

Department of Political Science
Faculty of Behavioral and Social Sciences
University of the Punjab, Lahore
Course Outline



Programme	BS Diplomacy and Strategic Studies	Course Code	SDSS-211	Credit Hours	02
Course Title	Cyber Warfare & International Security				
Course Introduction					
Cyber space is considered as the fourth war front after land, air and sea. It is predicted that next major war is not likely to be fought on the battle ground but in cyber space. Era of cyber warfare has already begun. This course will keep the students informed about the cyber technology in these changing times. Therefore the need for recognizing the importance of cyber warfare cannot be ignored in modern warfare.					
Learning Outcomes					
On the completion of the course, the students will: <div><div>1. Know the conceptual aspects related to cyber space</div><div>2. Explore the evolution of the cyber space & cyber warfare</div><div>3. Explore the methods to combat the cyber attacks</div><div>4. Find the link between international security and cyber warfare</div><div>5. Understand the new techniques role in warfare</div></div>					
Course Content					
Week 1	Unit-I				
	Concept of Cyber Space				
	Unit-II				
	International Security				
Week 2	Introduction to Cyber Space				
Week 3	Introduction to International Security				
Week 4	Evolution of the Concept Cyber Space				
Week 5	Concept of Cyber Warfare				
Week 6	Purpose of Cyber warfare in security paradigm				
Week 7	Learning of Cyber Weapons				
Week 8	Goals of Cyber Attacks				
Week 9	Mid Term Exam				
Week 10	Types of Cyber Warfare Attacks				
Week 11	Discussion on a Case Study of a Cyber Attack				

Week 12	Concept of Hacking	
Week 13	Cyber security link with Ethical Hacking	
Week 14	Hacking Techniques and methodology	
Week 15	Study of major Cyber Attacks	
Week 16	Cyber warfare Operations and Methods to Combat it	
	Discussion on a Case Study of a Cyber warfare operation	

Textbooks and Reading Material

- Stiennon, Richard. (2010), *Surviving Cyber War*, Rowman and Little Field, UK
- Stiennon, Richard. (2010) *There will be Cyber War*, Rowman and Little Field, UK
- Bidwell, Christopher. And Macdonald, Bruce. (2018), “Emerging Disruptive Technologies and their Potential Threats to Strategic Stability and National Security” Federation of American Scientists.
- Zetter, Kim, “An unprecedented look at Stuxnet, The World;s First Digital Weapon”, November 3, 2014, Retrieved from <http://www.wired.com/2014/11/countdown-to-zero--day-stuxnet>.
- Mishra, Abhinandan,”(2020), Concerns deeper about cyber attacks on SU 30, IAF starts inquiry”, Sunday Guardian Live, <http://www.sundayguardianlive.com>
- Shad, Muhammad.”(2020) Cyber Threat Land Scape and Readiness Challenge of Pakistan” Strategic Studies

Teaching Learning Strategies

1. Class Lectures
2. Distribution of the reading material to the students
3. Learning trough Case Studies
4. Guest Speaker lecture related to the subject matter

Assignments: Types and Number with Calendar

- | | |
|------------------|----------|
| 1. Class Quiz | 5 marks |
| 2. Short Test | 5 marks |
| 3. Presentations | 5 marks |
| 4. Assignment | 10 marks |

Assessment

Sr. No.	Elements	Weightage	Details
1.	Midterm Assessment	35%	Written Assessment at the mid-point of the semester.

2.	Formative Assessment	25%	Continuous assessment includes: Classroom participation, assignments, presentations, viva voce, attitude and behavior, hands-on-activities, short tests, projects, practical, reflections, readings, quizzes etc.
3.	Final Assessment	40%	Written Examination at the end of the semester. It is mostly in the form of a test, but owing to the nature of the course the teacher may assess their students based on term paper, research proposal development, field work and report writing etc.