Knight Foundation School of Computing and Information Sciences

Course Title: Emerging Topics in Digital Life **Date:** 11/04/2022

Course Number: CTS 1xxx

Number of Credits: 3

Subject Area: Cybersecurity	**Subject Area Coordinator:** Patricia McDermott-Wells, PhD **email:** mcdwells@fiu.edu
Catalog Description: Explore ever-changing boundaries between public and private digital lives, and the cultural and societal impacts of data collection, misinformation, media bias, cyber threats, and emerging technologies.	
Textbook: - Cybersecurity for Beginners, by Raef Meeuwisse, 2017 (978-1911452034)	
References: - Public Parts: How Sharing in the Digital Age Improves the Way We Work and Live, by Jeff Jarvis, 2011 (978-1451636000) - Emerging Media, by Jason Zenor, 2020 (978-1516536573) - Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity, by Erdal Ozkaya, 2019 (978-1789616194);	
Prerequisites Courses: None	
Corequisites Courses: None	

Type: General. *Potential UCC (University Core Curriculum), Global Learning*

This is a Global Learning Foundations course that counts toward the FIU Global Learning graduation requirement.

Prerequisites Topics:

- None

Course Outcomes:

1. Characterize the impact of digital data collection and use in our culture, our society, and our personal and employment-related digital lives [Understand]
2. Describe tactics used by bad actors to spread misinformation and influence media bias in the global digital arena [Understand]
3. Analyze legal, political, and governance ramifications influenced by the changing digital landscape, and how this differs in the global arena [Analyze]
4. Assess the need for personal and organizational planning to safeguard digital assets and meet compliance requirements [Evaluate]

5. Summarize the need for awareness related to information assurance and compliance across the career spectrum [Understand]

Global Learning Outcomes

6. Global Awareness: Students will demonstrate knowledge of the interconnectedness between our public and private digital lives that transcend national and international boundaries. [Apply]

7. Global Perspectives: Students will conduct a multi-perspective analysis of the impact of misinformation and bias in media across national and global contexts. [Analyze]

8. Global Engagement: Students will demonstrate a willingness to engage in activities that analyze the impact of technology and information manipulation in geopolitical disagreements and conflicts. [Create]

Relationship between Course Outcomes and Program Outcomes

BS in Computing: Student Outcomes	Course Outcomes
1) Analyze a complex computing problem and apply principles of computing and other relevant disciplines to identify solutions.	1, 6
2) Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline	N/A
3) Communicate effectively in a variety of professional contexts.	N/A
4) Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.	3, 5
5) Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.	8

Program Specific Student Outcomes

6) Apply computer science theory and software development fundamentals to produce computing-based solutions. [CS]	N/A

6) Apply security principles and practices to maintain operations in the presence of risks and threats. [CY]	2, 4, 7, 8

6) Use systemic approaches to select, develop, apply, integrate, and administer secure computing technologies to accomplish user goals. [IT]	2, 4, 8

Assessment Plan for the Course & How Data in the Course are Used to Assess Program Outcomes

Student and Instructor Course Outcome Surveys are administered at the conclusion of each offering, and are evaluated as described in the School's Assessment Plan: https://abet.cs.fiu.edu/

Outline

Topic	Number of Lecture Hours	Outcome

• Introduction to Digital Life Issues
  ○ Basic concepts of digital life
  ○ Overview of Issues
	2	6

• Fundamentals of Information Assurance
  ○ Concepts and definitions
  ○ CIA Principles
  ▪ Basic types of attacks
  ○ Data protection strategies (identity multi-factor authentication, authorization, access control)
  ○ Secure communication concepts (https)
  ○ Keeping applications up to date
  ○ Forensics concepts
	4	2, 4

• Media Issues
  ○ Social media issues
  ▪ Authenticity of social media accounts (real or bots)
  ▪ Censorship by social media platforms
	8	1, 2, 3, 6, 7

▪ Uses and dangers of locational data (GPS and geotags) ▪ Effects on user attention spans and learning, self-images o Impacts of misinformation, disinformation, mal information ▪ Political ramifications ▪ Fake online shopping reviews ▪ Foreign interference in governance ▪ Effects on public trust ▪ Media bias vs. journalism ▪ Deepfakes o Virtual Reality/ Augmented Reality ▪ The Metaverse – crossing geopolitical boundaries		
• Technology and Social Issues o Social Engineering ▪ Concepts: Phishing, whaling, spear fishing, watering hole approaches ▪ Scareware and ransomware ▪ Pretexting ▪ How Social Engineering differs by culture o Cybernetics and Cyberwarfare ▪ Human enhancement for warfare ▪ Collateral damage of cyberwarfare between geopolitical groups ▪ Hacking/Hactivism	3	1, 2, 3, 7, 8
• Privacy and Anonymity o Role of technology o Anonymity pros and cons o Government surveillance of its citizens in diverse areas of the globe o IoT and mobile device privacy issues o Legal and compliance aspects o Global issues/differences	4	1, 2, 3, 4, 6, 7, 8
o		

• Emerging Technology Issues o Blockchain ▪ Basic concepts ▪ Is it a solution for privacy, voting, etc.? ▪ Cryptocurrency concepts • Its use with ransomware ▪ NFTs o Artificial Intelligence ▪ Its use in decision making ▪ Social impact of bias in AI algorithms o Quantum computing ▪ Basic concepts ▪ Its role in security ▪ Global impacts	2	1, 3, 6
• Organizational Issues o Data storage – legal and compliance issues o IR/DR principles, planning, responses o Breaches – costs, reporting, legal and compliance issues o Hacking (ethical/unethical) & Pen Testing (red team/blue team concepts)	3	4, 5
• Careers and certifications in Information Assurance o Information assurance and compliance career paths o Information assurance and compliance certifications o Responsibilities of a CISO o Cyber threat resources used by information assurance professionals	4	5

Learning Outcomes: (Familiarity->Usage->Assessment)

<u>Human and Societal Digital Impacts:</u>

1. Analyze an incident related to the use of misinformation or disinformation involving public trust issues, buying trends, or local and global governance. [Assessment]

2. Assess the possible implications and impacts of media bias. [Assessment]

3. Analyze an incident in which cyberwarfare had global implications [Assessment]
4. Understand the potential legal and personal implications of the use of deepfake technology [Familiarity]
5. Understand how locational data is collected and used in our personal and professional lives [Familiarity]
6. Differentiate among the diverse types of social engineering. [Familiarity]
7. Analyze an incident in which social engineering led to a major data breach. [Assessment]

Blockchain

1. Identify the major benefits and uses of blockchain technology [Familiarity]
2. Compare and contrast pros and cons of digital currency with fiat currency [Usage]
3. Explore blockchain technology as related to voting [Familiarity]

Artificial Intelligence

1. Identify the major benefits of artificial intelligence for decision-making tasks. [Familiarity]
2. Summarize the major issues surrounding AI related to the possibility of biased results. [Familiarity]

Virtual Worlds

1. Identify the major benefits and disadvantages of virtual reality, augmented reality, and the metaverse. [Familiarity]
2. Describe the implication of virtual worlds on society and governance. [Usage]

Quantum Computing

1. Identify the major possible benefits and unintended consequences of quantum computing [Familiarity]

Basic Digital Information Assurance Concepts:

1. List the key components of the CIA principles of security. [Familiarity]
2. Identify tactics used by bad actors in the digital arena [Familiarity]
3. Describe the different personal and organizational practices that are necessary to protect against digital attacks. [Usage]

Privacy and Anonymity:

1. Compare and contrast the benefits and disadvantages of personal privacy protections and anonymity, on both a local and global scale. [Usage]
2. Analyze an incident where anonymity resulted in a significant negative outcome. [Assessment]
3. Compare and contrast the benefits and dangers of U.S. and foreign governments' surveillance of its citizens. [Usage]

4. Differentiate among regional differences in privacy legislation. [Familiarity]

Organizational Security Issues

1. Identify the need for organizational planning related to digital assets [Familiarity]
2. Identify the major phases and artifacts of disaster recovery planning. [Familiarity]
3. Describe the major legal and compliance requirements that organizations must meet. [Familiarity]

Certification and Career Opportunities in Information Assurance

1. Identify career paths in the fields of information assurance and compliance. [Familiarity]
2. Identify professional certifications in the fields of information assurance and compliance. [Familiarity]

Course Outcomes Emphasized in Laboratory Projects / Assignments

Outcome	Number of Weeks
1. Review case studies in social engineering, misinformation/media bias Outcomes: 1, 2, 3	2
2. Discussion forums (6) Outcomes: 1, 2, 6, 7, 8	6
3. Create a case study based on a global cyberwarfare incident (Group activity) Outcomes: 1, 2, 3, 4, 5, 6, 7, 8 Global learning will be assessed via this case study.	4

Oral and Written Communication:

Written Reports		Oral Presentations	
Number Required	Approx. Number of pages for each	Number Required	Approx. Time for each
6 Discussion Forums based on readings and other course material for: (1) Privacy and Anonymity, (2) Media Bias, (3) Misinformation and Media Bias, (4) Social Engineering, (5) Blockchain, (6) AR, VR and the metaverse	1-2	0	0

2 Review of case studies readings	1		
1 Reflection on invited guest speaker or other course-sanctioned co-curriculum activity	1		
1 Group project: Create a case study to analyze a recent cyberwarfare incident with global implications. Include an infographic/poster for display.	3-4		

Social and Ethical Implications of Computing Topics:

Topic	Class time	Student Performance Measures
Impacts of misinformation, disinformation, and mal information	4	Discussion forums, quizzes
Privacy and Anonymity – benefits and dangers	3	Discussion forums, quizzes
Hacking (ethical and unethical) & Penetration Testing (red team/blue team)	2	Quizzes
Cyberwarfare	6	Quizzes, group case study
AR, VR and the metaverse	3	Discussion forums, quizzes

Approximate number of credit hours devoted to fundamental CY topics[1]

Topic	Core Hours	Advanced Hours
Data Security:	8	0
Software Security:	2	0
Component Security:	0	0
Connection Security:	2	0
System Security:	2	0
Human Security:	16	0

[1] See https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf for a description of Knowledge units

Knight Foundation School of Computing and Information Sciences
CGS 1xxx
Emerging Topics in Digital Life

Theoretical Contents

Topic	Class time
Fundamentals of Information Assurance	4

Problem Analysis Experiences

Review and create case studies

The Coverage of Knowledge Units within Computer Science Body of Knowledge[2]

Area: Knowledge Unit	Topic	Lecture Hours
Data Security: Basic concepts	Fundamental concepts of digital life	1
Data Security: Data Privacy	Privacy & Anonymity issues Social engineering	1
Data Security: Information Storage Security	Organizational Issues Legal and compliance requirements	1
Data Security: Data Integrity and Authentication	Basic digital protection strategies	1
Data Security: Secure Communication Protocols	Secure communication concepts	1
Data Security: Digital Forensics	Fundamentals – hacking; red team/blue team; penetration testing	1
Software Security: Deployment & Maintenance	Keeping applications up to date	1
Software Security: Ethics	Hacking and Penetration Testing Media Bias Impacts of Misinformation, disinformation, mal information	2
Connection Security: World Wide Web	Secure Communication Concepts	1
Connection Security: Vulnerabilities and example exploits	Basic types of attacks Tactics used by bad actors Cyberwarfare	2

[2] See https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf for a description of Knowledge units

Knight Foundation School of Computing and Information Sciences
CGS 1xxx
Emerging Topics in Digital Life

System Security: System Management	Keeping applications up to date Basic types of attacks Tactics used by bad actors Hacking & penetration testing	1
System Security: System Testing	Hacking & penetration testing	1
Human Security: Social Engineering	Social Engineering Social Media Issues Misinformation, disinformation, mal information Media Bias	4
Human Security: Social & Behavioral Privacy	Privacy & Anonymity Issues Social Engineering	2
Human Security: Identity Management	Identification, multi-factor authentication, authorization	1
Organizational Security: Risk Management	Organizational Issues – Risk management	1
Organizational Security: Security Governance & Policy	Organizational Issues – Legal and compliance requirements Global issues/differences	2
Organizational Security: Laws, Ethics & Compliance	Organizational Issues – Legal and compliance issues	1
Organizational Security: Business Continuity, Disaster Recovery, and Incident Management	Organizational Issues – IR/DR principles	1
Societal Security: Cybercrime	Social Engineering Cyberwarfare Misinformation/disinformation	2
Societal Security: Cyber Law	Legal and Compliance Issues Privacy Data storage	1
Societal Security: Cyber Ethics	Hacking (ethical and unethical) Penetration testing (red team/blue team) Privacy policies Media Bias	1
Societal Security: Privacy	Privacy & Anonymity Misinformation/disinformation	1

Knight Foundation School of Computing and Information Sciences
CGS 1xxx
Emerging Security Topics in Digital Life

Week #	Topic Schedule	Assignments	Activities
1	Lecture: Course introduction; Key concepts in digital life; fundamentals of info assurance	Library Research Tutorial	
2	Lecture & Discussion: Privacy & Anonymity	Discussion Forum #1	Additional readings
3	Active learning session	Quiz #1	Case Study #1 - Privacy & Anonymity - in-class small group
4	Lecture & Discussion: Media Bias	Discussion Forum #2	Additional readings
5	Active learning session	Quiz #2	Small group research/presentation of assigned subtopics
6	Lecture & Discussion: Misinformation & Media Bias	Discussion Forum #3	Additional readings
7	Active learning session	Quiz #3	Case Study #2- Misinformation & Media Bias - in-class small group
8	Lecture & Discussion: Social Engineering	Discussion Forum #4	Videos; Additional readings
9	Active learning session	Quiz #4	Small group research/presentation of assigned subtopics
10	Lecture & Discussion: Intro to Block Chain & Cryptocurrencies	Discussion Forum #5	Additional readings
11	Lecture & Discussion: Intro to Artificial Intelligence & Data Mining	Quiz #5	Small group research/presentation of assigned subtopics
12	Lecture & Discussion: Augmented Reality, Virtual Reality, and the Metaverse	Discussion Forum #6	Begin group project: Cyberwarfare incident analysis
13	Lecture & Discussion: Hacking, Hacktivism, Cybernetics & Cyberwarfare	Quiz #6	Continue group project: Cyberwarfare incident analysis
14	Lecture & Discussion: Cybersecurity Careers; Organizational Issues; Legal Aspects & Compliance	Group Project paper	Continue group project: Cyberwarfare incident analysis
15	Active learning session: Group Presentations		Group presentations
16	Guest Lecturer: Various topics	Reflection written report	

Knight Foundation School of Computing and Information Sciences
CGS 1xxx
Emerging Security Topics in Digital Life

Activities/Assignment weighting	
Category	**Weight**
Quizzes: 6 at 3% each	18%
Library Research Tutorials	3%
Discussion Forums: 6 at 4% each	24%
Group Project Paper	25%
Group Project Presentation	20%
Guest Speaker Reflection Report	5%
Participation/Attendance	5%
	100%

Grading Scale	
Threshold %	**Letter Grades**
0	F0
20	F
60	D
73	C
77	C+
80	B-
83	B
87	B+
90	A-
93	A