Committee: DISEC (Disarmament and Security)

State: Spain

Agenda Item: Weaponization of Data and Cyber Security

Spain seems to be among one of the biggest victims of cybercrime out of the major European nations. Spain’s biggest cyber-attack endured 2011, affection of Telefonica, a Spanish multinational telecom company, by ransomware. Many users has badly affected by this attack due their own data is locked and the only possibility for them to access their data, was doing a payment to an anonymous account. As we have faced a cyber-attack of a big company before, we can definitely say that cyber-attacks of big companies has many risks of data theft for personal data of users or private data of companies. Stolen data can be weaponised and can be used against companies or persons. We firmly believe that providing the security of data by avoiding cyber-attacks is a global issue and it is the basis of avoiding data theft and Weaponization of data.

We used to deal with the issue by laws about data theft and by creating national organizations such as The National Centre for Critical Infrastructure Protection (CNPIC), The National Advisory Council on Cyber Security (CNCCS) and The National Advisory Council on Cyber Security (CNCCS). We are also part of Fourteen Eyes network, an intelligence alliance between major countries around the world, aiming to monitor cyber data to protect people. Some of the countries included in this network is the United States, the United Kingdom, France and Australia. Education of public and raising awareness regarding cyber-attacks used to have a big focus of our National Cyber Security Strategy. We believe that our people has to know what they are dealing with and this is one of the best ways to provide protection. Compared to the United Kingdom or Germany, the progress in our country has been slower.

Spain advocates that, for countries it is necessary to act collaboratively to ensure data security. With the developments of technology, the amount of data is increasing day by day. When the amount is large, it becomes difficult to prevent data theft in any cyber-attack. In order to improve security, data needs to be audited from multiple places. In this objective we want to discuss about feasibility of an international cyber security organisation. As data theft and Weaponization of individual’s personal data is a violation, we defend the requirement of strict laws. We believe, it is also important for the public to be conscious about protecting their own data. While the government is working on data security, the public should also do their part. Countries must work for ensuring awareness raising of their public.

References:

Cybersecurity in Spain – by Bernard Meyer. Accessed 5 June 2022 <https://cybernews.com/security/cybersecurity-in-spain/#:~:text=The%20primary%20cybersecurity%20institution%20in,and%20responding%20to%20cyber%2Dattacks>.

5-Eyes, 9-Eyes, and 14-Eyes agreement explained - by Tadas Švenčionis. Accessed 6 June 2022 <https://cybernews.com/resources/5-eyes-9-eyes-14-eyes-countries/>

COUNTRY: SPAIN. PDF file <https://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_spain.pdf>

Cybercrime Laws – Spain. Accessed 6 June 2022 <https://www.cybercrimelaw.net/Spain.html>

# Major Spanish firms among victims of massive global cyber-attack. Accessed 6 June 2022 <https://english.elpais.com/elpais/2017/05/12/inenglish/1494588595_636306.html>