RUTGERS

Politics of Cyber Warfare

COURSE Description: 790:558:01

Dr. Ihab Darwish **Email: ihab.darwish@rutgers.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

I. Course Description:

Cyber warfare is using information technologies against the sovereignty of other nations for the purpose of destruction or disabling vital and critical infrastructure and causing instability of services to achieve or force certain political agenda. Politics of Cyber warfare is our latest offering of cyber security classes aiming at discovering how the cyber was, is, and will continue to influence our modern politics. Facts and proofs of hacking and security breaching were found in our previous presidential election. The DNC were hacked by external entities and several US agencies including the FBI and the CIA have made allegations the tied the incident to other nations!

In this course we will provide several case studies and scenarios of critical political cyber warfare incidents with the intention to force the target opponent to follow certain hidden agenda. In cyber warfare, software and hardware exploitation is usually performed in order to damage the controlling processes within the targeted system. Therefore, from technical prospective and by using forensic science, we will investigate the characteristics of cyber warfare, cyber weapons, political hackers and hacktivism, cyber militias and strategies in use and misuse of cyber warfare that led to performing successful political hacking.

II. Course Objectives:

1. Introduction to Cyber Warfare and Politics
2. Cyber threats and vulnerabilities, WWW and Internet infrastructure, Internet organization including IETF and ICANN.
3. Characteristics of Cyber Warfare, Attack cycles
4. Cyber warfare infrastructure

5. Cyber weapons, Cyber Crime, Political hackers and hacktivism
6. Cyber Militias
7. Cyber Warfare strategies
8. US and international key laws and policies (the Law of Armed Conflict, UN Charter)
9. Case studies, 2016 US Election, 2015 attack on power grid in Western Ukraine, 2008 Stuxnet worm attack on Iranian Nuclear Facilities and 2007 Russian-Estonian conflict.
10. Mitigation strategies - The art of defense and counter attack

III. Grading Criteria

15 % - Articles – CRN

10% - On-site class participation

10 % - Forum Discussions Activities

20 % - Mid-Term – Key Concepts

45 % - Course Project Research Paper 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 warfare concepts. 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 cyber warfare security part from technical prospective and this item will represent 20% of the grade.

- A research project paper and presentations will be our final part. Each student will propose one or more topics and I will establish a pool of selected topics. One topic will be assigned to each student to work on and the student is expected to prepare a paper and a PowerPoint presentation to be presented in the class. This item will be 45% of the grade.

V. Academic Integrity

The consequences of scholastic dishonesty are very serious. Please review the Rutgers' academic integrity policy.

Academic integrity means, among other things:

- Develop and write all of your own assignments.
- Show in detail where the materials you use in your papers come from. Create citations whether you are paraphrasing authors or quoting them directly. Be sure always to show source and page number within the assignment and include a bibliography in the back.
- Do not fabricate information or citations in your work.
- Do not facilitate academic dishonesty for another student by allowing your own work to be submitted by others.

If you are in doubt about any issue related to plagiarism or scholastic dishonesty, please discuss it with your instructor.

Other sources of information to which you can refer include:

- Rutgers' Academic Integrity website http://academicintegrity.rutgers.edu/
- Code of Student Conduct
- Eight Cardinal Rules of Academic Integrity

VI. Cheating and Plagiarism

Short version: Don't cheat. Don't plagiarize.

Longer version: Cheating on tests or plagiarizing materials in your papers deprives you of the educational benefits of preparing these materials appropriately. It is personally dishonest to cheat on a test or to hand in a paper based on unacknowledged words or ideas that someone else originated. It is also unfair, since it gives you an undeserved advantage over your fellow students who are graded on the basis of their own work. In this class we will take cheating very seriously. All suspected cases of cheating and plagiarism will be automatically referred to the Office of Judicial Affairs, and we will recommend penalties appropriate to the gravity of the infraction. The university's policy on Academic Integrity is available at:

http://academicintegrity.rutgers.edu/files/documents/AI_Policy_9_01_2011.pdf [1]

I strongly advise you to familiarize yourself with this document, both for this class and for your other classes and future work. To help protect you, and future students, from plagiarism, we require all papers to be submitted through Turnitin.com.

Since what counts as plagiarism is not always clear, I quote the definition given in Rutgers' policy:

Plagiarism: Plagiarism is the use of another person's words, ideas, or results without giving that person appropriate credit. To avoid plagiarism, every direct quotation must be identified by quotation marks or appropriate indentation and both direct quotation and paraphrasing must be cited properly according to the accepted format for the particular discipline or as required by the instructor in a course. Some common examples of plagiarism are:

- **Copying word for word (i.e. quoting directly) from an oral, printed, or electronic source without proper attribution.**
- **Paraphrasing without proper attribution, i.e., presenting in one's own words another person's written words or ideas as if they were one's own.**
- **Submitting a purchased or downloaded term paper or other materials to satisfy a course requirement.**
- **Incorporating into one's work graphs, drawings, photographs, diagrams, tables, spreadsheets, computer programs, or other nontextual material from other sources without proper attribution.**[2]

A SPECIAL NOTE: Students often assume that because information is available on the Web it is public information, does not need to be formally referenced, and can be used without attribution. This is a mistake. ***All*** information and ideas that you derive from other sources, whether written, spoken, or electronic, must be attributed to their original source. Such sources include not just written or electronic materials, but people with whom you may discuss your ideas, such as your roommate, friends, or family members. They deserve credit for their contributions too!

Judgments about plagiarism can be subtle. If you have any questions, please feel free to ask for guidance.

---

[1] This web link was corrected on July 13, 2012. S. Lawrence
[2] http://academicintegrity.rutgers.edu/files/documents/AI_Policy_9_01_2011.pdfUpdated with the University's current language on July 13, 2012. S. Lawrence

VII. Class Schedule

Week	Date	Topics
1	**Jan 25th**	Course Introduction - What is Politics of Cyber warfare?
2	**Feb 1st**	Cyber threats and vulnerabilities, WWW and Internet infrastructure, Internet organization including IETF and ICANN.
3	**Feb 8th**	Characteristics of Cyber Warfare Attack cycles
4	**Feb 15th**	Cyber warfare infrastructure
5	**Feb 22nd**	Cyber weapons Cyber Crime Political hackers and hacktivism
6	**Feb 29th**	Cyber Militias
7	**Mar 7th**	Cyber Warfare strategies
8	**Mar 14th & Mar 21st**	**Mid – Term - Online** **Spring Recess - No Classes**
9		
10	**Mar 28th**	US and international key laws and policies (the Law of Armed Conflict, UN Charter)
11	**Apr 4th**	Case studies, 2016 US Election, 2015 attack on power grid in Western Ukraine, 2008 Stuxnet worm attack on Iranian Nuclear Facilities and 2007 Russian-Estonian conflict.
12	**Apr 11th**	Case studies, 2016 US Election, 2015 attack on power grid in Western Ukraine, 2008 Stuxnet worm attack on Iranian Nuclear Facilities and 2007 Russian-Estonian conflict.
13	**Apr 18th**	Mitigation strategies The art of defense and counter attack
14	**Apr 25st**	**Research Project Presentations**
15	**May 2nd**	**Research Project Presentations**

- **Research Project Presentation's due Date is April 21st, but the final paper will be due on May 2nd.**

VIII. Assigned Readings

[1] P.W. Singer and Allan Friedman. 2014. Cybersecurity and Cyberwar: What Everyone Needs to Know. New York, NY: Oxford University Press

[2] Andress, Jason & Winterfeld, S. (2013). Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners: Second Edition.

[3] Porche, Isaac R., Christopher Paul, Michael York, Chad C. Serena, Jerry Sollinger, Elliot Axelband, Endy M. Daehner and Bruce Held. Redefining Information Warfare Boundaries for an Army in a Wireless World. Santa Monica, CA: RAND Corporation, 2013. https://www.rand.org/pubs/monographs/MG1113.html. Also available in print form.

[4] Owen William, Kenneth Dam, and Herbert S. Lin. 2009. Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. National Research Council, 2009, available at https://www.nap.edu/read/12651/chapter/1