- Country: Norway
- Committee: GA:1 DISEC
- Topic: Weaponization of Data and Cyber Security

Cyber Security:

As we are advancing more on technology, we are unconsciously becoming more dependent on it in every domain: from healthcare to finances and most crucially in communication. Now it may seem that technology is the greatest thing mankind ever constituted however inconveniences such as Cambridge Analytica and campaign ads scandal made us have a second though on that. Since cyberspace is an electronic space where access from anywhere is possible it puts both our democracy and our citizens personal space in danger. A recent example can be the intrusion to Norway Parliment`s email system carried out on 19th July 2021. That event made it clear that technology was now a tool and both authorities and civilians were jeopardised.

The Norwegian Ministry of Justice and Public Security is responsible for coordinating public security in the civilian sector. It also has duty of outlining government policies including national cyber security requirements and recommending for public and private companies. However that does not mean they have the full control in technological domain. Since most digital products and services are developed by private companies or research and development communities, Norway`s critical digital infrastructure is owned and operated by private companies. Because of the differences between authorities and private company's responsibilities they supplement each other.

The issue of information security have been on the UN Agenda since December 4th 1998. The draft resolution was introduced by Russian Federation and it was adopted by the General Assembly as resolution 53/70. Since then technological tools used for transferring the information (ICT) in international security are being addressed in UN.

Beginning in 2004 six groups of GGE (Groups of Governmental Experts) have studied the possible threats that ICT brings and how they should be addressed. In total there have been made 4 substantiative reports. In December 2018, the General Assembly established an Open-Ended Working Group(OEWG).Since than 4 session have been organised.

It is hard to speak for Norway`s views on International Security resolutions since Norway did not take part in any of the sessions coordinated by OEWG. However United Nations Secretary-General António Guterres launching his agenda for disarmament and noting "Global interconnectivity means that the frequency and impact of cyberattacks could be increasingly widespread, affecting an exponential number of systems or networks at the same time." He further states that "in this context, malicious acts in cyberspace are contributing to diminish trust among States."Norwegian government's ambition to protect Norwegian citizens life makes us hope Norway will start attending OEWG sessions.

Even though Norway haven't been in many international events related to cyberspace, in "report to the storting (white paper) no.38" published by the Ministry of Justice and Public Security it can be seen that Norway has already though of possible solutions such as:

.Establish and practise a comprehensive framework for cyber incident management

.improve the national operational capability through co-location (majority and minority)

.Increase detection capabilities and compile a situational picture

.Strengthen capacity and expertise related to management of cyber attacks

.Establish a national Cyber Crime Centre

.Ensure strong specialist cybercrime units in the police districts

.Ensure an ICT infrastructure to support police crime prevention

.Ensure the balance between privacy and a more secure society

Weaponisation of Data:

As each day passes we doing more of our work in internet: Paying our bills, shopping , and reading the news.We may be thinking that our money is safe in our online bank account just as our personal information in social media but the "Cambridge Analytica Scandal" proved to us that our dependency on social media gives the ones in control to analyse and even lead our own thoughts.

In 2017, the national representative from the Progress Party Mazyar Keshvari incriminated the national daily Aftenposten of publishing fake news about immigration policy. Mazyar Keshvari expressed that this was an attempt to make readers view both him and the authorities in a particular way. He also argued that media tried create that view by selectively choosing the informations and comments and systematically placing them.

Even though scandals related to misinformation happened in Norway, the misusage of the term "misinformation" is looked down upon. Former Norwegian Minister of Culture from the conservative party, Linda Cathrine Hofstad Helleland saying "One should be very careful to define fake news based on a dislike of the the premise or the framing of a story " both explains the attitude towards the misusage of the word misinformation and points out the responsibilities that politicians have while making an accusation. These attitudes from powerful political figures may be why for the sixth year, Norway is heading the new World Press Freedom Index from Reporters Sans Frontiers (RSF).

Norwegian journalist had ambivalent feelings towards fact checking formats. Some believed that it would improve the quality in reports, while others had suspicions towards relying on a single source. Despite this Norway was the first Scandinavian country to develop fact checker : Faktasjekk (2005-2009) and 3 more between 2009-2017. This is main reason why Norwegians trust nearly 50% of the news overall.

Even though Norway has done an outstanding job identifying the issues related to cybersecurity and coming up with possible solutions nationwide, it still is inadequate when it comes to cyber attacks and propaganda targeted towards Norwegian civilians.

In CASHMUN 2022 study guide weaponisation of data was analysed brilliantly and possible solutions about unethically usage of our data where written.

One solution that we found applicable was to set limits on how companies and governments are able to use data of citizens. We need designated laws that should make companies both be transparent about their usage of personal data and stopping them accessing data where it violates citizens personal space. Failure to submit to these regulations should meet with financial penalty and all of the contributors of the exceeding should be judged on International Court of Justice.

In conclusion there are many possible solutions for both cyber security and weaponisation of data. We believe having a fact checker such as Faktasjekk coordinated by authorise across the UN might make it harder for misinformation to travel across the countries and lead the public to wrong ideas. As for the setting the regulations it may be hard to control since some countries are opposed to idea of not using personal data such as: China and Russia.

References:

https://static1.squarespace.com/static/57b632432994cab0b44562ae/t/623010923955d33f327e674c/1647317139127/DISEC+backgrounder+b+final.pdf

https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/414/62/PDF/N2141462.pdf?OpenElement

https://www.unidir.org/conferences/un-cyberspace-and-international-peace-and-security

http://www.munish.nl/pages/downloader?code=spc201&comcode=spc2&year=2019

https://www.ohchr.org/sites/default/files/Documents/Issues/Expression/ICCPR/Vienna/Annexes/Norway.pdf

https://inews.co.uk/inews-lifestyle/money/why-cant-we-do-free-and-trusted-media-like-the-norwegians-1617386

https://inews.co.uk/inews-lifestyle/money/why-cant-we-do-free-and-trusted-media-like-the-norwegians-1617386

https://www.cyberwiser.eu/sites/default/files/national-cyber-security-strategy-for-norway.pdf

https://www.regjeringen.no/contentassets/39c6a2fe89974d0dae95cd5af0808052/en-gb/pdfs/stm201620170038000engpdfs.pdf