**Country: Australia**

**Committee: GA1: DİSEC**

**Topic: Weaponization of Data and Cyber Security**

Weaponization of data means to use information at someone else’s expense. The marketing world is full of war metaphors designed to help marketers destroy the competition and win the battles they face every day. And It is thought that the weaponization of data in cyberattacks is becoming one of the biggest threats in the World. In 2021, there is an 82% increase in ransomware attacks compared to 2020, which involves weaponization of data or stealing data that attackers threaten to leak to the internet if their ransom demands are not met.

And Cybercrimes are the crimes that target the security of information system or the data connected to it or the user and are committed using the information system. This type of crime can also be called computer and internet spesific crimes. From the perspective of the Cybercrime Convention, cybercrime is the unauthorized and unlawful access to information system. In this crime, the target may be a person or the property of the person or the system itself. For example, actions such as damaging a system, deleting data, encrypting, adding data, preventing the use of the system, interfering with the privacy of private life, preventing communication, monitoring and recording communication without permission are considered in the category of cybercrime.

The Annual Cyber Threat Report, prepared by the Australian Cyber Security Center (ACSC) in collaboration with the Australian Criminal Intelligence Commision and the Australian Federal Police, revealed that nearly a quarter of all cyber security incidents affect critical infrastructures such as health, education and transportation. President of the ACSC, who prepares the report which includes key advice that can help Australians and Australian organizations protect themselves online from cyber attacks, took attention that malicious cyber actors are actively targetting Australians. After reviewing the report, Australian Deputy Defense Minister said that it is necessary that there should be more cyber security precautions for helping the struggle to the increase of cyber attacks. And Australian organisations are encouraged to urgently adopt an enhanced cyber security posture. organisations should act now and follow ACSC's advice to improve their cyber security resilience in light of the heightened threat environment.

There are some steps taken to prevent cyber attacks in our country. For example, an Australia-based company CSO Group has signed a four-year cybersecurity agreement to provide security, intelligence and remediation to the New South Wales (NSW) Department of Communities and Justice (DCJ). The 7 million dollars deal includes CSO Group’s Security Monitoring Service, Security Operations Center (SOC) solution. The contract is a part of New South Wales Deparment of Communities and Justice’s cyber renewal program and in addition to a 16 million dollars deal to the CSO Group to deliver new cybersecurity solutions for cloud, endpoint and email.

The Information and Privacy Advisory Committee, established by the NSW government at the end of last year, which aimed to provide the government with information, advice, assistance and training in how to best deliver information and privacy management practices. The committee is also tasked with facilitating cooperation between government, industry and academia. The state government has made a 240 million dollars commitment to improve NSW’s cybersecurity capabilities, including investments in maintaining existing systems, deploying new techologies and increasing its cyber workforce. The fund aims to create an army of NSW-affiliated cyber experts.

For another example of our initiatives to prevent cyber attacks is the 17 milliom dollars fund that we have allocated to empower the cybersecurity capabilities of our neighbour countries. Main aim of this project is creating an international framework to struggle to cyber crimes. Also Australian Government aims to support a new United Nations Action Program. And It is stated that there will be a new and permanent United Nations Forum to continue debates and bring this initiative to real life. Among the countries that Australia will support are the small island states in the region. This island states include Fiji, Samoa, Solomon Islands, Tonga and Vanutau.

**References:**

“Advisory issued for Australian Organisations”, updated on 28th of April 2022: <https://www.cyber.gov.au/>, <https://www.australia.gov.au/>

“International step to fight cybercrime for Australia”, updated on 22nd of April 2021: <https://sigutr.org/>

“More than 67,500 cyberattacks in a year in Australia”, updated on 15th of September 2021: <https://www.haberturk.com/>

“What is cybercrime?”: <https://www.egm.gov.tr/>

“Weaponizing Data versus Using It As a Tool To Humanize Consumers”, updated on 28th of October 2020: <https://www.forbes.com/>

“Impact of ‘ Weaponization of Data’ Attacks on Healthcare”, updated on 23rd of February 2022: <https://www.govinfosecurity.com/>

“Australia’s Cybersecurity Commited to a Company”, updated on 10th of July 2021: <https://www.pugat.org/>