

Country: Republic of Poland

Committee: DISEC

Agenda Item: Weaponization of Data and Cyber Security

The Republic of Poland is a unitary parliamentary republic located in Central Europe. With a population above 38 million, it is the eighth-most populated country in Europe. It borders Russia (Kaliningrad Oblast) and Lithuania to the northeast, Ukraine and Belarus to the east, the Czech Republic and Slovakia to the south, and Germany to the west. A technologically developed country, Poland’s information and communications technology market was estimated to value at 20.27 billion U.S. dollars in 2021. Because of this development in the information technologies field, Poland has always prioritised cybersecurity and data safety.

Every click on the internet contributes to the largest database the world has ever experienced, the internet. By performing basic actions and answering questions, a user contributes their personal information to the internet, unaware of where and how it will be stored. It is no surprise that all this data is controlled and manipulated by dominant figures for their benefit. The weaponisation of data has taken place in various forms throughout history, but the recent developments in communication technologies put the world at greater risk of malicious actions. Many institutions and governments collect people’s information without their consent and use it for their gain. In addition to being a violation of human rights; it is a significant threat to world peace if the data gets weaponised. Current laws cannot keep pace with the rapid evolution of technology. The Republic of Poland is willing to take the appropriate steps to ensure its citizens’ security and rights.

The Republic of Poland has been working diligently on securing the country’s information since the earliest days of modern technology, and the current crisis proved that those efforts were not pointless. The Russian invasion of Ukraine has put Poland, their mutual neighbour, at a greater risk of cyber attacks. The Polish Prime Minister’s Office reported a rise in distributed denial-of-service (DDoS) attacks against Polish institutions and domestic entities. Fortunately, Poland is not unprepared for such cybersecurity issues. The Polish Ministry of Digital Affairs was established in 2015 as one of the first worldwide. There are three nation-level computer emergency response teams (CSIRT) that form the national risk management system: the Internal Security Agency CSIRT, the National Research Institute CSIRT, and the Ministry of National Defence CSIRT. Those institutions operate in accordance with the *Act on the national security system*; they collaboratively recognise, prevent, record, and handle any events that violate network security. The CHARLIE-CRP level three alert was in effect from February 21 to March 15 due to increased attacks on government websites; the situation was taken under control owing to the comprehensive national cybersecurity system, and there was no substantial impact on the security of Poland.

We fully believe that its citizens’ private information is just as important as national data. People can better sense the dangers and protect their information when they are informed about the risks of the internet and how their data can be exploited.

One of the main goals of Poland’s strategy is to educate the citizens about cybersecurity. Modern societies are almost entirely dependent on digital technology, yet few know the truth behind it. Children and youth should undergo cybersecurity education before they enter the digital world in order to start learning the skills they will use throughout their lives. Schools play a crucial role in this aspect. Teachers should be guided in explaining this topic to students and be provided with the resources they need for this. Websites should be required to be fully transparent about whom third-party cookies are collected for and how they will be used. People need to know how their data is going to be used before they can genuinely consent to it. Additionally, the general population should be informed about misinformation and ways to verify the news they heard in order to avoid getting manipulated. There should be stricter regulations on the accuracy of the news and heavier penalties for misinformation. To take these cautions to an international level; the Republic of Poland supports the idea of creating an international law system that prevents and eradicates the weaponisation of data. We are interested in hearing other countries’ opinions and ideas regarding the details and effectiveness of this law system.

The Republic of Poland is aware that data misuse violates the fundamental human right of privacy and puts world peace in danger. In a world where our daily life revolves around the internet, every person must be able to perform vital actions safely. We are ready to take the necessary steps to ensure data safety and eliminate any conflicts.

**References:**

SAS, Adriana, “Value of the ICT market in Poland 2020-2021”, *Statista,* July 2021, <https://www.statista.com/statistics/1258937/poland-value-of-the-ict-market/>

[www.gov.pl](http://www.gov.pl), Cybersecurity Strategy of the Republic of Poland for 2019 – 2024

<https://www.cia.gov/the-world-factbook/countries/poland/#introduction>

<https://polishnews.co.uk/charlie-crp-alert-level-in-poland-there-is-a-decision-on-the-extension/>

<https://acn-marketing-blog.accenture.com/wp-content/uploads/2022/05/ACTI_POV_UkraineCrisis_20220428_TLP-WHITE-FINAL.pdf.pdf>

<https://www.euractiv.com/section/cybersecurity/news/cyber-incidents-on-the-rise-in-poland-no-major-impact-signalled-yet/>

<https://en.nask.pl/eng/activities/csirt-nask/3424,CSIRT-NASK.html>

<http://archiwum.mc.gov.pl/en/the-areas-of-our-activity>

<https://www.marshmclennan.com/insights/publications/2020/apr/we-need-to-start-teaching-young-children-about-cybersecurity.html>

<https://securiti.ai/blog/third-party-cookies/>