George Mason University
CFRS 768 – Cyber Warfare
CRN 17222, Sec 001
Spring 2015, January 23 – May 8, Fridays, 4:30-7:10PM
ENGR 5358

Instructor

Michael Robinson
mrobinsv@gmu.edu
Office Hours: Available upon request

Description

This course will explore the rapidly changing face of cyber warfare and cyber terrorism. Students will identify and characterize the fundamental aspects of cyber terrorism and the role of computers and the Internet in terrorist acts on information systems and critical infrastructure components. Students will analyze cyber warfare techniques, such as Denial of Service (DoS) attacks on critical infrastructure, man-in-the-middle attacks, sabotage, and espionage. Students will evaluate the various cyber crimes that are being used to finance terrorism and cyber criminal activities.

Learning Objectives

Upon completing the course, students will be able to:

- Compare several cyber attacks sponsored by rogue nations using open source intelligence and analyze the attack vectors that were implemented in each.
- Compare the motivations behind cyber warfare and cyber terrorist attacks against corporate and government systems.
- Select the appropriate computer security tools to detect and analyze indicators of an attack.
- Analyze the differences between a cyber warfare attack and a typical malware/virus attack.
- Design a mock scenario that simulates a cyber attack using current attack vectors to prepare for a cyber event.

Required Materials

The following texts will be used for the class:

Carr, J. (2012). Inside Cyber Warfare: Mapping the Cyber Underworld. Second Edition. O'Reilly Media, Inc. Sebastopol, CA

The following texts will be used and made available via Blackboard:

Applegate, S. D. (2013). "The Dawn of Kinetic Cyber." *5th International Conference on Cyber Conflict*. Tallinn, Estonia. pp. 1-15.

Bohn, L. E. and Satter, R. (2012, November 19.) "'Anonymous' targets Israeli websites over Gaza war." Retrieved on December 11, 2012 from the Yahoo! News website: http://news.yahoo.com/anonymous-targets-israeli-websites-over-gaza-war-220548299.html

Denning, D. E. (2000, May 23). “Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. Georgetown University.

Gamer, T. (2011, September 9). “Collaborative anomaly-based detection of large-scale Internet attacks.” *Computer Networks*. 56. Elsevier, Inc. Waltham, MA.

gHale. (2012, November 19). “Obama Inks Cyber Attack Directive.” Retrieved on December 3, 2012 from the ISS Source website: http://www.isssource.com/obama-inks-cyber-attack-directive/

Information Warfare Monitor. (2009, March 29). “JR02-2009: Tracking GhostNet: Investigating a Cyber Espionage Network.” Munk Centre for International Studies. University of Toronto. Toronto, CA. Retrieved from the Scribd web site: http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation. Santa Monica, CA.

Mandiant. (2013). “APT1: Exposing One of China’s Cyber Espionage Units.” Alexandria. VA.

Messmer, E. (2012, December 7). “ITU says 'network outage' after website cyberattack disrupted Dubai conference.” Retrieved on December 11, 2012 from the ComputerWorld website: http://computerworld.co.nz/news.nsf/security/itu-says-network-outage-after-website-cyberattack-disrupted-dubai-conference

Pras, A., et al. (2010, December 10). “CTIT Technical Report 10.41: Attacks by 'Anonymous' WikiLeaks Proponents not Anonymous.” *Design and Analysis of Communication Systems Group*. University of Twente, Enschede. The Netherlands.

Rattray, G. J. and Healey, J. (2011). “Chapter 5: Non-State Actors and Cyber Conflict.” *America’s Cyber Future: Security and Prosperity in the Information Age*.

Sanger, D. E. and Shanker, T. (2013, February 3). “Broad Powers Seen for Obama in Cyberstrikes.” Retrieved from The New York Times website: http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html?partner=rss&emc=rss&pagewanted=all&_r=0

Schwartz, M. J. (2012, February 7). “Who is Anonymous: 10 Key Facts.” Retrieved on November 28, 2012 from the Information Week website: http://www.informationweek.com/security/attacks/who-is-anonymous-10-key-facts/232600322 (view this page and the following 10 pages.)

Smith, D. J. (2012, July). “Russian Cyber Operations.” Potomac Institute for Policy Studies.

United Nations Office on Drugs and Crime. (2012). “The Use of the Internet for Terrorist Purposes.” United Nations. Vienna. Italy.

Waters, TJ. (2012, November 14). “Social Media and the Arab Spring.” Retrieved from the Small Wars Journal website: http://smallwarsjournal.com/jrnl/art/social-media-and-the-arab-spring

In addition to the above listed items, the following publications will be made available in Blackboard as optional readings to augment the required course content.

Giles, G. (2012). "Russia's Public Stance on Cyberspace Issues." *2012 4th International Conference on Cyber Conflict*. NATO CCD COE Publications. Tallinn, Estonia.

Koch, R., Stelte, B., and Golling, M. (2012). "Attack Trends in Present Computer Networks." *2012 4th International Conference on Cyber Conflict. NATO CCD COE Publications*. Tallinn, Estonia.

Liles, S. (2010). "Cyber Warfare: As a Form of Low-Intensity Conflict and Insurgency." *Conference on Cyber Conflict Proceedings 2010*. CCD COE Publications. Tallinn, Estonia.

Ottis, R. (2010). "From Pitchforks to Laptops: Volunteers in Cyber Conflicts." *Conference on Cyber Conflict Proceedings 2010. NATO CCD COE Publications*. Tallinn, Estonia.

Sharma, A. (2010). "Cyber Wars: A Paradigm Shift from Means to End." *Conference on Cyber Conflict Proceedings 2010*. NATO CCD COE Publications. Tallinn, Estonia.

Tyugu, E. (2012). "Command and Control of Cyber Weapons. *2012 4th International Conference on Cyber Conflict. NATO CCD COE Publications*. Tallinn, Estonia.

Graded Material

Each assignment, quiz, project, and exam will be graded on a 0-100 point scale.

The final average is calculated by the following weights:

Assignments – Six Annotated Bibliographies	25%
Classroom Discussions	10%
Mid-term	25%
Project – Cyber Warfare Tabletop Exercise	15%
Final Exam	25%
Total	100%

The following criteria will be used for the assignment of letter grades

A	92-100
A-	90-91
B+	87-89
B	83-86
B-	80-82
C	70-79
F	0-69

The course will adhere to the university's policies on grading.

Assignment Due Dates

All assignments are to be submitted by the due dates listed in the syllabus. Work will not be accepted late. Assignments are to be submitted via Blackboard.

Projects

Each student will prepare a written report, which describes a detailed war gaming exercise: A cyber attack simulated through a tabletop exercise. The requirements of the project will be posted in Blackboard by the second week of class. A tabletop exercise will be led during the second week of the course in class. The report will be due in the fourteenth week of the course.

Class Attendance

Attendance is mandatory. A number of classes will involve in-class discussions conducted through seminar-style lectures. In the event that a student cannot attend class due to an emergency or crisis, the student is to contact the instructor as soon as possible.

Responsible Use of Computing Policy

Use of computer equipment, including Internet connections within the classroom will be conducted in accordance with the University's Responsible Use of Computing (RUC) Policy. This applies to all academic and operational departments and offices at all university locations owned or leased. The policies and procedures provided herein apply to all Mason faculty, staff, students, visitors, and contractors.

The university provides and maintains general computing services, including web and Internet resources, and telecommunication technology to support the education, research, and work of its faculty, staff, and students. At the same time, Mason wishes to protect all users' rights to an open exchange of ideas and information. This policy sets forth the responsibilities of each member of the Mason community in preserving the security, confidentiality, availability, and integrity of Mason computing resources. To accomplish these ends, this policy supports investigations of complaints involving Mason computing abuse, including sexual harassment, honor code, federal, state, applicable industry, and local law violations.

University faculty and staff members, as state employees, are subject to the Freedom of Information Act, §2.2-3700, et seq., of the Code of Virginia, and all applicable state and federal rules and regulations. While this policy endeavors to maintain user confidentiality, it cannot create, nor should faculty or staff members presume, any expectation of privacy.

Violations of this policy may result in revocation of access, suspension of accounts, disciplinary action, or prosecution. Evidence of illegal activity will be turned over to the appropriate authorities. It is the responsibility of all users of Mason computing resources to read and follow this policy and all applicable laws and procedures (user sign-on agreement).

For more information regarding the RUC Policy, consult the student handbook.

University Policies

This course will be taught in compliance with George Mason University policies, which can be found online at http://universitypolicy.gmu.edu/

Important Dates

Last day to drop with no tuition penalty	January 27
Last day to drop with a 33% tuition penalty	February 10
Last day to drop with a 67% tuition penalty	February 20
Spring Break	March 9-15
Final Exams	May 6-13

The full calendar maintained by the University Registrar can be found online at: http://registrar.gmu.edu/calendars/2013fall/

Office of Disability Services

The Office of Disability Services (ODS) is available to serve all students with disabilities, including those with cognitive (e.g., learning, psychological, and closed head injury), sensory, mobility, and other physical impairments.

The Office of Disability Services serves qualified students with disabilities to ensure equal access to the university's programs and services. A qualified student with a disability is a student with a disability, who meets the academic and technical standards required for admission or participation in the university's educational program and services. As defined in the Americans with Disabilities Act (ADA), and section 504 of the Rehabilitation Act of 1973, a person has a disability if he/she:

- Has a physical or mental impairment which substantially limits one or more major life activities, or
- Has a record of such impairment, or
- Is regarded as having such impairment

Students requesting assistance should contact the Office of Disability Services at http://ods.gmu.edu/

Course Outline

The following is the course outline. It is subject to revision.

Week 1 **Introduction to Cyber Warfare and Course Familiarization**
1/23

Reading assignment

Carr, J. (2012). *Inside Cyber Warfare: Mapping the Cyber Underworld.* Second Edition. O'Reilly Media, Inc. Sebastopol, CA. pp. 1-14.

Applegate, S. D. (2013). "The Dawn of Kinetic Cyber." *5th International Conference on Cyber Conflict*. Tallinn, Estonia. pp. 1-15.

		Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation. Santa Monica, CA. pp. 117-138.
	Classroom material	Introduction.pptx
Week 2 1/30	**Cyber Warfare Table Top Exercise**	
	Classroom material	Table_Top_Exercise.pptx
Week 3 2/6	**Seminar Discussion on Cyber Warfare**	
	Reading assignment	Carr, J. (2012). *Inside Cyber Warfare: Mapping the Cyber Underworld.* Second Edition. O'Reilly Media, Inc. Sebastopol, CA. pp. 1-14. Applegate, S. D. (2013). "The Dawn of Kinetic Cyber." *5th International Conference on Cyber Conflict*. Tallinn, Estonia. pp. 1-15. Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation. Santa Monica, CA. pp. 117-138.
	Assignment	Annotated Bibliography #1 Topic: Cyber Warfare – Real or Fiction? Are there real examples? Due by 4:00PM on 2/6
Week 4 2/13	**The Russian Federation and Eastern European Countries**	
	Reading assignment	Carr, J. (2012). *Inside Cyber Warfare: Mapping the Cyber Underworld.* Second Edition. O'Reilly Media, Inc. Sebastopol, CA. pp. 161-171; 217-242. Giles, G. (2012). "Russia's Public Stance on Cyberspace Issues." *2012 4th International Conference on Cyber Conflict*. NATO CCD COE Publications. Tallinn, Estonia. Smith, D. J. (2012, July). “Russian Cyber Operations.” Potomac Institute for Policy Studies.
	Classroom material	Russian_Federation.pptx
Week 5 2/20	**Seminar Discussion on The Russian Federation and Eastern European Countries**	
	Reading assignment	Carr, J. (2012). *Inside Cyber Warfare: Mapping the Cyber Underworld.* Second Edition. O'Reilly Media, Inc. Sebastopol, CA. pp. 161-171; 217-242.

Giles, G. (2012). "Russia's Public Stance on Cyberspace Issues." *2012 4th International Conference on Cyber Conflict*. NATO CCD COE Publications. Tallinn, Estonia.

Smith, D. J. (2012, July). “Russian Cyber Operations.” Potomac Institute for Policy Studies.

Assignment — Annotated Bibliography #2
Topic: Russian-based Cyber Warfare
Due by 4:00PM on 2/20

Week 6 **The People’s Republic of China**
2/27

Reading assignment — Carr, J. (2012). *Inside Cyber Warfare: Mapping the Cyber Underworld.* Second Edition. O'Reilly Media, Inc. Sebastopol, CA. pp. 171-175; 257-258.

Information Warfare Monitor. (2009, March 29). "JR02-2009: Tracking GhostNet: Investigating a Cyber Espionage Network." Munk Centre for International Studies. University of Toronto. Toronto, CA. Pp. 16-45. (Skim all other pages.) Retrieved from the Scribd web site: http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

Mandiant. (2013). “APT1: Exposing One of China’s Cyber Espionage Units.” Alexandria. VA.

Week 7 **Seminar Discussion on The People’s Republic of China**
3/6

Reading assignment — Carr, J. (2012). *Inside Cyber Warfare: Mapping the Cyber Underworld.* Second Edition. O'Reilly Media, Inc. Sebastopol, CA. pp. 171-175; 257-258.

Information Warfare Monitor. (2009, March 29). "JR02-2009: Tracking GhostNet: Investigating a Cyber Espionage Network." Munk Centre for International Studies. University of Toronto. Toronto, CA. Pp. 16-45. (Skim all other pages.) Retrieved from the Scribd web site: http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

Mandiant. (2013). “APT1: Exposing One of China’s Cyber Espionage Units.” Alexandria. VA.

Assignment — Annotated Bibliography #3
Topic: The People’s Republic of China
Due by 4:00PM on 3/6

3/13 Spring Break

Week 8 **Mid-term**
3/20

Week 9 **Non-state Organizations (NSOs) and Cyber Attacks**
3/27

Reading assignment

Bohn, L. E. and Satter, R. (2012, November 19.) "'Anonymous' targets Israeli websites over Gaza war." Retrieved on December 11, 2012 from the Yahoo! News website: http://news.yahoo.com/anonymous-targets-israeli-websites-over-gaza-war-220548299.html

Carr, J. (2012). *Inside Cyber Warfare: Mapping the Cyber Underworld.* Second Edition. O'Reilly Media, Inc. Sebastopol, CA. pp. 15-30.

Messmer, E. (2012, December 7). "ITU says 'network outage' after website cyberattack disrupted Dubai conference." Retrieved on December 11, 2012 from the ComputerWorld website: http://computerworld.co.nz/news.nsf/security/itu-says-network-outage-after-website-cyberattack-disrupted-dubai-conference

Schwartz, M. J. (2012, February 7). "Who is Anonymous: 10 Key Facts." Retrieved on November 28, 2012 from the Information Week website: http://www.informationweek.com/security/attacks/who-is-anonymous-10-key-facts/232600322 (view this page and the following 10 pages.)

Rattray, G. J. and Healey, J. (2011). "Chapter 5: Non-State Actors and Cyber Conflict." *America's Cyber Future: Security and Prosperity in the Information Age*. pp. 67-83.

Classroom material

NSOs and Cyber Attacks.pptx

Week 10 **Seminar Discussion on Non-State Organizations (NSOs) and Cyber Attacks**
4/3

Reading assignment

Bohn, L. E. and Satter, R. (2012, November 19.) "'Anonymous' targets Israeli websites over Gaza war." Retrieved on December 11, 2012 from the Yahoo! News website: http://news.yahoo.com/anonymous-targets-israeli-websites-over-gaza-war-220548299.html

Carr, J. (2012). *Inside Cyber Warfare: Mapping the Cyber Underworld.* Second Edition. O'Reilly Media, Inc. Sebastopol, CA. pp. 15-30.

Messmer, E. (2012, December 7). "ITU says 'network outage' after website cyberattack disrupted Dubai conference." Retrieved on

December 11, 2012 from the ComputerWorld website: http://computerworld.co.nz/news.nsf/security/itu-says-network-outage-after-website-cyberattack-disrupted-dubai-conference

Schwartz, M. J. (2012, February 7). "Who is Anonymous: 10 Key Facts." Retrieved on November 28, 2012 from the Information Week website: http://www.informationweek.com/security/attacks/who-is-anonymous-10-key-facts/232600322 (view this page and the following 10 pages.)

Rattray, G. J. and Healey, J. (2011). "Chapter 5: Non-State Actors and Cyber Conflict." *America's Cyber Future: Security and Prosperity in the Information Age*. pp. 67-83.

Assignment — Annotated Bibliography #4
Topic: Non-State Organizations (NSOs) and Cyber Attacks
Due by 4:00PM on 4/3

Week 11 4/10 **Cyber Terrorism; Tools and Targets; The Role of Social Networking**

Reading assignment

Carr, J. (2012). *Inside Cyber Warfare: Mapping the Cyber Underworld.* Second Edition. O'Reilly Media, Inc. Sebastopol, CA. pp. 89-120; 131-160; 203-216.

Cowell, A. (2012, November 19). "Cyberwar and Social Media in the Gaza Conflict." Retrieved from The New York Times website: http://rendezvous.blogs.nytimes.com/2012/11/19/cyberwar-and-social-media-in-the-gaza-conflict/

Denning, D. E. (2000, May 23). "Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. Georgetown University. Pp. 1-6

Gamer, T. (2011, September 9). "Collaborative anomaly-based detection of large-scale Internet attacks." *Computer Networks*. 56. Elsevier, Inc. Waltham, MA.

Pras, A., et al. (2010, December 10). "CTIT Technical Report 10.41: Attacks by 'Anonymous' WikiLeaks Proponents not Anonymous." *Design and Analysis of Communication Systems Group*. University of Twente, Enschede. The Netherlands.

United Nations Office on Drugs and Crime. (2012). "The Use of the Internet for Terrorist Purposes." United Nations. Vienna. Italy. Pp. 1-14; 53-100

Waters, TJ. (2012, November 14). “Social Media and the Arab Spring.” Retrieved from the Small Wars Journal website: http://smallwarsjournal.com/jrnl/art/social-media-and-the-arab-spring

Classroom material

Cyber Terrorism.pptx
Tools and Targets.pptx
Social Networking.pptx

Week 12 **Seminar Discussion on Cyber Terrorism; Tools and Targets; The Role of Social Networking**
4/17

Reading assignment

Carr, J. (2012). *Inside Cyber Warfare: Mapping the Cyber Underworld.* Second Edition. O'Reilly Media, Inc. Sebastopol, CA. pp. 89-120; 131-160; 203-216.

Cowell, A. (2012, November 19). “Cyberwar and Social Media in the Gaza Conflict.” Retrieved from The New York Times website: http://rendezvous.blogs.nytimes.com/2012/11/19/cyberwar-and-social-media-in-the-gaza-conflict/

Denning, D. E. (2000, May 23). “Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. Georgetown University. Pp. 1-6

Gamer, T. (2011, September 9). "Collaborative anomaly-based detection of large-scale Internet attacks." *Computer Networks*. 56. Elsevier, Inc. Waltham, MA.

Pras, A., et al. (2010, December 10). “CTIT Technical Report 10.41: Attacks by 'Anonymous' WikiLeaks Proponents not Anonymous.” *Design and Analysis of Communication Systems Group*. University of Twente, Enschede. The Netherlands.

United Nations Office on Drugs and Crime. (2012). “The Use of the Internet for Terrorist Purposes.” United Nations. Vienna. Italy. Pp. 1-14; 53-100

Waters, TJ. (2012, November 14). “Social Media and the Arab Spring.” Retrieved from the Small Wars Journal website: http://smallwarsjournal.com/jrnl/art/social-media-and-the-arab-spring

Assignment

Annotated Bibliography #5
Topics: Cyber Terrorism; Tools and Targets
Due by 4:00PM on 4/17

Week 13 **U.S. Policies – Defensive and Offensive Cyber Initiatives**
4/24

Reading assignment	Carr, J. (2012). *Inside Cyber Warfare: Mapping the Cyber Underworld.* Second Edition. O'Reilly Media, Inc. Sebastopol, CA. pp. 31-44; 203-216. gHale. (2012, November 19). "Obama Inks Cyber Attack Directive." Retrieved on December 3, 2012 from the ISS Source website: http://www.isssource.com/obama-inks-cyber-attack-directive/ Sanger, D. E. and Shanker, T. (2013, February 3). "Broad Powers Seen for Obama in Cyberstrikes." Retrieved from The New York Times website: http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html?partner=rss&emc=rss&pagewanted=all&_r=0
Classroom material:	US Initiatives.pptx

Week 14 **Seminar Discussion on U.S. Policies – Defensive and Offensive Cyber Initiatives**
5/1

Reading assignment	Carr, J. (2012). Inside Cyber Warfare: Mapping the Cyber Underworld. Second Edition. O'Reilly Media, Inc. Sebastopol, CA. pp. 31-44; 203-216. gHale. (2012, November 19). "Obama Inks Cyber Attack Directive." Retrieved on December 3, 2012 from the ISS Source website: http://www.isssource.com/obama-inks-cyber-attack-directive/ Sanger, D. E. and Shanker, T. (2013, February 3). "Broad Powers Seen for Obama in Cyberstrikes." Retrieved from The New York Times website: http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html?partner=rss&emc=rss&pagewanted=all&_r=0
Assignment	Annotated Bibliography #6 Topics: U.S. Engagement in Cyber Warfare Due by 4:00PM on 5/1 Project – Cyber Warfare Tabletop Exercise

Week 15 **Final Exam**
5/8