|  |  |
| --- | --- |
| **ELEMENT** | **CONTENT** |
| DEPARTMENT | CIS |
| AUTHOR (S) | Jack Skoda |
| COURSE NUMBER | **CIS 4011** |
| COURSE TITLE | **Information Warfare** |
| SHORT TITLE | Info Warfare |
| COURSE LEVEL | 4000 |
| DATE CREATED |  |
| CHECKED/CHANGED | 2/28/2017 |
| PREREQUISITES | CIS 2151, 2230 |
| COREQUISITES |  |
| RESTRICTIONS |  |
| SPECIAL FEES | No |
| CREDITS | 3 |
| HOURS | 3 hours of lecture per week |
| SEMESTER | Spring |
| COURSE DESCRIPTION | This course is a strategic level examination of the use of the information instrument of national power. Topics covered include cyberspace operations, computer network operations, information operations, military strategy, and civil military relations |
| SUGGESTED TEXTS | *On War*; Carl von Clausewitz  *Cyberdeterrence and Cyberwar*; Martin Libicki |
| OPTIONAL TEXTS | DOD Joint Publication 1, 3-0, 3-12 |
| COURSE OUTCOMES | The successful student will be able to:   1. Describe sources of national strategic direction 2. Compare and contrast cyberspace operations with conventional operations 3. Explain computer incidents and related the importance of those incidents to strategic level effects 4. Correlate computer incidents with the appropriate agency or organization to assist with the incident handling process 5. Reflect on current events in cyberspace and examine possible policy outcomes |
| COURSE CONTENT | 1. What is war?    1. Strategy    2. Historical examples of warfare    3. Rules of war    4. UN articles related to war    5. US laws 2. Traditional war-fighting domains    1. Land    2. Sea    3. Air    4. Space 3. Cyberspace and the information doman    1. Definitions of cyberspace electromagnetic spectrum    2. Libicki’s three layers of cyberspace    3. Schmitt analysis (measuring impacts)    4. Civilian organizations (e.g., the Electronic Frontier Foundation)    5. The Tallinn Manual    6. Propaganda and public opinion 4. Attacker methods, anatomy of an attack    1. Information gathering    2. Enumeration    3. Exploitation    4. Securing access    5. Obfuscation 5. Types of attackers    1. Insider threats    2. State-sponsored    3. Hacktivists    4. Criminals    5. Nuisance attackers/script kiddies 6. Defensive measures    1. US-CERT    2. National intelligence community (e.g., CIA, NSA)    3. USCYBERCOM and the military    4. Infraguard and the FBI    5. Internet Storm Center    6. Electronic Frontier Foundation    7. Infosec companies (e.g., Symantec, Trend Micro, etc.) 7. Case Studies    1. Morris worm 1988    2. Estonia 2007    3. Conficker 2008    4. Bullitt County, KY 2009    5. Stuxnet 2010    6. The Arab Spring 2010 8. Strategic visions    1. Comprehensive National Cybersecurity Initiative    2. President’s Cyberspace Policy Review    3. Draft or new legislation (e.g., CISPA) |
| LAB/STUDIO OUTCOMES |  |
| LAB/STUDIO CONTENT |  |
| LECTURE CAPACITY | 32 |
| LAB CAPACITY |  |
| GRADED OR P/NP | Graded |
| EVALUATION | Participation, quizzes, exams, homework |
| DELIVERY METHOD | HYB |
| ROOM REQUIREMENTS |  |
| AUTHOR’S NOTES |  |