



Course Learning Outcomes for Unit VII

Upon completion of this unit, students should be able to:

- 8. Develop a homeland security strategy for counterterrorism.
 - 8.1 Express the importance of considering intelligence; border, immigration, and customs enforcement; transportation security; and cybersecurity and critical infrastructure protection when developing a homeland security strategy for counterterrorism.
 - 8.2 Describe the importance of involving U.S. citizens in a homeland security strategy for counterterrorism.
 - 8.3 Identify ways that the U.S. federal government can encourage U.S. citizens to become a part of a homeland security strategy for counterterrorism.

Course/Unit Learning Outcomes	Learning Activity
8.1	Unit VII Lesson Chapter 12 Chapter 14 Chapter 16 Unit VII Article Critique
8.2	Unit VII Lesson Flynn article Unit VII Article Critique
8.3	Unit VII Lesson Flynn article Unit VII Article Critique

Reading Assignment

Chapter 12: Border Security

Chapter 14: Cybersecurity Legislation and Critical Infrastructure Vulnerabilities, pp. 233–242

Chapter 16: Transportation Security, pp. 268–275

In order to access the following resource, please click the link below:

Flynn, S. (2011). Recalibrating homeland security. *Foreign Affairs*, 90(3), 130–140. Retrieved from <https://libraryresources.columbiasouthern.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=60123119&site=ehost-live&scope=site>

Unit Lesson

Securing the homeland relies heavily on the implementation of homeland security strategy. There are several factors that must be considered when developing, implementing, and evaluating such programs. Counterterrorism is a daunting task considering the current global climate experienced in post-9/11 society, and it is important to understand what factors make up a comprehensive homeland security strategy.

When developing a homeland security strategy for counterterrorism, you must take a systems approach in which you consider several overarching areas. By delving deeper into these critical areas, you will develop an understanding of how to approach counterterrorism strategy by studying how each of these areas work

together collectively. The four main areas researched during this unit have been identified by Bullock, Haddow, and Coppola (2016) as the following:

- intelligence;
- border, immigration, and customs enforcement;
- transportation security; and
- cybersecurity and critical infrastructure protection.

As discovered in previous units in this course, 9/11 prompted the largest reorganization of the federal government since the 1940s. The Homeland Security Act created the Department of Homeland Security (DHS) and brought 22 agencies under one umbrella. Although none of the federal government's intelligence agencies were incorporated into the DHS, the role of intelligence as it relates to homeland security and counterterrorism is paramount. The United States Intelligence Community, or IC, is comprised of 16 individual entities that exist under the executive branch and collaboratively gather intelligence crucial to national security (Bullock et al., 2016).

The IC collects intelligence and disseminates this information to policymakers, law enforcement, homeland security agencies, and the military as needed. Bullock et al. (2016) states that the following agencies have a mission related to intelligence and counterterrorism:

- Air Force Intelligence, Surveillance, and Reconnaissance Agency;
- U.S. Army Intelligence and Security Command;
- Central Intelligence Agency;
- Coast Guard Intelligence;
- Defense Intelligence Agency;
- Department of Energy, Office of Intelligence and Counterintelligence;
- Department of Homeland Security, Office of Intelligence and Analysis;
- Bureau of Intelligence and Research;
- Department of Treasury, Office of Terrorism and Financial Intelligence;
- Drug Enforcement Administration, Office of National Security Intelligence;
- Federal Bureau of Investigation, National Security Branch;
- National Geospatial-Intelligence Agency;
- National Reconnaissance Office;
- National Security Agency; and
- Office of Naval Intelligence.

The role of the IC is to collect intelligence useful in counterterrorism efforts. Such information collected encompasses terrorism; weapons proliferation; chemical, biological, radiological, nuclear, and explosives (CBRNE) attacks; cyber and infrastructure attacks; foreign intelligence and hostile activities; and other issues related to the protection of American interests here and abroad. The strategic goals and objectives of the IC have been guided in recent years by the recommendations of the 9/11 Commission Report. After 9/11, the homeland security strategy for counterterrorism, among other concerns, was evaluated, and many weaknesses prompted a shift within the IC. Proposed findings and changes urged by the 9/11 Commission include the following in an effort to provide for a comprehensive counterterrorism strategy:

- Barriers in performing joint intelligence work: There is a need for all-source analysis, and there must be a joint effort when it comes to national intelligence in order to connect the dots.
- Common standards across foreign and domestic operations: There must be a uniform body of standards regardless of whether the intelligence was collected, processed, shared, or analyzed here or abroad.
- Prioritization and allocation of resources: It is crucial for the Director of Central Intelligence (DCI) to have the power to reallocate efforts and resources across the intelligence agencies.
- Responsibility of the DCI: The DCI, having three jobs, loses the ability to effectively manage the IC. With this daunting task, the authority of the DCI is often not used.
- Complexity and secrecy: The complex level of the responsibilities and roles, in addition to the great level of secrecy among the 15 agencies at the time, clouds the path to clear objectives (National Commission on Terrorist Attacks Upon the United States, 2004).

The result of these proposed adjustments was the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). Among the many changes in the IRTPA was the creation of the Office of the Director of National Intelligence and the National Counterterrorism Center (Bullock et al., 2016). Such changes have maximized the effectiveness of intelligence collection and sharing in line with homeland security strategy for counterterrorism.

Border and immigration is another homeland security strategy that is highly debated and one that is of key importance in a post-9/11 United States. Securing U.S. borders is crucial because of the role that doing so plays economically and politically (DHS, n.d.). Border security is also important for national security. As the global economy and social climate grows, the concept of borders changes for several reasons. Globalization presents challenges to securing U.S. borders with an increase in travel, commerce, and trade. This also presents a challenge as it relates to homeland security (DHS, n.d.).

The role of border security belongs to the DHS. The DHS protects U.S. borders by managing border protection, immigration, and customs enforcement (Bullock et al., 2016). Homeland security hinges on border security and developing a comprehensive strategy for counterterrorism includes considering such issues as border patrol and surveillance, drug smuggling, and port security. Alperen (2017) notes the following as policy and strategy that guides border security:

- Homeland Security Act of 2002,
- Intelligence Reform and Terrorism Prevention Act of 2004 (Advanced Technology Northern Border Security Pilot Program),
- National Southwest Border Counternarcotics Strategy of 2009,
- Border Tunnel Prevention Act of 2012,
- Ultralight Aircraft Smuggling Prevention Act of 2012, and
- National Southwest Border Counternarcotics Strategy of 2013.

Transportation security also plays a critical role when considering homeland security strategy for counterterrorism. The events of 9/11 brought transportation to the forefront, and the DHS, among others, are responsible for securing the transportation sector. Homeland security hinges on securing the following:

- freight and rail;
- highways, roadways, and motor carrier networks;
- ports and intermodal freight;
- mass transit;
- air freight; and
- commercial aviation (Bullock et al., 2016).

The National Infrastructure Protection Plan outlines critical roles and responsibilities of the agencies responsible for protection in these sectors. These agencies, known as sector specific agencies, are guided by homeland security strategy to counter terrorism within the transportation sector in order to detect, deter, and prevent terrorism.

Finally, because of the technological world we occupy, cybersecurity is a crucial concern. Considering we rely on information security in all aspects of our lives, we are vulnerable to threats from this angle as well. Bullock et al. (2016) notes that significant threats come from the following:

- cyber terrorists,
- cyber spies,
- cyber thieves,
- cyber warriors, and
- cyber hackers.

The cyber infrastructure of the United States is vast and is growing each day, so it is prudent to ensure homeland security strategy is in place to protect such assets. Cyberterrorism is a new form of terrorism, and to help ensure that the cyber networks are protected, President Obama issued Executive Order 13636 to help improve critical infrastructure cybersecurity in response to the growing concern for more measures to counter threats within the critical infrastructure of the United States (Bullock et al., 2016). Cybersecurity strategy within the United States. is led by the Office of Cybersecurity and Communications (CS&C) within

the DHS. Within this office, there are five divisions that are charged with implementing such strategies, and they include the following:

- Network Security Deployment,
- Federal Network Resilience,
- Stakeholder Engagement and Cyber Infrastructure Resilience,
- National Cybersecurity and Communications Integration Center, and
- Office of Emergency Communications.

By considering these four elements when developing a homeland security strategy for counterterrorism, it is critical to understand that each compliments the other when taking a risk-based systems approach. Having a comprehensive understanding that each element collectively is responsible for the protection of the U.S. homeland.

References

Alperen, M. J. (2017). *Foundations of homeland security: Law and policy* (2nd ed.). Hoboken, NJ: Wiley.

Bullock, J. A., Haddow, G. D., & Coppola, D. P. (2016). *Introduction to homeland security* (5th ed.). Waltham, MA: Butterworth-Heinemann.

Department of Homeland Security. (n.d.). Border security. Retrieved from <https://www.dhs.gov/border-security>

National Commission on Terrorist Attacks Upon the United States. (2004). *The 9/11 Commission report*. Retrieved from <http://govinfo.library.unt.edu/911/report/911Report.pdf>