**Committee: GA-1 DISEC**

**State:Ireland**

**Agenda Item:** **Weaponization of Data and Cyber Security**

There is growing concern over the misuse of information and communications technologies (ICT) by terrorists, in particular the Internet and new digital technologies, to commit, incite, recruit for, fund or plan terrorist acts. Member States have stressed the importance of multi-stakeholder cooperation in tackling this threat, including among Member States, international, regional and sub regional organizations, the private sector and civil society.

Even if we are still on early stages of weaponization of data for cyber security but there are countries and big firms who started weaponization of data. As we, Republic of Ireland are on of the countries who think that it is important to weaponize datas and give a special interest to cyber security.

We started to use a new strategy about National Cyber Security in the terms of UN and EU. Ireland’s first National Cyber Security Strategy was agreed by Government and published in July 2015. It set out a road map for the development of the National Cyber Security Centre (NCSC) and a series of measures to better protect Government data and networks, and critical national infrastructure. This period since that time has seen the NCSC grow significantly in scale and capacity, and the introduction of EU Network and Information Security Directive 2016/1148 (NIS Directive), a significant set of measures to support Government Departments and Agencies in managing their systems.

We started our new policy on 2019. And our objectives were:

♣ To continue to improve the ability of the State to respond to and manage cyber security incidents, including those with a national security component

♣ To identify and protect critical national infrastructure by increasing its resilience to cyber attack and by ensuring that operators of essential services have appropriate incident response plans in place to reduce and manage any disruption to services

♣ To improve the resilience and security of public sector IT systems to better protect data and the services that our people rely upon

♣ To invest in educational initiatives to prepare the workforce for advanced IT and cybersecurity careers

♣ To raise awareness of the responsibilities of businesses around securing their networks, devices and information and to drive research and development in cyber security in Ireland, including by facilitating investment in new technology

♣ To continue to engage with international partners and international organisations to ensure that cyber space remains open, secure, unitary, free and able to facilitate economic and social development

♣ To increase the general level of skills and awareness among private individuals around basic cyber hygiene practices and to support them in this by means of information and training.

And our goal is continue use this policies and help other countries about their country’s cyber security.

**References:** <https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf>

<https://www.un.org/counterterrorism/cybersecurity>