Intermediate Topics in Cybersecurity

Konstantinos Karampidis[1], Emmanouil Lionakis[1] , Giorgos Papadourakis[1], Giorgos Kornaros[1], Przemyslaw Szczepanczyk[2], Rui Silva[3],

[1]Hellenic Mediterranean University
Department of Electrical and Computer Engineering
Heraklion, Crete 71410, Greece
{karampidis@hmu.gr}
{mtp318@edu.hmu.gr}
{papadour@hmu.gr}
{kornaros@hmu.gr}

[2]Lipinski University
Kielce Poland
{przemyslawszczepanczyk@lipinski.edu.pl}

[3]Instituto Politécnico de Beja
Beja Portugal
{rui.silva@ipbeja.pt}

Abstract: Intermediate topics in Cybersecurity is a three year European-funded project dedicated to raise awareness and strengthening the knowledge gap on cybersecurity. By fostering a network of experts and promoting cyber resilience, the project aims to establish the project's methodology as a recognized standard in cybersecurity education. Its activities span the creation of an online course focusing to four modules, namely i) Organised disinformation and threats in social media ii) Standards and recommendations in cybersecurity management iii) ENISA cybersecurity skills framework and iv) Use of AI in cybersecurity. Each module will comprise a syllabus, 50-100 pages of text & graphic content, an online lesson (60-90 mins. of audio and images), an introductory video (5-10 mins.), exam questions and quizzes, case studies with branching scenarios and a 20 page teachers' book with additional ideas for use in a regular classroom setting (group activities, discussion topics etc.). The expected outcomes include a significant boost in cybersecurity awareness and skills across students, the creation of an advanced training program tailored to today's needs and enhanced capabilities among instructors to teach cybersecurity effectively.