RUTGERS

Global Politics of Internet Security

COURSE SYLLABUS: 790:575:01

Prof. Ihab Darwish **Email:** idarwish@ccny.cuny.edu

Meetings Saturday 10:00 a.m. – 12:40 p.m., **Rooms**: HCK 612 & MMC N462

Textbooks Multiple resources will be available on our Online Learning System (SAKAI)

I. Course Description:

Global Politics of Internet Security course will offer "soft technology" analysis, an examination of the core public policy issues of cyber security and provides a "hands on" dimension though case studies. The course is multi-disciplinary covering: cyber space and cyber security fundamentals, policy, economics, regulations, etc. The class introduces the student to the field of Information Security. The managerial, legal, ethical and technical aspects of information security are covered. Students will learn about the need for information security, planning for security, and risk management. The function of firewalls, virtual private networks, intrusion detection systems, cryptography, and access control mechanisms will be discussed. Physical security and the role of the personnel in properly executing security standards and controls are also covered. Case studies and Hands on component will be covered throughout the course.

II. Course Objectives:

1. A "soft" technology component that introduces Cyber Security, Information Security, Security Key Concepts and the Security Model
2. Cryptography Understanding the cyber risk
3. Cyber Security Policies and Strategies
4. Defense-In-Depth Security Model
5. Cyberspace Technology and Applications
6. The six dimensions of cyber maturity
7. Security Threats and Types of Attacks
8. Prevention and Security Policies
9. Information System Forensics

10. Cyber Conflicts, Attacks Case studies

III. Grading Criteria

15 % - Articles – CRN

10% - On-site class participation

10 % - Forum Discussions Activities

20 % - Mid-Term – Key Concepts

45 % - Course Project Research and Presentations

IV. Course Structure – Requirements Details

The important structure of the course will be according to the following points.

- Links to three articles will be posted on SAKAI each week and the students are requested to choose only one article out of three and to prepare at least one full paragraph addressing some of questions presented and it does not have to be a full essay. This will be treated as a short form of CRN representing 15% of the grade.

- On-site class participation and debate to specific subject will make another 10% of the grade. This could be an open discussion or debate during the first half an hour of class time.

- **Reading assignments** on the other hand are different than the articles and they are more related to Cyber Security principles. Students are supposed to use the resources for each week to participate in the **forum discussion** according to the main post that I will be initiating. Students are expected to visit the forum at least once in order to perform one main post (usually it should be kept very concise). This item will be 10% of the grade. You are encouraged to participate more in the forum.

- There will be one midterm covering the security part from technical prospective (usually multiple choice type of questions) and this item will represent 20% of the grade.

- A research project paper and presentations will be our final part, each student will propose three different topics and at the end we will have 45 possible topics. Then I will discard some of the topics that are not relevant and I will assign one topic for each student to work on. Student is expected to prepare a paper and a presentation to be presented in our last two classes. This item will be 45% of the grade.

I. Class Schedule

Week	Date	Topics
1	Sept 9th	Course Introduction, Cyber Security, Information Security, Security Key Concepts and the Security Model
2	Sept 16th	Cyber Security, Information Security, Security Key Concepts and the Security Model
3	Sept 23rd	Legal, Ethical, and Professional Issues in Information Security
4	Sept 30th	Cyber Security Policies and Strategies Case Study - 1
5	Oct 7th	Cyber Risk Management Case Study - 2
6	Oct 14th	Cryptography Case Study - 3
7	Oct 21st	Defense-In-Depth Security Model Cyberspace Technology and Applications
8	Oct 28th	**Mid-Term**
9	Nov 4th	Intrusion Detection and Prevention Systems and Other Security Tools Physical Security, Implementing Information Security, Security and Personnel, Information Security Maintenance
10	Nov 11th	The six dimensions of cyber maturity
11	Nov 18th	Security Threats and Types of Attacks Prevention and Security Policies
12	**Nov 25th**	**Thanksgiving Recess—All University Offices Closed—No Classes**

13	**Dec 2nd**	Information System Forensics
14	**Dec 9th**	Cyber Politics and Conflicts Attacks Case studies
15	**Dev 16th**	**Research Project Presentations**

- **Research Project Due Date is Dec 1st**