

**WILLIAM J. PERRY CENTER FOR HEMISPHERIC DEFENSE STUDIES  
NATIONAL DEFENSE UNIVERSITY  
WASHINGTON, DC 20319-5066**



**CYBERSECURITY  
ISSUES IN NATIONAL AND INTERNATIONAL  
SECURITY**

**Sep 2013**

**Kevin P. Newmeyer**  
Assistant Professor of National Security Affairs

**Ken LaPlante**  
Acting Director, CHDS

**William J. Perry**  
Center for Hemispheric Defense Studies  
National Defense University  
Bldg 62, 300 5th Avenue, SW  
Washington, DC 20319-5066  
Teléfono: (202) 685-4670  
Fax: (202) 685-4674  
[www.ndu.edu/chds](http://www.ndu.edu/chds)

### **Disclaimer**

This document contains educational material designed to promote discussion by students of the William J. Perry Center for Hemispheric Defense Studies (Perry Center). It does not necessarily reflect the views of the National Defense University or the Department of Defense.

### **Perry Center Copyright Notice**

The contents of this document are the property of the U.S. Government and are intended for the exclusive use of the faculty and students of the Perry Center. No further dissemination is authorized without the express consent of the Perry Center.

### **Perry Center Policy on Non-attribution**

Presentations by guest speakers, seminar leaders, students and panelists, including renowned public officials and scholars, constitute an important part of university academic curricula. So that these guests, as well as faculty and other officials, may speak candidly, the Perry Center offers its assurance that their presentations at the courses, or before other Perry Center-sponsored audiences, will be held in strict confidence.

This assurance derives from a policy of non-attribution that is morally binding on all who attend: without the express permission of the speaker, nothing he or she says will be attributed to that speaker directly or indirectly in the presence of anyone who was not authorized to attend the lecture.

### **Policy and Procedures on Academic Integrity**

This statement on academic integrity applies to all components of the National Defense University. The purpose of this broad university policy is to establish a clear statement for zero tolerance for academic dishonesty and to promote consistent treatment of similar cases across the University on academic integrity and the integrity of the institution. This document should not be interpreted to limit the authority of the University President or the Provost and Vice President for Academic Affairs. This policy includes two key areas: academic integrity as it applies to students and participants at National Defense University; and academic integrity as it applies to assigned faculty and staff.

### **Academic Dishonesty**

Academic dishonesty is not tolerated. Academic dishonesty includes, but is not limited to: falsification of professional and academic credentials; obtaining or giving aid on an examination; having unauthorized prior knowledge of an examination; doing work or assisting another student to do work without prior authority; unauthorized collaboration; multiple submissions; and plagiarism.

- *Falsification of professional and academic credentials:* Students are required to provide accurate and documentable information on their educational and professional background. If a student is admitted to the University with false credentials, he or she will be sanctioned.

- *Unauthorized collaboration* is defined as students working together on an assignment for academic credit when such collaboration is not authorized in the syllabus or directed by the instructor.
- *Multiple submissions* are instances in which students submit papers or work (whole or multiple paragraphs) that were or are currently being submitted for academic credit at other institutions. Such work may not be submitted at the National Defense University without prior written approval by both the National Defense University professor/instructor and approval of the other institution.
- *Plagiarism* is the unauthorized use, intentional or unintentional, of intellectual work of another person without providing proper credit to the author. While most commonly associated with writing, all types of scholarly work, including computer code, speeches, slides, music, scientific data and analysis, and electronic publications are not to be plagiarized. Plagiarism may be more explicitly defined as:
  - Using another person's exact words without quotation marks and a footnote/endnote.
  - Paraphrasing another person's words without a footnote/endnote.
  - Using another person's ideas without giving credit by means of a footnote/endnote.
  - Using information from the web without giving credit by means of a footnote/endnote. (For example: If a student/professor/instructor/staff member enrolled or assigned to NDU copies a section of material from a source located on the internet (such as Wikipedia) into a paper/article/book, even if that material is not copyrighted, that section must be properly cited to show that the original material was not the student's).

### **Sanctions for Violations of Academic Integrity**

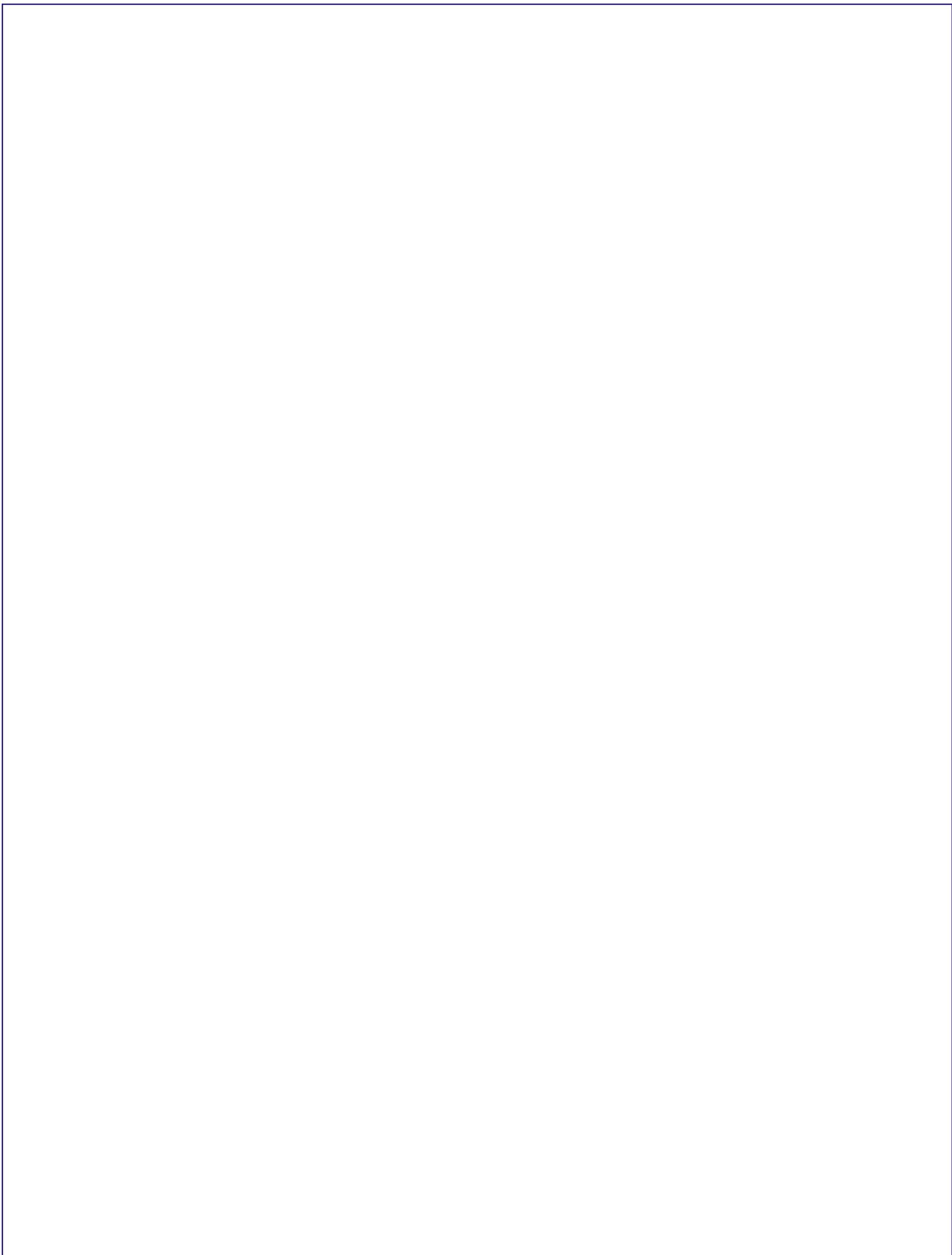
Sanctions for violating the academic integrity standards include but are not limited to: disenrollment, suspension, denial or revocation of degrees or diplomas, a grade of no credit with a transcript notation of "academic dishonesty;" rejection of the work submitted for credit, a letter of admonishment, or other administrative sanctions. Additionally, members of the United States military may be subject to non-judicial punishment or court-martial under the Uniformed Code of Military Justice.

### **Processing of Potential Violations of Academic Integrity**

The University is committed to establishing, maintaining, and enforcing a high level of academic integrity throughout the entire University community by implementing a very strict academic integrity policy. Cases in which a student is suspected of violating the academic integrity policy will be processed in accordance with the procedures set forth in the NDU Handbook, Section 5.12, entitled, "Student Disenrollment."

### **Perry Center Policy on Attendance of Classes and Activities**

Participants have the responsibility to attend all activities and classes punctually. Please refrain from scheduling meetings, or accepting invitations to attend other activities, visits or appointments with diplomatic representatives from your country, friends or acquaintances during class times and any other time where your presence is required at the Perry Center.



## Grading Standards for Participants in the William J. Perry Center for Hemispheric Defense Studies Courses

### I. Participants' Evaluations

The Perry Center applies several different mechanisms for evaluating a student's work including examinations, BOG contribution, and papers.<sup>1</sup>

### II. Grading Scale

Grade	Numerical Scale	Value
A+	100 – 97	Excellent
A	96.9 – 93	Very High
A-	92.9 – 90	High
B+	89.9 – 87	Above Average
B	86.9 – 83	Average
B-	82.9 – 80	Below Average
C+	79.9 – 77	Marginal
C	76.9 – 73	Passing
C-	72.9 – 70	Minimal Pass
F	69 or less	Insufficient
I		Incomplete

### III. Examinations

Tests and quizzes will be administered to assess participants' ability to understand and analyze the readings and the topics discussed in plenary as well as in BOG sessions.

The following guidance will be applied:

Grade	Value
A+ (97-100)	Organized, coherent and well-written responses that completely address the questions, convey all applicable major and key minor points, and demonstrate total grasp of the topic.
A (96.9 – 93)	Answers address all major and key minor considerations, demonstrate excellent grasp of the topic.
A- (92.9 – 90)	Well-crafted answer that discusses important ideas related to the topic.

<sup>1</sup> The Perry Center has adopted and adapted several standards used at College of International Security Affairs (NDU), the National War College (NDU), and the Naval War College.

B+ (89.9 – 87)	Answers reflect average graduate graduate-level performance, successfully considering the topic of each question.
B (86.9 – 83)	Answers address the questions but fail to address all relevant concepts or to demonstrate a clear understanding of the topic.
B- (82.9 – 80)	Cursory responses that do not fully address the questions or do not demonstrate clear understanding of the topic or relevant concepts.
C+ (79.9 – 77)	Answers demonstrate poor understanding of the topic, marginal support for arguments, and/or miss major analytical elements or concepts.
C (76.9 – 73)	Answers address the topic but do not provide sufficient discussion to demonstrate adequate understanding of the topic.
C- (72.9 – 70)	Answers address some of the ideas but response is incoherent.
F (69)	Insufficient

#### IV. Essay/Research Paper

The student's ability to gather information or to do research, to organize material logically, to compose and express thoughts in coherent and effective prose, and to use standard written language are crucial for paper content and composition. Submissions are to be typed (double-spaced) using 12-point Times New Roman

The following six elements are essential for a high-level paper:

1. It establishes the relevant question clearly;
2. It answers the question in a highly analytical manner;
3. It proposes a well-defined thesis, stated early on;
4. It presents evidence to support that thesis;
5. It addresses, explicitly or implicitly, opposing arguments or weaknesses in the thesis and supporting evidence (this constitutes a counterargument); and,
6. It accomplishes the above in a clear and well-organized fashion

The following guidance will be applied:

Grade	Value
A+ (97-100)	Offers a genuinely new understanding of the subject. Thesis is definitive and exceptionally well-supported, while counterarguments are addressed completely. Essay indicates brilliance.
A (96.9 – 93)	Work of superior quality that demonstrates a high degree of original, critical thought. Thesis is clearly articulated and focused, evidence is significant, consideration of arguments and counter-argument is comprehensive, and essay is very well-written.
A- (92.9 – 90)	A well-written, insightful essay that is above the average expected of graduate work. Thesis is clearly defined; evidence is relevant and purposeful, arguments and counter-argument are presented effectively.
B+ (89.9 – 87)	A well-executed essay that meets standards. A solid effort in which a thesis is articulated, the treatment of supporting evidence and

	counterargument has strong points, and the answer is well-presented and constructed.
B (86.9 – 83)	An essay that is a successful consideration of the topic and demonstrates average graduate performance. Thesis is stated and supported, counterarguments considered, and the essay is clear and organized.
B- (82.9 – 80)	Thesis is presented, but the evidence does not fully support it. The analysis and counterarguments are not fully developed and the essay may have structural
C+ (79.9 – 77)	The essay is generally missing one or more of the elements described above. The thesis may be vague or unclear, evidence may be inadequate, analysis may be incomplete, and/or the treatment of the counterargument may be deficient.
C (76.9 – 73)	While the essay might express an opinion, it makes inadequate use of evidence, has little coherent structure, is critically unclear, or lacks the quality of insight deemed sufficient to explore the issue at hand adequately.
C- (72.9 – 70)	Attempts to address the question and approaches a responsible opinion, but is conspicuously below graduate-level standards in several areas. The thesis may be poorly stated with minimal evidence or support and counterarguments may not be considered. Construction and development flaws further detract from the readability of the essay.
F (69)	Fails conspicuously to meet graduate-level standards. Essay has no thesis, significant flaws in respect to structure, grammar, and logic, and displays an apparent lack of effort to achieve the course requirements. Gross errors in construction and development detract from the readability of the essay
I	Incomplete

## V. Contribution to BOG Sessions

The diversity of the student's body is one of the main features of the Perry Center courses. Students come from all countries of the hemisphere, with different professional and personal background, this unique characteristic tremendously enriches the discussion in the BOG sessions. Professor serving as facilitators, evaluate the contribution made by each student, assessing the quality of the student's input. The goal in assigning a classroom contribution grade is not to measure the number of times students have spoken, but how well they have understood the subject matter, enriched discussion, and contributed to their seminar colleagues' learning. This caliber of commitment entails that each student come prepared to take part in discussion by absorbing the readings, listening attentively to presentations, and thinking critically about both. Students are expected to prepare for and be thoughtfully engaged in each session. Not to contribute or to say very little in class undercuts the learning experience for everyone in the BOG. Differences of opinion should be conveyed with appropriate regard for the objective, academic, and professional environment fostered at the Perry

Center. BOG preparation and contribution will be graded at according to the following standards:

Grade	Value
A+ (97-100)	Contributions indicate brilliance through a wholly new understanding of the topic. Demonstrates exceptional preparation for each session as reflected in the quality of contributions to discussions. Strikes an outstanding balance of “listening” and “contributing.” Respects fellow's ideas while challenging them when necessary.
A (96.9 – 93)	Contribution is always of superior quality. Unfailingly thinks through the issue at hand before comment. Can be relied upon to be prepared for every BOG session, and contributions are highlighted by insightful thought, understanding, and in part original interpretation of complex concepts. Ability to listen and comment fellow's ideas.
A- (92.9 – 90)	Fully engaged in seminar discussions and commands the respect of colleagues through the insightful quality of their contribution and ability to listen to and analyze.
B+ (89.9 – 87)	A positive contributor to seminar meetings who joins in most discussions and whose contributions reflect understanding of the material. Occasionally contributes original and well-developed insights.
B (86.9 – 83)	Average graduate level contribution. Involvement in discussions reflects adequate preparation for seminar with the occasional contribution of original and insightful thought, but may not adequately consider others' contributions.
B- (82.9 – 80)	Contributes, but sometimes speaks out without having thought through the issue well enough to marshal logical supporting evidence, address counterarguments, or present a structurally sound
C+ (79.9 – 77)	Sometimes contributes voluntarily, though more frequently needs to be encouraged to participate in discussions. Content to allow others to take the lead. Minimal preparation for seminar reflected in arguments lacking the support, structure or clarity to merit graduate credit.
C (76.9 – 73)	Contribution is marginal. Occasionally attempts to put forward a plausible opinion, but the inadequate use of evidence, incoherent logical structure, and a critically unclear quality of insight is insufficient to adequately examine the issue at hand. Usually content to let others form the seminar discussions.
C- (72.9 – 70)	Lack of contribution to seminar discussions reflects substandard preparation for sessions. Unable to articulate a responsible opinion. Sometimes displays a negative attitude.
F	Rarely prepared or engaged. Student demonstrates unacceptable preparation and fails to contribute in any substantive manner. May be extremely disruptive or uncooperative and completely unprepared for seminar

## **VI. Grade communication to the students.**

Feedback will be substantive, constructive, and timely. Test and papers will be returned to the students.

1. Professors will inform in writing and via Blackboard all tests and papers grades, including comments that explain the grade.
2. At the end of the course, professors will sent to the Registrar, a complete list of all grades as well as the final Evaluation of Academic Performance of each student.

## **VII. Challenging a Grade**

The Perry Center recognizes that all participants in its courses are entitled to request a review of the grades received as a result of coursework. In cases of a challenge to a grade, the burden of proof rests with the student. In all cases where there is a reasonable doubt, the grade originally given will be retained. Requests for a change of grade will not be approved if the new grade results from additional work performed after the initial grade has been assigned.

The following process will take place when a student contests a grade:

1. No later than 15 days after receiving the grade, the student will request in writing an Explanation of his/her from the professor who assigned the grade. The professor, no later than 15 days after receiving the request, will respond to the request explaining the basis for the student's grade.
2. If the student believes that the explanation is still unsatisfactory, he/she will request to the Associate Dean of Academic Affairs, Division of Education a Review of his/her grade. This request should be submitted no later than 15 days after receiving the Explanation. The student shall state the facts and must provide a clear and complete justification for the request.
3. After this communication, if the student still deems that the Review is not satisfactory, he/she is entitled to resort to a third and final instance by appealing the grade to the Dean of Academic Affairs, no later than 15 days after receiving the review. The Dean of Academic Affairs will convene a faculty committee of three Perry Center professors who did not participate in the previous two review instances. Within 15 days of receiving the appeal, the committee will review all pertinent information relating to the case, which may include interviewing the instructor and student if necessary. The Dean of Academic Affairs, will communicate the results to the student thus bringing the process to an end. The decision of the Dean of Academic Affairs is final.

## **COURSE INTRODUCTION AND GENERAL DESCRIPTION**

This is a five-week course, mixing on-line and in-residence activities to deepen students' understanding of the defense and security threats posed by cyber based threats to information systems and other types of critical infrastructure. The program takes place in two phases.

### **Distance Phase:**

During a three-week, on-line period, prospective participants will receive reading material – which they will be asked to analyze and evaluate. Simultaneously, they will be asked participate in threaded discussions on the weeks' topics. The evaluations of the reading analyses and the participation in on-line discussions will determine the student's eligibility to attend the resident phase of the course.

### **Resident Phase:**

During a two-week resident phase at CHDS, approved participants will spend their time engaged in an intensive program of lectures, conferences, seminars, case-studies, debates and readings. They will also be developing their policy paper and conducting research in the National Defense University library.

### **Pre-Requisites:**

As pre-requisites for the course, candidates must hold an accepted college degree and demonstrate ability to read texts in English. Those who are selected to attend will be asked to present a copy of all college transcripts, including a copy translated into English. These documents will be evaluated to confirm equivalence to a university degree and thus eligibility for this course. Selected participants will be given detailed instructions.

### **Reading Load:**

Participants must be aware that they will be required to read about 80-100 pages per week during the distance phase, and about 60 pages per day during the in-resident phase of the course.

### **Course Goal:**

Deepen the participant's understanding and analysis of the security challenges and threats posed by the growing dependence on cyber-based systems. Course graduates will be able to make preliminary assessments of cybersecurity and be able to articulate cyber risk within their organization's operations and processes.

## **COURSE OBJECTIVES**

Upon completion of the course the students will be able to:

1. Evaluate the importance of cybersecurity; understand the cyber risks to national and international security in developing and developed states.
2. Describe the risks of cybercrime, cyber terrorism, and cyber war.
3. Evaluate different paradigms for cybersecurity and determine the approach that best applies in an individual country.

4. Assess the strengths and weaknesses of the various international and national cybersecurity strategies.
5. Understand the role of government and the private sector in cybersecurity and critical infrastructure protection.

## **COURSE DEVELOPMENT/METHODOLOGY**

### **Distance Phase (3 weeks)**

The Distance phase of the course lasts three weeks and will be conducted via Blackboard and via email between the professor and the students. Communication via email and blackboard will take place in Spanish or English. The distance phase is designed to help the student familiarize themselves with the methodology of the course and refine their theoretical knowledge of policy development and cybersecurity necessary for the resident phase of the course, which will take place in Washington, D.C. This phase will establish a baseline understanding of the concepts to be explored in the resident phase. The most important task of the Distance Phase will be the policy paper proposal.

### **Resident Phase (2 weeks)**

The in-residence phase will be conducted at CHDS' premises. Students will engage in in-depth discussion on theoretical and practical discussions about cyber security policy, threats, and the various approaches to respond to them. They will be challenged to analyze complex circumstances related to these themes. Methodology to help students deepen their knowledge in this field will include lectures, conferences with experts and practitioners, seminars, and case-studies. Themes will be distributed in a way that students expand their understanding of the theories and issues surrounding these phenomena as well as the complexities of the various solution sets. Given present global challenges, the various paradigms and country approaches towards cybersecurity will be discussed in depth.

During this phase, students will be expected to take advantage of the National Defense University library and resources to continue the research and writing process on their policy papers. They will also be expected to take advantage of the presence of the professors to have one-on-one discussions to help guide and direct their research efforts.

### **Course Project**

During the residence phase, the students will be divided into 3-4 person teams that will draft a 2-3 page issue paper and accompanying presentation. The issue paper is to be targeted toward a minister/senior official in their nation's government that highlights a cybersecurity issue facing the country and establishes a notional plan of action to respond to the threat. The final presentations will be made during the last two days of the course.

**IMPORTANT: ALL PAPERS MUST INCLUDE THE FOLLOWING INFORMATION ON THE FRONT COVER WHETHER SUBMITTED ELECTRONICALLY OR HARD COPY:**

- STUDENTS' NAMES
- PAPER TITLE

- DATE

## COURSE GRADING

Grades will be ascribed according to the following distribution:

- Participation throughout course 50% (25% Distance, 25% Resident)
- Group project 50%

## DISTANCE PHASE

**Instructor's Note:** The main objectives of the Distance Phase are for the students to develop a baseline understanding of the theories and issues surrounding cybersecurity and cyber threats and how they might apply to their country. Distance phase participation is essential for students to be successful in the resident phase.

The weekly readings and analyses during the on line phase are very important. The initial analyses help the instructor determine the student's level of comprehension of the readings and their ability to do graduate level analysis. Because of this they are also critical in determining the eligibility of the student to attend the Resident Phase of the course. The reading analyses are due at the end of each week during the online phase.

### Week 1

**Goal:** Orient and inform participants about the course concept and its requirements and provide them with an overview on the main themes of the course.

#### Objectives:

- Participants should be able to give a general description of the course.
- Participants should be able to define cybersecurity.
- Participants should be able to identify cyber risks.

#### Assignment:

- Write a 1-2 page analysis of the mandatory readings.
- Participate as directed in the Blackboard discussion.

#### Mandatory Readings:

- English
  - Karas, T, Moore, J.H., & Parrott (2008) Metaphors for Cyber Security, Sandia Report No, SAND2008-5381. (PDF).
  - Symantec Internet Security Threat Report No. 18.

- Spanish
  - Joyanes Aguilar, L. (2010). Introducción: Estado del arte de la ciberseguridad. Cuadernos de Estrategia No. 149, pp. 13-41. (PDF)
  - Symantec Informe sobre amenazas a la seguridad en internet No. 18 (pdf) [http://www.symantec.com/es/mx/security\\_response/publications/threatreport.jsp](http://www.symantec.com/es/mx/security_response/publications/threatreport.jsp)

#### Recommended Reading

- SecDev Foundation & Insituto Igarape (2012). A fine balance: Mapping cyber (in)security in Latin America. (English only)
- Willis, H.H. (2007). Guiding resource allocations based on terrorism risk. *Risk Analysis* 27 (3), 597-606. doi: 10.1111/j.1539-6924.2007.00909.x
- Dito, B., Contreras, B., & Kellerman, T. (Eds.). (2013). Latin America and Caribbean cybersecurity trends and government responses. Trend Micro. Retrieved from <http://www.oas.org/cyber/documents/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf> (English) (Spanish)

#### Recommended Video

- DiploFoundation (2008). Internet governance- Internet Security (Video) [http://www.youtube.com/watch?v=HF-mnP\\_WDx8](http://www.youtube.com/watch?v=HF-mnP_WDx8)
- Blum, A. (2013). TED talk: What is the Internet really? (Video) [http://www.ted.com/talks/andrew\\_blum\\_what\\_is\\_the\\_internet\\_really.html](http://www.ted.com/talks/andrew_blum_what_is_the_internet_really.html)
- Glenny, M (2011) TED Talk: Hire the Hackers (Video) [http://www.ted.com/talks/misha\\_glenny\\_hire\\_the\\_hackers.html](http://www.ted.com/talks/misha_glenny_hire_the_hackers.html)

## Week 2

**Goal:** Provide an initial introduction to the questions of cyber risk and the threats to networks in an age of globalization.

**Objectives:** Participants will be able to identify international concerns and efforts regarding cybersecurity.

#### **Assignment:**

- Write a 1-2 page analysis of each of the mandatory readings.
- Participate in the Blackboard discussion as directed.

#### **Mandatory Readings:**

- English
  - UN General Assembly Res.57/139. Creation of a global culture of cybersecurity.
  - OAS General Assembly Res: AG / RES. 2004 (XXXIV-O/04), titled “The Inter-American Integral Strategy to Combat Threats to Cyber Security”

- Spanish
  - ONU Asamblea General Res.57/139. Creación de una cultura mundial de seguridad cibernética.
  - OEA Asamblea General Res: AG / RES. 2004 (XXXIV-O/04) la Estrategia Interamericana Integral para Combatir las Amenazas a la seguridad cibernética

**Recommended Websites:**

Organization of American States Cyber Security Program  
 English: <http://www.oas.org/en/sms/cyber/default.asp>  
 Spanish: <http://www.oas.org/es/ssm/cyber/default.asp>

International Telecommunication Union  
 English: <http://www.itu.int/cybersecurity/>  
 Spanish: <http://www.itu.int/cybersecurity/index-es.html>

Cybercrime Convention  
<http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG>

Covenio sobre la Ciberdelinuencia.  
[http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS\\_185\\_spanish.PDF](http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_spanish.PDF)

Recommended Video:

Hillis, D. (2013). TED Talk. The Internet could crash. We need a Plan B.  
[http://www.ted.com/talks/danny\\_hillis\\_the\\_internet\\_could\\_crash\\_we\\_need\\_a\\_plan\\_b.html](http://www.ted.com/talks/danny_hillis_the_internet_could_crash_we_need_a_plan_b.html)

**Week 3**

**Goal:** Understand the variety of national approaches to cybersecurity

**Objectives:**

- Participants should be able to discern between the different national approaches to cybersecurity policy

**Assignment:**

- Write a 1-2 page analysis of each of the mandatory readings.
- Participate in the Blackboard discussion as directed.

**Mandatory Readings:**

- English:

- The White House: International Strategy for Cyberspace (English Only)
- National Security Council: Cybersecurity  
<http://www.whitehouse.gov/administration/eop/nsc/cybersecurity>
- Spanish
  - Sanchez Medero, G. La ciberseguridad en Europa. (Pdf).
- Optional Readings

Canada's Cyber Security Strategy

ITU National Cybersecurity Strategy Guide (2011)

New Zealand's National Cyber Security Strategy

Cyber Security Strategy of the United Kingdom: Safety security and resilience in cyber space

Panama Cyber Security Strategy

Trinidad and Tobago National Cyber Security Strategy

Conopes (2011, July 11). Lineamientos de política para ciberseguridad y ciberdefensa. Documento Conopes 3701. (Colombian Cyber Security Strategy)

Estrategia Española de Seguridad

Luijff, E., Besseling, K. & de Graff, P. (2013). Nineteen national cybersecurity strategies. *International Journal of Critical Infrastructures*, 9(1/2), 3-31. doi: 10.1504/IJCIS.2013.051608

OECD (2012), "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy", *OECD Digital Economy Papers*, No. 211, OECD Publishing. <http://dx.doi.org/10.1787/5k8zq92vdgtl-en>

### **Recommended Videos:**

Google (2009). Google DC Talks: Developing a Natl Cybersecurity Strategy. [http://www.youtube.com/watch?v=vN0Ca\\_IFno](http://www.youtube.com/watch?v=vN0Ca_IFno) (This is a rather long but useful).

Errol (2013). UK Cyber Security Strategy Intelligence Briefing. <http://www.youtube.com/watch?v=9TnNHIQhTJ0>

Government of India (2013). National Cyber Security Policy- 2013 released. <http://www.youtube.com/watch?v=nQK735GeP8o>

## COURSE SCHEDULE AND READINGS

### RESIDENT PHASE

**Instructor's Note:** The Main objective of the Resident Phase is to develop a broadened understanding of cybersecurity and its role in national security and defense.

In addition to research, there will be daily discussions on topics related to cybersecurity challenges. These will include lectures by Perry Center faculty and guest speakers. Approximately 70% of the student's day will be dedicated to seminar and reading discussions.

**Daily Class Schedule:** Each day, students will attend approximately 7 hours of class with 1.5 hours for lunch. The day will consist of two lecture sessions and two BOG sessions. There will also be a daily Student Case presentation to start the day. During the case discussion students will present a cyber incident from their country and what policy impacts resulted.

#### DAY 1: ADMINISTRATION AND ORIENTATION DAY

##### Daily Objectives:

- Familiarize the Students with the overall structure and organization of the course.
- Define risk
- Review distance phase

##### Mandatory Readings:

###### English

Willis, H.H. (2007). Guiding resource allocations based on terrorism risk. *Risk Analysis* 27 (3), 597-606. doi: 10.1111/j.1539-6924.2007.00909.x

###### Spanish

Cardona, O. D. (1993). Evaluación de la amenaza, la vulnerabilidad y el riesgo. *En: A. Maskrey (ed.) Los desastres no son naturales*, 51-74.

Lavell, A. (2001). Sobre la gestión del riesgo: apuntes hacia una definición. *Biblioteca Virtual en Salud de Desastres-OPS*. Consultado el, 4.

##### Recommended Video

Cybenko, G. The future of cyber security risk (Video).  
[http://www.youtube.com/watch?v=zBx0hcj9\\_AU](http://www.youtube.com/watch?v=zBx0hcj9_AU)

## DAY 2: Cybersecurity Paradigms and Risk

### Daily Objectives:

- Examine the national security, economic, and public health paradigms for cybersecurity strategy and policy.
- Define risk with regard to cybersecurity and its impact on national security.

### **Mandatory Readings: Cybersecurity Paradigms**

#### **English:**

Mulligan, D. K. & Schneider, F.B. (2011). Doctrine for cybersecurity. *Daedalus* 140 (4), 70-92. doi: 10.1162/DAED\_a\_00116.

Charney, S. (2012). Collective defense: Applying the Public-Health Model to the Internet. *IEEE Security & Privacy* 10 (2), 54-59. doi:10.1109/MSP.2011.152

Harknett, R.J., & Stever, J.A. (2011). The new policy world of cybersecurity. *Public Administration Review*. 71 (3), pp. 455-460.

Moore, T. (2010). The economics of cybersecurity: principles and policy options. *International Journal of Critical Infrastructure Protection* 3 (3-4), 103-117, doi: 10.1016/j.cip.2010.10.002

#### **Spanish:**

. Fojon Chamoro, E. & Sanz Villalba, A.F. (2010). Ciberseguridad en Espana: una propuesta para su gestion. *ARI* 101, pp. 1-8

## DAY 3: Cybercrime

### Daily Objectives:

- Analyze the distinct manifestations of cybercrime.
- Understand the role of organized crime in cybercrime
- Identify the different strategies in place to combat cybercrime.
- Evaluate the effectiveness of these counter-cybercrime strategies and policies.

### **Mandatory Readings:**

#### • **English**

- Provos, N., Rajab, M.A., & Mavrommatis, P.(2009). Cybercrime 2.0: When the cloud turns dark. *Communications of the ACM* 52(4), pp. 42-47. doi: 10.1145/1498765.149782

#### • **Spanish**

- Salom Clotet, J. (2011). El Ciberespacio y el crimen organizado. Cuadernos de Estrategia No. 149, pp. 131-164.

### **Recommended Readings:**

- Measuring the cost of cybercrime. Presentation at 11<sup>th</sup> Workshop on the Economics of Information, Berlin, Germany. (2012). <http://lyle.smu.edu/~tylerm/weis12pres.pdf>
- Symantec Internet Security Threat Report No. 18. (pdf) English
- Symantec Informe sobre amenazas a la seguridad en internet No. 17 (pdf) Spanish.
- Sood, A., Enbody, R., & Bansal, R. (2012). Cybercrime: Dissecting the state of underground enterprise. *IEEE Internet Computing*. doi.  
<http://doi.ieeecomputersociety.org/10.1109/MIC.2012.61>

Video:

Percoco, N. (2013, February 28). The lifecycle of cybercrime. (Video)

<https://www.youtube.com/watch?v=rBbcep1rYEK>

## **DAY 4: Cyberterrorism**

### **Daily Objectives:**

- Evaluate the nature and threat of cyberterrorism
- Define critical infrastructure and why it might be a terrorism target.

### **Mandatory Readings:**

- **English**
  - Rollins, J. & Wilson, C. (2007). Terrorist capabilities for cyberattack: Overview and policy issues. *CRS Report to Congress: RL33123*.
  - Theohary, C.A. & Rollins, J. (2011). Terrorist use of the Internet: Information operations in cyberspace. *CRS Report to Congress. R41674*
- **Spanish**
  - Candau Romero, J. (2011) Estrategias nacionales de ciberseguridad. *Ciberterrorismo. Cuadernos de Estrategia No. 149*, pp. 259-321.
  - Jordan, J. & Torres, M.R. (2007). Internet y actividades terroristas: el caso de 11-M. *El Profesional de la Información 16*(2), pp. 123-130.
  - Video: *Ciberterrorismo: El lado oscuro de la red. TVE (2010)*.  
<http://www.rtve.es/alcanta/videos/television/informe-semanal-ciberterrorismo-lado-oscuro-red/798175/>

### **Recommended Readings**

Kan, P.R. (2013). Cyberwar in the underworld: Anonymous versus Los Zetas in Mexico. *Yale Journal of International Affairs 8* (1) 40-51.

Lachow, I., & Richardson, C. (2007). *Terrorist use of the Internet: The real story*. DTIC Document. Retrieved from <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA518156>

### **Recommended Video**

List 25 (2013, May 6) 25 biggest cyber attacks in history. (Video)  
[https://www.youtube.com/watch?v=ZI\\_BQoJqCIM](https://www.youtube.com/watch?v=ZI_BQoJqCIM)

Knowledge@Wharton (2012, December 6). Security Expert Amos Guiora: Cyberterrorism poses an enormous risk. (Video) <https://www.youtube.com/watch?v=-zzNtjxo-bk>

## **DAY 5: Cyberwar**

### **Daily Objectives:**

- Understand what the U.S. strategy and policies are regarding cyber war.
- Understand the applicability of international law to cyber conflict
- Discuss the strategic implications of cyber conflict to national security planning and policy.

### **Mandatory Readings:**

- **English**
  - Farwell, J.P. & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival: Global Politics and Strategy* 53(1), 23-40.
  - U.S. Department of Defense (2011). Department of Defense strategy for operating in cyberspace.
- **Spanish**
  - Diaz, del Rio Duran, J.J. (2010). La ciberseguridad en el ámbito militar. Cuadernos de Estrategia No. 149, pp. 215- 256..
  - Torres Soriano, M.R. (2011). Los dilemas estratégicos de la ciberguerra. *Ejercito: de tierra español* No. 839, pp. 14-19.

### **Recommended Readings:**

- Lewis, J.A. & Timlin, K. (2011). *Cybersecurity and cyberwar: Preliminary assessment of national doctrine and organization* in Resources: Ideas for Peace and Security. U.N. Institute for Disarmament Research. Retrieved from [http://unidir.org/bdd/fiche-ouvrage.php?ref\\_ouvrage=92-9045-011-J-en](http://unidir.org/bdd/fiche-ouvrage.php?ref_ouvrage=92-9045-011-J-en)

### **Video**

- Clarke, R. A. (2012, December 12) Cyberwar in 2013. Economist.(Video). [https://www.youtube.com/watch?v=6\\_ek8mugOUc](https://www.youtube.com/watch?v=6_ek8mugOUc)

## **DAY 6: International Efforts on Cybercrime and Cybersecurity**

**Daily Objectives:**

- Identify the strengths and limitations of a current international approaches to cybersecurity
- Identify the strengths and weaknesses of current international approaches to cybercrime
- Determine how counterfeiting undermines the licit economy and governance.

**Mandatory Readings:**

Newmeyer, K. (2010). FATF as a model for Internet governance. *IEEE Second Worldwide Summit on Cybersecurity, London* pp. 1-5

Council of Europe Cybercrime Convention, Budapest 2001.

English Text: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

Spanish Text: [http://www.coe.int/t/dghl/standardsetting/t-cy/ETS\\_185\\_spanish.PDF](http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_spanish.PDF)

**Recommended Readings:**

Rosenzweig, P. (2012). The international governance framework for cybersecurity. *Canada-United States Law Journal*, 37(2), 405-432.

Scholberg, S. & Ghernaoui-Heilie, S. (2011). A global treaty on cybersecurity and cybercrime (2<sup>nd</sup> Ed.).  
[http://www.cybercrimelaw.net/documents/A\\_Global\\_Treaty\\_on\\_Cybersecurity\\_and\\_Cybercrime\\_Second\\_edition\\_2011.pdf](http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime_Second_edition_2011.pdf)

OAS Declaration on Strengthening Cyber Security in the Americas (March 2012) English and Spanish text at <http://www.cicte.oas.org/Rev/En/Documents/Declarations.asp>

OAS AG/RES. 2004(XXXIV-O/04) Adoption of a Comprehensive Inter-America Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity.

English Text: [http://www.cicte.oas.org/Rev/En/Documents/OAS\\_GA/AG-RES.%202004%20\(XXXIV-O-04\)\\_EN.pdf](http://www.cicte.oas.org/Rev/En/Documents/OAS_GA/AG-RES.%202004%20(XXXIV-O-04)_EN.pdf)

Spanish Text: [http://www.cicte.oas.org/Rev/En/Documents/OAS\\_GA/AG-RES.%202004%20\(XXXIV-O-04\)\\_SP.pdf](http://www.cicte.oas.org/Rev/En/Documents/OAS_GA/AG-RES.%202004%20(XXXIV-O-04)_SP.pdf)

Waz, J., & Weiser, P. (2013). Internet governance: The role of multistakeholder organizations. *Journal of Telecommunications and High Technology Law*, 10(2). Retrieved from [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2195167](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2195167)

**Video:**

IMD Business School (2013, February 26). Internet governance (Video) <https://www.youtube.com/watch?v=rRxZDe0XsUs>

France 24 (2011, October 31). Who rules the web? :ITU vs. ICANN (Video) [https://www.youtube.com/watch?v=V5FytTp\\_dTw](https://www.youtube.com/watch?v=V5FytTp_dTw)

## DAY 7: National Cybersecurity Models

### Daily Objectives:

- Identify the strengths and weaknesses of various national cybersecurity models
- Identify the different national interests behind national cybersecurity strategies.

### Mandatory Readings:

- Newmeyer, K (2012), “Who Should Lead U.S. Cybersecurity Efforts?” PRISM 3, no. 2, [http://www.ndu.edu/press/lib/pdf/prism3-2/prism115-126\\_newmeyer.pdf](http://www.ndu.edu/press/lib/pdf/prism3-2/prism115-126_newmeyer.pdf)
- Luijff, E., Besseling, K. & de Graff, P. (2013). Nineteen national cybersecurity strategies. *International Journal of Critical Infrastructures*, 9(1/2), 3-31. doi: 10.1504/IJCIS.2013.051608

### Spanish

- GdE (2011a) *Estrategia Española de Seguridad: Una responsabilidad de todos*, Gobierno de España, Madrid, Spain, available at <http://www.lamoncloa.gob.es/NR/rdonlyres/D0D9A8EB-17D0-45A5-ADFF-46A8AF4C2931/0/EstrategiaEspanolaDeSeguridad.pdf>
- Conopes (2011, July 11). Lineamientos de política para ciberseguridad y ciberdefensa. Documento Conopes 3701.

### Recommended Readings:

- Department of Defense 2011 Strategy for Operating in Cyberspace [http://www.defense.gov/home/features/2011/0411\\_cyberstrategy/docs/DoD\\_Strategy\\_for\\_Operating\\_in\\_Cyberspace\\_July\\_2011.pdf](http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf)
- White House International Strategy for Cyberspace [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/international\\_strategy\\_for\\_cyberspace.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf)
- NATO CCD COE National Cybersecurity Framework Manual. Klimberg, A. (2012). <http://ccdcoe.org/369.html>
- ITU National Cybersecurity Strategy Guide <http://www.itu.int/ITU-D/cyb/publications/index.html>
- ITU National Cybersecurity Strategy Guide for Developing Nations (2009 ed). <http://www.itu.int/ITU-D/cyb/publications/index.html>

ENISA (2012) *National Cyber Security Strategies*, European Network and Information Security Agency, Heraklion, Greece (ENISA), [http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategiesncsss/cyber-security-strategies-paper/at\\_download/fullReport](http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategiesncsss/cyber-security-strategies-paper/at_download/fullReport)

## DAY 8: Critical Infrastructure Protection and Role of the Private Sector in Cybersecurity

### Daily Objectives:

- Evaluate the role of the private sector in cybersecurity and critical infrastructure protection
- Evaluate the obligations of the individual in cybersecurity

### Mandatory Readings:

- Cerf, V. (2012, January 4). Internet access is not a human right. *New York Times*.
- Williams, P. (n.d.). Organized crime and cyber-crime: Implications for business.

### Recommended Readings:

- Reich, P.C. (2008). Cybercrime, cybersecurity, and financial institutions worldwide.
- Cordes, J.J. (2011). An overview of the economics of cybersecurity and cybersecurity policy. GW-CSPRI-2011-6
- Van Eeten, M. & Bauer, J.M. (2009). Emerging threats to Internet security: Incentives, externalities and policy implications. *Journal of Contingencies and Crisis Management* 17(4), 221- 232.

## DAY 9: CYBER EXERCISE and GROUP PRESENTATIONS

The participants will be involved in a half-day cyber exercise. The event will examine issues of critical infrastructure protection, national response, and risk assessment. The event will include multimedia inputs and facilitated discussions.

The participants will be divided into three- four person groups. Each group will outline a proposed national cybersecurity strategy and propose an implementation plan. The groups will have to identify key themes for the strategy, identify the key stakeholders within their country that will have to be included in the process, and proposed implementation strategy. The group will produce a 2-3 page point paper to be used to brief a senior decision maker as well as a 20-30 minute presentation for a group of senior officials.

## DAY 10: CLOSING CEREMONY FOR THE RESIDENT PHASE

The participants will be divided into three- four person groups. Each group will outline a proposed national cybersecurity strategy and propose an implementation plan. The groups will have to identify key themes for the strategy, identify the key stakeholders within their country that will have to be included in the process, and proposed implementation strategy. The group will produce a 2-3 page point paper to be used to brief a senior decision maker as well as a 20-30 minute presentation for a group of senior officials.