**Country: Republic of Estonia**

**Committee: United Nations General Assembly First Committee (the Disarmement and International Security Committee)**

**Agenda Item: Weaponization of Data and Cyber Security**

Republic of Estonia is a Northern European country located in the east of the Baltic sea . It is bordered to the north by the Gulf of Finland across from Finland, to the west by the Baltic Sea across from Sweden, to the south by Latvia, and to the east by Lake Peipus and Russia.

After Estonia gained its independence in the early 1990s, there was no communication infrastructure other than the copper wire infrastructure left by the Russian army when leaving the country. It was impossible to know how these lines, which were left from the Russians, connecting the communist party, the KGB, the military intelligence, the railways and some of the party's organs, were also connected to each other, because no infrastructure diagram or map was left . However, the new Estonian government saw the lack in this area as an opportunity and encouraged R&D work in the fields of information technology and telecommunications. As a result of these studies, the country has made many innovations. For example, the software used in the preparation of Skype was of Estonian origin. In 2005, for the first time in the world, the Estonian government offered its citizens the opportunity to vote electronically. In this period, nearly 60 percent of the people were in need of the internet for a significant part of their daily needs. Approximately 96 percent of banking transactions in the country were carried out online. Therefore, in the country where every citizen has a digital identity that allows them to connect to government institutions and banks over the internet, there were 355 government agencies in the virtual world.

Launched in 2001, the data exchange layer X-Road program connects Estonian public institutions and citizens. This is the most common application example in terms of e-government applications. However, in this whole process where important breakthroughs were experienced, the information technology infrastructure was giving a weak appearance because the Estonian government did not do the necessary studies on internet security and cyber defense. In other words, this situation in Estonia both drew the reactions of ethnic minorities in terms of political conjuncture and strengthened the possibilities of cyber attacks in terms of technological infrastructure. Ultimately, the Parliament's decision to remove the Bronze Soldier statue in Tallinn square not only drew strong reactions from the ethnic Russian minority, but Russia also reacted strongly to the decision. Finally, on the evening of April 26, 2007, a large-scale cyber-attack of unknown origin had begun. It was not possible to detect the attacks in the first 24 hours. The first targeted site was the web page of the ruling Reform Party. In a short time, the pages of other political parties, state websites and the Estonian Parliament had to shut down their servers as a result of attacks.

At the point reached today, the role of the Russian state in the attacks is unknown. In fact, shortly after the attacks began, Estonian government officials openly blamed Russia. It was even detected that one of the followed attacker IPs belonged to the Russian state. However, it soon became clear that this computer was also a zombie. Today, it is estimated that the attackers are largely composed of people with hacking experience, mostly organized in Russian on blog and forum pages. It can be said that hackers mostly acted on their own, although it is possible that they were somewhat manipulated by the Russian state.

After these attacks, Estonia established a Cyber Defense Unit consisting of volunteers, focusing on cyber security. This unit was strengthened by training the country's leading IT specialists, selected through security screening and protected anonymity, by the Ministry of Defense. These volunteers are the type of private sector resource that the government can't usually employ. They use their spare time to defend their country in the event of a cyber attack on a government agency or a vital service provider. Since the early days of Estonia's digital transformation, the government's philosophy has always been to utilize private sector services, not to employ programmers in the public sector. This is the international competitiveness of the Estonian IT sector.

Cyber attacks on Estonia became a milestone in terms of international security. It has started discussions on when cyber attacks are considered a cause of war and how we should perceive them. Many countries, especially the UK and the USA, have started to determine a cyber security strategy. Therefore, the fact that the Estonian cyber-attack is considered the "first" lies in the capacity of global states to revise their defense policies.

As Estonia, we have been exposed to such situations a lot, especially after the massive attack we experienced in 2007, we became conscious about cyber security and we are trying to take our measures as much as we can in this regard. That's why we think that the creation of a national cyber army that will always be present and the establishment and development of two institutions that will prevent the emergence and spread of fake news in the country are very important for the existence and security of our country, and we will do our best to establish and develop these institutions. Internationally, we think that the United Nations' establishment of an institution that will monitor countries in cyber terms by establishing certain criteria has a very important place in terms of ensuring international peace and security.

**SOURCES**

-https://e-estonia.com/

-https://en.unesco.org/courier/2017-april-june/global-lessons-estonia-s-tech-savvy-government

-https://www.bbc.com/news/business-22317297

-www.bbc.co.uk

- https://en.wikipedia.org/wiki/Estonia

- https://www.bbc.co.uk/turkish/news/story/2007/05/070517\_estonia\_cyber.shtml