Spring 2017

CYBERSECURITY

17.447-17.448 / 15.580
Room E62-350

Monday 1:00 – 3:00 pm

Professor Nazli Choucri
Political Science Department
nchoucri@mit.edu

Professor Stuart Madnick
Sloan School of Management
smadnick@mit.edu

With participation of
Joel Brenner (CIAIL), David D. Clark (CSAIL), Howard E. Shrobe (CSAIL), Michael Siegel (Sloan)

Course Description

Multidisciplinary approach to cybersecurity, focusing on sources & manifestations of threat, operations & impacts, as well as solution strategies – in technical, economic, political, & strategic terms.

Part I is an overview of cybersecurity. Drawing on multiple perspectives, it focuses on diversity of threats, intents & capabilities – as well as uncertainties.

Part II examines geostrategic, political & economic “realities” of cybersecurity, including new markets with new policy challenges. Considers case-studies, data & metrics, agency & actors, with attendant gains & losses.

Part III is on national & international policies, formal & informal, as well as alternative solution strategies in a dynamic cyber ecology.
### Course Schedule

<table>
<thead>
<tr>
<th>Week/Date</th>
<th>Details</th>
<th>Instructor</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PART I CONTEXT, CONCEPTS &amp; CONTENTIONS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 February 13</td>
<td>Introduction - Context, Meanings, Impacts, Uncertainties</td>
<td>Choucri/Madnick</td>
</tr>
<tr>
<td>2 February 27</td>
<td>New Global Challenge – What We Know &amp; Not Know</td>
<td>Choucri</td>
</tr>
<tr>
<td>3 March 6</td>
<td>Cyberspace – Internet Architecture &amp; Complexity of Security</td>
<td>Clark</td>
</tr>
<tr>
<td>4 March 13</td>
<td>International Institutions to Address Cyber Threats</td>
<td>Choucri</td>
</tr>
<tr>
<td><strong>PART II COMPARATIVE PERSPECTIVES – CASES &amp; CONDITIONS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 March 20</td>
<td>National Security – Cyber Threats, &amp; Potentials for Cyberwar</td>
<td>Brenner</td>
</tr>
<tr>
<td>6 March 27</td>
<td>Failure Points &amp; Control Fields</td>
<td>Clark</td>
</tr>
<tr>
<td>7 April 3</td>
<td>Insurance for Cybersecurity &amp; Other Imperatives</td>
<td>Shrobe</td>
</tr>
<tr>
<td>8 April 10</td>
<td>Policy &amp; Prospects – Views from Computer Science</td>
<td>Clark</td>
</tr>
<tr>
<td><strong>PART III POLICY RESPONSES – STRATEGY &amp; IMPLICATIONS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 April 24</td>
<td>Management's Role in Cybersecurity: Cybersafety Analysis of the TJX case</td>
<td>Madnick</td>
</tr>
<tr>
<td>10 May 1</td>
<td>Markets for Malware &amp; Vulnerabilities</td>
<td>Siegel</td>
</tr>
<tr>
<td>11 May 8</td>
<td>Understanding the Role of Organizational Cybersecurity Culture</td>
<td>Madnick</td>
</tr>
<tr>
<td>12 May 15</td>
<td>Alternative Futures: What Next?</td>
<td>Choucri/Madnick</td>
</tr>
</tbody>
</table>

### Course Requirements

- Active Seminar Participation
- Critical Approach to Materials
- Class presentation – format to be announced
- Special Assignment – introduced in class
- Mid Term Essay
- End of Term Essay, OR Research Paper

### Contact Details

Professor Nazli Choucri E53-493, nchoucri@mit.edu, or
OUTLINE

PART I CONTEXT, CONCEPTS & CONTENTIONS

Part I provides an overview of the cybersecurity issue area; multidisciplinary perspectives, anchored on the internet, but indicating varieties of views, threats, definitions, ambiguities; the goal is to frame a general “model” – in static form -- of sources, operational dynamics, and impacts, and highlight the technical and political issues. It highlights the key themes covered and carried throughout the course – in modular as well as linkage terms.

Week 1 Introduction – Context, Meanings, Impacts, Uncertainties

Emergence of cybersecurity as an issue area, and threats to cybersecurity as a policy dilemma; intrusion modes and motivations; actors; general “ecology,” etc., recent changes; from low politics to high politics and the like. Meanings of security; threats to and in the cyber domain. This session provides the Initial Framing for the Course.

February 13 Choucri, Madnick

Week 2 New Global Challenge – What We Know & Do Not Know

Evolution of global system; transformation and change; issues of evidence; information, metrics; markets for malware, new players, new rules, shadow of cyberwar; relevance of escalation models, anonymity, and uncertainty; comparisons of “real” vs. “cyber” domains.

February 27 Choucri

Week 3 Cyberspace—Internet Architecture & Complexity of Security

Review of Internet architecture; salient points; perspectives of firms, states (national security), individuals, communities formal and informal etc., state sponsored vs. private actions – does that matter? Layers view and situating actors; noting levels of analysis; and potential sources and targets of threat.

March 6 Clark

Week 4 International Institutions to Address Cyber Threats

New entities and organization - FIRST, CERTS System and Others – advantages and disadvantages; what should or can be done? European Community, IMPACT, ITU, others; what seems to work what does not; expectations vs realities etc, organizational and legal imperatives.

March 13 Choucri
PART II Comparative Perspectives – Cases and Conditions

This Part focuses on transition from problem and theory to empirical “realities” defined in geostrategic, political, technological & economic terms; covering case narratives, metrics, data & problems thereof; emergence of new markets surrounding cybersecurity arena; new actors, activities; entities, and the various playing fields.

Week 5 National Security – Cyber Threats & Cyber War Potential

Situating cybersecurity in overall national security; institutional responses and responsibilities; information coordination; accountability, redundancies, responsibility, other? Cyber Command; relation to traditional services; cyber security re: operations on the ground; software and hardware; the human element.

March 20 Brenner

Week 6 Failure Points & Control Fields

Introducing control point analysis; illustrating with cases; types of vulnerabilities on Internet and in world politics; reminder of the virtual-real contexts and connections; architecture and design norms relevant to cybersecurity issues.

March 27 Clark

Week 7 Insurance for Cybersecurity & Other Imperatives

Society develops insurance and other protective mechanisms for almost all human activities. Can insurance measures be applied to or developed for cyber security? What are the possibilities and the impediments? Who insures for what?

April 3 Schrobe

Week 8 Management’s Role in Cybersecurity: Cybersafety Analysis of the TJX Case

The management of cyber systems generates new challenges that require new ways if addressing threats to security for business, industry, government, and other major users. General assessment and case specific examples.

April 10 Madnick
### PART III POLICY RESPONSES — STRATEGY & IMPLICATIONS

This Part covers national and international responses, highlights the ecology in place, actors, entities and activities, expected vs. actual impacts; challenges and problems – and proposed solution strategies. Highlights implications of Parts I, II, and III for theory and policy.

<table>
<thead>
<tr>
<th>Week 9</th>
<th><strong>Policy &amp; Prospects — Views from Computer Science</strong></th>
<th>April 24</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>What does cyber policy mean from the perspective of computer science? What are the processes, tools, and instruments and the mechanisms of decision making? What is the interface with national policy making?</td>
<td>Clark</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Week 10</th>
<th><strong>Markets for Malware &amp; Vulnerabilities</strong></th>
<th>May 1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dynamic interactions in malware market contexts; actors and activities; who gains and how; illustrating via system dynamics; showing system-wide impacts of actions and reactions; addressing interests of actors shaping these markets</td>
<td>Siegel</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Week 11</th>
<th><strong>Understanding the Role of Organizational Cybersecurity Culture</strong></th>
<th>May 8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Introducing “House of Security”; corporate considerations; measures, metrics, services, actors, interests etc.; attention to collaborative, competitive or other relations to government; role of overall cybersecurity policies for the private and public sectors.</td>
<td>Madnick</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Week 12</th>
<th><strong>Alternative Future: What Next?</strong></th>
<th>May 15</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This question is addressed from multiple perspectives – technology, internet and cyber domain, geopolitics and traditional strategic context; global politics, and national security.</td>
<td>Choucri/Madnick</td>
</tr>
</tbody>
</table>
COURSE REQUIREMENTS

• Active Seminar Participation – Critical Approach to Materials

• Class presentation – format to be announced

• Mid Term Essay – Choices of Questions
  ▪ Posted on April 3, 2017
  ▪ Due on April 10, 2017

• End of Term Essay -- Choices of Questions
  ▪ Posted on May 1, 2017
  ▪ Due on May 8, 2017

• Research paper can be substituted for the End of Term Essay
  ▪ Topic to be approved
  ▪ One paragraph on focus
  ▪ Brief outline
  ▪ You can now proceed
  ▪ Due date May 15, 2016

• Website Identification Project – to be introduced in class no later than February 27 and due on May 1

Books for Reading Assignment on Reserve in Dewey Library

• Nazli Choucri, Cyberpolitics in International Relations (MIT Press, 2012).


All other Required and Recommended Materials:

  o Available on the Course Stellar-site.
  o Required readings for everyone
  o Recommended readings a for graduate students

Please Note
  Chapters from the course books (listed above) are not reproduced on Course Stellar-site

  All other assigned readings are on the course Stellar-site
Laptops: No Laptops in Class

Grade distribution:

- Class attendance participation 20%
- Class presentation 15%
- Midterm (take home) 20%
- Website Identification Project 20%
- End of term Essay (Take home) 25%
  or
  Research paper on topic of your choice with approval of instructor
ASSIGNED READINGS

Week 1 Introduction – Context, Meanings, Impacts, Uncertainty
February 13, 2017

Emergence of cybersecurity as an issue area, and threats to cybersecurity as a policy dilemma; intrusion modes and motivations; actors; general “ecology,” etc., recent changes; from low politics to high politics and the like. Meanings of security; threats to and in the cyber domain. This session provides the initial framing for course.

Required


Recommended


http://onlinelibrary.wiley.com.libproxy.mit.edu/book/10.1002/9781118241530;jsessionid=A05A59E88257F475807BFD68FD5A7993.f03t02
Week 2  New Global Challenge – What We Know & Do Not Know
February 27, 2017

Evolution of global system; transformation and change; issues of evidence; information, metrics; markets for malware, new players, new rules, shadow of cyberwar; relevance of escalation models, anonymity, and uncertainty; comparisons of “real “ vs.“cyber“ domains.

Required


Recommended


Week 3  Cyberspace – Internet Architecture & Complexity of Security
March 6, 2017

Review of internet architecture; salient points; perspectives of firms, states (national security), individuals, communities formal and informal etc., state sponsored vs. private actions – does that matter? Layers view and situating actors; noting levels of analysis; and potential sources and targets of threat.

**Required**


**Recommended**

Week 4   International Institutions to Address Cyber Threats
March 13, 2017

New entities and organization - FIRST, CERTS System and Others – advantages and disadvantages; what should or can be done? European Community, IMPACT, ITU, others; what seems to work what does not; expectations vs. realities etc., organizational and legal imperatives.

Required


Choucri, Nazli Cyberpolitics in International Relations, MIT Press, 2012, Chapters 7 and 8.


Recommended


Week 5 National Security – Cyber Threats & Potentials for Cyberwar
March 20, 2017

Situating cybersecurity in overall national security; institutional responses and responsibilities; information coordination; accountability, redundancies, responsibility, other? Cyber Command; relation to traditional services; cyber security re: operations on the ground; software and hardware; the human element.

Required


Recommended


**Week 6 Failure Points & Control Fields**  
March 27, 2017

Introducing control point analysis; illustrating with cases; types of vulnerabilities on Internet and in world politics; reminder of the virtual-real contexts and connections; architecture and design norms relevant to cybersecurity issues.

**Required**


**Recommended**


Week 7  Insurance for Cybersecurity and Other Imperatives
April 3, 2017

Society develops insurance and other protective mechanisms for almost all human activities. Can insurance measures be applied to or developed for cyber security? What are the possibilities and the impediments? Who insures for what?

Required


Recommended

Week 8: Management’s Role in Cybersecurity: Cybersafety Analysis of the TJX Case

April 10, 2017

The management of cyber systems generates new challenges that require new ways if addressing threats to security for business, industry, government, and other major users. General assessment and case specific examples.

Required


Recommended

Week 9  Policy & Prospects – Views from Computer Science
April 24, 2017

What does cyber policy mean from the perspective of computer science? What are the processes, tools, and instruments and the mechanisms of decision making? What is the interface with national policy making?

Required


Recommended


Week 10 Markets for Malware & Vulnerabilities
May 1, 2017

Dynamic interactions in malware market contexts; actors and activities; who gains and how; illustrating via system dynamics; showing system-wide impacts of actions and reactions; addressing interests of actors shaping these markets.

Required


Recommended


Week 11  Understanding the Role of Organizational Cybersecurity Culture
May 8, 2017

Introducing “House of Security”; corporate considerations; measures, metrics, services, actors, interests etc.; attention to collaborative,competitive or other relations to government; role of overall cybersecurity policies for the private and public sectors.

Required


Recommended


Week 12  Alternative Futures of Cyberspace—What Next?  
May 15, 2017

This question is addressed from multiple perspectives – technology, internet and cyber domain, geopolitics and traditional strategic context; global politics, and national security.

Required


Recommended:

