Country: Iran

Committee: Disarmament and International Security Committee

Agenda Item: Weaponisation of Data and Cyber Security

Iran is a important middle east country. Geopolitically Iran's location is crucial . Iran, which has signed many physical wars in its history, is now coping with cyber attacks. Iran has a cyber army called the "The Iranian Cyber Army" against attacks by the other countries.

Iran's Cyber Army is a group comprising highly skilled specialists in information technology and professional hackers who avoid revealing their identities. This group is not officially registered and till today no agency or government organization has assumed responsibility for it. Still, incontestable evidence suggests that the group is affiliated with the IRGC (Islamic Revolutionary Guard Corps). Behrouz Esbati holds a key position in the management of Iran's defensive cyber operations as commander of the Cyber Headquarters under the Armed Forces General Staff (AFGS). The AFGS is responsible for coordinating activities between the different branches of Iran's military, namely the Iranian Army and, to a more limited extent, the IRGC. The AFGS Cyber Headquarters appears to play a similar role in the coordination of cyber policy in Iran's military. The Intelligence, Defense and Information and Communication Technology ministries also cooperate with the AFGS Cyber Headquarters to identify weaknesses and track threats to Iran's cyber infrastructure.

Iran is not only the victim of the most prominent cyber-attack to have been conducted to date, the US and Israeli initiated Stuxnet virus which targeted Iranian centrifuges, but also a major source of attacks itself. It may only be a "third tier" power in this area, but it can still do some damage. A few years ago, Google CEO Eric Schmidt pointed out that "Iranians are unusually talented in cyber war for some reason we don't fully understand". We don't want to show our cyber war skills. According to us cyber wars in the whole world must be ended soonly.

As Iran, we propose the creation of an institution that will carry out its work under UNOCT (United Nations Counter-Terrorism Office) and focus only on cyber attacks and massive information pollution. In addition, we should set common and not very inclusive rules for the countries of the United Nations. In our opinion, these may be some of the rules:

-Member countries to have their own cyber rights and rules and declare them on an international platform.

-Member states shouldn’t steal other countries’s datas or attack other countries’s cyber creations and web sites.

-Reliability of local media of the member states should be checked by the creation mentioned above.

-Member states to have sanctions for the offensive hacker groups which are in their country.

References:

- http://www.strato-analyse.org
- https://en.wikipedia.org/wiki/Iranian_Cyber_Army
- https://www.criticalthreats.org/analysis/iranian-cyber-strategy-a-view-from-the-iranian-military
- https://web.archive.org/web/20131003104343/http://blogs.telegraph.co.uk/news/shashankjoshi/100239562/iran-the-mossad-and-the-power-of-cyber-warfare/
- https://www.inss.org.il/publication/?ptype=399