Homeland Security: Two Decades of Protecting the Nation

Week 2
Terrorism, Cybersecurity, Disaster Response
What We’ll Learn in Week 2

- The Homeland Security Enterprise takes a broad “All Hazards” approach to threats—preventing and responding to both man-made and natural threats.
- Terrorism, Cyber, other Man-Made, and Natural Threats are reviewed in Week 2.
- U.S. interagency responses to these threats have improved since 9/11—but are far from totally ready.
Fundamental and Powerful Concept: DHS “All Hazards” Threat

- **State** *(define)*: all natural and man-made hazards that can threaten the US homeland.

- **Elaborate**: includes natural hazards and threats, e.g., weather, geologic, disease, etc., and man-made hazards and threats to include both accidents and deliberate attempts to harm people, infrastructure, or resources.

- **Exemplify**: a hurricane is a natural hazard, a bridge or dam collapse is a man-made accident (hazard), a terrorist attack is a man-made hazard. An attack by a foreign military on U.S. territory is not an all hazards attack for DHS action—but is a national security issue to be handled by DOD.

- **Illustrate**: as doctors must diagnose and treat a person for all manner of different diseases and other afflictions, the Homeland Security Enterprise is responsible for preparing and responding to U.S. “all hazard” threats.
Defining the Virginia “All Hazards” Threat

- **Terrorism-Related**: WMD (Nuclear/Radiological (Dirty Bombs), Chemical, Biological), Explosive Devices (IED, etc.), Cyber Attacks (plus armed robbery, extortion, assassination, kidnapping, etc.)

- **Transnational Crime-Related**: Drug Trafficking, Illegal Immigration, Sex Trafficking, Other Transnational Crime (economic smuggling, etc.)

- **Man-Made**: Transportation Accidents, Energy-Related Hazards (Power Shortages /Outages), Dam Failure, Nuclear Power Accident, other Structural Failures

- **Weather-Related**: Floods, Tornadoes, Hurricanes, Tropical Storms, Thunderstorms, Winter Storms (ice and snow), Hail Storms, Droughts, Heat Waves

- **Earth-Related**: Earthquakes, Forest Fires/Wild Fires, Landslides, Mine Collapse, Sinkholes, Animal & Plant Disease, Epidemiological Outbreak
2014 HS Quadrennial Review

- Prevent Terrorism and Enhance Security
  - Prevent Terrorist Attacks
  - Prevent the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities
  - Manage Risks to Critical Infrastructure, Key Leadership, and Events
Terrorism is a Complex Behavior

- **State-Supported** Terrorism: use as a political tool
- **Revolutionary** Terrorism: to replace a government
- **Religious/Ideological** Terrorism: to right or avenge a perceived wrong
- **Issue Specific** Terrorism: environment, abortion, etc.

---

**FACES OF GLOBAL TERRORISM**


DIPLOMATIC SECURITY | REWARDS FOR JUSTICE
www.rewardsforjustice.net • rfj@state.gov • 1-800-US REWARD
Definition of Terrorism

...the term “...terrorism” means activities that—(A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State; (B) appear to be intended—(i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and (C) occur primarily outside the territorial jurisdiction of the United States (international).... or inside U.S. territory (domestic).... (modified from 18 USC 2331)
Understanding Causes of Terrorism

- Easiest to understand through broad brush of Frustration-Aggression Theory:
  - A group has political, economic, or social grievances that they are unable to resolve through the existing political or social structures (creates frustration).
  - The groups then becomes impatient and makes a conscious decision to turn to violence in an attempt to resolve their grievances (results in aggression).
Tactics of Terrorism

**To Generate Fear**
- Assassination
- Arson
- WMD
- Suicide Bombings
- Random Targeting
- Cyber Attacks
- Innovative Methods (IED, aircraft as missiles, etc.)

**For Terrorist Support**
- Armed Robbery
- Weapons Thefts
- Extortion
- Kidnapping
- Cyber Attacks
- Ransacking Populations (money, food, drink, vehicles, etc.)
Revolution versus Terrorism

- **Revolution**: an overthrow or repudiation and the thorough replacement of an established government or political system.

- **Terrorism**: the use of violence and threats to intimidate or coerce, especially for political purposes.

Source: Dictionary.com

How should ISIS be labeled?
A little Middle East/Islamic History

The Roman Empire (0 CE) 
Time of Jesus of Nazareth

The Arab Empire (634-1258)
Time of the Islamic Caliphate

Rise of the Ottomans (1258-1500 CE)
Finally Dissolved 1922

Prophet Muhammad (570-632 CE)
Crusades (1096-1272 CE) led by France, England, & Holy Roman Empire

Islamic World Today
What ISIS & al Qaeda Want?

1. Remove Western and other outside influences from Islamic World, seize territory (ISIS), overthrow existing governments, re-establish the Islamic Caliphate
2. Force Western and local governments to over-react to their actions and thus use situation to recruit more followers and soldiers
3. Govern with a literal interpretation of the Koran/Quran and Sharia (ethics code) (ISIS more radical interpretation than al Qaeda)
Terrorism risk in the MENA region

The map below shows that terrorism risk in the Middle East and North Africa (MENA) region is concentrated in a handful of countries; namely, Syria, Iraq, Yemen, Egypt and Libya. These states have conditions that are conducive to terrorism, including severe political polarisation, intense sectarianism / tribalism, oppressive governance, discrimination of local populations, a lack of rule of law, war, external intervention and porous borders. While these conditions in combination do not apply to all of the above-mentioned countries, all witness severe political polarisation, oppressive governance and discrimination. The map also shows that those countries on the north-western and south-eastern perimeter of the MENA region – namely Morocco, the UAE and Oman – are least exposed to the threat of terrorism.

Terrorism Risk 2015-Q2
- Red: Extreme risk
- Yellow: Low risk
- Orange: High risk
- Grey: No data
- Medium risk

Data sources: Verisk Maplecroft, 2015; GAD, 2015; Natural Earth, 2012
© Verisk Maplecroft 2015
Western Domestic Threat from International Terrorist Groups

- **Directed Attacks** from Outside Groups
  - Infiltrate own attackers
  - Recruit and direct attackers through Internet using extremist ideologies
  - May provide logistics support (weapons, funding, etc.)

- **Inspired Attacks** from Within
  - Radicalized attackers through direct contact or Internet
  - Attackers provide own logistics support

---

TERRORISM
U.S. Domestic Threat: Lone-Wolf Terrorists

- A lone wolf or lone-wolf terrorist is someone who prepares and commits violent acts alone, outside of any command structure and without material assistance from any group. However, he or she may be influenced or motivated by the ideology and beliefs of an external group (international or domestic), and may act in support of such a group (inspired attacks).
U.S. Hate Groups Can Use Terror Tactics

38 Active Hate Groups in Virginia: Black Nationalist, White Nationalist, Neo-Nazi, Racist Skinhead, KKK, Neo-Confederate, Anti-Muslim, Anti-Immigrant, Anti-LGBT, Neo-Völkisch (Southern Poverty Law Center, 2018)
Ideologies: The Sacred Texts of Terror

- Koran/Quran
- Sharia (Ethics)

- Mein Kampf by Adolf Hitler
- The Constitution
- Holy Bible
- The Lost Cause
- The Communist Manifesto
- Guerrilla Warfare
Southern Poverty Law Center
Hate Group Statistics
Other US Domestic Terrorists: usually single issue groups
U.S. Left Now Reacting to Hate Groups

“Hate the Haters”
Time for a 10 Minute Break!
2014 HS Quadrennial Review

- Safeguard and Secure Cyberspace
  - Create a Safe, Secure, and Resilient Cyber Environment
  - Promote Cybersecurity Knowledge and Innovation
“It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.”

Executive Order 13636
February 12, 2013

Issued After Senate Rejected Obama Administration Bill to Increase Cyber Security Readiness on Private-Owned Critical Infrastructure Sites and Businesses
DHS Focus on Cyber Security

16 DHS Critical Infrastructure Sectors

- Chemical Sector: The Department of Homeland Security is designated as the Sector-Specific Agency for the Chemical Sector.
- Commercial Facilities Sector: The Department of Homeland Security is designated as the Sector-Specific Agency for the Commercial Facilities Sector.
- Financial Services Sector: The Department of Treasury is designated as the Sector-Specific Agency for the Financial Services Sector.
- Food and Agriculture Sector: The Department of Agriculture and the Department of Health and Human Services are designated as the Co-Sector-Specific Agencies for the Food and Agriculture Sector.
- Communications Sector: The Department of Homeland Security is designated as the Sector-Specific Agency for the Communications Sector.
- Critical Manufacturing Sector: The Department of Homeland Security is designated as the Sector-Specific Agency for the Critical Manufacturing Sector.
- Government Facilities Sector: The Department of Homeland Security and the General Services Administration are designated as the Co-Sector-Specific Agencies for the Government Facilities Sector.
- Healthcare and Public Health Sector: The Department of Health and Human Services is designated as the Sector-Specific Agency for the Healthcare and Public Health Sector.
- Nuclear Reactors, Materials, and Waste Sector: The Department of Homeland Security is designated as the Sector-Specific Agency for the Nuclear Reactors, Materials, and Waste Sector.
- Dams Sector: The Department of Homeland Security is designated as the Sector-Specific Agency for the Dams Sector.
- Defense Industrial Base Sector: The Department of Defense is designated as the Sector-Specific Agency for the Defense Industrial Base Sector.
- Information Technology Sector: The Department of Homeland Security is designated as the Sector-Specific Agency for the Information Technology Sector.
- Energy Sector: The Department of Energy is designated as the Sector-Specific Agency for the Energy Sector.
- Transportation Systems Sector: The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.
- Water and Wastewater Systems Sector: The Environmental Protection Agency is designated as the Sector-Specific Agency for the Water and Wastewater Systems Sector.
DHS works to prevent critical infrastructure cyber attacks and inform partners of attack information

- Denial of Services Attacks
- Virus Dissemination
- Computer Vandalism
- Cyber Terrorism
- Software Piracy
- Other Criminal Activities (pornography, financial crimes, data theft, etc.)

Recently DHS has focused on voting system protection and countering foreign dis-information operations targeting US elections, including through Social Media
Selected Federal Cybersecurity Efforts

- **DHS** – protect own systems and focus on protecting U.S. critical infrastructure, ICE has Cyber Crimes Center
- **FBI** – protect own systems and conduct investigations related to counterterrorism and criminal acts
- **DOD:**
  - **USCYBERCOM** (at NSA) – military cyberspace operations
  - Military Services & Other DOD Agencies – protect own systems and support own missions
- **Other US Agencies** – protect own systems and support own missions
- There is no federal “Cyber Czar” to coordinate the above!
2014 HS Quadrennial Review

- Strengthen National Preparedness and Resilience
  - Mitigate Hazards
  - Enhance Preparedness
  - Ensure Effective Emergency Response
  - Rapidly Recover
TYPES OF DISASTER

Natural Disasters
- Meteorological
- Topographical
- Environmental

Man-made Disasters
- Technological
- Industrial accidents
- Security related
Disasters: Deadly, destructive, and disruptive events occurring when a hazard interacts with human vulnerability. Disasters often exceed the capabilities of local emergency services.

- Disaster management in the United States is decentralized and fragmented.
Legal Guidance for Disaster Prevention and Response

- Robert T. Stafford Disaster Relief and Emergency Assistance Act and Related Authorities (1988)
- Homeland Security Act of 2002
  - Reorganized FEMA
  - Enhanced FEMA Responsibilities and Autonomy in DHS
  - Added new Leadership Positions and Missions
  - Amended Stafford Act and HS Act of 2002
**Integrated Emergency Management System**: Unity of effort among all levels of government and local communities to increase emergency management capabilities and readiness

- **National Response Framework (NRF)**:
  - Guide to how U.S. conducts “all-hazard” response
  - 15 Emergency Support Functions designated (must be in EM Plans)
  - Federal interagency support during emergencies and disasters

- **National Incident Management System (NIMS)**:
  - Establishes standardized incident management processes, protocols, & procedures
  - Applicable regardless of the incident cause, size, or complexity

- **Incident Command System (ICS)**:
  - Field operations response processes, protocols, procedures
  - Incident action plans (objectives, strategies, tactics, logistics, etc.)
  - Incident-level decision making and resource allocation
  - Command may change as incident progresses
How did we do at Hurricane Maria (2017)?

- Territory of Puerto Rico: 3.5 Million U.S. Citizens affected, $90 Billion in damage, 2,975 direct and indirect deaths (may have been more)
- Electrical power and communications lost, roads/bridges washed out, rough geography, and lack of helicopters, all contributed to failure of situational awareness—FEMA admitted it underestimated the fragility of the island’s infrastructure—large-scale suffering as electric not fully restored for 11 months
- FEMA qualified personnel and emergency pre-staged supplies were low due to recent responses to Harvey (Texas) and Irma (Florida)—resulting in inordinate need for private contractors to provide assistance—Jones Act made problems more difficult—ended up more of a man-made disaster due to severe response and recovery problems (lack of Congressional Oversight hearings)
- Ongoing Puerto Rican debt problems contributed to poor local disaster preparation and infrastructure failures
Lessons Learned (so far) from Hurricanes Florence & Michael (2018)

• Florence (17 deaths) was more of a rain/flooding damage event

• Michael (26 deaths—as of Oct. 17) was more of a wind damage event

• State and local leadership was key to response efforts

• Volunteers—local and outside (Cajun Navy, etc.) assisted response

• Citizen failure to evacuate added to death count and made search and rescue efforts more extensive

• Many citizens did not have proper insurance coverage (if any)
In Week 3 we review the Homeland Security mission areas of Border Security and Immigration Enforcement