCE) and the North Atlantic Cooperation Council (NACC). It also participates in some of the most important UN peacekeeping missions. As per the statement made by the First Deputy Permanent Representative Dmitry Polyanskiy at UNSC briefing on cooperation between the UN and regional organizations, we are in favour of developing cooperation between the UN and regional and sub-regional organizations based on the UN Charter – first and foremost its Chapter VIII. It should also be organized around this basis and within the framework of the UN General Assembly resolution 65/276 of 2011.

Russian views on the nature, potential and use of cyberspace differ significantly from the Western consensus. Russia has deep concerns on the principle of uncontrolled exchange of information in cyberspace, and over the presumption that national borders are of limited relevance there. Circulation of information which poses a perceived threat to society or the state, and sovereignty of the “national internet”, are key security concerns in Russia. Hacktivists and cyber-criminal syndicates have been a central feature of Russian offensive cyber operations, because of the anonymity they afford and the ease with which they can be mobilized. However, the crowd-sourced approach that has typified how the Kremlin has utilized hackers and criminal networks in the past is likely to be replaced by more tailored approaches, with the FSB and other government agencies playing a more central role. The two most recently released public statements of Russian policy on cyberspace: the “Draft Convention on International Information Security“ (released 24 September 2011) and the Russian military cyber proto-doctrine “Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space” (released 22 December 2011) in order to describe the Russian public stance on cyberspace.

The 2013 Security Council’s Basic Principles on International Information Security confirmed this broad understanding and the panoply of threats related to information security and saw information technology as a weapon that can be used for political and military purposes to violate a state’s sovereignty and territorial integrity. In official documents, the government lists policy goals that outline a primarily defensive and collaborative posture designed in response to aggressive adversaries and entities that threaten Russia, which aims to contain or prevent aggression in cyberspace through legal frameworks and partners. Such national-level policies include the “development and adoption of regulatory legal acts of the Russian Federation establishing the liability of legal entities and individuals for unauthorized access to information, its illegal copying, distortion and illegal use” and enhancement of “the security of critical information infrastructure”.

The adoption of the Russian resolution shows that the world community urgently needs to develop a universal, comprehensive and open-ended convention on countering cybercrime due to its having become a transnational, cross-border issue. The resolution proposed by Russia essentially enhances states’ digital sovereignty over their information space and ushers in a new page in the history of global efforts to counter cybercrime. By suggesting such a resolution, Russia framed itself as a defender of the rules-based international order, committed to multilateral solutions to international challenges.

The government of Russian Federation believes that it is in the committee’s interest’s to resurrect the long-shelved debate on the agenda and re-open it for active discussion and subsequent recommendation to the UN General Assembly for the purpose of improving the resolution and adopting it uniformly across the UN and it’s member states. In conclusion, the delegate of Russia believes that the upcoming session would be most productive if the House would move in favour of constructive deliberation and debate upon advancing state behaviour in cyberspace by not only taking into account the current scenario but also the past conflicts and resolutions - all whilst demonstrating cohesion, cooperation and understanding between all members of this esteemed Committee.