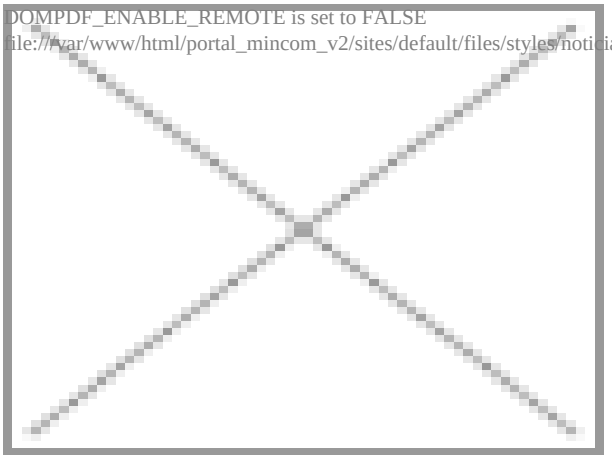

Source:
Source Misiones Minrex

Source: Misiones Minrex
Mr. President:
Member States face a variety of threats concerning information security.
The increasing development of cyber-offensive capabilities and the inclusion in the national security strategies of some States of the use of offensive cyber weapons and the conduct of cyber-offensive operations; as well as the possibility of preemptive cyber-attacks to deter adversaries, may turn cyberspace into a new theater of conflict. This danger is increased by doctrines that consider the use of force as a legitimate response to a cyber attack..
The covert and illegal use of computer systems of other nations, by individuals, organizations and States, to carry out computer attacks against third countries, can also be a catalyst for international conflicts.
The misuse of information and communications technologies and media platforms, including social networks and radio and electronic broadcasts, as a tool for interventionism through the promotion of hate speech, incitement to violence, subversion, destabilization, dissemination of false news and misrepresentation of reality against any State for political purposes and as a pretext for the threat or use of force, also represent a threat to nations and contravene the principles of international law.
These actions are part of the so-called fourth generation warfare, which works on the basis of the manipulation of emotions, from the use of information stored and processed in violation of the protection of personal data rights, in which companies that turn this model of action into a business participate.
We reaffirm the right and duty of States to fight, within the framework of their constitutional prerogatives, the dissemination of false or distorted news that may be interpreted as interference in the internal affairs of other States or as prejudicial to the promotion of peace, cooperation and friendly relations among States and nations.
Cuba has repeatedly denounced how access to platforms and services is limited, social network accounts are blocked, investments for the development of ICT infrastructure are hindered, and alternatives are hypocritically promoted to promote services outside state control for subversive purposes.
All of this takes place in an international context of constant threats to peace and security from armed conflicts, unconventional wars, attempts at regime change and frequent violations of the United Nations Charter and international law, as well as terrorist acts, including state terrorism.
In order to counter these threats, a global commitment is required on the use of ICTs for exclusively peaceful purposes, for the benefit of cooperation and the development of peoples. The use of ICTs as a pretext for unleashing wars, threatening or using the force or as a tool for interventionism, subversion, destabilization, dissemination of false news and misrepresentation for political purposes; as well as for media campaigns of disinformation against sovereign governments should be prohibited. A clear opposition to the militarization of cyberspace must be established..
The colossal technological gap and the obstacles imposed on developing countries to invest in the security of

their ICT infrastructures, which limit their capacity to face the growing and complex current and potential threats, must be addressed.

It is necessary to adopt, within the framework of the United Nations, a legally binding international instrument, which complements the applicable international law, responds to the significant legal gaps in cybersecurity and allows to effectively address the growing challenges and threats, through international cooperation.

Taking all this into account, we would like to share some actions that could contribute to address current and potential threats in the ICT environment:

1. Increasing cooperation in dealing with cyber incidents, exchanging information that does not compromise the privacy of States with respect to their capabilities or contravene national legislation.
2. Establishing technical assistance mechanisms for capacity building, including those to improve the protection of critical infrastructure, based on respect for the national legislation of the States.
3. Exchanging best practices in dealing with cyber incidents, especially among Computer Emergency Response Teams (CERTs), to increase countries' operational capabilities in the event of a cyberattack.
4. Standardizing, to the extent possible, the nomenclature of cyber incidents in the search for a common terminology, which facilitates the exchange of information on incident response.
5. Establishing a multilateral mechanism to determine, impartially and unequivocally, the origin of incidents related to the use of ICTs.

Thank you