 Committee: GA1:DISEC

Topic: Weaponization of Data and Cyber Security

Country: Hungary

Hungary is a landlocked country in central Europe, neighbors; Austria and Slovenia to the west, Slovakia to the north, Romania and Ukraine to the east, and Serbia and Croatia to the south. Hungary, whose capital is Budapest, is a member of the OECD, NATO, EU, Visegrád Group and Schengen. The official language is Hungarian. Population 9,730,000 in 2020. Hungary's economy is the 57th largest in the world. At the same time, Hungary focuses on foreign trade and is therefore the 35th largest exporter in the world. The main economic branches are food processing, pharmaceuticals, motor vehicles, information technology, chemicals, machinery, electrical products and tourism. Over the past 20 years, Hungary has also become an important hub for mobile technology, information security and related hardware research.

Before we get into these, what does data mean, what is the weaponization of data? The way that the information in the computer environment is compiled and formulated in order to ensure that it can be processed by programs is called data. We can call the weaponization of data an attack over the data in short. There have been many incidents related to this (weaponization of data) from past to present. An example of this is the allegations that Russia interfered in the elections of a country that invested heavily in cyber security, such as the USA, brought cyber attacks to the agenda of the world again. Previous attacks on Iran, Ukraine, North Korea and many other countries had serious consequences; power cuts, internet access barriers, personal data theft caused considerable damage. However, so to speak, such a huge and sensational cyber attack between these two poles of the world, east and west, attracted the most attention. Of course, as it happens to every country, a cyber attack has happened to our country, Hungary. To describe the event briefly; The primaries in Hungary have been suspended due to a cyber attack. According to Channel New Asia, the reason for the suspicion of the attack was the collapse of the system. Officials said they needed 36 hours to investigate the matter. Let me now talk about Hungary's work on these issues. Hungary does not see any country as a competitor and wants to solve its problems peacefully based on international law and the UN Convention. Hungary attaches great importance to cooperation and involvement in the structure of multilateral organizations. For this reason, NATO and EU membership is the basis of Hungary's security policy. In addition, they know how important information technologies are for the state. It is also aware that the unstoppable spread of scientific and technological developments and the efforts of these technologies by states, non-state actors and even terrorist groups to disrupt the normal flow of the state's information technologies and communication system will pose a risk to Hungary, and is ready to deal with threats and risks to its cyber defense and is ready to deal with critical national ensures the security of the infrastructure. They provide this security with the "National Cyber ​​Security Strategy of Hungary", which was prepared in line with the principles on cyber security and adopted on March 21, 2013, and then the "National Security Authority", which was established on July 1, 2013 to deal with cyber security. In addition, in the global cyber security index of the International Telecommunication Union, Hungary ranks 12. out of 76 countries.

We think Hungary has been very successful in this regard. Of course, this can increase its success. There are several ways to do this. To give one example; a search engine that does not accept fake news can be developed.

<https://en.wikipedia.org>

<https://docplayer.biz.tr/>

<https://afyonluoglu.org/>

<https://thinktech.stm.com.tr/>

<https://tr.euronews.com/>

<https://www-avrupa-info-tr>