CityUniversity of Seattle

Syllabus

SCHOOL OF TECHNOLOGY & COMPUTING (STC)

ISEC 540: Cyber Warfare

3 Credits
Effective: Winter 2020

Access to the Internet is required.
All written assignments must be in Microsoft-Word-compatible formats.
See the library's APA Style Guide tutorial for a list of resources that can help you use APA style.

FACULTY

Faculty Name: Jon Helmus

Contact Information: Helmusjonathan@cityu.edu

COURSE DESCRIPTION

Cyber Space has joined air, land, sea and space as the latest domain of warfare. This course examines warfare in the cyber domain beginning with an understanding of how it fits within the context of traditional theory of war. The course examines how countries prepare and apply capabilities and strategies, the impacts of non-state actors, and the future development of cyber warfare. Students participate in a Cyber Warfare Strategic Exercise (CWSX). Students are prepared to understand the impact of the extension of warfare into the cyber domain.

COURSE RESOURCES

Required and recommended resources to complete coursework and assignments are available from the Course Document Lookup.

CITYU LEARNING GOALS

This course supports the following City University learning goals:

- Professional competency and professional identity
- Strong communication and interpersonal skills
- Diverse and global perspectives

COURSE OUTCOMES

In this course, learners:

- Predict the future evolution of cyber warfare.
- Evaluate the place of cyber warfare in the context of information warfare.
- Evaluate the impact of non-state actors on cyber warfare.
- Compare and contrast the cyber war strategies and capabilities of different countries.
- Assess cyber warfare in the context of the theory of war.

CORE CONCEPTS, KNOWLEDGE, AND SKILLS

1. The Theory of War
   1.1. Understand basic theory of war.
   1.2. Discuss the 9 principles of war.
   1.3. Explain the concepts of the OODA cycle.

2. Defining Cyber War
   2.1. Describe the evolving landscape of warfare.
   2.2. Appraise how cyber warfare varies from traditional warfare.
   2.3. Circumscribe the scope of cyber warfare.
   2.4. Differentiate between Acts of War and Acts Short of War.
   2.5. Formulate what constitutes crossing the Kinetic Boundary.
   2.6. Distinguish between State and Non-state actors.

3. Information War
   3.1. Structure a vision the broader context of Information Warfare.
   3.2. Outline Information Tasks and their intended effects.
   3.3. Compare and contrast the elements of information warfare engagement.
   3.4. Appraise the capabilities needed for personnel engaged in various information warfare tasks.
   3.5. Critique traditional military approaches to information warfare capacities.
   3.6. Assess the existence of boundaries between cyber and information warfare.
   3.7. Propose the ideal cyber force.
   3.8. Differentiate between military and non-military cyber force components.

4. The Cyber War Offense
   4.1. Assess the Order of Battle of nations with known cyber capabilities.
   4.2. Define the Spectrum of Conflict.
   4.3. Outline known and potential offensive capabilities of cyber warfare participants.
   4.4. Describe the operational planning process.
   4.5. Explain Desired End State in terms of operational planning.
   4.6. Evaluate the use of effects based planning.
   4.7. Categorize the Anatomy of a Cyber Attack in military terms.
   4.8. Discuss the problem of attribution.
   4.9. Investigate issues with the involvement of 3rd parties.

5. International Cyber Strategies
   5.1. Describe the Russian Cyber Strategy.
   5.2. Describe Chinese Cyber Strategy.
   5.3. Describe the North Korean Cyber Strategy.
   5.4. Consider other international strategies as directed.
   5.5. Compare and contrast national cyber strategies.

6. US Domestic Cyber Strategies
   6.1. Describe the US Cyber Strategy.
   6.2. Outline the components of the US Cyber Command and their capabilities.

7. Cyber Terrorism
   7.1. Characterize what makes an attack an act of terrorism.
   7.2. Describe the current use of Cyber Space by terrorists.
   7.3. Analyze potential targets of cyber terrorists.

7.4. Evaluate what steps can reduce the threat of cyberterrorism.

8. The State of Cyber Warfare
   8.1. Understand significant cyberattacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars.
   8.2. Understand the history of cyberattacks.
   8.3. Understand Google's battle against fake news, and international cybercriminal activity

9. Non-state Actors and Hacktivists
   9.1. Evaluate relative advantages and disadvantages non-state actors have in developing capabilities.
   9.2. Compare and contrast how the variety of trans-state actors (jihadists, anarchists, political activists, criminal organizations, etc.) differ in their approaches to the possibilities for cyberwar.
   9.3. Judge whether cyberwarfare provides impetus or significance to the emergence of new forms of conflict or protest.
   9.4. Assess the impact of vigilantes, hacktivists, sympathetic hackers on crisis management and war termination.
   9.5. Suggest how cyberwarfare influences approaches to peacekeeping and peacemaking.
   9.6. Explore the possibility for cyberwarfare to increase the potential for failed states.

10. Cyber War Management
   10.1. Discuss proposals for Cyber Arms Controls.
   10.2. Debate the merits of Cyber Treaties.
   10.3. Critique other proposals for treatment of cyber warfare.

OVERVIEW OF COURSE GRADING

The grades earned for the course will be derived using City University of Seattle's decimal grading system, based on the following:

OVERVIEW OF REQUIRED ASSIGNMENTS	% OF FINAL GRADE	POINTS
Virtual Labs • Lab 1: Configuring a VPN tunnel using the pfSense Firewall • Lab 2: Linux Attack and Response • Lab 3: Log Analysis of Linux Systems with Grep and Gawk • Lab 4: Attacking and Defending Linux • Lab 5: Cracking Passwords on Linux Systems • Lab 6: Identifying & Analyzing Network Host Intrusion Detection System • Lab 7: Vulnerability Scanning of a Linux Target • Lab 8: Encrypting Data using TrueCrypt and Attacking the TrueCypt password using truecrack • Lab 9: Creating a Proxy Server and an SSL Certificate using the pfSense Firewall • Lab 10: Steganography	35%	350 = 35 points * 10 weeks

Research Paper • Paper 1: International Country Assessment • Paper 2: US Cyber Posture Assessment • Paper 3: Cyber Warfare Attack Analysis	45%=15% + 15% + 15%	450 = 150 points * 3
Instructor Determined Assignments • The Muddiest Point • Discussion Board	20%=5% + 15%	50 = 5 points * 10 weeks 150 = 15 points * 10 weeks
TOTAL	**100%**	**1000 points**

SPECIFICS OF COURSE ASSIGNMENTS

The instructor will provide grading rubrics that will provide more detail as to how this assignment will be graded.

International Country Assessment

Teams of students will complete an in-depth study of the cyber strategy and capabilities of a country of their choosing. The study should include inferred, as well as acknowledged, capabilities and strategies. The study should include a broad sketch of the overall defense/military posture, economic status, political situation, and foreign relations of the country.

Remember that military capabilities can be inferred from civilian capabilities. For example, countries which can produce cars and trucks for the civilian market are capable of producing vehicles for military use. Programmers who program consumer products can ...

The students in the team will organize the team to cover the necessary information. Each student will be assigned at least one aspect for which they have sole responsibility. Some areas can be handled as joint responsibilities.

The results of the country assessment will be provided as a presentation. The students will arrange the format and details of delivery of the presentation with the instructor.

Components	***% of Grade***
Strategies and Capabilities	50%
Teamwork/Group Work	20%
Presentation of Results	30%
TOTAL	**100%**

US Cyber Posture Assessment

For as long as long as there has been a concept of "cyber warfare", the US government, and military in particular has been struggling with the best way to organize itself both offensively and defensively. Explore some of the strategic benefits and drawbacks to the model that is currently in place within the DoD as it shifts from a decentralized to a more centralized model under a different reporting structure. Consider this in the context of the traditional military approach to warfare, and an "ideal" approach to a cyber force's organization, how it's managed, and operated.

The paper should be roughly 6 pages in length; should contain at least 4-6 references; and should be in proper APA format.

Components	***% of Grade***
Strategic Analysis	60%
Style and Mechanics	20%
APA Style (citation / references)	20%
TOTAL	**100%**

Cyber Warfare Attack Analysis

Select a cyber-attack that has occurred within the last 5 years and prepare a report on it. While there is almost always some disagreement on who is behind cyber warfare / cyber-attacks, to support the tie-in to traditional warfare, select an attack that is generally credited to a nation-state or military actor (ISIS/ISIL is acceptable, Anonymous is not). Your report should include information such as the nature, duration, impact, and effectiveness of the attack, countermeasures, immediate response to, and consideration of the larger impact off the attack on future related cyber or real-world warfare or political actions – put a different way, did the attack make the strategic impact in the environment that the instigator likely wanted?

The paper should be roughly 6-8 pages in length; should contain at least 4-6 references; and should be in proper APA format.

Components	***% of Grade***
Attack Analysis	60%
Style and Mechanics	20%
APA Style (citation / references)	20%
TOTAL	**100%**

Instructor Determined Assignments (Including Discussions)

Assignments, discussion questions, and muddiest points as determined by the instructor.

Components	***% of Grade***
Meets requirements of the activity in a timely manner	25%
Adds insightful or new ideas, comments, or questions relevant to the activity and/or to other students' posts	25%
Appropriately references readings, material in course sessions and other postings	25%
Writes clearly, concisely, and grammatically	25%
TOTAL	**100%**

COURSE POLICIES

Late Assignments

Late assignments will be penalized according to CityU's policy.

Participation

Participation will be graded based on discussion board assignments. All students are required to have an initial post and 2 responses to other student post.

Professional Writing

Assignments require error-free writing that uses standard English conventions and logical flow of organization to address topics clearly, completely, and concisely. CityU requires the use of APA style.

UNIVERSITY POLICIES

You are responsible for understanding and adhering to all of City University of Seattle's academic policies. The most current versions of these policies can be found in the University Catalog that is linked from the CityU Web site.

Scholastic Honesty

Scholastic honesty in students requires the pursuit of scholarly activity that is free from fraud, deception and unauthorized collaboration with other individuals. You are responsible for understanding CityU's policy on scholastic honesty and adhering to its standards in meeting all course requirements. A complete copy of this policy can be found in the University Catalog in the section titled *Scholastic Honesty* under *Student Rights & Responsibilities*.

Attendance

Students taking courses in any format at the University are expected to be diligent in their studies and to attend class regularly.

Regular class attendance is important in achieving learning outcomes in the course and may be a valid consideration in determining the final grade. For classes where a physical presence is required, a student has attended if s/he is present at any time during the class session. For online classes, a student has attended if s/he has posted or submitted an assignment. A complete copy of this policy can be found in the University Catalog in the section titled *Attendance Policy for Mixed Mode, Online and Correspondence Courses*.

SUPPORT SERVICES

Disability Resources

If you are a student with a disability and you require an accommodation, please contact the Disability Resource Office as soon as possible. For additional information, please see the section in the University Catalog titled *Students with Special Needs* under *Student Rights & Responsibilities*.

Library Services

CityU librarians are available to help you find the resources and information you need to succeed in this course. Contact a CityU librarian through the *Ask a Librarian* service, or access library resources and services online, 24 hours a day, seven days a week.

Smarthinking

As a CityU student, you have access to 10 free hours of online tutoring offered through Smarthinking, including writing support, from certified tutors 24 hours a day, seven days a week. Contact CityU's Student Support Center at help@cityu.edu to request your user name and password.