BAKER COLLEGE
STUDENT LEARNING OUTCOMES

HLS 4110 AI, Runaway Technology and
Weapons of Mass Destruction
3 Semester Credit Hours

Student Learning Outcomes and Enabling Objectives

1. Compare the relationship between Artificial Intelligence (AI) and the potential threats posed by Weapons of Mass Destruction (WMDs) in the context of homeland security.
   a. Compare emerging technologies and their implications for homeland security, with a particular focus on AI-driven innovations and their potential applications in preventing or exacerbating WMD threats.
   b. Summarize how AI can automate cyberattacks, enhance surveillance capabilities, and enable autonomous weapons systems.
   c. Discuss AI-generated "deepfakes" and misinformation campaigns and their effects on public trust and overall security.
   d. Analyze existing policies, regulations, and international agreements related to AI and WMDs in the context of homeland security.
   e. Propose recommendations for enhancing regulatory frameworks.
2. Evaluate the possible negative effects on security of Quantum computing, autonomous weapons and nuclear power.
   a. Explain how quantum computers have the capability to compromise all personal data, including classified government information, and render current cybersecurity infrastructure obsolete.
   b. Examine the ethical and moral concerns of autonomous weapons, also known as Lethal Autonomous Weapons Systems (LAWS) or killer robots, the Quantum computer and nuclear power and their potential negative effects on national security.
   c. Discuss technology and the arms race, as they relate to national and global security, international collaboration, and weaponization.
   d. Explore the need to balance the benefits and risks of nuclear power and the Quantum computer with the associated security challenges.
3. Explore the future application of new and emerging technology and its effect on law enforcement, corrections and human rights.
   a. Discuss robotics as it relates to law enforcement, corrections and armed forces.

b. Explore the ethical considerations of using mass surveillance technology in law enforcement, including facial recognition and biometric data collection, as it relates to concerns of privacy and civil liberties.
   c. Explain the ethical controversy surrounding human cloning and its potential for future warfare.
4. Explore how malicious actors use various methods of cyber attacks to disrupt critical infrastructure, steal sensitive data, shutdown websites and organizations or to conduct espionage.
   a. Discuss the differences and similarities between ransomware attacks, Distributed Denial of Service (DDoS) and Advanced Persistent Threats (APTs).
   b. Discuss the common profiles of those who commit cyberattacks and their various motives and objectives.
5. Predict how the advances in biotechnology may enable the creation of bioweapons, genetically modified organisms (GMOs) for nefarious purposes, and/or the accidental release of dangerous pathogens posing risks related to biohacking and synthetic biology.
   a. Discuss what international treaties address the use of bioweapons.
   b. Explore how geoengineering or bioterrorism can be exploited to cause ecological or agricultural harm.
   c. Explain the ethical issues surrounding biohacking and synthetic biology.

Big Ideas and Essential Questions

Big Ideas
- AI and Weapons of Mass Destruction

- Biohacking and Synthetic Biology Effects

- Emerging Technologies

- Cyber Attacks

- Ethical and Moral Concerns and Challenges

Essential Questions
1. What are the most dangerous threats to humanity and how can they be managed or stopped?

2. What regulates current and emerging technology and protects citizens?

3. How can emerging technologies be applied positively and negatively in criminal justice?

4. How do emerging technologies change the global power structure and the use of weaponry?

5. What are the ethical, privacy and moral use concerns surrounding technological advancements?

These SLOs are approved for experiential credit.

Effective: Fall 2024