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

CYBER POLICY DEVELOPMENT
(CYBER)

NOTIONAL SYLLABUS

PLEASE BE ADVISED THAT THIS IS A NOTIONAL SYLLABUS.

THERE MAY BE DIFFERENCES IN THE TOPICS PRESENTED IN THIS SYLLABUS VERSUS WHAT IS COVERED IN THE ACTUAL COURSE. A COURSE-SPECIFIC SYLLABUS AND A DAILY SCHEDULE WILL BE MADE AVAILABLE DURING THE ONLINE PHASE.

William J. Perry
Center for Hemispheric Defense Studies
National Defense University
Bldg. 62, 300 5th Avenue, SW
Washington, DC 20319-5066
Phone: (202) 685-4670
Fax: (202) 685-4674
www.williamjperrycenter.org

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

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 as one that limits 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 Honesty

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.

Perry Center Policy on Attendance of Classes and Activities

Participants have the responsibility of attending 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 when your presence is required at the Perry Center.

Course Introduction

This course, about cybersecurity and advanced persistent threats, is one of the flagship courses offered by the William J Perry Center. It is designed to deepen understanding and analysis of the challenges of a growing dependence on cyberspace.

Course Description

This course aims to:

- Strengthen the fundamental understanding and working knowledge of a wide range of cyberspace activities. This includes everything from individual privacy to political and public concerns that are of national importance.

- Provide the necessary and sufficient information to understand possible and appropriate use of cyberspace tools. Understand how these tools could be abused or distorted and how myths about them can obscure reality and lead to ignorant or inappropriate reactions.

- Promote the formulations of defense strategies and policies in the cybersecurity domain that allow decisive decision making and promote national, regional, and international cooperation.

- Develop an environment that incentivizes the exchange of ideas and knowledge through mutual trust, understanding, and learning.

Educational themes of the course include:

- Critical thought and analysis of cyber defense and security at policy level: Develop a process to analyze formally or informally a problem from its identification to evaluating its solutions and consequences in cyberspace.

- Basic terms and concepts used in cyber space research: Know the fundamental concepts for comprehension, analysis, and evaluation of defense, security, and governance problems in cyberspace.

- Background about the current state of advanced persistent threats and challenges for cyber security: understand and analyze the feasibility of an adversary being able to identify and exploit your own vulnerabilities. What would happen if they did attack?

- Areas of political and strategic analysis: Analyze cyberspace through deterrence, defense, and offense. Analyze the linkages between the military and other government institutions, as well as private enterprise operating in cyberspace such as internet providers and electric companies.

- Emerging digital technology and its impact on cybersecurity: Understand and analyze how digital technology has impacted the public and private sectors in general and specifically the perception of cybersecurity in cyberspace.

- Big Data and its impact on cyber security: Know and understand how big data is used and its relationship with power, wealth (and the risks associated with manipulation of money), espionage, and reputation.

- Critical infrastructure and cyberspace: connected, dependent, and vulnerable: Analyze the advances of digital technology and its possible use by non-state and criminal actors to attack critical infrastructure

- The Internet of things and its impact on cybersecurity: Understand and analyze the way the Internet of Things is operated and used as well as its strengths, vulnerabilities, and impacts on cybersecurity.

In addition to political and strategic affairs in cybersecurity, the course will also focus on the importance of demystifying cyberspace if we hope to achieve security in this area. This class also develops personal expertise about cybersecurity at a political-strategic level through a complex and interconnected relationship between the security and defense expert and the computer technician. Finally, we will avoid overly simplistic or inappropriate solutions by understanding the motivations, costs, and tensions behind every situation.

Graduates of the Cybersecurity course will become key members of the community that researches cybersecurity in the region. Through interaction with professors and colleagues, participants will learn the common terminology used in the field to describe concepts, problems, and challenges. Additionally, this experience gives participants the opportunity to create networks and contacts that will extend outside the classrooms of the Perry Center.

Course Objectives

The objective of this course is to deepen participant's understanding of the global cyber environment from two policy and strategic perspectives: National State Power and Competitiveness.

This course is designed to provide the opportunity for strategic and analytical thought about cybersecurity tools and mechanisms. At the end of this course each student will be able to:

- Identify and understand the language of cyberspace;

- Evaluate the advanced persistent threats that are both criminal acts and as a result of the digital age;

- Analyze and evaluate current areas of risk to cybersecurity systems at a national, regional, and international level. Use this information to then design strategies and policies to combat cybercrime.

- Conceptualize new ways to combat cybercrime in Latin America and the Caribbean.

- Role of criminal and non-state actors in cyber space: Understand the complex process to design, implement, and develop a defense and security policy for cyberspace and the impact it has on the public. Recognize the importance that non-state actors have when planning strategy in light of complex threats.

- Governance of cyberspace: Understand and analyze the role that the State has in controlling the use of the internet, communications and information that are exchanged without regard to physical borders, and the international effort to create international treaties to govern the internet.

- International and regional cybersecurity institutions: Identify the challenges that international and regional institutions face when they try to increase global cybersecurity.

CYBER will support participants in the acquisition and/or enhancement of the following functional competencies:

Competency 1: An understanding of Big Data, strategic potential and current uses.

Competency 2: The use of predictive analytics in Big Data to provide advance intelligence for cybersecurity.

Competency 3: Structured Threat Information eXpression (STIX™) as a foundation for a collaborative community-driven effort to convey and prioritize of cyber threats.

Competency 4: Strategic Nation State data informed decision making.

Course Participants

The admissions process for this course allows the participation of a diverse group of professionals that work in fields related to cybersecurity. These participants will benefit from an intense dialogue that will be facilitated through four weeks of distance interaction and one week in Washington, DC. Participants should be a part of one of the following groups:

- Officials in Defense and Security Ministries that work in cybersecurity politics and strategy;

- Officials from other government institutions that interact with cybersecurity affairs such as members of the legislative branch, external affairs, or government planning and control offices;

- Members of nongovernmental organizations and academia, business men and women, members of political parties, journalists, and universities or other research institutions;

- Military and police officials that work in cybersecurity affairs preferably at the political and strategic level.

Instructional Methodology

The Perry Center strives to teach participants how to think, not what to think. There are no Perry Center-approved solutions for resolving national and regional security dilemmas. Rather, the Perry Center offers individual perspectives of members of its highly experienced international faculty regarding the security and defense challenges facing the hemisphere in a globalized world. Through a combination of lectures, break-out group (BOG) discussions and exercises, civilian and military participants become aware of and apply concepts critical to defense and security issues. Participants approach course topics through a five-step learning process:

1. Reading and analyzing assigned articles in preparation for each class.
2. Active participation in class and during lectures given by Perry Center professors or invited experts.
3. Group discussion and analysis of relevant current problems for cybersecurity using what participants have learned in class.
4. Participation in discussion forums about cybersecurity
5. Creating individual projects regarding cybersecurity

Course Development/Methodology

Online Phase (4 weeks)

This course is designed to have an online and residence phase. The online phase is four weeks long. This phase includes a week dedicated to familiarizing participants with the educational platform Blackboard and the basic cybersecurity terms and definitions. The residential phase is two weeks long and will take place at the William J Perry Center's facilities at the National Defense University in Washington. DC.

Residential Phase (2 weeks)

The course will be conducted at the Perry Center in Washington DC. Students will be exposed to defense and security theories, policies, frameworks and practice. The students will be challenged to analyze complex circumstances related to these themes through

readings, lectures, working groups, table-top exercises and a course project called a Defense or Security Action Plan.

Expectations regarding Student Participation

The value of the Perry Center's academic events depends to a high degree on the enthusiasm and willingness to contribute to learning of the course participants themselves. The Perry Center professors and facilitators are active agents for that process, but the level of understanding that each student carries back to his or her home country upon course completion depends to a very high degree upon that participant's investment of time and attention in the course program. Additionally, the reputation that each student leaves with his/her fellow participants can be an important incentive for continued collaboration on national and regional levels.

Aside from demonstrating a positive and constructive approach to the course, each participant is expected to read approximately 30 pages per week during the distance phase and 50 pages per day during the residence phase and be prepared to contribute to a discussion of that material in the BOG. Additional suggestions designed to promote a climate of mutual respect and camaraderie will be presented during the first day of instruction.

The quality of this course depends on the ability of participants to conduct themselves professionally and ethically. Participants should understand academic standards and avoid inappropriate conduct such as: arriving late, using cell phones or electronic devices during class time, leaving the class to get coffee, talking during class or when someone is presenting.

Organization of the Participants

Participants will be organized into breakout groups (BOGs) with the goal of providing a space for analysis and discussion of the topics addressed in class. These groups will be led by a professor from the Perry Center. During the online phase participants will communicate with their group leader through Blackboard or via email. During the residential phase participants will coordinate with their group during class. Group work will take place in individual rooms for each group.

Course Certification

Participants will be granted a Certificate of Competence for each of the three professional competencies listed above as well as documentation specifying the number of hours dedicated to each major activity developed during the course.

Course Standards and Grading

During the online phase students are evaluated based on their participation in discussion forums and their preparation for their final projects. The residential phase will be

evaluated based on students' participation in BOGs as well as the quality of the final project they submit.

Grades will be ascribed according to the following distribution:

- Participation, Online Phase 20%
- Participation, Residential Phase 30%
- Final Project Presentation, Residential Phase 50%

Grades will be assigned as follows:

No Pass:	<75%
Pass:	75% - 94%
Pass with Distinction:	95 – 100%

Specific Course Topics

The following lists potential lecture topics by instructor for the entire course. A detailed syllabus and daily schedule is posted online prior to the beginning of the course.

DISTANCE LEARNING PHASE

Week 1

- Participants will receive guidance from the Registrar on how to access and use the Blackboard Learning System.
- As a familiarization exercise, each participant will enter the Discussion Forum section of Blackboard and in the thread titled 'Introductions' will introduce themselves, where they are from and the role they play in their organization or place of work.
- Over the course of the Distance Learning Phase participants are required to read the publications provided (all readings will be accessible via a web link unless otherwise noted). They should be read in their entirety over the course of the Distance Learning Phase.

Week 2

During this second week of the Distance Learning Phase each participant will read the following reports:

a) (required) UK Government Chief Scientific Adviser. *The Internet of Things: Making the Most of the Second Digital Revolution*. Rep. no. 14-1230. The Government Office for Science, Dec. 2014. Web. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf
b) (recommended, not required) Data Breach Digest: Perspective is Reality: http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-perspective-is-reality_xg_en.pdf

After the reading, participants are assigned the following questions to answer:

Question 1: What is the public opinion of the Internet of Things and how does it change?

Question 2: What are some sectors that could be improved by Internet of Things and how?

Week 3

During this third week of the Distance Learning Phase each participant will read the following reports:

a) Smith, R. (2016, July 14). How America Could Go Dark. *The Wall Street Journal* Retrieved from https://www.wsj.com/articles/how-america-could-go-dark-1468423254

Essay 2 /Distance Learning Phase. After the reading, participants are assigned the following questions to answer:

> Question 1: How can small substations be a risk for the greater security of critical infrastructure?
>
> Question 2: What types of security changes should be made to prevent attacks in the future?

Week 4

During this third week of the Distance Learning Phase each participant will read the following report:

a) Russom, Phillip. Big Data Analytics. Rep. TDWI Research, 2011. Web. Apr. 2017. https://vivomente.com/wp-content/uploads/2016/04/big-data-analytics-white-paper.pdf

After the reading, participants are assigned the following questions to answer:

> Question 1: Define Big Data in terms of the 3 Vs
>
> Question 2: What are the challenges of conducting big data analytics? Be sure to address tools, techniques, and trends.

RESIDENTIAL PHASE

WEEK I

DAY 1
Introduction and Orientation

Lectures/Panels:
1. Course Introduction
2. Keynote Address

DAY 2
The Internet of Things

Lectures:
1. Internet of Things: Big Data and Cybersecurity
2. Conceptual Framework for the Strategic Political Analysis of Cybersecurity
3. Cybersecurity: A Regional Perspective

DAY 3
Critical Infrastructure

Lectures/Panels:
1. Critical Infrastructure & Cybersecurity
2. Public-Private Partnerships for Critical Infrastructure Protection

DAY 4
Big Data

Lectures/Panels/Visits:
1. Analyzing Big Data Analytics
2. Solutions for Government: Cloud Computing Initiative
3. Big Data Analytics – Consolidation of Institutional Control for Cooperation

DAY 5
The Way Forward

Lectures/Panels/Case Studies:
1. The Way Forward: Cloud Computing in Government
2. Mexico and Colombia Cybersecurity: An Overview