Committee: Disarmament and Security Council

Country: Republic of Lithuania

Agenda Item(s): Weaponization of Data and Misinformation

Lithuania, the biggest country of the Baltic States; with Russia, Poland the Baltic Sea to its west, Belarus and Latvia to its east, is located in Eastern Europe. It is a member of the European Union since 2004 and a member of the Eurozone as of 2015. With a population of just under 2.9 million, country’s government type is a semi-presidential republic. Lithuania is a developed country, with a high-income advanced economy; ranking very high in the Human development Index and has an estimated purchasing power of 102.7 billion dollars.

Misuse and weaponization of data is a global issue at the moment. Even simple magazine websites are making thousands of dollars just by claiming a celebrity is pregnant. Not only this is an invasion of the person’s privacy whom the article is about, but also very confusing for the readers. News websites are doing the same thing in a bigger way; big companies like Twitter and Meta are making millions if not billions by selling people’s personal data, which should be privileged, to other companies. And these examples are the very small tip of the iceberg.

Lithuania published a comprehensive cyber security strategy in 2011, nevertheless there are still some loop holes in this policy; besides the information on its implementation remains limited. From what we know, some of the main problems with this strategy is:

* There isn’t any legislations/policies that requires the establishment of a written information security plan.
* There isn’t no discrete critical infrastructure protection strategy or plan in place.
* There isn’t any legislations/policies that requires the establishment of a written information security plan.
* There is no legislation or policy in place in Lithuania that requires a public report on cyber security capacity for the government.
* There is no defined public-private partnership for cybersecurity in Lithuania.
* There is basically no sector-specific cybersecurity plan.

The Strategy's implementation aims to strengthen the state's cyber security and develop cyber defense capabilities, as well as to ensure the prevention and investigation of criminal offenses committed using cyber security objects, to promote a cyber-security culture and innovation, to improve public-private collaboration as well as international cooperation, and to ensure the fulfillment of international obligations.

4 years after this strategy in 1 January 2015, the new Lithuanian Law on Cyber Security defining the organization of a cyber-security system, its management and control, has entered into force. This law established the authorities in charge of developing and implementing cyber security policies, as well as their competences, functions, rights, and responsibilities.

And being not so independent from cyberwarfare, data weaponization and “fake-news” are huge problems both globally and nationally. There isn’t any one ultimate definition of fake news, but as a working definition we assume in this paper that disinformation or fake news means deliberately presenting false information as new to profit an individual or a group”

Traditional media organizations solve this problem of fake news by verifying presented information. With digital media, however, search engines and social media networks are in charge of communication. The latter see themselves as technological companies and, for the most part, reject any social responsibilities that traditional media companies are required to follow. Over the last years, main social media platforms like Facebook, Twitter, and Google have been heavily criticized for allowing false information to spread on their platforms. So, the trust towards traditional and online media is rapidly decreasing, meaning that the liability of the souces are rapidly decreasing as well.

We as the Republic of Lithuania not only acknowledge the fact that cyberspace is being used as a new separate military space and a tool for hybrid warfare, but also as of 2011 have been taking action about it continuously. We see and acknowledge that there are much more we can do about this. So, we are ready to cooperate with other countries to decrease weaponization and misuse of data in a noticeable amount.

References:

https://ccdcoe.org/uploads/2018/10/Lithuania\_Cyber-Security-Strategy-2018\_English.pdf

https://cybersecurity.bsa.org/assets/PDFs/country\_reports/cs\_lithuania.pdf

https://data.worldbank.org/country/LT

https://www.cia.gov/the-world-factbook/static/18699e77bcb0bc15988ab1d1f2dad9d9/LH-summary.pdf

https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ceb0e7b291ad11e8aa33fe8f0fea665f?jfwid=

https://en.wikipedia.org/wiki/Lithuania

https://www.orangesmile.com/common/img\_country\_maps/lithuania-map-0.jpg

https://cejc.ptks.pl/attachments/cejoc132-1-88-106\_2020-06-24\_09-19-13.pdf