BOTANY

Ethical Questions in Cybersecurity

DESCRIPTION

The game specifically examines the influence of external cyber-attacks on electoral processes and which defensive or offensive strategies attacked nation states have to guarantee fair elections.

SCENARIO & PROCEDURE

Botany is a middle-sized western pro-European country that finds itself in the middle of the presidential elections. An anonymous hacker informed the government of Botany that the autocratic state of Hackania is about to conduct a multi-level cyber-attack on all electoral channels possible to manipulate the electoral process. This alarming news puts the current Administration under huge pressure and a quick response is needed, which exposes the current Administration to a variety of dilemmas on the national and international level. Slipping into the roles of different stakeholders such as politicians, as well as representatives of Intelligence agencies, privacy organisations or social media giants, participants are required to decide how a nation state should react to a cyber-threat coming from an external source. Therefore, the Botanian Advisory Council for Cyber Security (ACCS) comes together for an emergency meeting. In two committees, politicians and experts from different sectors discuss what measures are to be taken on the national and international level. Ethical questions emerging from this discussion mainly regard privacy vs. security topics, the potential violation of international law, whether or not this kind of cyber-attack should be considered an act of war, which agencies should be responsible for navigation, reaction, and finally the authorization of a nation state to apply offensive strategies to fight a cyber-attack. The ACCS is supposed to formulate recommendations for the President of Botany for potential reactions.

AIMS

The main goal is engage participants in the current ethical and legal questions around possible responses of states to cyber threats and cyber-attacks. The game sets out to promote a comprehensive understanding of interests of different stakeholders within an emergency situation and how diverging interests can be bridged to come to possible conclusions. Thus not only a change of perspective and coherent argumentation is needed, but also the participant's willingness to engage with the complex and abstract thematic of cybersecurity and cyber defense strategies.

Learning Targets:

- Understanding ethical and legal dilemmas within cybersecurity and cyber defense
- Engagement with interests of different stakeholders from different agencies in the cyber world
- Personal negotiation skills in order to persuade others and to formulate comprehensive policy recommendations

Target-Group: Specialists dealing with strategic communication and cyber security
Participants: 20-30
Duration: 4 hours up to 1 day
Type: fictitious
Languages: English