ABSTRACT
As the IoT technologies continue to permeate communities of all sizes, the nation’s cyber and cyber-physical assets are vulnerable in proportion to the increase in connectedness. Critical infrastructures, including the national power grid, health care systems, transportation systems, are highly vulnerable to cyberattacks [1-2]. So are the technologies that make cities SMART. As one author stated, “...the Internet of Things (IoT), the technology underpinning these complex and interconnected urban networks, offers a considerably expanded attack surface for cyber adversaries of all kinds...”[3]. Researchers agree that the human factor plays a crucial role in preventing and limiting the impact of a cyber incident. Recent reports from various cybersecurity and data analysis firms[4-5] clearly show that human error causes up to 90% of the data breaches for corporations. Despite this, more than 40% of employees do not get regular cybersecurity training[6]. This lack of training and the resulting inadequate awareness of the connectedness is an individual gap that we aim to lessen. Even more startling, cybersecurity experts agree there has been an exponential increase in cybercrime during the ongoing COVID-19 crisis. While government agencies and the private sector have implemented available security frameworks[7-8], an organizational gap exists as many state, local, and critical private sector organizations continue to face deficiencies in their ability to prevent cyberattacks on their IoT technologies.

WHY CRAVRE?
As Internet of Things (IoT) technologies continue to permeate communities, emergency planning and response organizations struggle to mitigate the increasing vulnerabilities created by the ubiquity of these technologies. CRAVRE focuses on developing strategies to detect, identify, manage, and potentially mitigate a cyber-attack as it occurs in the midst of a concurrent incident (e.g. natural disaster, terrorist attack, etc). The course addresses incident management skills, staff responsibilities, and the related situational awareness skills needed in such situations

HOW DOES CRAVRE WORK?
CRAVRE uses scenario-based, virtual reality immersive experiences to call awareness to the complexities and vulnerabilities of the connected work of the IoT technologies. This web-based course presents participants with a challenging and adaptive environment, utilizing AI-powered personalized learning to optimally meet the cybersecurity training needs of individuals and their organizations. The training is designed to interface with a diverse selection of devices, including mobile SMART phones, tablets, laptop and desktop computers, and virtual reality headsets.

LITERATURE CITED

COURSE OBJECTIVES
• Students will be able to identify and interpret widely available known vulnerabilities in IoT, Critical Infrastructures (CI), Supervisory Control and Data Acquisition Systems (SCADA) as well as potential vulnerabilities during the face of natural disasters such as pandemics.*
• Students will be able to demonstrate knowledge, skills, and abilities to protect the aforementioned systems, information, and services from unauthorized access, adversarial impacts, and exploitation.
• Students will be able to apply laws, guidelines, and digital forensics best practices pertinent to public (law enforcement) and private sector (corporate) investigations after any incidents occur. *
* Related to FEMA’s Response and Recovery mission areas.