Commitee : GA-1 :DİSEC (Disarmament and International Security)

Country :  Bolivarian Republic of Venezuela

Agenda item:weaponization of data and cyber security

The weaponization of data and cyber security are the most consequential topics of today's world as the world is developing and accordingly, the technology and the social media that is why the world is becoming cyberspace unintentionally. As a result ‘’fake news’’ is expanding and replacing the real information. Due to the actions of turning the data into weapons to use against individuals, States, and organizations, everyone’s personal information is at stake. Moreover, Statistical data demonstrate as cyber-attacks on websites and ICT webs are made more and more with the help of oblivious users who become gullible puppets similarly, to carry out illegal movements ranging from removal of information style to the advancement of terror. According to these events and the past events, for instance, the second red scare of the 1950s and the problems that occurred because of the fake announcement in Italy prove that it becomes even more urgent, the need to analyze the issue of cybersecurity, with the task of describing the outlines of possible remedies and tools of intervention, by looking to the possibility of using, in addition to the usual regulatory instruments, also tools and technical information shared and adopted on a global scale

Venezuela has experienced many hardships since Venezuela, under the authoritarian rule of Nicolás Maduro, remains in a deep economic and humanitarian crisis worsened by the Coronavirus Disease 2019 (COVID-19) pandemic couldn’t develop in the cyber area. The best examples to be given are the blackout on 7 March 2019 that was suspected to be done by U.S. hackers, he said "These attacks were carried out with the use of high scientific achievements, there were electromagnetic attacks against national electric lines.'' The reason behind it was to damage the Guri Dam which is one of the world's largest hydroelectric stations and the main power supply to Venezuela's electrical grid. But we are trying to develop in the cyber world to protect our people’s and country's rights also on misinformation.İn Venezuela about this matter on June 30, 2020, the Atlantic Council’s Adrienne Arsht Latin America Center, in partnership with the Digital Forensic Research Lab (DFRLab), Transparencia Venezuela, and Universidad de Navarra, hosted the event “Trust in Elections and Disinformation in Venezuela.” The virtual public discussion focused on disinformation operations in Venezuela amid a complex humanitarian crisis and their possible impact on December 2020 parliamentary elections. The event was part of the #AlertaVenezuela project, an Atlantic Council initiative to identify, expose, and explain disinformation organizations in Venezuela.

**While cyber-attacks and threats are an ongoing fight, they can be prevented by being aware of the various types of protocols, exploits, tools, and resources used by malicious actors. We have some solutions for his ongoing fight against ‘’fake news’’ and cyber attacks.İn order to maintain the cyber security first solution is to develop an In-house** Many large organizations have their security team in place to perform cybersecurity services. This do-it-yourself policy allows you to take control of your security and privacy with staff that knows your business and it's exact needs. We can put this system into work as the governments. For the purpose that, misinformation is gonna diminish one of the most important things governments around the world can do to reduce the misinformation is to encourage self-sustaining, reel, and professional journalism. Furthermore, Governments should avoid crackdowns on the news media’s ability to cover the news. Those activities limit freedom of expression and hamper the ability of journalists to cover political developments. Plus, Governments should avoid censoring content announcements doesn't have to be pretty but they have to be true. Technology firms should invest in technology to find fake news and identify it for users through algorithms and crowdsourcing. For instance, companies like İntgerrityISR.