Course Summary

In the more than a decade following the terrorist attacks of September 11th, 2001, a revolution took place in the relationship among federal, state, and local homeland security, law enforcement and intelligence organizations. At the federal level, the Department of Homeland Security (DHS) was created, the “wall” between law enforcement and intelligence was nearly obliterated, some law enforcement organizations have become more like intelligence agencies, and the foreign intelligence community was fundamentally reformed. The impact at the State level was even larger. State governments were assigned the lead role in many Homeland Security missions. Most States responded by bringing together existing public security, law enforcement, and emergency response capabilities, linking them to similar local assets, and opening channels to adjoining States. But there was a missing piece. Prior to 9/11, none of the States had a robust intelligence capability. Most now have created multiple intelligence cells in existing structures, as well as fusion centers which, for the first time, connect state and local homeland security and law enforcement—and especially the new intelligence organizations--with the federal community, and in some cases,
foreign intelligence services. There has also been a dramatic increase in intelligence capabilities within the private sector.

This course examines how Homeland Security Intelligence functions at the Federal, State, and local government levels and within the private sector.

Course Objectives

After participating in this course, students will be able to conduct a sophisticated, nuanced discussion addressing the following questions:

--What is “homeland security”? Who are the major stakeholders? What are their specific missions?

--What is intelligence? Who are the major intelligence producers?

--What are the roles and functions of the DNI and the Intelligence Community in meeting Homeland Security intelligence requirements? What is the role of State, local, and private intelligence producers?

--Why does the intelligence community have its current array of capabilities and to what degree should these be emulated or complemented at the State level to support homeland security customers?

--How do the Department of Homeland Security and the National Counter-Terrorism Center interface with intelligence at the national level? At the State, local, and private levels?
What can intelligence provide to assist homeland security customers – both governmental and in the private sector -- in counter-terrorism and cybersecurity?

Class Sequence and Content

Beginning in Class 3, we will start each class with a brief discussion of articles/op ed pieces in the previous week’s NY Times and local newspapers that relate to homeland security intelligence. I will assign two students each week to role-play the Director, FBI and the Secretary of Homeland Security. You should identify one story out of the New York Times or your local paper on a terrorism issue. After briefly summarizing the story, you will spell out why the Director, FBI or the Secretary of DHS (depending on your role) would be interested in this development and what intelligence your character would need to take appropriate action. You will each also respond to the issue brought up by the other participant. Depending on time available, I might raise other news items or ask the class for additional news items.

Also beginning in Class 3, individual students or teams will make presentations on their homework exercise. The class will then discuss their thoughts on the research issues raised in the previous week’s lecture.

We then move on to my lecture presenting the week’s new material. In the course of this presentation, I will identify next week’s research issue and homework assignment.

Class 1. Introduction to the course. We will begin the course by walking through the syllabus to ensure we have a common understanding of what the course will cover and what students
need to accomplish to be successful. We will also discuss a reading on *Surviving a Nuclear Attack on Washington, D.C.* By Sydney J. Freedberg Jr., *National Journal*. Steiner, Homeland Security Intelligence, Introduction.

**Part 1, Classes 2 – 5** US Homeland Security and US Intelligence

The United States has massive, overlapping homeland security and intelligence enterprises. Homeland security intelligence is at the nexus of these two structures and impacts on most of the organizations in both communities. In these lectures, I will provide a foundational understanding of the structure, organization and functions of both enterprises and then explore how they relate to each other in one functional area – intelligence support to the development of policy.

**Class 2** describes our Homeland Security Enterprise. It begins by defining HS. Then we look at the mandate for homeland security; the major HS missions and objectives; and the primary HS actors at the federal, state, local, private, non-governmental, and public levels. The Chapter concludes with a brief overview of the risk-management process which is at the heart of HS policy and resource allocation. Steiner, Chapter 1.

**Classes 3 and 4** are an introduction to and brief history of the US intelligence enterprise. Once again, we begin by defining intelligence and introducing the intelligence cycle and intelligence collection disciplines before laying out the history and current capabilities of major intelligence producers at the federal, State and local government, and private sector levels. Class 4 concludes with a presentation of the mandate for intelligence support to homeland security. Steiner, Chapter 2.
**Class 5** brings the homeland security and intelligence worlds together by taking a first look at how intelligence supports homeland security. This lecture uses actual intelligence and policy products to lay out the intelligence support process at the national level. The lecture concludes with a brief discussion of the requirement for intelligence support in the development of homeland security policy by State and local governments and private sector entities. Steiner, Chapter 3.

**Part II, Classes 6 – 7. Taking the Offensive: Intelligence Support to the Prevent Mission**

Offensive counterterrorism operations are intelligence-led and intelligence intensive. As we shall see, all of the major departments and agencies conducting counterterrorism operations in this mission area are long-time federal users of intelligence, have access to both national and departmental intelligence products at all classification levels, and know how to drive intelligence collection systems and assets to get the information they need to do their jobs. Further, all of these customers are sophisticated in terms of understanding what intelligence can and should do for them and in demanding excellent and comprehensive support.

The National Strategy for Counterterrorism (2011) calls for “maintain(ing) our focus on pressuring al-Qa’ida’s core while emphasizing the need to build foreign partnerships and capacity”\(^1\). This is an offensive, action-oriented directive and clearly spells out a specific mandate, led by the federal government abroad, to disrupt, dismantle, and destroy the enemy. (Class 6, Steiner Chapter 4).

At home, counterterrorism is a law enforcement function; the Attorney General officially has the lead role; the Federal Bureau of

---

Investigation (FBI) has been designated to direct all major investigations; and the FBI has established a system of Joint Terrorism Task Forces (JTTFs) to bring other federal, state, and local law enforcement into FBI-led investigations (Class 7, Steiner, Chapter 5).

If the federal government is in charge of all counterterrorism operations and investigations at home and abroad, then what is the role for state and local law enforcement in terrorism prevention? In Class 6 we will see that they have no role overseas. In Class 7 we see that State and local LE has a limited role in domestic terrorism investigations – liaising with the FBI through their officers seconded to local Joint Terrorism Task Forces (JTTF) and gathering CT intelligence and leads which are sent to the JTTF for action. Only in the case of an on-going or imminent attack such as those that occurred at Fort Hood in 2009 or the Boston Marathon bombing in 2013 do State and local law enforcement have a significant direct “prevent” role.

Part III, Classes 8 - 10 Securing the Homeland: Intelligence Support to the Protect Mission

In the next three classes we examine the major federal, state, local, and private organizations responsible for protecting our country and its human, physical, and cyber assets against terrorist and other attacks and the intelligence they require to accomplish this goal. In the Prevent mission, we saw how the National Security Council (NSC), the National Counter-Terrorism Center (NCTC), and the National Joint Terrorism Task Force (NJTTF) constitute interagency forums for developing a single integrated plan for actively going after any given terrorist plot or threat. To use a sports analogy, when you are on the offensive you huddle before each play and the quarterback has the final say on the field regarding what action is to be taken.
The protect mission is more like playing defense than offense. You do not need to huddle before every play because each team member knows the fundamental responsibilities of his position. There is still coordination, but it does not take place in a single, real-time, highly structured “huddle” like we see at the NSC, the NCTC, and the NJTTF processes. Rather, the layers of defense encompassed by the protect mission are coordinated on an a-periodic basis by regional or federal authorities. Of course, specific, offensive “protect” operations require local cooperation and coordination but the constructs that fulfill these roles are normally ad hoc and temporary.

In these three classes we will see that the distributed, defensive, 24/7/365 protect mission requires a different type of intelligence support than that provided to the preventers. Defenders need continuous, comprehensive intelligence on the full range of threats they might face, including not only terrorism but also a broad range of criminal activity. They also require the highly detailed intelligence crucial to conducting their aperiodic offensive operations.

In Class 8 (Steiner, Chapter 6) we see how the federal effort to protect the nation and the borders can draw on the federal intelligence community for robust support. In Class 9, (Steiner, Chapter 7) we look at all the players involved in protecting critical infrastructure and the dominant role of the private sector in this mission. Finally, in Class 10 (Steiner, Chapter 8) we will focus on the cybersecurity threat and our whole of the nation response to that threat.

Part IV, Class 11. Preparing for the Aftermath: Intelligence Support to the Respond and Recover Missions

Since 11 September 2001 there have been only two clearly successful international terrorist attacks within the US – the lone-
wolf shooter at Fort Hood in 2009 and the Boston Marathon bombing in 2013. Nevertheless, our risk-based approach to homeland security prudently calls for a substantial effort to prepare for the aftermath of a wide range of terrorist threats, from another lone wolf attack up to and including detonation of a nuclear weapon within the US.

In Class 11, we will examine the role of intelligence in helping governments, the private sector, communities, and the public prepare to respond to and recover from such attacks. We have already seen that the type of intelligence needed to go on the offensive and disrupt, dismantle and destroy terrorist organizations is quite different from the intelligence needed to defensively protect the country, its borders, and its critical infrastructure, including our cyber assets. The intelligence required by our first responder community and those responsible for planning both response and economic recovery is once again distinctly different.

Once a terrorist attack has occurred, the homeland security mission shifts into response mode and later into economic recovery. Especially in the initial response segment, long range threat intelligence embedded into threat scenarios is required to develop and exercise the response procedures and capabilities that will be crucial to mission success. For example, if the threat intelligence is warning of multiple IED attacks rather than a major chemical attack, then the rescue and medical preparations will be significantly different and a chemical attack could have a magnified impact because the proper response protocols have not been developed and the required medical supplies have not been stockpiled.

We need intelligence on the threats – both the enemy’s intentions and capabilities – so we can prepare to respond and prepare to recover from a successful attack even as we vigorously attempt
both to prevent any such attack and to protect potential targets. Steiner, Chapter 9.

**Classes 12– 14 --** Student Presentations on their major paper/project.

**Class 15 --** Assessing Homeland Security Intelligence. In this wrap-up class we will review the entire course to identify the challenges remaining in ensuring we have a world-class homeland security intelligence capability. Students will also submit their major paper for the course. (Steiner, Epilogue).

**Homeland Security Intelligence – Major Paper**

Perhaps the single most important theme in this course is that intelligence must be tailored to the needs of each specific client in the diverse homeland security customer set. Implicit in this theme is the assertion that in meeting this imperative, the intelligence product will be significantly different depending on the role of the customer.

For example, consider the characteristics of the intelligence product produced for the Governor of New York to help him and his staff in the risk analysis and management process leading to appropriate funding levels in the State budget for cybersecurity as opposed to funding for counterterrorism. Now think about the intelligence product required by the federal immigration officer at a port of entry trying to spot an Al Quaida operative attempting to enter the US.

Clearly, these two customers (one strategic, one tactical) whose positions require them to address very different dimensions of
homeland security (resource allocation, border protection) demand and deserve very different intelligence products.

Major Paper Assignment: I will assign each student two distinct homeland security intelligence customers. Briefly describe how the major characteristics of their jobs shape their intelligence needs. Who should provide intelligence support to each customer? Describe the characteristics of the intelligence product that will help them significantly. Prepare a sample intelligence product for each customer. Finally, compare and contrast these two intelligence products.

Does your analysis support the assertion that the intelligence products will be significantly different depending on the role of the customer?

Course Requirements and Grades

Press exercises and class participation, including discussion of research issues, constitute one-third of your grade.

Every student will prepare at least three powerpoint presentations/short papers as part of our weekly homework exercises and this will constitute one-third of your grade.

Each student will prepare an in-depth research paper described above. This paper will constitute the final one-third your course grade.

Students enrolled in the undergraduate section of this course (RPAD 456 rather than RPAD 556) will be expected to participate in all in-class and homework individual and team exercises. Reading requirements, however, will be significantly less demanding for the undergraduate section. Further, their major
papers will be shorter and require less original research. Finally, undergrads will be judged by different criteria for grading.

Required Text:

In addition to the text below I have prepared lists of readings for each class which are constantly updated. These files are on the first page of your Blackboard for this course.