

# Batch: *A-4* Roll No.: *16010422211* Experiment No.: 02

**Aim:** Study of Cyber Law for Specific country.



**Resources needed:**



# Theory:

# (Students need to write the comntent here)

# *GREECE*

# *The Greek National Cyber Security Strategy (NCSS) was implemented on September 1, 2017, and it serves as a comprehensive plan for enhancing cybersecurity in Greece. The strategy establishes the primary principles, strategic objectives, and the framework for action to achieve these objectives. The implementation of the NCSS is overseen by the newly created National Cyber Security Authority.*

# *The eight individual objectives outlined in the NCSS are:*

# *1. Upgrade the level of prevention, evaluation, analysis, and deterrence of threats against the security of ICT systems and infrastructure:*

# *- This objective focuses on enhancing Greece's ability to prevent, assess, analyze, and deter threats against its information and communication technology (ICT) systems and critical infrastructure. It includes measures to strengthen cybersecurity defenses and identify potential threats early.*

# *2. Enhanced ability of public and private sector stakeholders to prevent and handle cybersecurity incidents and to improve the resilience and recoverability of ICT systems following a cyber-attack:*

# *- This objective aims to improve the readiness of both public and private sector entities in Greece to prevent, respond to, and recover from cyberattacks. It emphasizes the importance of preparedness, incident response, and resilience.*

# *3. Create an effective coordination and cooperation framework by determining the individual competences and roles of the various public and private sector stakeholders involved in the implementation of the National Cyber Security Strategy:*

# *- To ensure effective implementation of the NCSS, this objective focuses on establishing a clear framework for coordination and cooperation among various stakeholders. It defines the roles and responsibilities of both public and private sector entities involved in cybersecurity efforts.*

# *4. Ensure the State's active participation in international cybersecurity initiatives and actions by international organizations, for the enhancement of national security:*

# *- This objective underscores Greece's commitment to participating in international efforts to enhance cybersecurity. It involves collaborating with international organizations and initiatives to strengthen national security and address global cyber threats.*

# *5. Make all social institutions aware and inform users regarding the secure use of cyberspace:*

# *- This objective promotes cybersecurity awareness and education among all segments of society, including institutions and individual users. It aims to empower people with the knowledge and tools needed for safe online behavior.*

# *6. Continuously adapt the national institutional framework to new technological requirements and to EU directions for effective handling of illegal acts linked to cyberspace activity:*

# *- This objective acknowledges the evolving nature of cybersecurity and the need to adapt to emerging threats and technological advancements. It also emphasizes alignment with European Union (EU) directives for effective cybersecurity management.*

# *7. Promote innovation, research and development in security issues and cooperation between the stakeholders involved:*

# *- This objective encourages innovation, research, and development in cybersecurity technologies and practices. It promotes collaboration between stakeholders to drive advancements in security measures.*

# *8. Make use of best international practices:*

# *- This objective underscores the importance of learning from and adopting international best practices in cybersecurity. It encourages Greece to draw upon successful approaches and strategies used by other countries and organizations.*

# *The Anti-Crime Policy Program in Greece focuses on specific goals concerning cybercrime and ICT-facilitated crimes:*

# *1. Tracing of individuals or networks activated in trafficking child pornography:*

# *- Goal: Identify and combat child pornography networks and individuals involved in such activities.*

# *- Actions:*

# *- Continuous education and training for the staff of the Directorate of Electronic Crime Prosecution, both in Greece and abroad, to enhance their expertise in investigating child pornography cases.*

# *- Cooperation with foreign law enforcement agencies through international channels like INTERPOL and EUROPOL for tracing and prosecuting offenders with international connections.*

# *2. Fighting against cyberbullying:*

# *- Goal: Combat online harassment and bullying.*

# *- Actions:*

# *- Education and training of officers in the Directorate of Electronic Crime Prosecution to address cyberbullying cases effectively.*

# *- Implementation of informative conferences and seminars to educate parents and students about safe internet use and how to avoid becoming victims of cyberbullying.*

# *3. Fighting against internet fraud:*

# *- Goal: Prevent and combat various forms of internet fraud.*

# *- Actions:*

# *- Strengthen cooperation with the Hellenic Banks Association to prevent and address internet-related financial fraud.*

# *- Collaborate with relevant authorities to secure evidence and handle internet fraud cases efficiently.*

# *4. Fighting against circulation of forged traveling documents and drugs via the internet:*

# *- Goal: Identify and combat the illegal circulation of forged documents and drugs online.*

# *- Actions:*

# *- Cooperation with the Directorate of Electronic Crime Prosecution to methodize the appropriate procedures for securing evidence in cases involving the internet.*

# *- Collaboration with international law enforcement agencies through channels like INTERPOL to address crimes with international dimensions.*

# *5. Fighting against human trafficking victim solicitation via the internet:*

# *- Goal: Prevent and combat the solicitation of human trafficking victims online.*

# *- Actions:*

# *- Ongoing patrols on the internet to prevent and suppress such criminal activities.*

# *- Cooperation with foreign law enforcement agencies to address international human trafficking cases via legal communication channels like EUROJUST.*

# *6. Fighting against intrusions-cyber attacks:*

# *- Goal: Detect and counter cyberattacks and unauthorized intrusions.*

# *- Actions:*

# *- Continuous education and training of staff in the Directorate of Electronic Crime Prosecution to improve their skills in handling cybercrime cases.*

# *- Daily patrols on the internet to proactively prevent and suppress cybercriminal activities.*

# *7. Dissuasion of suicides announced on the internet:*

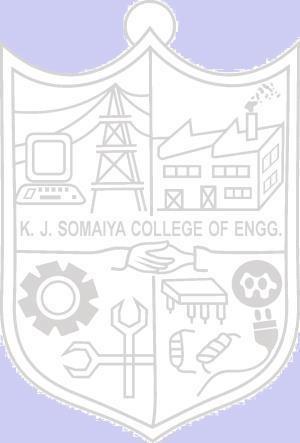
# *- Goal: Prevent and address online content related to suicide announcements.*

# *- Actions:*

# *- Implementation of a memorandum of police actions for managing signs of suicidal intentions expressed online.*

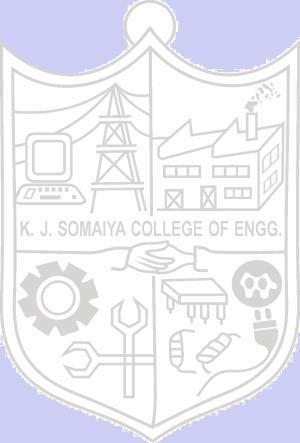
# *- Active participation in public awareness campaigns to inform individuals about the dangers of such content and provide guidance on appropriate interventions.*

# *Overall, the Greek National Cyber Security Strategy outlines a comprehensive approach to cybersecurity that encompasses prevention, preparedness, response, cooperation, and continuous improvement to protect the country's critical infrastructure and digital assets. These goals and actions form a comprehensive strategy in Greece to combat various forms of cybercrime, protect victims, and ensure the safe use of the internet. This strategy involves a combination of education, training, cooperation with international agencies, and proactive monitoring of online spaces to achieve its objectives.*





**Procedure:give the steps which you have followed .**





**Results: (Document printout/handwritten)**

.



# Outcomes:



**Conclusion:**

**References:(students need to write the refernces they have used)**

1. Nina Godbole, Sunit Belapure Cyber Security-Understanding “CyberCrimes,ComputerForensics

and Legal Prespectives”, Wiley- India 1st Edition, 2011

2. N S Nappinai Technology Laws Decodded, LexisNexis 1st Edition, 2017

3. Nandan Kamath Laws relating toComputers, Internet and E- Commerce Universal Law Pub. Co.,

2000 5th Edition 2012