Ministry of Communications
Published on *Ministry of Communications* (https://www.mincom.gob.cu)

Source:
Institutional Communication Office

The Vice Minister of Communications of #Cuba, Ernesto Rodríguez Hernández, is attending the Internet Governance Forum, which takes place from 8 to 12 October in Kyoto, Japan and will speak at the High Level segment on Cybersecurity.
"The growing 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 deployment 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 other nations' computer systems by individuals, organizations and states to carry out cyber attacks against third countries can also be a trigger for international conflicts.

"The misuse of information and communication technologies and media platforms, including social networks and radio and electronic broadcasting, 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, are also a threat to nations and contravene the principles of international law.

"These actions are part of the so-called fourth generation war, which works on the basis of the manipulation of emotions, based on 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," said the Cuban Vice Minister of Communications.
Ernesto Rodriguez Hernandez stated: "To counteract the above threats, we need:

"A global commitment to the use of ICTs for exclusively peaceful purposes, for the benefit of cooperation and development of peoples.

"To address and eliminate the colossal technology gap and the obstacles imposed on developing countries to invest in the security of their ICT infrastructures, which limit their capabilities to face the growing and complex current and potential threats.

"To adopt, within the context of the United Nations, a legally binding international instrument, which complements the applicable international law, responds to the significant legal gaps in the field of Cybersecurity and allows to effectively address the growing challenges and threats, through international cooperation.

"To increase cooperation to deal with cyber incidents, exchanging information that does not compromise the privacy of States with respect to their capabilities or contravene national legislations.

"To implement technical assistance mechanisms for capacity building, including those to improve critical infrastructure protection, based on respect for the national legislation of the States.

"To exchange best practices in dealing with cyber incidents, especially among Computer Emergency Response Teams (CERTs), to increase countries' operational capabilities in the event of a cyber attack.

"To standardize, to the possible extent, the nomenclature of cyber incidents in the search for a common terminology, which facilitates the exchange of incident response information.

"To establish a multilateral mechanism under the umbrella of the United Nations to determine, impartially and unequivocally, the origin of incidents related to the use of ICTs."

Ernesto Rodriguez Hernandez added in his speech:

"Cyberspace is an extremely dynamic scenario, where the nature of the events that trigger disputes differs from other areas with an impact on international security. For example, the determination of the origin of incidents related to the use of ICTs encounters difficulties and unilateral attributions are questionable, given that there is no multilateral mechanism to determine, impartially and unequivocally, the origin of incidents. Nor is there any common terminology to facilitate understanding among States regarding cyber incidents and their response.

"In this context, we observe a tendency to simplistically assume the applicability of existing international law to the ICT environment and the rejection of the need for new standards.

"Attempts are being made to force consensus on conceptions that seek to equate a cyber attack with a traditional armed attack in an attempt to justify, in the context of Cybersecurity, the supposed applicability of the legitimate self-defense provided for in Article 51 of the United Nations Charter.

"It is also a matter of strengthening the notion of the applicability of international humanitarian law to the use of ICTs in the context of international security. It should be remembered that the conventions that make up international humanitarian law were agreed upon to deal with armed conflict scenarios and are only applicable in such cases. Assuming that these norms apply to ICTs would imply tacit acceptance of the possibility of an armed conflict scenario in this area; it would contribute to the militarization of cyberspace and would be a first step towards equating a cyberattack with a traditional armed attack.

"All of the above reinforces that it cannot be claimed that threats associated with the malicious use of ICTs can be confronted and mitigated by the automatic application of existing international law tools.

"As a consequence, the debate on how international law should apply to the use of information and communication technologies reinforces its relevance. This, however, cannot selectively consider certain issues related to international law over others.

"We therefore reaffirm the validity of the principles of international law and the Charter of the United Nations in cyberspace, in particular those of sovereignty, territorial integrity and non-intervention in the internal affairs of States, in the use of information and communication technologies."

Finally, he considered that ITU can play an important role in achieving these objectives; the nature of cyberspace and its technological complexity require that multilateral debates strike the necessary balance between political-diplomatic arguments and those of a technical nature, otherwise there is a risk of failing to achieve the active and responsible participation of all humanity, as well as peace and sovereignty in this space of diffuse borders in which daily life takes place.