



**Course ID and Title:** PPD 599 An Exploration of the Intelligence Community – From Policy to Cyber Espionage

**Units:** 4 Units

**Term—Day—Time:** Spring 2020, Wednesday, 6-9:20pm

**Location:** **VKC - 201**

**Instructor:** Professor Michael Orosz

**Office:** **TBD**

**Office Hours:** **TBD**

**Contact Info:** [mdorosz@isi.edu](mailto:mdorosz@isi.edu), 310-448-8266 (office), 310-486-2150 (cell). Instructor will respond to messages within 24 hours

**Teaching Assistant:**

**Office:** **TBD**

**Office Hours:** **TBD**

**Contact Info:** **TBD**

**IT Help:** **TBD**

**Hours of Service:** **TBD**

**Contact Info:** **TBD**

## **Course Description**

The objective of the course is to provide students with an introduction to the intelligence community with an emphasis on policy and open source intelligence (OSINT). The course will cover the US and foreign intelligence communities, collection methods and analysis techniques, open source intelligence, cyber espionage, policy considerations and geopolitical concerns. The course targets students from various backgrounds (policy, planning, international relations, engineering, computer science) who want to know more about the community from a general interest perspective, career interest or to help with understanding and decision-making. For example, a political science major might take this course to help increase understanding of the discipline as it relates to policy-making in government.

There are no course prerequisites, however, knowledge of introductory algebra, statistics and completion of PPD 683 may be helpful. More advanced topics (such as mathematical explorations of signals intelligence (SIGINT), search and analytical techniques) will be offered to students for exploration outside of the course, however, students will not be required to know this advanced information for the semester class project, midterm exam or final project.

## **Learning Objectives**

The main goal of the course is to provide the student with a general understanding of the following topics as they relate to the Intelligence Community:

- An understanding of the different intelligence sources; how this intelligence is collected, analyzed and used; and the strengths and weaknesses of these sources
- The policy and geopolitical factors that shape how intelligence is collected, analyzed and used

Classroom meetings and selected readings will expose the learners to the knowledge and skills that are required to understand, and in many cases, apply the basic collection, analysis and reporting methods used by the Intelligence Community.

There will be a midterm examination and a final semester project. Students will also be required to complete a semester-long project on an instructor-provided topic.

After successfully completing this course, the student will be able to:

- Describe and know how to use the different collection methods traditionally (i.e., non-cyber) employed by the intelligence community;
- Describe and in many cases apply the various cyber methods to collect intelligence employed by the intelligence community
- Describe and apply tools and approaches to collecting and analyzing open source intelligence (OSINT)
- Describe the various policies that govern the collection and processing of intelligence, the impacts these policies have on the intelligence community and be able to formulate approaches to address these policies
- Provide examples of policy violations
- Explain the basic geopolitical implications that must be considered when deciding to collect

and act on intelligence

- Provide examples of geopolitical outcomes resulting from Intelligence Community activities

**Prerequisite(s):** None

**Co-Requisite(s):** None

**Concurrent Enrollment:** None

**Recommended Preparation:** Algebra or Statistics, PPD 683

### **Course Notes**

Copies of selected lecture slides will be posted on Blackboard.

### **Technological Proficiency and Hardware/Software Required**

N/A

### **Required Readings and Supplementary Materials**

The primary text for the course is *Intelligence: From Secrets to Policy, 7<sup>th</sup> Edition*, by Mark M. Lowenthal (see reading list). Supplemental readings are listed after the course schedule (see below). This list may be adjusted prior to the start of the semester to reflect current events. Additional lecture materials will be provided by the instructor.

### **Description and Assessment of Assignments**

There will be a midterm exam, a final project and a semester-long project.

#### **Exam:**

The midterm exam (25% of course grade) is a closed book written test for which the student is only required to bring a pen or pencil. The midterm will have 3-4 multi-part written questions along with 10-15 multiple choice questions. A mini exam (vaccine) will be held before the midterm to familiarize the students with the material and format of the upcoming examination.

- Students who are not able to attend the mid-term examination (medical or other emergency) must notify the instructor before the test (phone message at 310-486-2150 or email at [mdorosz@isi.edu](mailto:mdorosz@isi.edu) ).

#### **Class Project:**

The class project constitutes 35% of the overall individual grade. In the first week of class, the instructor will introduce the concept of the presidential intelligence brief (PIB). For the course, the instructor will assume the role of the Director of National Intelligence (DNI) who is responsible for providing a bi-weekly intelligence briefing (i.e., the PIB) to the president. Students will assume the role of an intelligence manager/director responsible for a topic of interest to the U.S. Government that is assigned by the instructor during the first week of the course. For example, a student may be assigned to manage the “North Korea Desk” and be

responsible for collecting, analyzing and reporting of intelligence related to North Korea (e.g., potential missile test, possible famine, etc.). These reports (2-3 pages) will be due the 2<sup>nd</sup>, 4<sup>th</sup>, 6<sup>th</sup>, 8<sup>th</sup>, 10<sup>th</sup> and 12<sup>th</sup> week of the semester. Each report builds on the previous report by highlighting new intelligence collected, new/modified assessments and discussions on new policy, privacy or security issues that have presented themselves.

For each intelligence report, students will analyze information collected from open sources (i.e., Open Source Intelligence – OSINT) such as social media, news media, the Dark Web and other sources of information that can be legally accessed by anyone (either freely or for a fee). As part of the course, the instructor will discuss methods for accessing and analyzing open source intelligence.

Each report will provide the following content (format of the report can be found later in the syllabus):

- A summary of the target (e.g., the topic in which intelligence is being collected) – this can be repeated from the previous report
- Importance to the U.S. Government (i.e., what policy is the intelligence supporting?) – this can be repeated from the previous report
- Analysis results (assessments) – A summary (Bottom Line Up Front – BLUF)
  - What does the intelligence tell us?
  - Impact the intelligence/assessment has on U.S. policy
  - What changed from the previous report?
  - What actions are recommended (e.g., collect more intelligence, take an action, etc.)?
  - Reasons for changing assessments
- Description of the intelligence collected (including sources)
- Summary of analytical methods used
- Gap analysis: What intelligence – if able to collect – could possible help with the assessment (e.g., imaging, etc.)
- Tipping and cueing opportunity: List any collected intelligence that although not pertinent to the topic assigned, may be of use to another intelligence director (i.e., another “desk” or target)

The final semester-long project report will consist of both a written and oral in-class presentation that provides an overall summary of the six bi-weekly intelligence reports generated during the semester. The summary will include the following content (format of the report is found later in the syllabus):

- Summary of the target/issue in which the intelligence was collected (i.e., what issue or event is the focus?)
- The final assessment along with a description of how that assessment changed during the semester.
- What is the impact of your assessment on U.S. Government policy?
- What assumptions did you use in your assessments? List potential biases you may have that could have influenced your assessments

- Summary of the intelligence collected and list of sources (prioritized by importance to your assessment).
- What intelligence – if available – would have helped in your assessment?
- List intelligence collected that could have helped others with their collection (i.e., tipping and cueing opportunities)

The point of the class project is to provide the students the opportunity to assume the challenging role of an intelligence manager/director involved in the collecting, analyzing and reporting on a problem of national security importance. In addition, because each student will bring different experiences to the problem space, students will have an opportunity to observe (via the Week 15 class presentations) how analysis and decision-making can differ based on these differences.

The first report (week 2) will not be graded. These initial reports will be evaluated and comments with suggested recommendations (e.g., OSINT sources to search, policy issues missed, etc.) will be provided to the student by week 3. Reports for weeks 4, 6, 8, 10 and 12 will be evaluated and graded. Grading will be based on the quality of the analysis provided as assessed by the instructor.

Each project will be evaluated based on the quality of the intelligence collected and analyzed as assessed by the instructor from the weekly reports, the Week 15 presentation and the submitted final report. The formats of the bi-weekly status reports, final report and final project presentation are listed later in the syllabus.

**Final (Semester-end) Report:**

The final project report that constitutes 40% of the overall individual grade. In the 12<sup>th</sup> week of the semester, each student, using the tools, techniques and processes covered in class, will be asked to take the remaining three weeks of the semester to research and critique how intelligence was used in the decision-making behind a significant event (provided by the instructor). Included in the critique is an analysis of the available intelligence, how policy was or wasn't considered, how geopolitics was or wasn't considered and, based on the available intelligence and processes whether the event was an intelligence success, failure or neutral. For example, the students in the class may be asked to critique the intelligence decision-making behind the decision to invade Iraq in 2013.

**Extra Credit:**

To earn extra credit (up to 5 points) to be applied to the final grade point total, students are invited to write a paper (5-7 pages) describing an intelligence challenge or topic that is pertinent to the course. At the start of the semester, a list of potential extra credit topics will be presented. In addition, based on class discussions and/or current domestic and world events, additional topics will be offered throughout the semester. Students interested in writing and submitting an extra credit paper are required to notify the instructor before attempting to research and write the paper.

**Grading Breakdown**

Assignment	Points	% of Grade
Mid-term exam	25	25%
Final project	40	40%
Bi-weekly intelligence reports (5 reports, 4pts/report)	20	20%
Course project/report	15	15%
<b>TOTAL</b>	<b>100</b>	<b>100%</b>
Extra Credit (1 paper)	5	

### Grading Scale

Course final grades will be determined using the following scale

A	95-100
A-	90-94
B+	87-89
B	83-86
B-	80-82
C+	77-79
C	73-76
C-	70-72
D+	67-69
D	63-66
D-	60-62
F	59 and below

### Assignment Rubrics

None

### Assignment Submission Policy

For the class project, each student will submit six intelligence briefings (weeks 2, 4, 6, 9, 10 and 12) describing the instructor assigned target/issue; the importance the target/issue is to the country (i.e., why should we care?); the current situation based on collected OSINT (cite sources); an analysis of the collected intelligence; recommendations on courses of action and a discussion of the policy, privacy and security implications associated with the collection and use of intelligence on the target/issue.

Each briefing (report) is due at the beginning of class based on the following schedule.

Briefing Number	Date Due	Graded/Not-graded
1	January 22, 2020	Not graded
2	February 5, 2020	Graded
3	February 19, 2020	Graded
4	March 11, 2020	Graded
5	April 1, 2020	Graded
6	April 15, 2020	Graded

Because these bi-weekly briefings are time sensitive, for each day a briefing is late, one point will be deducted from the overall grade given to that briefing.

The following table summarizes the format of the bi-weekly intelligence reports.

<b>Intelligence Brief (2-3 pages – including images/tables): Weeks 2, 4, 6, 8, 10 and 12</b>		
<b>Topic</b>	<b>Content</b>	<b>Suggested page budget</b>
Title page	Project title, one sentence description of the assigned project, student's name and contact information	One page (doesn't count towards the page count)
Target/issue description	Detailed description of the target/issue and the importance the target is to the country (United States). Should include discussions on the geopolitical, economic and national security concerns of the country	Quarter to half page
Assessment/analysis	<ul style="list-style-type: none"> <li>• What does the intelligence tell us?</li> <li>• Impact the intelligence/assessment has on U.S. policy</li> <li>• What changed from the previous report?</li> <li>• What actions are recommended (e.g., collect more intelligence, take an action, etc.)?</li> <li>• Reasons for changing assessments</li> </ul>	Half to one page
Summary of collected intelligence	Provide brief summary of previous intelligence collected and then list what has been collected from OSINT since the previous report. List sources	Quarter to half page (list sources at end of report if summary exceeds half-page)
Analytical methods/processes used	Summary of analytical methods and/or processes used. Issues encountered, missing intelligence that might help with the assessments.	Half to one page

Tipping and cueing opportunities	List collected intelligence that although not useful for your assessment/analysis, might be useful for other targets/interests (and cite them if possible)	Quarter to half page
References	List of references (e.g., source of intelligence that were not listed in main report, etc.)	No page limits.
Supporting Material (optional)	Attached anything you feel is relevant to your analysis and recommendations	No page limits. This an optional item that might include additional URLs to relevant material, files or other electronic information

<b>Class Presentation (6-11 Slides): Week 15</b>		
<b>Format: Each student will present for 15-20 minutes, followed by a 5-minute Q&amp;A session with the class.</b>		
<b>Topic</b>	<b>Content</b>	<b>Suggested page budget</b>
Title slide	Description of topic, presenter name, date)	First slide
Summary of the topic/issue	Discuss what the target/issue is, its importance to the US, what policies are impacted	Second slide (additional slides can be used if necessary, but brevity is key)
Assessments	Discuss the following: <ul style="list-style-type: none"> <li>• Assessments derived from the collected intelligence...include the assessment history</li> <li>• Impact assessments have on US policy</li> <li>• What intelligence led to your assessments</li> <li>• Reasons for changes in the assessments</li> <li>• What intelligence sources – if available – could have helped improve assessments</li> <li>• What assumptions were used?</li> </ul>	Third slide (additional slides can be used if necessary, but brevity is key)



	<ul style="list-style-type: none"> <li>List personal biases that might impact analysis</li> </ul>	
Summary of collected intelligence	Summary of all intelligence collected – including a list of sources (prioritized by importance to your analysis)	Fourth slide (additional slides can be used if necessary)
Intelligence collected that could benefit others (i.e., tipping and cueing)	Discuss what intelligence that was collected (if any) that may be of use to others	Fifth slide (additional slides can be used if necessary, but brevity is key)

<b>Final Semester Project Report (8-12 pages – including images/tables): Week 15</b>		
<b>Topic</b>	<b>Content</b>	<b>Suggested page budget</b>
Title page	Project title, one sentence description of the assigned project, student's name and contact information	One page (doesn't count towards the page count)
Target/issue description	Detailed description of the target/issue and the importance the target is to the country. Should include discussions on the geopolitical, economic and national security concerns of the country	One to two pages
Assessment/analysis results	<ul style="list-style-type: none"> <li>What does the intelligence tell us?</li> <li>Impact the intelligence/assessment has on U.S. policy</li> <li>List (in chronological order) how the assessments have changed over the semester</li> <li>Reasons for the assessments changing over the semester</li> <li>What actions are recommended (e.g., collect more intelligence, take an action, etc.)?</li> <li>List assumptions used in the analysis</li> </ul>	Two to three pages

	<ul style="list-style-type: none"> <li>List possible biases brought to the analysis</li> </ul>	
Summary of collected intelligence	Provide summary of OSINT collected and list sources by importance of source to the analysis	Two to three pages (list sources at end of report if summary exceeds three pages)
Analytical methods/processes used	Summary of analytical methods and/or processes used. Issues encountered, missing intelligence that might help with the assessments.	One to two pages
Tipping and cueing opportunities	List collected intelligence that although not useful for your assessment/analysis, might be useful for other targets/interests (and cite them if possible)	One to two pages
References	List of references (e.g., source of intelligence that were not listed in main report, etc.)	No page limits.
Previous intelligence briefs	Include the six bi-weekly reports	No page limits
Supporting Material (optional)	Attached anything you feel is relevant to your analysis and recommendations	No page limits. This an optional item that might include additional URLs to relevant material, files or other electronic information

<b>Extra Credit Paper (5-7 pages – including images/tables)</b>		
<b>Topic</b>	<b>Content</b>	<b>Suggested page budget</b>
Title page	Project title, one sentence description of the paper topic, student's name and contact information	One page (doesn't count towards the page count)
Topic description	Detailed description of the topic being explored. Instructor needs to agree to the topic prior to the student undertaking the effort. List specifically what the topic is, its importance to US policy, importance to the intelligence community and	Two to four pages

	proposed plan for investigating.	
Investigation Results	<ul style="list-style-type: none"> <li>• What have you learned?</li> <li>• What resources were used (cite resources)</li> <li>• Do the results meet your original objective?</li> </ul>	Three to four pages
References	List of references	No page limits.
Supporting Material (optional)	Attached anything you feel is relevant to your analysis and recommendations	No page limits. This an optional item that might include additional URLs to relevant material, files or other electronic information

<b>Final Project Report (8-12 pages – including images/tables): Finals Week</b>		
<b>Topic</b>	<b>Content</b>	<b>Suggested page budget</b>
Title page	Project title, one sentence description of the problem event, student's name and contact information	One page (doesn't count towards the page count)
Target/issue description	Detailed description of the target/issue and the importance the target is to the country. Should include discussions on the geopolitical, economic and national security concerns of the country	One to two pages
Assessment/analysis results	<ul style="list-style-type: none"> <li>• Summary of intelligence used by decision-makers</li> <li>• Summary of geopolitical factors that influenced decision-making</li> <li>• Identify gaps in intelligence collection and analysis</li> <li>• Discuss policy issues involved</li> <li>• Did bias or other outside influences possibly contribute to the analysis?</li> <li>• Discuss alternative interpretations and</li> </ul>	Two to three pages

	courses of action that the decision-makers might have considered	
Summary of collected intelligence	Provide summary of OSINT collected and list sources by importance of source to the analysis	Two to three pages (list sources at end of report if summary exceeds three pages)
Analytical methods/processes used	Summary of analytical methods and/or processes used. Issues encountered, missing intelligence that might help with the assessments.	One to two pages
References	List of references (e.g., source of intelligence that were not listed in main report, etc.)	No page limits.
Supporting Material (optional)	Attached anything you feel is relevant to your analysis and recommendations	No page limits. This an optional item that might include additional URLs to relevant material, files or other electronic information

**Grading Timeline.**

Results from the midterm exam will be available one week after the student has taken the exam. Exam results include a letter grade and possibly comments on additional or alternative options/directions that the student might have considered. Grades and/or responses to each of the intelligence reports, extra-credit paper and class and final project will be available one week after submission.

**Additional Policies**

Students are expected to attend each class as the material covered will be necessary for completion of the course project and will also be covered in the midterm and final exams. Electronic communication devices (phones, smartphones, laptops, and similar) that are used for *personal communications* must be turned off or placed away during lectures and laboratories. You can check them at the break. Likewise, you should not use instant messenger or similar chat programs during lectures or labs. On the other hand, devices capable of accessing the Internet via WiFi can be used as part of course instruction – for example, when exploring the Dark Web.

## Course Schedule: A Weekly Breakdown

	Topics/Daily Activities	Readings and Homework	Deliverable/ Due Dates
<b>Week 1</b>	<p>What is the intelligence community?</p> <ul style="list-style-type: none"> <li>• What is intelligence?</li> <li>• The need for secrecy</li> <li>• History of the US Intelligence Community</li> <li>• The foreign intelligence community</li> <li>• The “Holy Grail” of the intelligence community</li> <li>• <b>Project:</b> Introduction of project topic(s)</li> </ul>	<ul style="list-style-type: none"> <li>• Lowenthal Chapters 1-3, 15</li> <li>• Kerr</li> <li>• ONDI</li> <li>• Lecture and reading materials presented at beginning of semester</li> </ul>	Class participation
<b>Week 2</b>	<ul style="list-style-type: none"> <li>• Collection and Collection Management <ul style="list-style-type: none"> <li>• The OODA Loop and TCPED</li> <li>• INTs (SIGINT, IMINT, GEOINT, HUMINT, MASINT, OSINT)</li> <li>• Collection methods (overhead, air breathers, ground, human, cyber)</li> <li>• Risk mitigation</li> <li>• Order of battle and the electronic order of battle</li> </ul> </li> <li>• Introduction to OSINT</li> </ul>	<ul style="list-style-type: none"> <li>• Lowenthal, Chapter 5</li> <li>• Lecture and reading materials presented at beginning of semester</li> </ul>	<ul style="list-style-type: none"> <li>• Class participation.</li> <li>• <b>January 22, 2019:</b> First class project report (2-3 pages) – describe topic, strategic importance, initial assessment, intelligence collected and issues (not graded)</li> </ul>
<b>Week 3</b>	<p>A. Intelligence Analysis</p> <ul style="list-style-type: none"> <li>• Fundamentals</li> <li>• Multi-INT vis All Source Challenges/issues: bias, group think and other failures</li> <li>• Challenges/issues: privacy and security</li> </ul>	<ul style="list-style-type: none"> <li>• Lowenthal, Chapter 6</li> <li>• Jackson</li> <li>• Tang, <i>et al.</i></li> <li>• Friedman, <i>et al.</i></li> <li>• ACLU #1 and #2</li> <li>• Rosenzweig &amp; Scardaville</li> <li>• Lecture and reading materials presented at beginning of semester</li> </ul>	• Class participation
<b>Week 4</b>	<p>A. Intelligence and Policy – Part 1</p> <ul style="list-style-type: none"> <li>• Local, national and international operations</li> <li>• Title 10, title 50, CFR 28 (Part 23) and other regulations/guidelines</li> </ul>	<ul style="list-style-type: none"> <li>• Lowenthal, Chapter 9</li> <li>• US Congress (95-511)</li> </ul>	<ul style="list-style-type: none"> <li>• Class participation</li> <li>• <b>February 5, 2019:</b> Second class project report (2-3 pages) - graded</li> </ul>

	<ul style="list-style-type: none"> <li>• The Patriot Act</li> </ul>	<ul style="list-style-type: none"> <li>• Richard Clarke, <i>et al</i></li> <li>• CNN</li> <li>• Lecture and reading materials presented at beginning of semester</li> </ul>	
<b>Week 5</b>	<p>A. Intelligence and Policy – Part 2</p> <ul style="list-style-type: none"> <li>• Foreign implications</li> <li>• Challenges/Issues: Technology changes</li> <li>• Challenges/Issues: Privacy and security</li> <li>• USA Freedom Act</li> <li>• FISA</li> <li>• Case histories</li> </ul>	<ul style="list-style-type: none"> <li>• Lowenthal, Chapter 10</li> <li>• Silberman &amp; Robb</li> <li>• Woodruff &amp; Hennessey</li> <li>• Wall</li> <li>• Lieberthal, et al.</li> <li>• Miscik</li> <li>• Lecture and reading materials presented at beginning of semester</li> </ul>	<ul style="list-style-type: none"> <li>• Class participation</li> </ul>
<b>Week 6</b>	<p>A. Intelligence and Policy – Part 3</p> <ul style="list-style-type: none"> <li>• Oversight</li> <li>• Agendas</li> <li>• Case histories</li> </ul> <p>B. Sample midterm exam</p>	<ul style="list-style-type: none"> <li>• US Army</li> <li>• US Government (EO 12291)</li> <li>• Lecture and reading materials presented at beginning of semester</li> </ul>	<ul style="list-style-type: none"> <li>• Class participation.</li> <li>• <b>February 19, 2019:</b> Submission of third course project status report (graded)</li> </ul>
<b>Week 7</b>	<p><b>Midterm Exam</b></p> <ul style="list-style-type: none"> <li>• Covers materials from weeks 1-6</li> </ul>	No readings or assignments	<p><b>February 26, 2019:</b> Completion of midterm exam</p>
<b>Week 8</b>	<p>Open Source Intelligence: Cyber - Search and processing tools</p> <ul style="list-style-type: none"> <li>• Search tools and usage – including advanced search</li> <li>• Customized tools: APIs, JavaScript and more</li> <li>• Social media</li> <li>• Policy impacts/considerations</li> <li>• Example applications</li> </ul>	<ul style="list-style-type: none"> <li>• US Army (ATP 2-22.9)</li> <li>• Additional materials provided at beginning of semester</li> </ul>	<ul style="list-style-type: none"> <li>• Class participation.</li> </ul>
<b>Week 9</b>	<p>A. Open Source Intelligence: Data fusion</p> <ul style="list-style-type: none"> <li>• Why fuse data?</li> <li>• Data fusion principals and tools</li> <li>• Multi-INT products</li> </ul>	Lecture and reading materials presented at	<ul style="list-style-type: none"> <li>• Class participation</li> <li>• <b>March 11, 2019:</b> Submission of fourth course</li> </ul>

	<ul style="list-style-type: none"> <li>• Example applications (e.g., GEOINT, etc.)/considerations</li> <li>• Policy impacts</li> </ul>	beginning of semester	project status report (graded)
<b>Spring Break (15-22 March)</b>			
<b>Week 10</b>	<p>A. Cyber Espionage</p> <ul style="list-style-type: none"> <li>• Cyber space: an overview <ul style="list-style-type: none"> <li>○ Security features, operations, vulnerabilities</li> </ul> </li> <li>• Attack vectors: <ul style="list-style-type: none"> <li>○ Fishing, spear fishing, viruses, worms, botnets and other vectors</li> </ul> </li> <li>• Insider threats</li> <li>• Policy impacts/concerns</li> <li>• Example applications</li> </ul>	Lecture and reading materials presented at beginning of semester	<ul style="list-style-type: none"> <li>• Class participation</li> </ul>
<b>Week 11</b>	<p>Cyber: Deep Web</p> <ul style="list-style-type: none"> <li>• What is the deep (or dark) web?</li> <li>• Need for anonymity</li> <li>• Onion routing basics</li> <li>• Using TOR and other anonymous search engines</li> <li>• Precautions</li> <li>• Policy concerns</li> <li>• Example searches</li> </ul>	<ul style="list-style-type: none"> <li>• Chertoff Group</li> <li>• Additional materials presented at beginning of semester</li> </ul>	<ul style="list-style-type: none"> <li>• Class participation.</li> <li>• <b>April 1, 2019:</b> Submission of fifth course project status report (graded)</li> </ul>
<b>Week 12</b>	<p>Ethics, Morals and Consequences</p> <ul style="list-style-type: none"> <li>• Domestic vs foreign collection</li> <li>• Whistle blowers</li> <li>• Political influences</li> <li>• Reform</li> </ul>	<ul style="list-style-type: none"> <li>• Lowenthal, Chapters 13 and 14</li> <li>• US Congress (Executive)</li> <li>• Reitman</li> <li>• Von Solms, et al.</li> <li>• US Congress (911 Report)</li> <li>• Kerr</li> <li>• Additional materials presented at beginning of semester</li> </ul>	<ul style="list-style-type: none"> <li>• Class participation.</li> </ul>
<b>Week 13</b>	<p>A. Geopolitical considerations and consequences</p> <ul style="list-style-type: none"> <li>• Actions and reactions</li> <li>• Cost and benefits</li> <li>• Case histories</li> </ul> <p>B. Final Report Topic</p>	<ul style="list-style-type: none"> <li>• Lowenthal, Chapters 11 and 12</li> <li>• Irahim</li> <li>• Lieberthal, et al.</li> <li>• Additional materials presented at</li> </ul>	<ul style="list-style-type: none"> <li>• Class participation</li> <li>• <b>April 15, 2019:</b> Submission of sixth course project status report (graded)</li> </ul>

		beginning of semester	
<b>Week 14</b>	The geopolitical climate today <ul style="list-style-type: none"> <li>• Current topics and issues</li> <li>• Concerns</li> <li>• Predictions</li> <li>• The future</li> </ul>	<ul style="list-style-type: none"> <li>• Dan Coats – DNI</li> <li>• DSS</li> <li>• FBI</li> <li>• Additional materials presented at beginning of semester</li> </ul>	<ul style="list-style-type: none"> <li>• Class participation</li> </ul>
<b>Week 15</b>	Project presentations <ul style="list-style-type: none"> <li>• Class presentations (15-25 minutes each)</li> <li>• Report submission</li> </ul>	None	<b>April 29, 2019:</b> Class participation and final report
<b>FINAL</b>	Final project due		<b>Wednesday, 6 May</b>

### Reading List

Required Text			
Author	Title	Link	Comments
Mark M. Lowenthal	Intelligence: From Secrets to Policy, 7 <sup>th</sup> Edition, Los Angeles: CQ Press (2017)	Purchase at USC Bookstore or via Amazon.com	Course text
Supplemental Readings			
Author	Title	Link	Comments
Andru E. Wall	Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action	<a href="https://harvardnsj.org/wp-content/uploads/sites/13/2012/01/Vol-3-Wall.pdf">https://harvardnsj.org/wp-content/uploads/sites/13/2012/01/Vol-3-Wall.pdf</a>	Overview of Title 10 and Title 50 authorities.
Brian Jackson (ed.)	The Challenge of Domestic Intelligence in a Free Society	<a href="http://www.dtic.mil/dtic/tr/fulltext/u2/a493749.pdf">http://www.dtic.mil/dtic/tr/fulltext/u2/a493749.pdf</a>	An examination on the need for domestic intelligence
Richard Clarke, et. al	Liberty and Security in a Changing World (“The NSA Report”)	<a href="https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf">https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf</a>	Report commissioned by President Obama to review current intelligence operations with respect to problems, privacy and



			security. Also called “The NSA Report”
CNN Staff Writers	Report: Iraq intelligence 'dead wrong'	<a href="http://www.cnn.com/2005/POLITICS/03/31/intel.report/index.html">http://www.cnn.com/2005/POLITICS/03/31/intel.report/index.html</a>	CNN summary of the report
Uri Friedman	The Ten Biggest American Intelligence Failures – Foreign Policy	<a href="http://foreignpolicy.com/2012/01/03/the-ten-biggest-american-intelligence-failures/">http://foreignpolicy.com/2012/01/03/the-ten-biggest-american-intelligence-failures/</a>	Brief overview of some of the worse US intelligence failures
Judy Woodruff, Susan Hennessey	The privacy concerns at the heart of the FISA renewal debate	<a href="https://www.pbs.org/newshour/show/the-privacy-concerns-at-the-heart-of-the-fisa-renewal-debate">https://www.pbs.org/newshour/show/the-privacy-concerns-at-the-heart-of-the-fisa-renewal-debate</a>	PBS News Hour report on debate over Section 702 of the FISA act
Laurence Silberman & Charles Robb (Co-Chairs)	Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (Report)	<a href="http://www.nytimes.com/packages/pdf/politics/20050331_wmd_report.pdf">http://www.nytimes.com/packages/pdf/politics/20050331_wmd_report.pdf</a>	The 601-page report on the findings of the commission (read first 37 pages)
US Congress (95-511)	"Foreign Intelligence Surveillance Act of 1978 (Public Law 95-511)	<a href="https://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf">https://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf</a>	ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES
Rainey Reitman	3 Years Later, the Snowden Leaks Have Changed How the World Sees NSA Surveillance	<a href="https://www.eff.org/deeplinks/2016/06/3-years-later-snowden-leaks-have-changed-how-world-sees-nsa-surveillance">https://www.eff.org/deeplinks/2016/06/3-years-later-snowden-leaks-have-changed-how-world-sees-nsa-surveillance</a>	Summary of Snowden impact on the NSA and other intelligence agencies. Links to other sites
Raymond Ibrahim – Middle East Forum	Impervious Hubris: How U.S. Intelligence Failures Led to ISIS	<a href="http://www.meforum.org/6293/how-us-intelligence-failures-led-to-isis">http://www.meforum.org/6293/how-us-intelligence-failures-led-to-isis</a>	Discusses how US Intelligence Experts got it wrong regarding motivation behind Islamic Jihadism
Paul Rosenzweig and Michael Scardaville	Principles and the Total Information Awareness Program	<a href="https://www.heritage.org/homeland-security/report/the-need-protect-civil-liberties-while-combating-terrorism-legal">https://www.heritage.org/homeland-security/report/the-need-protect-civil-liberties-while-combating-terrorism-legal</a>	Discussion on the need to protect civil liberties while collecting intelligence to combat terrorism

US Army (ATP 2-22.9)	Open Source Intelligence	<a href="https://fas.org/irp/doddir/army/atp2-22-9.pdf">https://fas.org/irp/doddir/army/atp2-22-9.pdf</a>	Army Technical Publication 2-22.9 (ATP 2-22.9). Good overview of open source intelligence from the DoD perspective
US Congress (911 Report)	9/11 Commission Report	<a href="http://govinfo.library.unt.edu/911/report/911Report.pdf">http://govinfo.library.unt.edu/911/report/911Report.pdf</a>	The 9/11 Commission Report summarizing challenges discovered in the US Intelligence Community.
US Congress (Executive)	9/11 Commission Report Executive Summary	<a href="http://govinfo.library.unt.edu/911/report/911Report_Exec.pdf">http://govinfo.library.unt.edu/911/report/911Report_Exec.pdf</a>	Executive summary of 9/11 Commission Report
US Government (EO 12291)	CFR 28 Part 23 – Criminal Intelligence Systems Operating Policies	<a href="https://it.ojp.gov/documents/28cfr_part_23.pdf">https://it.ojp.gov/documents/28cfr_part_23.pdf</a>	Describes Executive Order 12291 which governs intelligence collection and analysis in domestic law enforcement
Sune von Solms & Renier van Heerden	The Consequences of Edward Snowden NSA Related Information Disclosures	<a href="https://www.researchgate.net/publication/275019554_The_Consequences_of_Edward_Snowden_NSA_Related_Information_Disclosures">https://www.researchgate.net/publication/275019554_The_Consequences_of_Edward_Snowden_NSA_Related_Information_Disclosures</a>	Cover the Edward Snowden disclosures/leaks
Orin Kerr – Washington Post	Edwin Snowden’s Impact	<a href="https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/04/09/edward-snowdens-impact/?utm_term=.b1cb17f3c599">https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/04/09/edward-snowdens-impact/?utm_term=.b1cb17f3c599</a>	Edward Snowden disclosure/leaks
Kenneth Lieberthal (Brookings Institute)	The U.S. Intelligence Community and Foreign Policy: Getting Analysis Right	<a href="https://www.brookings.edu/wp-content/uploads/2016/06/09_intelligence_community_lieberthal.pdf">https://www.brookings.edu/wp-content/uploads/2016/06/09_intelligence_community_lieberthal.pdf</a>	Provides an overview of the current US Intelligence Community, identifies

			challenges and possible solutions
Jami Miscik (Foreign Affairs)	Intelligence and the Presidency – How to Get it Right	<a href="https://www.foreignaffairs.com/articles/united-states/2017-04-17/intelligence-and-presidency">https://www.foreignaffairs.com/articles/united-states/2017-04-17/intelligence-and-presidency</a>	Provides overview of the US Intelligence Community from a policy perspective
US Gov't	ONDI	<a href="https://www.dni.gov/index.php/who-we-are">https://www.dni.gov/index.php/who-we-are</a>	Link to ONDI website
John C. Tang, et al.,	Reflecting on the DARPA Red Balloon Challenge	<a href="http://courses.cse.tamu.edu/caverlee/csce438/readings/red-balloon.pdf">http://courses.cse.tamu.edu/caverlee/csce438/readings/red-balloon.pdf</a>	OSINT crowdsourcing, misdirection, connectivity, social networks
Dan Coats - DNI	Worldwide Threat Assessment of the US Intelligence Community Senate Select Committee on Intelligence	<a href="https://www.intelligence.senate.gov/sites/default/files/documents/os-coats-051117.pdf">https://www.intelligence.senate.gov/sites/default/files/documents/os-coats-051117.pdf</a>	Yearly report by the Director of National Intelligence (in this case Dan Coats) to the US Senate on threats to the US
DSS – Defense Security Service	Targeting US Technologies – A Trend Analysis of Cleared Industry Reporting - 2017	<a href="http://www.dss.mil/documents/ci/2017_CI_Trends_Report.pdf">http://www.dss.mil/documents/ci/2017_CI_Trends_Report.pdf</a>	Discusses where threats are, and methods used to collect information and technologies
FBI	FBI Newark Division Strategic Partnership Newsletter AUGUST 2017	To be provided by instructor at beginning of semester	Presents information on individuals/groups/organization involved in espionage, etc.
Michael Chertoff Group	A Public Policy Perspective of the Dark Web	<a href="https://www.chertoffgroup.com/files/docs/ChathamHouseCyberJournal_MichaelChertoff_DarkWebArticle.pdf">https://www.chertoffgroup.com/files/docs/ChathamHouseCyberJournal_MichaelChertoff_DarkWebArticle.pdf</a>	Good policy discussion regarding dark web and Tor. Also does a decent job of describing the surface web, the deep web and the dark web

### Statement on Academic Conduct and Support Systems

**Academic Conduct:**

Plagiarism – presenting someone else’s ideas as your own, either verbatim or recast in your own words – is a serious academic offense with serious consequences. Please familiarize yourself with the discussion of plagiarism in *SCampus* in Part B, Section 11, “Behavior Violating University Standards” [policy.usc.edu/scampus-part-b](http://policy.usc.edu/scampus-part-b). Other forms of academic dishonesty are equally unacceptable. See additional information in *SCampus* and university policies on scientific misconduct, <http://policy.usc.edu/scientific-misconduct>.

**Support Systems:**

*Student Counseling Services (SCS) – (213) 740-7711 – 24/7 on call*

Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention. [engemannshc.usc.edu/counseling](http://engemannshc.usc.edu/counseling)

*National Suicide Prevention Lifeline – 1 (800) 273-8255*

Provides free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week. [www.suicidepreventionlifeline.org](http://www.suicidepreventionlifeline.org)

*Relationship and Sexual Violence Prevention Services (RSVP) – (213) 740-4900 – 24/7 on call*

Free and confidential therapy services, workshops, and training for situations related to gender-based harm. [engemannshc.usc.edu/rsvp](http://engemannshc.usc.edu/rsvp)

*Sexual Assault Resource Center*

For more information about how to get help or help a survivor, rights, reporting options, and additional resources, visit the website: [sarc.usc.edu](http://sarc.usc.edu)

*Office of Equity and Diversity (OED)/Title IX Compliance – (213) 740-5086*

Works with faculty, staff, visitors, applicants, and students around issues of protected class. [equity.usc.edu](http://equity.usc.edu)

*Bias Assessment Response and Support*

Incidents of bias, hate crimes and microaggressions need to be reported allowing for appropriate investigation and response. [studentaffairs.usc.edu/bias-assessment-response-support](http://studentaffairs.usc.edu/bias-assessment-response-support)

*The Office of Disability Services and Programs*

Provides certification for students with disabilities and helps arrange relevant accommodations. [dsp.usc.edu](http://dsp.usc.edu)

*Student Support and Advocacy – (213) 821-4710*

Assists students and families in resolving complex issues adversely affecting their success as a student EX: personal, financial, and academic. [studentaffairs.usc.edu/ssa](http://studentaffairs.usc.edu/ssa)

*Diversity at USC*

Information on events, programs and training, the Diversity Task Force (including representatives for each school), chronology, participation, and various resources for students. [diversity.usc.edu](http://diversity.usc.edu)

*USC Emergency Information*

Provides safety and other updates, including ways in which instruction will be continued if an officially declared emergency makes travel to campus infeasible. [emergency.usc.edu](http://emergency.usc.edu)

*USC Department of Public Safety – UPC: (213) 740-4321 – HSC: (323) 442-1000 – 24-hour emergency or to report a crime.*

Provides overall safety to USC community. [dps.usc.edu](http://dps.usc.edu)

## **Biography**

Dr. Michael Orosz directs the Decision Systems Group at the University of Southern California's Information Sciences Institute and is a Research Associate Professor in USC's Sonny Astani Department of Civil and Environmental Engineering. Dr. Orosz has over 30 years' experience in government and commercial software development, basic and applied research and development, project management, academic research, and has developed and deployed several successful products in both the government and commercial sectors. He also serves as a subject matter expert to the government in the areas of intelligence analysis – particularly in the area of Open Source Intelligence (OSINT) and cyber exploitation. His research interests include decision systems, open source intelligence analytics, data analytics, cyber-physical security, predictive analysis, operational risk management, smart buildings and intelligent human-computer interfaces.

Dr. Orosz has successfully led projects in developing command and control, intelligence analysis and model-based decision-support systems for applications ranging from protecting the Nation's food supply, ensuring aviation and maritime security, protecting the Nation's infrastructures and cities against terrorism events and enhanced C2I and analytics technologies used in the Intelligence Community. From 2004 to 2015, he served as a Principal Investigator at the DHS National Center for Risk and Economic Analysis of Terrorism Events (CREATE) where he led the development of InfraSec -an infrastructure terrorism risk assessment and security resource allocation system focused on venues such as airports and seaports and iSARs -a suspicious activity reporting intelligence and decision analysis system.

Dr. Orosz was also the Principal Investigator of a National Science Foundation-funded initiative to investigate and model the behavior of attackers, defenders and end-users in the cyber environment and used this knowledge to help improve cyber-physical security. Dr. Orosz recently was a Principal Investigator at the DHS National Center for Food Protection Defense (NCFPD) and the DHS National Center for Foreign Animal and Zoonotic Diseases (FAZD) where he served as the Information Analytics Science Group Leader. In addition, Dr. Orosz has recently or is presently managing intelligence-focused projects funded by DARPA, DHS, IARPA, NRO, NSA, NSF, USAF and the USMC. He frequently lectures to the intelligence, defense and law enforcement communities on cyber-space and OSINT analytics. In his role as a subject matter expert, Dr. Orosz frequently embeds within various DoD and law enforcement environments.

Dr. Orosz received a B.S. in Engineering from the Colorado School of Mines, a M.S. in Computer Science from the University of Colorado, and a Ph.D. in Computer Science from the University of California, Los Angeles.