PSC 259 *Cyber Warfare and Cyber Politics* **Prof. Farkas Spring 2020**

COURSE DESCRIPTION:

Cyber politics is a new frontier in the realm of politics. This is a political science course focusing on the cutting edge use of electronic and related technologies in managing people. Government is the principle actor but certainly not the only actor in this relationship. It will emphasize the vulnerability of political systems when government lags behind adversaries or hostile parties in developing cyber capabilities. Conflict has already begun to take the form of Cyber War where the combatants are sovereign states, criminal organizations, dissident groups, malicious thieves and intellectual experimenters. Twenty-first century warfare is qualitatively different from the conflicts of the past. There is little controversy that students familiar with dimensions of these phenomena will be more prepared for positions in public management and government service and will find themselves on the frontline defending the system and its people.

This course locates itself on the emerging frontier of thinking about the relationship between technology, politics, and conflict. Specifically, to examine the way that what has come to be called cyber warfare and cyber politics impact on characteristics of democracy including participation, communication and legitimacy. The crucial element is how or if "cyber Politics" – the use of electronic devices and cybernetics by governments and competitors – can change the balance between stability/order and change.

COURSE MATERIALS:

Schmidt & Cohen, The New Digital Age, Vintage, paper, 2014

Goodman, Future Crimes, Anchor, paper, 2016

Whyte & Mazanec, Understanding Cyber Warfare, Routledge, paper, 2019

COURSE OBJECTIVES for Cyber Politics

1. ***Provide students with a forward-facing vision of politics.***
2. ***Challenge students to work through and glean from data sets.***
3. ***Create depth of understanding of cultural, economic and managerial differences in various political systems around the world.***
4. ***Sharpen a student's ability to identify and articulate global trends and their likely consequences.***

COURSE OBJECTIVES for Cyber Crime and Cyberwarfare

1. ***Grasp the scope of the vulnerability that comes with technology***
2. ***Recognize WHO is able and inclined to use technology to assault***
3. ***Inventory the ways that damage can be levelled by cyber crime and cyber warfare***
4. ***Reflect on individual and systemic remedies and their costs***

FACULTY-STUDENT CONTACT

Experienced university students know that it is wise to use the opportunity to visit and consult with professors during their office hours. Our Spring Quarter situation is creating many limitations. It is YOUR responsibility to use our communication options to clarify questions you, raise questions or thoughts about other ideas, or simply to come to understand better the professor's thinking about any subjects at all. If you do this, it will be easier for your professors to deal with you and your uniqueness. This will take more than the usual effort. It remains very important.

Students are certainly entitled to all the guidance and assistance that we can provide. This course is committed to that principle. Only you know when and how you need help. Try to remember that it is your education and YOU must do your part to sketch in how this plan (syllabus) best works for you. I am looking forward to knowing and working with you! As veteran students, you should not need prodding in this direction.

Office: 990 W. Fullerton Ave. Room 2211
Office phone: 773 325-1977 cell phone: 847 251-2671
dfarkas@depaul.edu What's App 847 251 2671

ACADEMIC INTEGRITY

"Academic honesty" is crucial to our enterprise. The faculty has effective ways of investigating suspicious cases. To avoid any possibility, cite all sources and consult with your professor if you have any questions.

TERM PAPER:

Each student will create an examination of the prospects for and vulnerability to cyber assault. It should begin with an empirical analysis and end with a normative assessment. In it one should (a) identify the nature of the vulnerability, (b) identify the most probable perpetrator, (c) identify the target's capacity to defend itself, and (d) the systemic implications of cyberwarfare.

DISCUSSION POSTS:

Each student will have the responsibility to post every **Wednesday** (between 6am and 11pm). The post should identify ONE idea drawn from that module's reading. It should be the idea that you find most interesting, curious or controversial. You will state the idea (one sentence), cite the page or section of the reading from which you took the idea, and share, at most, two sentences about why you find it worthy of sharing. Students must not repeat the substance of other student's posts. Do not write a lengthy treatise! On **Thursday** (between 6am and 11pm) after reading your classmates Thursday posts, make one comment responding to any one of those posts. We will use this system for the first eight (8) modules. You will receive 0, 1 , or 2 points for each post and response based upon clarity and thought. That means that every week, a student can receive from 0 to 4 points per module.

USING ZOOM:

The extraordinary situation we face requires that we find a way to discuss the things we are trying to learn about and understand. This has been made far more difficult. Our interim solution is ZOOM. This course requires you to become very familiar with the software BEFORE we begin. We have few options without meeting. It will take dedication and flexibility to have the robust conversations we need to have. Be diligent and prepare for this challenge. We need to pull together to make this work productively. Formal zoom sessions EVERY

MID-TERM Exam: A mid-term exam is scheduled for Saturday, May 2nd. You will be able to parcel a 90 minute period to take the exam anytime between 6am and 11pm. More information about the structure will be shared during the term.

FINAL GRADES:

components: discussion posts, mid-term exam, term paper, final exam

Course Schedule: tentative; changes possible/likely during quarter

Module 1	March 30	Cyber Politics	New Digital Age Ch 1 & 2
		Subjects: E-Government E-citizen EGDI E-Participation ICTs	
Module 2	April 6	Cyber Politics	UN E-Government Surveys
		Subjects: "Democracy" & digital politics	
Module 3	April 13	The Nature of Vulnerability	New Digital Age, Ch. 3,4,5
			Understanding, Ch. 1, 2
Module 4	April 20	Cyber Crime	Future Crimes, Part 1
Module 5	April 27	Cyber Crime	Future Crimes, Part 2

Mid-term Exam *Saturday, May 2 (between 6am and 11pm)*

Module 6	May 4	Cyberwarfare	New Digital Age, Ch. 6, 7
			Understanding, Ch. 3,4
Module 7	May 11	Cyberwarfare	Understanding, Ch. 5,7,8
Module 8	May 18	Cyberwarfare	Understanding, Ch. 9,11
Module 9	May 25	Facing Forward / Remedies?	Future Crimes, Part 3
			Understanding, Ch. 12
Module 10	June 1	Synthesis	*Final Term Papers due June 4 11pm*

Final Exam *Saturday, June 6 (between 6am and 11pm) instructions to follow …*