WORKING DRAFT

Strategic National Risk Assessment 2015

SNRA Working Papers

May 2015

Homeland Security

PRE-DECISIONAL DRAFT

Not for Public Distribution or Release

Table of Contents

Contents

The following contents comprise the basis for many of the qualitatively identified threats and hazards in the 2015 Strategic National Risk Assessment. Participants from across the Federal government contributed to these narratives in an effort further increase awareness and understanding of many of the risks our nation is currently facing.

The narratives are in varying stages of progress, and are presented in no particular order. The events listed in this document were not quantitatively assessed and did not result in comparative risk findings in the 2015 SNRA. This in no way diminishes the importance of these events as national-level risks, as identified by the SNRA project team. While insufficient time and/or data was available to mature these products to where comparative risk statements could be made, the narratives themselves are important in characterizing threats and hazards identified in the SNRA.

The SNRA project team believes that the following contents may serve as the basis for updates to future iterations of the SNRA and other risk related projects.

Electric Grid Failure (Natural / Accidental)

Event Description

Electric Power Grid Failure: A significant regional power-grid failure that extends beyond the geographic area of the initiating incident, which is due to natural disaster/hazards, equipment failure, distribution/transmission failure/disruptions, or public appeals to reduce usage (brown-to blackouts).

Event Background

Electric Power Grid Failures are common. Significant ones are often associated with large-scale natural hazards, such as hurricanes, earthquakes, solar storms, and major winter storms. In addition to the natural physical effects of the events and the damage on the generation, transmission, and distribution equipment, the power grid is designed to fail "safely," which is to say, the control systems and operating protocols will intentionally shut down undamaged elements of the grid if sudden changes in supply and demand make the grid unstable. The Electric Power Grid Failure scenarios under evaluation are those that are attributable to the physical destruction of natural disasters, equipment failure, distribution/transmission disruptions and public appeals to reduce usage.

There is no single interconnected national grid for the U.S. Instead, the continental U.S. is served by four separate grids, which cannot be impacted by the failure of their neighbors, though it is feasible for events to impact more than one of the grids within the U.S.

The four separate networks are:

- The Western Interconnection, which serves those contiguous states west of the Rockies as well as their Canadian neighbors and portions of Northwestern Mexico;
- The Electric Reliability Council of Texas, which serves only the state of Texas,
- The Eastern Interconnection which serves all states (and Canadian Provinces) east of the Rockies and South of the Great Lakes and New York, and
- The Quebec Interconnection, which serves New York, New England, and Canadian provinces east of Manitoba.

The Eastern Interconnection is actually made up of four interconnected but separately managed grids, allowing some cascading failures within this large, heavily populated area.

No scenario exists for a national U.S. power grid failure, except apocalyptic events that may make power restoration issues seem minor.

A quantitative analysis of data provided by the National Protection and Programs Directorate (NPPD) regarding electric power grid outages from 2005 through 2014 was performed using those reported outages caused by 16 natural, equipment and public appeals for reduction of usage categories. Adversarial and Space Weather outages were not addressed in this analysis, but are covered elsewhere in the Strategic National Risk Assessment Summary; however, the resulting economic impacts may be comparable.

Over 10 years that cover the reported events, it is understood that more events occurred but only the reported events that resulted in outages were considered. These events led to significant

Megawatt (MW) Demand Loss to the electric power providers and significant economic loss to the customers. The overall average frequency of failure regardless of mechanism is 61.2 report events per year. The number of deaths that might be associated with power outages was not considered in this analysis for these reasons; 1) the information was not provided, 2) it is difficult to determine if a death is directly related to an outage, and 3) this analysis is not tracking deaths. This analysis looked at the economic impact that outages have in 2014 dollars using residential, small/medium businesses, and large businesses from 2012 and 2013 census data.

The following tables present the risk of grid failure to the Nation as a whole. The actual failure causative agents are localized in nature, and the failures do not affect the whole Nation at the time of the failure. The data does indicate these failures show the aggregate MW Demand Loss and economic impact that is incurred. Table 1 is a compilation of the 16 failure causes that occurred over the 10-year period outlining the resultant impact—in this case, on the MW Demand Loss that was incurred by the power industry providers and the numbers of customers affected by the outage.

Table 1: Electric Power Grid Reported Failure Loss – 2005–2014

Failure Cause	Number of Reported Events	Total Outage Hours	Average Outage Hours	Total MW Demand Loss	Average MW Demand Loss/Event	Average MW Demand Loss/Event Hour	Total Customers Affected[1]	Average Number of Customers[1] Affected/Event
Flooding	1	432.5	432.5	200	200	0.46	21000	21000.00
Earthquake	3	67.57	22.52	1375	458.33	20.35	420886	140295.33
Tornados	4	189.02	47.26	2335	583.75	12.35	363294	90823.50
Hurricanes/ Tropical Storms	18	2200.96	122.28	15106	839.22	6.86	4389780	243876.65
Brush/Wildfires	11	51.39	4.67	10412	946.55	202.69	3632732	330248.36
Ice Storms	23	2168.53	94.28	9709	422.13	4.48	3009934	130866.70
Severe Winter/ Winter Storms	40	2836.94	70.92	14649	366.23	5.16	9309160	232729.00
Wind	50	2482.73	49.65	11624	232.48	4.68	7024603	140492.06
Thunderstorms/ Lightning	94	3357.80	35.72	44959	478.29	13.39	16259599	172974.46
Storms/Severe Storms	81	4275.30	52.78	33250	410.49	7.78	16070627	198402.80
Electrical System Failures	100	561.44	5.61	66005	600.50	1176.56	5722055	57220.55
Equipment Fires	4	12.79	3.20	1081	270.25	84.45	128654	32163.50
Distribution/ Transmission/ Generator Failures	72	1980.71	27.51	32918	457.19	16.62	6755455	93825.76
Fuel Supply Disruption	24	3410.96	142.12	14760	615.00	4.33	140001	5833.38
Load Shedding/ Voltage Reduction	74	692.64	9.36	23435	316.69	33.83	6156567	83196.85
Public Appeals Reduction	13	375.10	28.85	18645	1434.23	49.71	4277859	329066.08
TOTAL	612	24096.38	39.37	300463	490.95	12.47	83682206	136765.63

[1] All customers affected – residential; small, medium, and large retail businesses and industry.

Table 2 provides the breakdown and total of the numbers of electricity customers/consumers for the Nation using the most recent census data. These numbers provided a baseline for the data presented in Table 3, Table 4, and Table 6.

Table 2: Electricity Consumers in the United States

Consumer Segment	Subtotal of Segment	Percent of Total	Census
Residential	132,802,859	95	2013
Small–Medium Business[2]	6,232,434	4	2012
Large Business[2]	1,199,374	1	2012
TOTAL ALL	140,234,667	100	

Table 3 addresses the impact to the Nation as a whole should the entire "national" grid suffer a catastrophic failure and the resultant significant economic impact regardless of the causative or aggregate failure agent(s).

Table 3: Power Outage Economic Impact to Consumers

Consumer Segment	Subtotal of Segment	Average Cost Factor per Hour[3] (2004 $)	Economic Impact per Outage Hour (2004 $)	Inflation Factor (2004 – 2014)[4]	Economic Impact per Outage Hour (2014$)
Residential	132,802,859	$3.00	$398,408,577	1.253	$499,205,947
Small–Medium Business	6,232,434	$1200.00	$7,478,920,800	1.253	$9,371,087,762
Large Business	1,199,374	$8200.00	$9,834,866,800	1.253	$12,323,088,100
NATIONAL TOTAL	140,234,667		$17,712,196,177	1.253	$22,195,381,809

[2] Small–Medium businesses are those that employ 0 to 499 employees. Large businesses are those that employ 500 or greater employees.
[3] Understanding the Cost of Power Interruptions to U.S. Electricity Consumers (2004), U.S. Department of Energy and Lawrence Berkeley National Laboratory
[4] U.S. Inflation Calculator, U.S. Bureau of Statistics

Table 4 presents the economic and social impact resulting from data in Table 6 which addresses the economic impact that resulted from the reported failures over the 10-year reporting period 2004 to 2014.

Table 4: Table of Findings

Category	Description	Metric	Low	Medium	High
	All Events	MW Demand Loss	200	490.95	66005
	All Events	Outage Hours	12.79	39.37	4275.30
Economic	Economic Residential	Dollars/Event	$75,012.00	$18,682,052.49	$58,079,287.63
Economic	Economic Small-Medium Business	Dollars/Event	$1,263,024.00	$314561410.50	$977,917,322.26
Economic	Economic Large Business	Dollars/Event	$2,157,666.00	$537,375,546.10	$1,670,608,759.85
Economic	Economic Residential	Average Dollars/Event Hour	$173.44	$896,866.89	$3,643,347
Economic	Economic Small-Medium Business	Average Dollars/Event Hour	$2,920.29	$15,101,108.81	$61,345,325.47
Economic	Economic Large Business	Average Dollars/Event Hour	$4,988.82	$25,797,728.22	$104,798,264.34
Social	All Events	Household Displacement	1,995.00	496,863.10	1,544,661.91

Table 5 shows the frequency or likelihood that a failure may occur each year associated with a particular failure cause. The table shows, as well, the total failures that may or likely occur each year regardless of the causative agent.

Table 5: Event Frequency of Occurrence

Failure Cause	Flooding	Earthquake	Tornados	Hurricanes/Tropical Storms	Brush/Wildfires	Ice Storms	Severe Winter/Winter Storms	Wind	Thunderstorms/ Lightning	Storms/Severe Storms	Electrical System Failures	Equipment Fires	Distribution/Transmission/ Generator Failures	Fuel Supply Disruption	Load Shedding/Voltage Reduction	Public Appeals Reduction	TOTAL
Report Events Frequency/ Year	0.1	0.3	0.4	1.8	1.1	2.3	4	5	9.4	8.1	10	0.4	7.2	2.4	7.4	1.3	61.2

Table 6 shows the overall economic impact each of the failure causes have on the economy broken down to residential, small–medium businesses, and large businesses along with, for planning purposes, the expected social displacement of households for shelter planning.

Summary

These tables present a wealth of information. The failure causes are isolated events that affect only a relatively small geographical area and rarely an entire region. As such, from a national risk assessment they may not necessarily be considered as risk. These failures and the resultant outages do have an economic impact, but it is isolated and is more a local nuisance than anything more. However, as we look at the aggregates of each failure cause then we begin to see that the economic impact begins to be significant, and the risk becomes nationally strategic. This becomes even more evident as we examine the result of all of the failures occurring at the same time or if the entire national grid and the four components that make up the national grid are affected at the same time catastrophically. Should this happen, the economic impact would be billions of dollars an hour (See Table 3), and if prolonged, would be economically unrecoverable. The social displacement from a catastrophic failure would be such that civilization as we currently know it would no longer exist because of the tremendous reliance the Nation's population has upon electric power. It is not unreasonable to expect that the social upheaval would be catastrophic as well. A prolonged catastrophic failure regardless of the causative agent(s) to society could lead to indeterminate collateral deaths, which could be in the tens to hundreds of million within the first year.

Table 6: Electric Power Grid Economic Loss – 2005–2014

Event Cause	Report Events	Total Outage Hours	Average Outage Hours	Total Customers Affected (100%)	Average Number of Customers Affect/Event	Residential Customers Affected (95%)	Small-Medium Business Affected (4%)	Large Business Affect (1%)	Impact Cost Factor[5] Res.	Impact Cost Factor[5] S – M	Impact Cost Factor[5] Large	Econ Impact/ Event Res.	Econ Impact/ Event S – M	Econ Impact/ Event Large	Aver. Econ Impact/ Event Hour Res.	Aver. Econ Impact/ Event Hour S – M	Aver. Econ Impact/ Event Hour Large	Displaced Households[6]
Flooding	1	432.5	432.5	21000	21000.00	19950.00	840.00	210.00	$3.76	$1503.60	$10274.60	$75012.00	$1263024.00	$2157666.00	$173.44	$2920.29	$4988.82	1995.00
Earthquake	3	67.57	22.52	420886	140295.33	399841.70	16835.44	4208.86	$3.76	$1503.60	$10274.60	$1503404.79	$25313767.58	$43244352.96	$66758.65	$1124057.18	$1920264.34	39984.17
Tornados	4	189.02	47.26	363294	90823.50	345129.3	14531.76	3632.94	$3.76	$1503.60	$10274.60	$1297686.17	$21849954.34	$37327005.32	$27458.45	$462335.05	$789822.37	34512.93
Hurricanes/ Tropical Storms	18	2200.96	122.28	4389780	243876.65	4170291.00	175591.20	43897.8	$3.76	$1503.60	$10274.60	$15680294.16	$264018928.32	$451032335.85	$128232.70	$2159134.19	$3688520.90	417029.10
Brush/ Wildfires	11	51.39	4.67	3632732	330248.36	3451095.40	145309.28	36327.32	$3.76	$1503.60	$10274.60	$12976118.7	$218487003.41	$373248682.07	$2778612.14	$46785225.57	$79924771.32	345109.54
Ice Storms	23	2168.53	94.28	3009934	130866.70	2859437.30	120397.36	30099.34	$3.76	$1503.60	$10274.60	$10751484.25	$181029470.50	$309258678.76	$114037.80	$1920125.91	$3280215.09	285943.73
Severe Winter/ Winter Storms	40	2836.94	70.92	9309160	232729.00	8843702.00	372366.40	93091.60	$3.76	$1503.60	$10274.60	$33252319.52	$559890119.04	$956478953.36	$468870.83	$7894671.73	$13486730.87	884370.20
Wind	50	2482.73	49.65	7024603	140492.06	6673372.85	280984.12	70246.03	$3.76	$1503.60	$10274.60	$25091881.92	$422487722.83	$721749859.84	$505375.27	$8509319.69	$14536754.48	667337.29
Thunderstorms/Lightning	94	3357.80	35.72	16259599	172974.46	15446619.05	650383.96	162595.99	$3.76	$1503.60	$10274.60	$58079287.63	$977917322.26	$1670608759.85	$1625959.90	$27377304.65	$46769562.12	1544661.91
Storms/ Severe Storms	81	4275.30	52.78	16070627	198402.80	15267095.65	642825.08	160706.27	$3.76	$1503.60	$10274.60	$57404279.64	$966551790.29	$1651192641.74	$1087614.24	$18312841.80	$31284438.06	1526709.57
Electrical System Failures	100	561.44	5.61	5722055	57220.55	5435952.25	228882.20	57220.55	$3.76	$1503.60	$10274.60	$20439180.46	$344147275.92	$587918263.03	$3643347.68	$61345325.47	$104798264.34	543595.23
Equipment Fires	4	12.79	3.20	128654	32163.50	122221.30	5146.16	1286.54	$3.76	$1503.60	$10274.60	$459552.09	$7737766.18	$13218683.88	$143610.03	$2418051.93	$4130838.71	12222.13
Distribution/ Transmission/ Generator Failures	72	1980.71	27.51	6755455	93825.76	6417682.25	270218.20	67554.55	$3.76	$1503.60	$10274.60	$24130485.26	$406300085.52	$694095979.43	$877153.25	$14769177.95	$25230679.00	641768.23
Fuel Supply Disruption	24	3410.96	142.12	140001	5833.38	133000.95	5600.04	1400.01	$3.76	$1503.60	$10274.60	$500083.57	$8420220.14	$14384542.75	$3518.74	$59247.26	$101214.06	13300.10
Load Shedding/ Voltage Reduction	74	692.64	9.36	6156567	83196.85	5848738.65	246262.68	61565.67	$3.76	$1503.60	$10274.60	$21991257.32	$370280565.65	$632562632.98	$2349493.30	$39559889.49	$67581477.82	584873.87
Public Appeals Reduction	13	375.10	28.85	4277859	329066.08	4063966.05	171114.63	42778.59	$3.76	$1503.60	$10274.60	$15280512.35	$257287551.70	$439532900.81	$529653.81	$8918112.71	$15235109.21	406396.61
TOTAL	612	24096.38	39.37	83682206	136765.63	79498095.70	3347288.24	836822.06	$3.76	$1503.60	$10274.60	$298912839.83	$5032982597.66	$8598011937.68	$7592401.32	$127838013.66	$218389940.00	7949809.57

[5] *Understanding the Cost of Power Interruptions to U.S. Electricity Consumers* (2004), U.S. Department of Energy and Lawrence Berkeley Laboratory. (2004 Residential: $3/hr., Small/Medium Business: $1200/hr., Large Business: $8200/hr. These values were multiplied by the inflation factor rise of 1.253 (25.3%) from 2004 to 2014 (U.S. Inflation Calculator, U.S. Bureau of Statistics).

[6] Displaced Household values derived from using the planning metric of 10% of evacuated residents will seek shelter. Displacement values are for planning purposes only. Actual displacement of residents is dependent upon a number of variables. Not all event causes will necessitate a displacement.

Heat Wave

An extended period (typically two days or longer) of abnormally high temperature and humidity that causes temporary modification in lifestyle and that may have adverse health consequences for the affected population.

The SNRA Heat Wave hazard event is currently part of the SNRA's qualitatively described research base. Substantial work towards the fully quantitative analysis of the Heat Wave event within the SNRA framework has been undertaken, and the data sources and interim analysis in progress are provided below for the next analyst or project team to continue this work.

Interim estimates are provided in Table 8 at the end of this summary sheet, for the convenience of the reader or reviewer. These numbers are still under review, and may change substantially when the quantitative analysis of this hazard has been completed.

Event Background[7]

Extreme summer weather is characterized by a combination of very high temperatures and exceptionally humid conditions. When persisting over time, it is called a heat wave. The National Weather Service (NWS) defines a heat wave as a period of time (typically two days or longer) where the temperature is abnormally hot and unusually humid.[8] The Environmental Protection Agency expands on the definition, noting that an excessive heat event (EHE) can be defined in different ways based on location:

> Because how hot it feels depends on the interaction of multiple meteorological variables (e.g., temperature, humidity, cloud cover), EHE criteria typically shift by location and time of year. In other words, Boston, Philadelphia, Miami, Dallas, Chicago, San Diego, and Seattle are likely to have different EHE criteria at any point in the summer to reflect different local standards for unusually hot summertime weather. In addition, these criteria are likely to change for each city over the summer. As a result, reliable fixed absolute criteria, e.g., a summer day with a maximum temperature of at least 90°F, are unlikely to be specified.[9]

Research shows that behavioral, cultural, physical, and social adaptations are made in regions where summers are consistently hot and humid.[10,11] Thus, thresholds for what is considered a heat wave may need to be set higher in those areas. One proposed definition suggests that a heat wave for a given location is a period of at least 48 hours during which both the overnight lows and daytime highs do not fall below the NWS heat stress thresholds of 80°F and 105°F

---

[7] This section is substantially adapted from Chapter 8, Federal Emergency Management Administration (1997), Multi-Hazard Identification and Risk Assessment (MHIRA): A Cornerstone of the National Mitigation Strategy: FEMA Mitigation Directorate, at https://www.fema.gov/media-library/assets/documents/7251?id=2214 (retrieved April 2013); and U.S. Environmental Protection Agency, U.S. Centers for Disease Control and Prevention, National Weather Service, Federal Emergency Management Agency (2006, June). Excessive Heat Event Guidebook, EPA 430-B-06-005, at http://www.epa.gov/heatisland/about/pdf/EHEguide_final.pdf (retrieved December 2012).

[8] National Weather Service, Glossary [electronic resource]: http://w1.weather.gov/glossary/index.php?letter=h (retrieved December 2012).

[9] U.S. Environmental Protection Agency, U.S. Centers for Disease Control and Prevention, National Weather Service, Federal Emergency Management Agency (2006, June). Excessive Heat Event Guidebook, EPA 430-B-06-005; page 9. At http://www.epa.gov/heatisland/about/pdf/EHEguide_final.pdf (retrieved December 2012).

[10] Robinson, P. J. "On the Definition of a Heat Wave," Journal of Applied Meteorology 40 (2001): 763.

[11] Chestnut, L. G. and others. "Analysis of Differences in Hot-Weather-Related Mortality Across 44 U.S. Metropolitan Areas," Environmental Science & Policy 1 (1998): 59.

respectively, except where more than one percent of annual heat index observations exceed the NWS thresholds. In those locations (typically, the South and Southwest), the one percent high and low values would be used.[12]

There appears to be a strong relationship between heat-wave-related mortality and geographic region. Generally, the greatest levels of heat-wave-related mortality have occurred in metropolitan areas of the Northeast (e.g., Baltimore, Boston, and New York) and the Midwest (e.g., Chicago, Kansas City, and Minneapolis). These regions have mortality ranges of 2.5 - 5 heat-related deaths per 100,000. Southern (Atlanta, Houston, and Miami) and Western (Phoenix, Salt Lake City, and San Diego) metropolitan areas have significantly lower rates, less than one death per 100,000.[13,14]

To account for the interactions of heat stress and local adaptation, some have suggested sequentially defining heat events. For example, to address periods that may appear to be heat waves but that do not meet threshold criteria, *warm spell* and *hot spell* have been used.[15] An alternative that builds from the existing definition uses heatwave, severe heatwave, and extreme heatwave. A *heatwave* occurs when heat index thresholds are exceeded for two days (the current NWS definition). The intensity may be viewed as uncomfortable, but there is little social impact or adaptation. A *severe heatwave* would cause some social adaptation, with vulnerable population sectors (e.g., the aged, poor, or socially isolated) most affected. Finally, *extreme heatwaves* are characterized by cascading failures of the power, transportation, and health systems that usually protect the larger population.[16]

Heat Wave Characteristics

Independent of how the heat wave was defined, research indicates that communities typically face one to two heat waves per year, with little regional variation. Most heat waves last two to three days; heat waves lasting seven to ten days are very rare.[17, 18]

Heat wave mortality rates are influenced by a heat wave's intensity, duration, and occurrence during the season. As one might expect, long duration events with an intense heat/humidity combination increase the relative risk of mortality. Early and first in-season heat waves generate higher mortality rates than subsequent and later in-season heat waves.[19]

Each year, many areas of the United States experience periods of prolonged high temperatures combined with high humidity. In susceptible areas, people usually are aware of the hazard, anticipate it, and are accustomed to avoiding its potentially dangerous effects. However, extreme summer heat does strike areas not accustomed to the phenomenon, where people tend to be less prepared.

---

[12] Robinson, "On the Analysis of a Heat Wave," 762.
[13] Chestnut, "Analysis of Differences…," 63.
[14] Anderson, G. B. and Bell, M. L. "Heat Waves in the United States: Mortality Risk during Heat Waves and effect Modification by Heat Wave Characteristics in 43 U.S. Communities," Environmental Health Perspectives 119, no. 2 (2011): 212.
[15] Robinson, "On the Analysis of a Heat Wave," 766.
[16] Nairn, J. and Fawcett, R. Defining Heatwaves: Heatwave Defined as a Heat Impact Event Servicing All Community and Business Sectors in Australia, CAWCR Technical Report No. 060 (Kent Town, South Australia: Bureau of Meteorology, 2013), 13.
[17] Anderson, "Heat Waves in the United States:…," 212.
[18] Robinson, "On the Analysis of a Heat Wave," 766-767.
[19] Anderson, "Heat Waves in the United States:…," 212-216.

Extreme heat events are a public health threat because they often increase the number of daily deaths (mortality) and other non-fatal adverse health outcomes (morbidity) in affected populations. The major threat of extreme summer weather is heatstroke, a medical emergency that can be fatal.

Heat waves pose the greatest danger to outdoor laborers, the elderly, children, people having physical challenges or mental impairments, and people residing in homes without air conditioning. Specific high-risk groups typically experience a disproportionate number of health impacts from extreme hot weather conditions. The following populations have physical, social, and economic factors that put them at high risk:

- Older persons (age > 65)
- Infants (age < 1)
- The homeless
- The poor
- People who are socially isolated
- People with mobility restrictions or mental impairments
- People taking certain medications (e.g., for high blood pressure, depression, insomnia)
- People engaged in vigorous outdoor exercise or work
- People under the influence of drugs or alcohol.

While the SNRA considers heat waves as contingent risks (incidents discrete in time) rather than persistent risks (total annualized loss), current estimates of average annual fatalities due to extreme heat events in the United States range from 1,000-2,000 fatalities and upward,[20] making extreme heat one of the largest non-disease causes of deaths in the U.S.

The combined effects of high temperatures and high humidity are more intense in urban centers than in rural areas, and most heat wave deaths occur in urban areas. One reason is the relative poverty of some urban areas: low-income people are less able to afford cooling devices, and the energy needed to operate them. Other reasons include specific environmental factors of urban areas. Poor air quality may exacerbate severe conditions. The masses of stone, brick, concrete, and asphalt that are typical of urban architecture absorb radiant heat energy from the sun during the day and radiate that heat during nights that would otherwise be cooler. Tall city buildings may effectively decrease wind velocity, thereby decreasing the contribution of moving air to evaporative and convective cooling.

The heat waves of 1995 caused hundreds of fatalities in the Chicago metropolitan area. Many deaths were among low-income elderly in residential units not equipped with air conditioning. Local utilities were forced to impose controlled power outages because of excessive energy demands, and water suppliers reported very low levels of water in storage.

The primary economic losses from heat waves are agricultural. Except for the August 1995 heat wave/drought, which is not otherwise counted, agricultural losses from heat wave/drought

[20] EPA/CDC/NWS/FEMA (2006), pp 7, 12-13 (both counts of combined metropolitan areas are a floor of fatalities in the Nation as a whole).

historical incident records are considered under the Drought national-level event to avoid double-counting. However, extreme heat can also cause damage to physical infrastructure, including roads, bridges, and railroads. High temperatures can be partially responsible for deflection of rails, raising the risk of railroad accidents.

Concern over the potential future health impacts of heat waves follows research conclusions that excessive heat events may become more frequent, more severe, or both in the United States.[21]

While droughts and heat waves can occur at the same time, they are separate meteorological events and have been assessed independently in the SNRA.[22] For further information on droughts, please see the Drought risk summary sheet.

Assumptions

The Spatial Hazard Events and Losses Database for the United States (SHELDUS)[23] was used to conduct the assessment. SHELDUS is a county-level hazard data set maintained by the University of South Carolina. The selected time period was from1990 to 2011. It was decided by the SNRA project team that a narrower time period was appropriate and consistent with the assessment conducted on wildfires for the SNRA. At this point, however, it is possible to use data from 1967 – 2011.

SHELDUS provides data based on reports from individual counties, so the SNRA project team had to aggregate data in order to account for the accurate amount of economic loss, fatalities, and injuries. Events in the data set were combined into a single heat wave event if the entries had the same beginning and end date. There were 566 unique heat wave events during the time period from 1990 to 2011. Of the 566, six met the consequence threshold of 100 fatalities.

The SNRA project team chose to use 100 fatalities per event that are attributed to heat as a minimum threshold.

Frequency

The best-estimate frequency is the average frequency of occurrence of heat waves in the selected 21 year period. The low frequency is the inverse of the longest time interval between heat waves in this set (in days, measured from the start of the event); the high frequency is the highest number of heat wave events that occurred in one year.

Health and Safety

There were three events in 1999 that met the threshold of 100 or more fatalities, which happened during a long-term heat wave that struck the central United States in July 1999. The shortest period of time between each significant event determined the upper bound of the frequencies.

---

[21] EPA/CDC/NWS/FEMA (2006), p 5.

[22] To avoid double counting, for heat wave/drought historical records in the SHELDUS database which overlapped in time (e.g., when aggregated for each of the two events according to its threshold criteria), human fatality and injury and property damage amounts were counted under the Heat Wave event, while crop damage amounts were counted under the Drought event.

[23] Hazards & Vulnerability Research Institute (2011). The Spatial Hazard Events and Losses Database for the United States (SHELDUS), version 8.0 [online database]. Columbia, SC: University of South Carolina. Available from http://www.sheldus.org.

Direct Economic Loss

Except for heat incidents overlapping in time with those counted for the drought national-level event, and for which crop losses were subtracted to avoid double counting, property loss and crop loss for counted incidents were combined to reflect total direct economic loss (see Table 7 below). All values are adjusted for inflation and represent the economic loss in 2011 dollars.

Social

SHELDUS does not provide data on social displacement. Although temporary relocation of large numbers of at-risk persons to cooling centers and public facilities with air conditioning is a pillar of current community heat wave emergency response, collated estimates of numbers of persons leaving their homes for extended periods in historical heat wave incidents could not be found in the literature. This field requires further research.

Psychological

In the absence of estimates for what the project team expected would be a non-negligible level of social displacement, the SNRA measure of psychological distress, which uses social displacement as a key input, could not be calculated.

Environmental

The environmental consequence estimate, which was assessed for the 24 original national-level events of the 2011 SNRA by subject matter experts from the U.S. Environmental Protection Agency (EPA), could not be assessed for the heat wave event added to the SNRA in calendar year 2012.

Potential Mitigating Factors

Mitigation efforts to reduce the frequent severity of heat waves are related to a reduction in the burning of hydrocarbons through a decreased global dependence on fossil fuels. These mitigation efforts are focused on reduced occurrence and decreased severity rather than individual measures that can be taken to reduce heat-related mortality (e.g., use of air conditioners, limiting element exposure).

Table 7: Heat Wave Events

Date	Fatalities[†]	Injuries	Total Loss (Property + Crop Loss) Adjusted for Inflation in 2011 Terms
7/15/1995	859	617	$17,196,587
8/3/1995	145	150	$588,681,793
7/5/1999	161	824	$0
7/23/1999	136	576	$4,472,369
7/31/1999	131	11	$67,763
8/1/2006	117	365	$11,196

Table 8: Summary of Interim Data[24]

Category	Description	Metric	Low	Best	High
Health and Safety	Fatalities[25]	Number of Fatalities	117[26]	258	859
	Injuries and Illnesses[27]	Number of Injuries or Illnesses	11	424	824
Economic	Direct Economic Loss	U.S. Dollars	$0	$102 Million	$589 Million
	Indirect Economic Loss	U.S. Dollars	N/A		
Social	Social Displacement	Displaced from Homes ≥ 2 Days	N/A	N/A	N/A
Psychological	Psychological Distress	Qualitative Bins	N/A		
Environmental	Environmental Impact	Qualitative Bins	N/A		
Likelihood	Frequency of Events	Frequency of Events[28]	TBD		

[24] The quantitative analysis for this hazard event is still in progress. The above estimates from the data that have been collected and analyzed to date are provided for convenience, but they should NOT be considered as final SNRA estimates.
[25] Minimum, mean, and maximum values of fatalities for historical events in the SHELDUS database meeting threshold criteria. See Methodology and Assumptions for details.
[26] 100 is the minimum number of fatalities because it represents the minimum consequence threshold for a national level event.
[27] Minimum, mean, and maximum values of Total Affected of the subset of events reporting this measure. See Methodology and Assumptions for details.
[28] Minimum, mean and maximum frequencies. See Methodology and Assumptions for details.

Oil Spills

The United States produces, distributes, and consumes large quantities of oil every year to fuel the Nation's factories and homes, to produce plastics and pharmaceuticals, to provide transportation, and to provide fuel for a small number of power plants. In 2013, the US consumed 18.49 million barrels of oil per day[29], or 283.5 billion gallons per year. From the production, storage, transport, and use of oil, an estimated 18,000-24,000 oil spills are reported and 10-25 million gallons of oil (or .003% - .009% of oil consumed) are spilled annually. The average size of a spill is 50 gallons.[30] The likelihood of a large spill is inversely proportional to the size of the spill.

All non-adversarial maritime oil spills are included in the Oil Spills national-level event. Also excluded from this analysis are large oil spills attributed to hurricanes. From 1964 to 2009, there were 2807 off shore spills greater than one barrel (42 gallons). Of those, 2175 events spilled an average of 3 barrels, 390 events spilled an average of 19 barrels, 210 events spilled an average of 186 barrels, and 32 events spilled an average of 16,052 barrels.[31] For comparison with pipeline spills, from 1968 to 2007, there were 7828 coastal and inland pipeline spills greater than one barrel. Of those, 16% were 10 barrels or less, 40% were 100 barrels or less, 84% were 1000 barrels or less, and 99% were 10,000 barrels or less.[32]

For the purpose of this risk assessment, we have divided oil spills into two categories: small oil spills ranging in size from 25 barrels but less than 2500 barrels, and large oil spills that are greater than 2500 barrels. Small oil spills create significant cleanup costs, particularly when they occur near coastlines. Large oil spills require contingency / surge operations to mitigate the effects of the spill, perhaps before it reaches a coastline.

Small oil spills in the maritime domain are often overlooked due to their localized effects and create a unique challenge due to containment issues, weather, geography, currents, waterways, and other factors. Although not given much national attention, smaller scale oil spills happen frequently with substantial economic impacts. For example, a 100 foot fishing vessel can hold thousands of gallons of fuel. In the event of sinking or grounding, most of this oil is frequently spilled.

Large scale oil spill events are infrequent but cause significant impacts to human health and safety, the environment, the economy, and surrounding communities. Large oil spills may or may not be declared a Spill of National Significance, as this designation reflects a determination of the potential magnitude and impact of the disaster which depends on multiple factors (in particular, location), not a release volume threshold fixed by plan or statute.

---

[29] http://www.eia.gov/countries/index.cfm?view=consumption

[30] Dagmar Schmidt, Etkin, "Analysis of Oil Spill Trends in the United States and Worldwide," Environmental Research Consulting, Presented at 2001 International Oil Spill Conference, p.1291.

[31] Anderson, Mayes, LaBelle, "Update of Occurrence Rates for Offshore Oil Spills," Department of the Interior, June 2012, p. 38.

[32] Dagmar Schmidt Etkin, "Analysis of U.S. Oil Spillage," Environmental Research Consulting, API Publication 356, August 2009, p. 40.

Event Background

Oil releases in maritime environments threaten public health and safety by fouling drinking water, causing fire and explosion hazards, diminishing air and water quality, compromising agriculture, destroying recreational areas, and wasting nonrenewable resources. Oil spills also have a severe environmental impact on ecosystems by harming or killing wildlife and plants, and destroying habitats and food.

The severity of impact of an oil spill depends on a variety of factors, including characteristics of the oil itself. Even large spills of refined petroleum products, such as gasoline, evaporate quickly and cause only short-term environmental effects. On the other hand, crude oils, heavy fuel oils, and water-in-oil mixtures may sink or cause widespread and long-lasting physical contamination of shorelines. Natural conditions, such as water temperature and weather, also influence the behavior of oil in the marine environment.

The rate at which an oil spill spreads is a primary determinant of its effect on the environment. Most oils tend to spread horizontally into a smooth and slippery surface, called a slick, on top of the water. Oil spilled immediately begins to move and weather, breaking down and changing its physical and chemical properties. Crude oil spilled at sea may mix with sea water and become submerged as a cloud. This occurred in during the Deepwater Horizon oil spill in 2010.[33]

After oil is spilled, the most volatile and toxic substances in it evaporate quickly. Therefore, plant, animal, and human exposure to the most toxic substances are reduced rapidly with time, and are usually limited to the initial spill area. However, although some organisms may be seriously injured or killed very soon after contact with the oil in a spill (lethal effects), chronic toxic effects are more subtle and often longer lasting. For example, marine life on reefs and shorelines is at risk of being smothered by oil that washes ashore, or of being slowly poisoned by long-term exposure to oil trapped in shallow water or on beaches.

Catastrophic oil spills, where large amounts of oil can freely flow into the environment for days or weeks, can occur at sea when an oil well or tanker fails. While minor oil spills occur hundreds of times a year, spills of 10,000 barrels or more occur only a couple of times a decade, and the United States has experienced only three spills of 100,000 barrels or more in the past 40 years.[34]

Assumptions

Many of the assumptions used in this assessment are included in the footnotes.

The SNRA project team used the following to estimate health and safety consequences resulting from major oil spills ranging from catastrophic events (all off shore) to smaller pipeline and rail events.

- Historical Events: The SNRA project team analyzed a set of four historical maritime events in which large amounts of oil were spilled. A detailed listing of these events is found in

[33] Ramseur, Jonathan L.; Hagerty, Curry L. (31 January 2013). Deepwater Horizon Oil Spill: Recent Activities and Ongoing Developments, CRS Report for Congress, Congressional Research Service, R42942.

[34] Exxon Valdez in March 1989, Mega Borg in June 1990, and Deepwater Horizon in 2010. A fourth large spill occurred in the Gulf of Mexico in June 1979 when the Mexican IXTOC 1 well ruptured. Since this was not a U.S. spill, it is not included in the analysis in this report.

Table 9 under "Additional Relevant Information." Additionally, the analysis does not take into account possible higher-consequence events that have not yet occurred, but rather assumes maximum fatalities and injured counts from the Exxon Valdez oil spill, the Deepwater Horizon oil spill, and the Mega Borg oil spill.

Environmental Impact

Large oil spills on the scale of those from the Exxon Valdez and Deepwater Horizon are among the most catastrophic environmental hazards in the homeland security mission space. By reference to these rare, large events, small oil spills as a national-level event typically have a much smaller environmental impact, as these events include oil spill incidents occurring dozens of times every year.

Potential Mitigating Factors

Maritime oil spills are becoming less frequent and less severe overall,[35] but catastrophic risk remains due to continued increase in oil imports and explorations in deeper water, as exemplified by the Exxon Valdez event and the Deepwater Horizon event. Much of this decrease is due to preventive actions put in place in the 1970s, 1980s, and 1990s. These improvements include double hulled ships and the use of GPS, RADAR, and SONAR for navigation.

While much of the responsibility for the response and recovery for an event rests within the private sector, state and territorial governments and the Federal Government also coordinate responses through the US Coast Guard (USCG) for off-shore spills and spills in the Great Lakes, and the US Environmental Protection Agency (EPA) for inland waterways. Specific activities include cleaning up the spill on land, removing soil exposed to oil, and cleaning up the spill on water by removing oil from water using controlled burns, or dispersing agents and sunlight to evaporate the spill.

Several methods exist for mitigating the effects of oil spills in the aquatic environment include rapidly containing and cleaning up the spills. Mechanical equipment, such as booms and skimmers, is often used to block the spread of oil, concentrate it into one area, and remove it from the water. Chemical and biological treatment of oil can be used in place of, or in addition to, mechanical methods, especially in areas where untreated oil may reach shorelines and sensitive habitats in which cleanup becomes difficult and expensive.

Cleaning shorelines after an oil spill is a challenging task. Factors that affect the type of cleanup method used include the type of oil spilled, the geology of the shoreline, and the type and sensitivity of biological communities in the area. Natural processes such as evaporation, oxidation, and biodegradation help to clean the shoreline. Physical methods, such as wiping with sorbent materials, pressure washing, and raking and bulldozing can be used to assist these natural processes.

In addition, the application of reparations for economic damages to individuals and businesses have been effective means of reducing the frequency and magnitude of events.

[35] Etkin, D.S., Environmental Research Consulting, "Analysis of U.S. Oil Spillage", August 2009.

Additional Relevant Information

Table 9 lists the maritime events analyzed and includes total fatalities and injuries for each event.

Table 9: List of Analyzed Events

#	Event	Date	Fatalities	Injuries
1	Ixtoc 1 Well[36]: 39.9 million gallons of oil, 1100 square miles, 162 miles of US shoreline	6/3/1979	0	0
2	Exxon Valdez Ship[37]: 11 million gallons of oil, 11,000 square miles, 1,300 miles of US shoreline	3/24/1989	0	0
3	Mega Borg Ship[38]: 4.6 million gallons, 300 square miles, little shoreline impact	6/08/1990	4[39]	17[22]
4	Deepwater Horizon[40]: 210 million gallons, 68,000 square miles, 1,074[41] miles of shoreline impact	4/20/2010	11[42]	17[43]

[36] Linda Garmon (25 October 1980). "Autopsy of an Oil Spill". Science News 118 (17). pp. 267–270.
[37] "Questions and Answers". History of the Spill. Exxon Valdez Oil Spill Trustee Council.
[38] Leveille, Thomas P. "The Mega Borg Fire and Oil Spill: A Case Study." U.S. Coast Guard Marine Safety Office Oil Spill Conference (1991): n. pag.ioscproceedings.org. Web. 21 Jan. 2014.
[39] Belkin, Lisa (June 11, 1990). "Flaming Oil Is Spilled Into Gulf as Blasts Rack Tanker". New York Times.
[40] "On Scene Coordinator Report on Deepwater Horizon Oil Spill," September 2011. http://www.uscg.mil/foia/docs/dwh/fosc_dwh_report.pdf
[41] Polson, Jim (15 July 2011). "BP Oil Still Ashore One Year After End of Gulf Spill". http://www.bloomberg.com/news/2011-07-15/bp-oil-still-washing-ashore-one-year-after-end-of-gulf-spill.html
[42] Kaufman, Leslie (24 April 2010). "Search Ends for Missing Oil Rig Workers". The New York Times. p. A8.
[43] Brenner, Noah; Guegel, Anthony; Hwee Hwee, Tan; Pitt, Anthea (22 April 2010). "Coast Guard confirms Horizon sinks". Upstream Online (NHST Media Group). http://www.upstreamonline.com/live/article212769.ece

Pipeline Failure

A failure of a major pipeline, including crude oil, petroleum, natural gas transmission and natural gas distribution pipelines.

The SNRA Pipeline Failure hazard event is currently part of the SNRA's qualitatively described research base. Substantial work towards the fully quantitative analysis of the Pipeline event within the SNRA framework has been undertaken, and the data sources and interim analysis in progress are provided below for the next analyst or project team to continue this work.

Interim estimates are provided in Table 12 at the end of this summary sheet, for the convenience of the reader or reviewer. These numbers are still under review, and may change substantially when the quantitative analysis of this hazard has been completed.

Event Background

While many forms of transportation are used to move products such as crude oil, refined petroleum products, and natural gas to marketplaces throughout the U.S., pipelines and pipe networks are major carriers because they are the safest, most efficient, and most economical way to transport all manner of liquid and gaseous commodities throughout the Nation.[44]

Although pipelines have proven to be a safe means of transportation, they are still susceptible to significant and costly failures. These failures may result in system impacts, economic impacts, fatalities and injuries, and can also result in significant environmental impact. When failures occur they result in release of the transported product to the environment, with potential for fire, explosion, and toxic exposure. The nature of the system consequences will vary according the system, the materials involved, and the length of time the system is out of operation. There is a wide variety of causes for the accidents.

Pipelines transport hydrocarbon-based liquids and gases from one site to another, sometimes at great distances as part of a large system. These resources are found in completely different locations than where they are eventually processed or refined into fuels. They are also in very different locations from where they are consumed. While many forms of transport are used to move these products to marketplaces, pipelines remain the safest, most efficient and economical way to move these natural resources.

The U.S. depends on a network of more than 185,000 miles of liquid petroleum pipelines, nearly 320,000 miles of gas transmission pipelines, and more than 2 million miles of gas distribution pipelines to safely and efficiently move energy and raw materials to fuel our Nation's economic engine. This system of pipelines serves as a national network to move the energy resources from production areas or ports of entry throughout North America to consumers, airports, military bases, population centers, and industry every day.[45]

For the purposes of understanding the risk profile of pipelines, it is useful to consider four different types of pipeline:

- Crude oil pipelines

[44] http://www.pipeline101.com/why-do-we-need-pipelines
[45] http://www.eia.gov/forecasts/steo/special/pdf/california.pdf

- Petroleum product pipelines
- Natural gas transmission lines (including natural gas gathering lines and liquid natural gas pipelines)
- Natural gas distribution piping networks

When a *crude oil* pipeline fails, the movement of crude oil into a refinery is disrupted and the refinery may need to scale back production when its feed stocks are reduced (typically one to two weeks). If disruptions to a crude oil pipeline are frequent or prolonged, a refinery could be forced to shut down. Crude oil also produces environmental contamination and clean-up costs. Crude oil pipeline failures may also present significant restart challenges for very heavy crude oil requiring heating to flow; loss of pipeline flow can cause the heavy crude oil to begin to solidify, requiring clearing that could result in an extended loss of service to the refineries they serve, depending on the conditions under which the system managers are operating.[46]

Refined petroleum products move in the pipeline consecutively. Each distinct product is referred to as a "batch" and when several products are placed together in the line, they are called a "batch train." As a batch train moves through the pipeline, adjacent products commingle, forming the "interface" zone. The extent of commingling, or the length of the interface, is a function of velocity, density difference between the two products, viscosity, pipe diameter, and distance traveled [47] The long-term failure of a petroleum product pipeline disrupts the supply chain to all of the distribution points downstream, forcing the use of tanker trucks and trains as an inefficient alternative.

Typically when a petroleum pipeline fails there are few fatalities or injuries. Release of other hazardous chemicals may result in fatalities or injuries, but often in small numbers. During 2012 and 2013 (the latest analyzed at a national level) a total of 762 hazardous liquid pipeline incidents occurred. Five of these were classified as serious, resulting in four fatalities and nine injuries. For comparison, there were a total of 1,188 accidents for all pipeline classes in 2012 and 2013, with a total of 22 fatalities and 113 injuries. According to Pipeline Hazardous Materials Substances Administration (PHMSA) data, the hazardous liquid pipeline failures in that two-year period resulted in $412 million in property damage.[48]

Approximately 114,200 barrels were lost due to these incidents, with an estimated current value of over $14 million, based on an average crack spread of $25 per barrel during 2012 to 2013[49] and an average value crude oil price of $100 per barrel.[50] This might be considered a fairly common event, with relatively low consequences, though the costs of environmental remediation have not been captured. This information is provided for the purpose of clarifying the pattern of risks for non-gas pipelines, but was not included in this assessment as a separate break-down of incident types. However, a failure of a major land pipeline transporting refined petroleum products could result in direct economic damages of $100 million or greater.

---

[46] http://www.ogj.com/articles/print/volume-96/issue-40/in-this-issue/pipeline/batching-treating-keys-to-moving-refined-products-in-crude-oil-line.html

[47] http://www.ogj.com/articles/print/volume-96/issue-40/in-this-issue/pipeline/batching-treating-keys-to-moving-refined-products-in-crude-oil-line.html

[48] http://www.phmsa.dot.gov/pipeline/library/datastatistics/pipelineincidenttrends

[49] http://marketrealist.com/2013/07/crack-spread-101-part-4-effect-on-refiner-margins/

[50] http://www.eia.gov/forecasts/steo/realprices/

In July 2010 a six-foot break in Enbridge's 6B pipeline occurred, releasing more than 20,000 barrels of heavy tar sands crude into Talmadge Creek, a tributary of the Kalamazoo River in Michigan. The clean-up from this spill has totaled $1.21 billion to date, and is still on-going. It represents the largest inland U.S. oil spill and one of the costliest spills in U.S. history.[51]

The potential for much more problematic petroleum pipeline failures exist on the floor of the Gulf of Mexico, as evidenced by the 2010 Deepwater Horizon spill. These pipelines are not subject to the same maintenance, inspections, and regulations that surface pipelines are, and due to the constant motion of the water, are difficult to precisely locate. The routine observed rate of failure is lower for such pipelines, however, than incidents on land. Maritime oil spills due to pipeline ruptures are discussed more in the Oil Spill section of this assessment.

Natural gas transmission pipeline system accidents are also fairly common (229 during the period of 2012-2013), and more likely than petroleum pipelines to result in casualties. However, the casualty numbers typically are still low because these pipelines are not commonly found in heavily populated areas. No fatalities and nine injuries from natural gas transmission pipeline incidents we reported in 2012-2013, and property damages of just over $109 million for all 229 accidents, or an average of close to $476 thousand per incident. While the average transmission accident is more costly, because of its comparative rarity and lower casualty count, transmission pipeline accidents pose lower fatality and injury risk than other pipeline accidents.

When a natural gas transmission pipeline ruptures in an urban area, it can result in a substantial amount of destruction. A good example of this is the explosion of a 30 inch pipeline in downtown San Bruno, CA on September 9, 2010. The loud roar and shaking caused people in the community to initially think it was an earthquake. The USGS registered the explosion and resulting shockwave as a magnitude 1.1 earthquake.[52] Eyewitnesses stated that the initial explosion resulted in a wall of fire more than 1000 feet high. Eight people died in the explosion and 58 people were injured[53]. The explosion also destroyed 35 homes and damaged many more. It took PG&E, the owner of the pipeline, 90 minutes to shut off the natural gas flow through the ruptured pipeline. On April 9, 2015, the California PUC fined PG&E $1.6 billion for the event.[54]

Natural gas distribution pipelines are located in heavily populated areas and, thus, are exposed to more frequent accidents from excavators and other sources of outside force. There were a total of 197 incidents on distribution systems in 2012-2013, resulting in about $43.4 million in property damages. This is an average of close to $220.5 thousand per incident, or less than half the average cost for a transmission pipeline failure. However, there were a total of 18 fatalities and 85 injuries in 2012-2013, considerably higher than those for transmission pipeline failures. These occurrences, although carrying a lower average economic cost, are considered higher risk for its higher fatality rate and a higher frequency than the natural gas transmission system failures.

Natural gas distribution systems carry an additional societal burden and potential cascading risk. Loss of supply to residential and commercial customers necessitates, because of safety reasons,

---

[51] http://www.mlive.com/news/grand-rapids/index.ssf/2014/11/2010_oil_spill_cost_enbridge_1.html
[52] "Magnitude 1.1 – San Francisco Bay Area, California". United States Geological Survey. 09 September 2010.
[53] Melvin, Joshua (October 28, 2010). "Death toll in San Bruno pipeline explosion climbs to eight". San Jose Mercury News.
[54] http://www.mercurynews.com/business/ci_27880159/san-bruno-pg-e-faces-record-penalty-punishment

the relighting of pilot lights, which cannot be initiated until system integrity has been restored. The added time to complete the relight phase can create a major problem. If the reduction in capacity were to occur during the winter, many people in the Midwest and Pacific Northwest (and wherever residential customers rely on natural gas for residential heating) would be without heat. (Residential customers in the New England states typically use fuel oil for heating.) To cope with the situation, many may purchase electric heaters, putting strains on the power distribution system that the system design may be unable to accommodate. This, in turn, could lead to frequent power outages at the distribution level. There is also concern that impatient customers would attempt their own relighting. It is strongly recommended that a qualified service technician light any pilot light that has gone out. If the customer attempts to relight the pilot he is taking the risk of starting a fire or an explosion.[55]

Natural gas pipeline systems are involved not only in the transportation of product but also in its delivery to the end user.

Assumptions

The SNRA project team used the following assumptions:

- The low, best, and high frequency estimates reflect the low, mean (arithmetic average), and high counts of incidents of major failures of pipelines of all types, as defined and recorded by the PHMSA of the U.S. Department of Transportation (DOT), from 1995 through 2014.
- The best estimates of fatalities, injuries, and direct economic damages reflect the average fatalities, injuries, and direct economic damage per incident of major pipeline failures from the same data set. These were calculated by dividing the 20 year total fatalities, injuries, and direct economic damage by the average annual number of major pipeline failures.
- Low estimates of 0 fatalities and injuries were assumed by the SNRA project team.
- As this PHMSA data set did not report a per-incident breakdown, but only annual totals, high estimates of fatalities and injuries and low and high direct economic damage estimates were not determined by the SNRA.

Direct Economic Loss

Direct economic losses are difficult to assess at the national-level due to the variety of scenarios presented in the PHMSA dataset across the four pipeline-types assessed. The best estimate for direct economic loss based on PHMSA is just under $1,000,000 per incident ($978,639) with the low at $135,735 and high estimate approximately $2.4 million. The Event Background section provides an overview of historical economic impacts in the context of each pipeline: crude oil, petroleum, natural gas transmission, and natural gas distribution.

Social

While social displacement estimates were not reported by this PHMSA data set, an assumption of 0 civilian U.S. residents displaced from their homes for two or more days was made for the

[55] http://staging.usepropane.com/safe-source-of-energy/homeowner-safety-information/#Link 11

low and best estimates by the SNRA project team for the purposes of reporting the SNRA in this document. A high estimate was not made.

By analogy with other technological accidents not releasing highly toxic chemical gases or radioactive substances assessed by subject matter experts for the 2015 SNRA project, a provisional Event Familiarity Factor of 1.0 was assigned to the Pipeline Failure national-level event by the SNRA project team for the purposes of reporting psychological distress estimates for the final SNRA documentation (see Psychological consequences below).

Psychological

Psychological consequences for the SNRA focus on significant distress and prolonged distress, which can encompass a variety of outcomes serious enough to impair daily role functioning and quality of life. Observation of gasoline consumers' behavior in cities where pipeline accidents have disrupted fuel supplies suggest that the psychological impact of a pipeline's disruption would be minimal. A major pipeline failure would likely affect those in the transportation sector because it is heavily dependent on pipelines to transport motor fuel.

Environmental

A pipeline accident on land within the scope of the national-level event as defined by the SNRA data set—occurring with a frequency of about one every week in this country—could have minor environmental impact, but would most likely have moderate but localized impacts. Exceptional cases where a very large pipeline ruptures in a sensitive or protected ecosystem could have very high negative environmental consequences, as shown by the 2010 Enbridge crude oil pipeline failure in Michigan. In this incident, a 30-inch diameter pipeline carrying heavy tar sands crude (diluted bitumen or "dilbit") ruptured, pumping an estimated 20,000 barrels of crude oil into the Kalamazoo River near the town of Marshall, Michigan. This event was so severe that cleanup work continued for four years, closing a thirty-five mile section of the river for two years, affected wildlife both in the river and on land.[56] Final cleanup costs to date are in the area of $1.21 billion.

Potential Mitigating factors

The aging of the Nation's transportation infrastructure is a risk that can be addressed through proactive inspection, maintenance, repair, and replacement of deteriorating assets; however, this requires significant investment from the Federal, state, and local levels, and therefore, such activities will have to be prioritized based on criticality, risk, available funds, and other factors. The recent Federal requirement that state DOTs engage in risk-based asset management[57] to better strategically plan for transportation infrastructure investment and improvement, can make more effective use of existing funding, but expanded funding may also be required for effective mitigation of risk. Additionally, complementary action may be taken for enhanced contingency, response, and emergency preparedness planning. In the event of a transportation system failure, better emergency preparedness and response planning will enable agencies to more immediately respond to and mitigate direct impacts, and better contingency planning (e.g., establishing

[56] http://archive.freep.com/article/20130623/NEWS06/306230059/Kalamazoo-River-oil-spill
[57] Moving Ahead for Progress in the 21st Century Act (MAP-21), U.S. Public Law 112-141 – July 6, 2012

detouring and rerouting plans around higher risk assets) can mitigate indirect costs associated with disruption to the transportation system and supply chain, and associated congestion.

Additional Relevant Information

On June 26, 1996, a pipeline owned by Colonial Pipeline ruptured near Fork Shoals, South Carolina, releasing over 1 million gallons of diesel fuel into the Reedy River, one of the largest inland oil spills in U.S. history. The resulting spill was devastating to the Reedy, essentially wiping out the entire food chain throughout a 23-mile stretch of the river. Mammals, waterfowl, and shorebirds dependent upon the riverine / riparian food chain were also affected, or at least temporarily extirpated from the Reedy corridor. This disastrous spill was particularly incredible because the reach of the Reedy in southern Greenville and Laurens Counties had previously been among the more healthy reaches of the river.[58]

Another high-end scenario for pipeline failure may be construed to be something comparable to the Deepwater Horizon accident, which resulted in $20 billion paid by BP, and a $4.5+ billion fine. It would take a number of complex interacting failures to have such an incident be considered a pipeline failure. If a deep-water drill head was in safe operating condition, but somehow the ability to shut it off failed, and a downstream physical failure in the pipeline resulted in uncontrolled leakage within the deep-water environs, a comparable physical event could be postulated. However, it is likely that a much more prompt repair to the controls that would allow the wellhead to be shut off would be feasible if it were not also the source of the spewing crude. Thus, an analytic judgment is made that this event is not a suitable analogy.

Table 10: National All Pipeline Systems Serious Incidents from 1995-2014

Year	Number	Fatalities	Injuries	Property Damage (current year dollars)	Gross barrels Spilled
1995	59	21	64	$7,435,010	6,564
1996	63	53	127	$19,501,368	14,315
1997	49	10	77	$6,145,793	20,000
1998	70	21	81	$57,738,002	11,117
1999	66	22	108	$74,664,129	54,456
2000	62	38	81	$8,846,912	10,981
2001	40	7	61	$6,058,891	16,114
2002	36	12	49	$6,067,785	0
2003	61	12	71	$12,162,651	0
2004	44	23	56	$11,250,326	860
2005	39	16	47	$21,354,868	4,048

[58] http://www.friendsofthereedyriver.org/the-river/

2006	32	19	34	$8,550,884	4,513
2007	43	16	46	$20,235,909	12,176
2008	37	8	55	$52,261,149	6,755
2009	46	13	62	$20,101,704	364
2010	34	19	104	$406,772,532	3,105
2011	32	12	51	$13,421,557	0
2012	28	10	54	$11,020,309	1,500
2013	24	9	44	$16,750,062	23,702
2014	29	19	96	$94,563,684	14,270
20 year Totals	894	360	1,368	$874,903,525	204,840
5 Year Average (2010-2014)	29	14	70	$108,505,629	8,515
10 Year Average (2005-2014)	34	14	59	$66,503,266	7,043
20 Year Average (1995-2014)	45	18	68	$43,745,176	10,242

Table 11: Pipeline Consequence Statistics

Totals	Number	Fatalities	Injuries	Property Damage	Gross Barrels Spilled
Median	41.5	16.0	61.5	$15,085,810	6,660
5th	27.8	8.0	43.5	$6,067,340	0
95th	66.2	38.8	109.0	$110,174,126	25,240
Mean	44.7	18.0	68.4	$43,745,176	10,242
Min	24	7	34	$6,058,891	0
Max	70	53	127	$406,772,532	54,456
Per Incident, Average		0.403	1.530	$978,639	229
Per Incident, 5th Percentile		0.18	0.97	$135,735	0
Per Incident, 95th Percentile		0.87	2.44	$2,464,746	565

Table 12: Summary of Interim Data[59]

Category	Fatalities	Metric	Low	Best	High
Health and Safety	Fatalities	Number of Fatalities	060	0.40	0.87
	Injuries and Illnesses	Number of Injuries or Illnesses	061	1.53	2.44
Economic	Direct Economic Loss	U.S. Dollars	$135,735	$978,639	2,464,746
	Indirect Economic Loss	U.S. Dollars	N/A		
Social	Social Displacement	Number of Displaced from Homes for ≥ 2 Days	0	0	N/A
Psychological	Psychological Distress	Qualitative Bins	N/A		
Environmental	Environmental Impact	Qualitative Bins	Low (See Discussion)		
Likelihood	Frequency of Events	Number per Unit of Time	TBD		

[59] The quantitative analysis for this hazard event is still in progress. The above estimates from the data that have been collected and analyzed to date are provided for convenience, but they should NOT be considered as final SNRA estimates.
[60] Calculated value is 0.18. Lowest likely assumed to be 0
[61] Calculated value is 1.1. Lowest likely assumed to be 0

Urban Fire / Urban Conflagration

Synopsis

Trend analysis[62,63] demonstrates a decline in the incidents of fire and fire death in the United States (U.S.), which may explain why a survey of articles found few selections on the topic of urban conflagration[64] in the U.S. Current conflagration research focuses on the challenges of developing nations. Articles that focused on the U.S. tend to do so from a historical perspective.

While articles from the past five years agree that the U.S. does not have a strong risk of conflagration from traditional causes, literature demonstrates that urban areas might be at an increased risk of urban fires caused by natural and man-made hazards. The literature review examines the nexus of urban fire and hurricanes (i.e., Superstorm Sandy), earthquakes, and the Wildland Urban Interface. The final theme evaluated was literature demonstrating that lighter building materials and modern furniture means hotter, faster fires and a need for a change in firefighting tactics.

Literature Review – Urban Fire/Urban Conflagration Viewed as Unlikely, but When Combined with Other Hazards May Become a More Frequent Occurrence

Introduction

Event Description

For purposes of this assessment, urban[65] fire/urban conflagration is defined as a fire, other than a wildfire, occurring within the U.S., with major building-to-building flame spread over some distance.[66,67]

Event Background

An Overview of Fire Frequency and Consequences

Historically, the U.S. fire rate, on a per capita basis, has been higher than most of the industrialized world.[68] From 1979 to 2007, the fire death rate in the U.S. declined by 66 percent

[62] USFA. Fire Death Rate Trends: An International Perspective. (2011). Topical Fire Report Series, Volume 12 (Issue 8). Pg. 4. Figure 3. Retrieved from http://www.usfa.fema.gov/downloads/pdf/statistics/v12i8.pdf.

[63] National Fire Protection Association (NFPA). (March 2015). Trends and Patterns of U.S. Fire Losses in 2013. Pgs. 1-2 (Figures 1 and 2) and Pg. 6 (Figures 8 and 9). Retrieved March 24, 2015, from http://www.nfpa.org/research/reports-and-statistics/fires-in-the-us/overall-fire-problem/trends-and-patterns-of-us-fire-losses.

[64] As noted in the Event Background, for SNRA purposes, Urban Fire/Urban Conflagration is defined as a fire, other than a wildfire, occurring within the U.S. resulting in ten or more reported fatalities, a declaration of emergency, or a request for international assistance.

[65] For purposes of this qualitative assessment a precise definition of urban is not necessary. As a point of reference, the NFPA uses the U.S. Census Bureau's definition for Urban: An area with at least 1000 people per square mile. Similarly, suburban is defined as an area with between 500 people and 1000 people per square mile.

[66] NFPA Fire Protection Handbook, 19th edition. Quincy, MA: NFPA, 2003. Of note, conflagration is not defined in the NFPA 2014 standards glossary.

[67] Historically, conflagrations implied city-wide fires or at least multiple city blocks. In more recent years, fire professionals have used the term more loosely to imply major fires that spread from building-to-building. Merriam-Webster's Dictionary defines conflagration as a large disastrous fire.

[68] USFA. Fire Death Rate Trends: An International Perspective. (2011). *Topical Fire Report Series*, Volume 12(Issue 8). Pg. 1. Retrieved from http://www.usfa.fema.gov/downloads/pdf/statistics/v12i8.pdf.

and the U.S. moved from having the third highest death rate in 1979 to the tenth highest death rate in 2007 out of twenty-four industrialized nations.[69]

In 2013, the most recent year of completed and published statistics from the National Fire Protection Association (NFPA)[70], there were 1,240,000 fires, 3,240 civilian deaths, 15,925 civilian injuries, and $11.5 billion in property damage caused by fires.[71,72]

Over the years, there has been little change in the proportion of fires, deaths, injuries, and dollar loss by the type of property involved. In terms of numbers of fires, the largest category continues to be outside fires (46 percent) in fields, vacant lots, trash, and wild spaces. Vehicle fires comprise another 15 percent of reported fires. While there are many of these two kinds of fires, they are not the source of most fire damage or deaths. Structure fires accounted for 86 percent of fire deaths, 76 percent of injuries, and 82 percent of dollar loss of all U.S. fires in 2013.[73] Residential properties in particular, account for the largest percentage of deaths from all fires in 2013 (85 percent),[74] with the majority of these in one- and two-family dwellings.[75] Residential and nonresidential structure fires together comprise 39 percent of all fires, with residential structure fires outnumbering nonresidential structure fires by over three to one.[76] From 1980-2013 there were twenty-two residential fires with ten or more fatalities, none of which occurred between the period of 2009-2013.[77]

The NFPA threshold for their annual Catastrophic Multiple-Death Fire Report is "fires or explosions in homes or apartments that result in five or more fire-related deaths, or fires or explosions in all other structures and outside of structures, such as wildfires and vehicle fires that claim three or more lives".[78] The NFPA's 2013 report documented 10 residential fires resulting in five or more fire-related deaths, and six non-residential structural fires with three or more fire-related deaths.[79,80]

The NFPA also documents "large-loss" fires on an annual basis, which they define as losses in excess of $10 million.[81,82] In 2013, there were 17 structure fires, resulting in a total property loss of $387.7 million. Only three of these fires were residential structures, accounting for $76.9 million in losses. The majority of large-loss fires, in both frequency and dollars lost, occur in

[69] USFA (2011). Pg. 1.
[70] The USFA's latest statistics are based on 2011 data. The USFA Statistics page directs users to view the NFPA's website for more statistics on U.S. Fire Loss.
[71] Karter, Jr., M. (2014). Fire Loss in the United States During 2013. Retrieved March 2015, from http://www.nfpa.org/research/reports-and-statistics/fires-in-the-us/overall-fire-problem/fire-loss-in-the-united-states
[72] Direct property damage figures do not include indirect losses, like business interruption.
[73] Karter (2014). pp iii-vi.
[74] Karter (2014). p 10. Non-residential, structure fires account for only 1% of deaths.
[75] Karter (2014). p 45.
[76] Karter (2014). pp iii-vi.
[77] Home Fires with Ten or More Fatalities, 1980-2013. (2014, August 1). Retrieved March 24, 2015, from http://www.nfpa.org/research/reports-and-statistics/fires-in-the-us/multiple-death-fires/homes-fires-with-ten-or-more-fatalities
[78] Since this analysis is focused on non-wildfires, the numbers cited in the narrative account for only structural fires.
[79] Badger, S. (2014, September). Catastrophic Multiple-Death Fires in 2013. Retrieved March 2015, from http://www.nfpa.org/research/reports-and-statistics/fires-in-the-us/multiple-death-fires/catastrophic-multiple-death-fires
[80] The NFPA's non-residential figures include fires caused by Industrial Accidents. For SNRA purposes, Industrial Accidents are evaluated as a separate hazard.
[81] Badger, S. (2014, November). Large-Loss Fires in the United States. Retrieved March 24, 2015, from http://www.nfpa.org/research/reports-and-statistics/fires-in-the-us/large-property-loss/large-loss-fires-in-the-united-states
[82] The SNRA economic threshold for a "national-level" event is $100 million.

non-residential structures such as manufacturing properties, properties under construction, or other commercial properties.[83,84]

While residential fires in single and two-family homes account for the majority of deaths from all fires, including multiple-fatality fires,[85,86] the rare fires causing ten or more fatalities are disproportionately concentrated in multiple-family dwellings such as apartment buildings, group homes, and non-residential structures (e.g., nightclubs, hotels).[87]

Fire Risks Vary by Region

The risks and consequences of urban fires and conflagration are directly related to the condition and infrastructure of the built environment, and is affected by issues such as zoning and transportation networks. Typically, older Northeast, Southeast and Rust Belt urban areas are more susceptible to conflagration than other areas due to the age and construction of the built environment and condition of water distribution services. Newer Southwest and Western urban areas have addressed many of the "historic errors" of urban development, and addressed conflagration concerns through enhanced building codes with aggressive requirements for fire resistance, roof coverings, and built-in fire protection systems; wider transportation infrastructure to prevent horizontal fire spread via radiation; and, up-to-date water storage and distribution systems (e.g., more storage capacity, larger distribution mains, strategically placed hydrants, looping and redundancy, inspection, maintenance, testing). Increasingly, communities encroaching on the wildland are at risk for conflagration because typical construction methods in those areas consist of combustible materials and closely spaced buildings.

Federal, State and Local Government Firefighting Responsibilities

State, Local, Tribal, and Territorial Responsibilities

Firefighting is an inherently local responsibility. Local fire resources often receive assistance from other fire departments/agencies through established mechanisms identified in local mutual aid agreements.[88]

---

[83] Badger, S. (2014, November). Six of these structure fires occurred in manufacturing properties: a fertilizer plant, an egg processing plant, an oil reprocessing plant, a steel mill arc-furnace building, a plastics laminate plant, and an aluminum die-cast plant. These six fires resulted in total losses of $202.6 million. Four more fires occurred in special properties. Two of the properties were apartment buildings under construction and two were a highway tunnel and a highway interchange that were severely damaged following separate vehicle crashes. The combined loss of these four fires was $52.7 million. Another three fires occurred in residential properties, one each in a single-family home, a high-rise apartment building, and a cluster of rental cabins. The combined losses for these fires totaled $76.9 million. Of the final four structure fires, two occurred in restaurants and resulted in a combined loss of $25 million. The third and fourth fires occurred in a warehouse and a high school, and produced losses of $20 million and $10.5 million, respectively.

[84] The NFPA's non-residential figures include fires caused by Industrial Accidents. For SNRA purposes, Industrial Accidents are evaluated as a separate hazard.

[85] USFA (2013, July). Multiple-fatality fires in residential buildings (2009-2011). USFA Topical Fire Report Series 15(6). Retrieved January 2014 from http://www.usfa.fema.gov/downloads/pdf/statistics/v14i6.pdf.

[86] This is also true of total economic loss and the proportion of the most costly fires, which are generally wildfires destroying residential properties across large geographic areas. See the SNRA Wildfire Assessment for details.

[87] While the characteristics of all fires and multiple-fatality (two or more) fires, and the overall small relative proportion of total fatalities from the 10+ fatality fires, come from USFA and NFPA sources as cited, this judgment on the relative proportions of structure fires for the 10+ fatality fires is based solely on the data in Appendix 1-Table 1. These data come from the U.S. Government-funded international disaster database EM-DAT, but not from the USFA.

[88] This paragraph is directly from Emergency Support Function (ESF) #4 – Firefighting Annex, 2013. See: http://www.fema.gov/media-library/assets/documents/32180

There are roughly 1.1 million active firefighters in the U.S., of which just under three-fourths (73%) are volunteer firefighters. Nearly half of the volunteers serve in communities with less than 2,500 people.[89] In 2006, these organizations reported:

- 11% of the Nation's estimated 32,000 fire departments can handle a technical rescue with Emergency Medical Services (EMS) at a structural collapse of a building with 50 occupants with local trained personnel. Only communities of 500,000 or more people had a majority of departments report that they were both responsible for such an incident and had enough local specially trained personnel.
- 24% of fire departments can handle a wildland/urban interface fire affecting 500 acres with local trained personnel. Another 49% said this was within their responsibility, but they would need specially trained people from outside their local area. 27% said such incidents were outside of their responsibility.[90]

Further assistance can be obtained through an established intrastate mutual aid system. If additional assistance is required, firefighting resources can be requested from other jurisdictions through processes established under mutual aid agreements, state-to-state or regional compacts, or other agreements. If the governor of the affected state declares an emergency, firefighting resources may be requested through the Emergency Management Assistance Compact (EMAC). If the President declares an emergency or major disaster under the Stafford Act, firefighting resources may also be requested through Emergency Support Function (ESF) #4. Using existing authorities and agreements, ESF #4 can mobilize wildland and structure firefighting resources from across the country and from several foreign countries through the national firefighting mobilization system to incidents anywhere in the U.S.[91]

As a result of community risk analysis and budget limitations, municipal fire services generally are not resourced for conflagrations. Major urban fire services may be an exception, but likely are limited to command and control of a single large-scale event. Multiple events could compromise service delivery. Participation in joint fire suppression automatic or mutual aid compacts is voluntary. Depending on local services provided (e.g., fire-based emergency medical services), life safety and rescue may take priority over fire suppression and deplete resources that would normally be committed to fire control.[92]

Shortages of critical firefighting resources are adjudicated at the lowest jurisdictional level. Many firefighting agencies provide additional functions such as emergency medical services, technical rescue, and hazardous materials response. During a Federal response, these resources may support multiple ESFs in support of different core capabilities.[93]

---

[89] USFA/NFPA. (2006). *Four Years Later – A Second Needs Assessment of the U.S. Fire Service*. Report No. FA-303. United States Fire Administration, Emmitsburg, Maryland. Retrieved from http://www.usfa.dhs.gov/downloads/pdf/publications/fa-303-508.pdf

[90] USFA/NFPA (2006).

[91] This paragraph is directly from Emergency Support Function (ESF) #4 – Firefighting Annex, 2013. See: http://www.fema.gov/media-library/assets/documents/32180

[92] This paragraph was pulled from the 2011 SNRA Risk Summary Sheet.

[93] This paragraph is directly from Emergency Support Function (ESF) #4 – Firefighting Annex, 2013. See: http://www.fema.gov/media-library/assets/documents/32180

Federal Government

Within the National Response Framework the United States Forest Service (USFS) is the coordinator and primary agency for ESF #4, Firefighting. The mission of ESF #4 includes coordinating Federal firefighting activities and providing resource support to rural and urban firefighting operations. The United States Fire Administration (USFA) plays a support and advisory role for the urban environment.[94]

In addition to the USFS and USFA, the Department of Commerce, Department of Defense, Department of State, Department of the Interior, Army Corps of Engineers, Environmental Protection Agency, and United States Coast Guard all have responsibilities under ESF #4. Federal Government agency actions are described in ESF #4, pages 4-6.[95]

Literature Review

Urban Conflagration in the U.S. Mostly Viewed Through Historical Lenses

Recent articles and studies evaluating urban conflagration within the U.S. examine the topic from an historic perspective.

William M. Shields's article, "Urban Conflagrations in the United States", explores the history of the Great Fires in the 18th, 19th, and earliest part of the 20th centuries and identifies the technological and social causes of conflagrations in U.S. cities.[96,97] Shields identifies the lessons learned and risk mitigation efforts taken after the fires to address the causes, and in doing so, explains how such mitigation efforts, combined with technological improvements and social and political changes, eventually eliminated the city-destroying fires. He asserts that by the 1920s, all "major sources of conflagration risk" had been reduced, and U.S. cities "felt confident that they were no longer at serious risk" of citywide fires.[98]

It is unclear if the document was peer reviewed, but the article is well footnoted and was recently referenced by a joint Resilient Cities initiative involving the University of Cambridge (see footnote 23). The primary reason to include it in this literature review is to demonstrate what appears to be the de facto assumption that conflagrations, at least for the U.S., are an issue of the past. In fact, in framing the term "conflagrations", Shields calls them "devastating fires" suffered by American cities from earliest colonial times until the early part of the 20th century.[99]

George Bankoff's book, *Flammable Cities: Urban Conflagration and the Making of the Modern World*, published by the University of Wisconsin Press, takes a broader view both in scope of the cities studied as well as the time frame. [100] *Flammable Cities: Urban Conflagration and the*

---

[94] Emergency Support Function (ESF) #4 – Firefighting Annex, 2013. See: http://www.fema.gov/media-library/assets/documents/32180

[95] ESF #4 – Firefighting Annex, 2013. See: http://www.fema.gov/media-library/assets/documents/32180

[96] Shields, W. M., Ph.D. (c.2009-2010) "Urban Conflagrations in the United States." Retrieved March 2015 from http://www.tvsfpe.org/_images/conflagrations.pdf.

[97] Shields' article previously (June 2013) resided on the U.S. Department of Energy's (DOE) website at this link: http://www.hss.energy.gov/nuclearsafety/nfsp/fire/workshop2010/shields/conflagrations.pdf. The article is not dated, however, the latest citation in the article is from 2009 and the DOE web link indicates it was used at a DOE workshop in 2010, therefore it is was likely written between 2009-2012. The article does not provide a publication source – appearing to be a 'White Paper', and thus likely has not been peer reviewed. It was cited by a November 2013 paper, "Building Resilient Cities: From Risk Assessment to Redevelopment," published jointly by Ceres, The Next Practice, and the University of Cambridge Programme for Sustainability Leadership.

[98] Shields (c.2009-2010) P 16.

[99] Shields (c. 2009-2010) P 1.

[100] Bankoff, G. (2012). Flammable cities urban conflagration and the making of the modern world. Madison: University of Wisconsin Press.

Making of the Modern World provides a series of essays examining the role of conflagrations in planning and building the world's cities. It covers 18 cities and regions across the world from the 17th to the 21st centuries. The essays are grouped into three parts: Part I: Cities as Fire Regimes; Part II: Fire as Risk and as Catalyst of Change; and Part III: The Politics of Fire. Part III addresses conflagrations in the 20th and 21st centuries, and may provide relevant findings for the current risk evaluation.

In the introduction, Bankoff acknowledges that "most wealthy countries today" view fire as an "occasional and isolated threat".[101] The book suggests that this may not be an accurate view of reality: "The Flammable cities of the past may prove to be the forebears of the flammable cities of the future, and the much touted "fire gap" more a temporal phenomenon than a spatial one."[102] This argument is largely focused on the urban slums in developing countries. However, the book includes an essay studying the case of Cleveland in the 1960s and 1970s (with references to Detroit and Los Angeles), and points out that even in modern, developed cities, fire "has continued to be a weapon of the weak, used to throw the social order into disarray and register protests that would otherwise go unheard, as well as a tool of elites, used to manipulate the urban poor and to reconfigure physical social space in the city to serve their own interests." [103]

Recent examples of civil unrest that involved acts of arson include the November 2005 French Riots[104], the August 2011 London Riots[105], and most recently, the riots in Ferguson, Missouri in November 2014.[106] A 2014 study by the Cambridge Centre for Risk Studies asserts there has been an increase in civil unrest around the globe and in the U.S., citing examples such as the Arab Spring movement (2010-2013) and the Occupy movement (2011-2012), and that it is likely to continue, in part due to the amplifying effect of social media.[107] The focus Bankoff's book, and likely publication date, did not allow for more in-depth exploration of this latter point.[108]

[101] Bankoff (2012). Introduction.

[102] Bankoff (2012). Introduction.

[103] Bankoff (2012).

[104] "The rioters . . . caused over €200 million in damage as they torched nearly 9000 cars and dozens of buildings, daycare centers, and schools. The French police arrested close to 2900 rioters; 126 police and firefighters were injured, and there was one fatality." – Sahlins, P. (2006, October 24). Civil Unrest in the French Suburbs, November 2005. Retrieved March 2015 from http://riotsfrance.ssrc.org.

[105] The United Kingdom's Home Office reports 266 recorded crimes of arson during the August 2011 riots. An Overview of Recorded Crimes and Arrests Resulting from Disorder Events in August 2011. (2011, January 1). Retrieved March 2015 from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/116257/overview-disorder-aug2011.pdf.

[106] More than a dozen buildings were set on fire the night of November 25, 2014, in protest against a grand jury's decision. Retrieved March 2015 from http://abcnews.go.com/US/additional-national-guardsmen-headed-ferguson-fires-burn-city/story?id=27157986.

[107] Bowman, G.; Caccioli, F.; Coburn, A.W.; Hartley, R.; Kelly, S.; Ralph, D.; Ruffle, S.J.; Wallace, J.; 2014, Millennial Uprising Social Unrest Scenario; Cambridge Risk
Framework Series; Centre for Risk Studies, University of Cambridge. Retrieved March 2015 from http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&ved=0CFkQFjAI&url=http%3A%2F%2Fcambridgeriskframework.com%2Fgetdocument%2F22&ei=P0sPVcfGHJP9oQSYkIKgCg&usg=AFQjCNHkzJQi_94TE5Gn6rf46VPO73RChA&sig2=6KFs2UiHsfpQ37wh7MqS1g&bvm=bv.88528373,d.cGU .

[108] Flammable Cities was published in January 2012. The London Riots had occurred only five months earlier, and while the Arab Spring Movement and Occupy Movement had been underway for two years, there was likely insufficient research at the time of their drafting to make a stronger case.

Urban Fires as a Consequence of Natural Disasters

Superstorm Sandy

The fires in Breezy Point, Queens, New York caused by Superstorm Sandy on October 29, 2012 were called a conflagration by major media outlets and trade journals.[109,110,111,112] The images of the fire damage were called one of the "most shocking photographs taken in the wake of Hurricane Sandy's rampage."[113] The response to the fire was complicated by not only the high-winds that caused the fire to climb higher than 60 feet and jump houses easily, but also the severe flooding that slowed access to the area and prevented use of fire hydrants.[114] 135 homes were destroyed by fire.[115] That there were no fatalities or serious injuries, particularly to the firefighters, was called miraculous.

The New York Fire Department (FDNY) Assistant Chief Joseph Pfeifer[116] was the Incident Commander for the Breezy Point fire and in 2013 he wrote a detailed account of the incident for Fire Engineering Magazine.[117] He introduces the topic of conflagration and provides background on the early "Great Fires" of New York City, as well as the recent great fires: the 9/11 World Trade Center fires and the 2006 Greenpoint Terminal Market fire in Brooklyn. Chief Pfeifer was present at both of these incidents, which makes his account of the Breezy Point fire all the more valuable.

Pfeifer's article provides a detailed narrative of what happened that night, describing the evolution of the fire, the complications of fighting the fire based on the conditions, and the strategy and tactics used to attack the fire, including a "three-pronged attack that combined flanking strategies with direct tactics to contain the fire".[118] Pfeiffer puts into context the importance of the FDNY's preparedness efforts (the previous summer they ran tabletop exercises on hurricanes in several communities including the Rockaways), and draws out lessons learned for Incident Commanders. One of his primary themes is that a "major characteristic of complex disasters is the presence of novelty" (events not seen before).[119] Novelty slows down decision-

[109] For example: Dolnick, S. and Kilgannon, C.(2012, October 30). Wind-Driven Flames Reduce Scores of Homes to Embers in Queens Enclave. The New York Times. Retrieved March 2015 from http://www.nytimes.com/2012/10/31/nyregion/wind-driven-flames-burn-scores-of-homes-in-queens-enclave.html?_r=0.

[110] Tangel, A. (2013, October 29). Breezy Point looks back a year after Superstorm Sandy. Los Angeles Times. Retrieved March 2015 from http://articles.latimes.com/2013/oct/29/nation/la-na-breezy-point-20131030.

[111] Also references at Footnote 43 and 47.

[112] There are varying opinions as to whether these fires were conflagrations in the strictest, historical understanding of the term. However, this assessment uses a broader definition of the term to ensure the full spectrum of the risk is evaluated.

[113] Breezy Point Inferno: Photo that Captures the Horror of Queens. (2012, October 31). The Week. Retrieved March 2015 from http://www.theweek.co.uk/us/hurricane-sandy/49854/breezy-point-inferno-photo-captures-horror-queens.

[114] Tangel (2013, October 29).

[115] Tangel (2013, October 29).

[116] Pfeifer is currently the Chief of Counterterrorism and Emergency Preparedness for FDNY. During his career he has commanded some of the largest fires and emergencies in New York City's history: he was the first chief at the World Trade Center attack on the morning of September 11, 2001, played a major command role during Hurricane Sandy in 2012, served as an Incident Commander at the Metro North commuter train Derailment in 2013, and assisted in developing the Ebola response in New York City in 2014. Pfeifer is a Senior Fellow of the Program on Crisis Leadership at Harvard Kennedy School and has presented in several of the program's Executive Education programs, including Leadership in Crises and China Crisis Management. He is also Senior Fellow at the Combating Terrorism Center at West Point and has spoken about crisis leadership and disaster management at Harvard University, Columbia University, Wharton, the Naval Postgraduate School, the United States Military Academy, the Federal Bureau of Investigation (FBI), and Tsinghua University in Beijing, China. He holds a Masters in Public Administration from Harvard University's Kennedy School, a Masters in Security Studies from the Naval Postgraduate School, and a Masters in Theology from Immaculate Conception. He writes frequently and is published in various books and journals.

[117] Pfeifer, J. (2013, May). Conflagration in Breezy Point, Queens. Fire Engineering, 61-67.

[118] Pfeifer, J. (2013, May). P 64.

[119] Pfeifer, J. (2013, May). P 63.

making, and Pfeiffer recommends that in such cases, the commanders must "narrow the focus of units to achieve specific missions".[120]

That same night, there were four other simultaneous multiple-structure incidents in the Queens borough of New York City. Chief Robert Maynes, the Queens Borough Commander, was the incident commander for the Belle Harbor fire where 29 homes, two businesses and three garages were burned. In an article[121] that evaluates FDNY's overall Incident Management response[122] (not just fire related) to Superstorm Sandy, Kat Sonia Thomson[123] highlights Chief Maynes' approach because he drew upon his experience with wildland fires to design his attack strategy to the Belle Harbor fire. Chief Maynes worked on the Idaho East Zone Complex Wildland fire in 2006, and when assessing the Belle Harbor fire, realized the fire was "mimicking the behavior of a wind-driven wildfire."[124] He determined he could not rely on the typical structure-by-structure approach and instead used wildland fire tactics (i.e., approach the "head of the fire" when it is safe to do so and focus limited resources in a "flanking action").

Thomson's article provides suggestions for additional areas of study to ensure future improvements to the use of an All-Hazards Incident Management Team (IMT) in large incidents. However, the primary point of her article is to draw connections between wildland and structural fires and show how both communities can learn from one another. She argues that the "instance of multiple-structure, wind-driven conflagration is becoming far too common to continue to ignore," and that both communities should "work together to collect, analyze and implement a new typology of conflagration operations that incorporates concepts from wildland and structural operations."[125]

Professor Charles Jennings of the John Jay College of Criminal Justice, The City University of New York, provides a more scholarly account of the fires caused by Superstorm Sandy in an article for Fire Safety Science News, an international newsletter from the International Association for Fire Safety Science.[126] It was published only four months after the incident, and thus is primarily a narrative record of the event, similar to the other literature reviewed, albeit with more precision of language and perhaps a more neutral perspective. A key observation in his article is that fire caused by hurricanes has "received scant attention in the scholarly fire engineering community and even in the trade press," and that a "casual review of scholarly indexes shows scarcely any mention of the topic".[127]

---

[120] Pfeifer, J. (2013, May). P 63.

[121] Thomson, K. (2013, July). When a Hurricane Becomes a Wildfire. Wildfire Magazine, 14-18.

[122] Thomson explains the FDNY implemented the use of the All-Hazards Incident Management Team (IMT) and Incident Command System (ICS) after its value was demonstrated by wildland firefighters deployed to assist FDNY in the aftermath of 9/11. In addition to the structural changes and training the IMT approach required, FDNY regularly deployed its teams to support other hazards around the country, including hurricanes and wildland fires.

[123] Kat Sonia Thomson, BA Urban Studies, MPA, Ph.D. Candidate, has worked in wildland fire and aviation operations since 1998, and currently serves as an Air Attack Officer for the Government of Alberta. In the off-season, she consults on structural fire department operations and performance management in New York City.

[124] Thomson, K. (2013, July). P 15.

[125] Thomson, K. (2013, July). P 18.

[126] Jennings, C. (2013). Fires During the 2012 Hurricane Sandy in Queens, New York: A First Report. Fire Safety Science News, (Newsletter No. 34), 26-28. Retrieved March 2015 from http://www.iafss.org/portal/wp-content/uploads/No-34-Fire-Safety-Science-News-March-2013.pdf

[127] Jennings, C. (2013). P 26.

Earthquakes

Earthquake-induced conflagrations are a recognized hazard. A 2008 U.S. Geological Survey report describe these events in the following way:

> Fire following earthquake refers to series of events or stochastic process initiated by a large earthquake. Fires occur following all earthquakes that significantly shake a human settlement, but are generally only a very significant problem in a large metropolitan area predominantly comprised of densely spaced wood buildings. In such circumstances, the multiple simultaneous ignitions can lead to catastrophic conflagrations that are by far the dominant agent of damage for that event. Regions of high seismicity with large metropolitan area predominantly comprised of densely spaced wood buildings include Japan, New Zealand, parts of Southeast Asia and western North America. A large earthquake such as a M7.8 event on the San Andreas fault in southern California (or comparable events in northern California, Puget Sound, or the Lower Mainland of British Columbia) combines all the requisite factors for major conflagrations that, depending on circumstances, can be of uniquely catastrophic proportions.[128]

The report notes "the two largest peace-time urban conflagrations in history have been fires following earthquakes – 1906 San Francisco and 1923 Tokyo, the latter resulting in the great majority of the 140,000 fatalities".[129]

On October 17, 1989, the San Francisco Bay Area was hit by a M6.9 earthquake that killed 67 people and caused more than $5 billion in damages.[130] In contrast to the 1906 San Francisco earthquake, fire was a minor factor.[131] There was one major fire in the Marina District: approximately eight apartment buildings were destroyed on one street.[132] The remaining fire losses were two homes and one auto repair shop.[133] A National Institute of Standards and Technology (NIST) study of the earthquake found that a number of factors might have contributed to the low fire-rate[134]:

- There was low wind. Had there been wind, the researchers found, it was quite possible the Marina District fire could have developed into a multi-block conflagration.
- It rained shortly before the earthquake, resulting in high moisture in the ground and wild lands. Downed power lines in the Santa Cruz Mountains served as ignition sources and some minor fires occur. They were able to be managed locally, "But had the hills been dry and/or a strong wind been present, a different result could well have occurred."

The study found that the fire services for the affected communities "were left in a condition where it is doubtful that they could have halted a serious spreading fire."[135] Fire services were

[128] Scawthorn, C. (2008). Fire Following Earthquake: The ShakeOut Scenario Supplemental Study. Prepared for U.S. Geological Survey and California Geological Survey, by SPA Risk, LLC. (Berkeley, CA). P 6.
[129] Scawthorn, C. (2008). P 7.
[130] U.S. Geological Survey. October 17, 1989 Loma Prieta Earthquake webpage: http://earthquake.usgs.gov/regional/nca/1989/
[131] Nelson, H. (1990). "Performance of Fire Protection Systems". Chapter 6 of Performance of Structures During the Loma Prieta Earthquake of October 17, 1989. Edited by Lew, H. U.S. Department of Commerce, National Institute of Standards and Technology. P 6-2. Retrieved April 2015 from http://www.nist.gov/customcf/get_pdf.cfm?pub_id=908823.
[132] Nelson, H. (1990). P. 6-1.
[133] Nelson, H. (1990). P. 6-1.
[134] Nelson, H. (1990). P. 6-1.
[135] Nelson, H. (1990). P. 6-1.

overwhelmed responding to search and rescue efforts, communications were disrupted or overtaxed, and significant underground breakage of water mains eliminated the principal source of firefighting water.[136]

Five years later and further south, a M6.7 earthquake struck the San Fernando Valley region of Los Angeles. The Northridge earthquake killed 60 people and more than 9,000 were injured.[137] From the initial main shock at 4:31AM to midnight, there were approximately 110 earthquake related fires.[138] A NIST sponsored study of the fires following the Northridge earthquake found that:

- More than 70% occurred in single- or multiple-family residences;
- The major cause of ignition was electric arcing as the result of a short circuit, although gas flame from an appliance is also a recurring source of ignition; and
- Where identification could be made, escaping natural gas (presumably from a broken gas line) is the single most common ignition material.[139]

Other consequences that inhibited firefighting:

- Several instances of significant communications impairment
- The earthquake caused approximately 1,400 water system leaks, and pump stations and storage tanks also sustained damage. This resulted in a lack of water pressure at hydrants in certain portions of San Fernando Valley, and the Los Angeles Fire Department (LAFD) resorted to using water tankers and drafting from alternative sources.[140]

The NIST study determined that while a significant number of fires occurred in the hours after the earthquake, the resources of the Los Angeles region were sufficient to deal with the fires, as well as the other earthquake emergencies. However, the study indicates if the fires had turned into a conflagration the diminished water supply would not have been sufficient to address it.[141]

While these studies identify valuable lessons learned, they are based on the last major earthquakes to strike the U.S. mainland, which occurred over 20 years ago. Not surprisingly, several of the studies cited in this section are older than those usually selected for the literature review.[142] While there is value in understanding the history of earthquake caused fires, they are less reliable sources for assessing risk. Current firefighting capabilities and technology have evolved significantly in twenty years. Federal, state, and local preparedness and capabilities for catastrophic events has improved since the terrorist attacks of September 11, 2001.[143]

---

[136] Nelson, H. (1990). P. 6-2.
[137] Scawthorn, C. (2008). P 10.
[138] Scawthorn, C., Cowell, A., and Borden, F. (1998, March). EQE Fire-related aspects of the Northridge Earthquake. Prepared for the U.S. Department of Commerce, National Institute of Standards and Technology, Building and Fire Research Laboratory. International, Inc. (San Francisco, CA) P iv.
[139] Scawthorn, C., Cowell, A., and Borden, F. (1998, March). P v.
[140] Scawthorn, C., Cowell, A., and Borden, F. (1998, March). P v-vi.
[141] Scawthorn, C., Cowell, A., and Borden, F. (1998, March). P vi.
[142] The target range for this Literature Review is publications from the past five years (2010-2015).
[143] Examples of improvements include: interoperable communications, situational awareness standard operating procedures, Incident Command Systems, exercises, training, and enhanced equipment.

Simultaneously, there are factors that may increase the risk of fires following earthquakes including:

- Recent severe droughts in the west have significantly depleted water supplies. The inability to quickly access water, will lead to more conflagrations.
- Increased drilling near populous areas and more refineries and tank farms; "When strongly shaken, oil refineries and tank farms have typically had large fires which have burned for days."[144]
- Wildland Urban Interface – as discussed below, increased development in wildland areas has led to an increased number of significant fires and conflagrations. They are also further exacerbated by extreme drought conditions.

Wildland Urban Interface

One of the most common topics found during this literature review was Wildland Urban Interface (WUI). Nine of the 25 costliest fires in U.S. history, in terms of property loss, were forest, wildland or WUI fires.[145] Over 46 million homes in 70,000 communities are said to be at risk of WUI fires.[146] The Natural Resource Conservation service estimates that since 1990, the U.S. has converted 3 acres per minute, 4,000 acres per day and close to 2 million acres per year of wildlands to WUI.[147,148] The International Association of Wildland Fire reports that the number of structures lost to WUI fires has "grown significantly over the past 20 years."[149] A number of factors contribute to the trend: "increased development in rural areas, fuel management policies, and climate change, all of which are projected to continue for the foreseeable future."[150]

The SNRA addresses wildfires as a stand-alone topic, separate from Urban Fire/Urban Conflagration. Increasingly however, wildfires move into populated areas and cause extensive damage. The NFPA defines WUI as: "The presence of structures in locations in which the [authority having jurisdiction] determines that topographical features, vegetation fuel types, local weather conditions, and prevailing winds result in the potential for ignition of the structures within the area from flames and firebrands of a wildland fire." Or more simply: "The location where humans and their development meet or are intermixed with wildland fuels."[151]

A 2010 article in the International Journal of Wildland Fire, written by experts from NIST and the National Oceanic and Atmospheric Administration (NOAA), assessed the current approaches

[144] Scawthorn, C. (2008). P 10.
[145] Almand, K. (2014, September 3). Interface Investigation: The need for a closer look at how structures burn in the wildland/urban interface. National Fire Protection Association Journal. September-October 2014. Retrieved April 2015 from http://www.nfpa.org/newsandpublications/nfpa-journal/2014/september-october-2014/columns/research
[146] Bailey, D. (2013) WUI Fact Sheet, International Association of Wildland Fire and International Code Council. Retrieved April 2015: http://www.iawfonline.org/pdf/WUI_Fact_Sheet_08012013.pdf
[147] Bailey, D. (2013).
[148] Bailey, D. (2013) reference is a useful WUI fire fact sheet and provides many more statistics on WUI fires.
[149] Almand, K. (2014, September 3).
[150] Almand, K. (2014, September 3).
[151] Both definitions are found in the 2014 NFPA Glossary. NFPA. "NFPA Glossary of Terms: 2014 Edition". (2014, September). Retrieved March 2015 from http://www.nfpa.org/got

and research needs for the WUI fire problem.[152] The study asserts that the WUI fire problem is a structure ignition problem and the best approach to reducing the severity of the problem is to reduce the potential for structure ignition.[153] The paper provides "an overview of the WUI fire problem, a short review of current approaches to addressing the WUI fire problem and reducing structure ignitions, a discussion and assessment of further needs, and an overview of the ongoing work at the National Institute of Standards and Technology (NIST) to address some of the research needs".[154]

As of 2010, the authors stated there is no standardized method of risk assessment that can be applied nationwide to WUI communities in the U.S. They review and evaluate the limitations of several narrowly tailored risk assessment methodologies. A section on residential fuels, the definition of which includes both structures and vegetation, points out that most of the focus is on vegetation-to-structure fire spread. They believe this is valid for WUI communities with sufficiently low housing density, however, insufficient for medium to high housing density areas. Citing analysis of four separate WUI fires, structure-to-structure fire spread played a key role in the overall fire behavior. They assess that existing guidelines (as of 2010) for homeowners to mitigate WUI fire risk were developed for lower housing-densities and may not be applicable for the medium to high housing density areas.[155]

A more recent article in the NFPA Journal by Kathleen H. Almand, suggests that there is still a need for better research.[156] The article reviews current efforts underway to address WUI fire:

- The NFPA reorganized its technical committees to better address the WUI fire problem.
- NIST, USFS and the Insurance Institute for Business & Home Safety are actively pursuing research programs to better understand the spread of fire from the wildland to structures.
- The Fire Protection Research Foundation, a foundation that supports the NFPA mission, issued a report in March 2015, Pathways for Building Fire Spread at the Wildland Urban Interface.[157] The purpose of the report is to serve as a bridge between emerging research and NFPA's codes and standards so that their prevention and protection strategies reflect the new and growing understanding of WUI firespread.[158]

Lighter Building Materials, Modern Furniture Means Hotter, Faster Fires and a Change in Fire Fighting Strategies

As one would expect, many articles in the fire trade journals are focused on the nuts and bolts of daily firefighting. An interesting theme within the past five years of literature is the impact that

[152] Mell, W., Manzello, S., Maranghides, A., Butry, D., and Rehm, R. The Wildland-Urban Interface Fire Problem – Current Approaches and Research Needs. (2010). P 238. International Journal of Wildland Fire. Vol 19. Retrieved April 2015 from http://www.firescience.gov/projects/07-1-5-08/project/07-1-5-08_Mell_etal_WUIresearch_needs_ijwf2010.pdf

[153] Mell, W., Manzello, S., et. al. (2010). P 238. Which cites: Cohen JD (2008) The wildland–urban interface fire problem. *Forest History Today* (Fall), 20–26.

[154] Mell, W., Manzello, S., et. al. (2010). P 238.

[155] Mell, W., Manzello, S., et. (2010). P 242.

[156] Almand, K. (2014, September 3).

[157] Gollner, M., Hakes, R., Caton, S., and Kohler, K. (2015, March). Pathways for Building Fire Spread at the Wildland Urban Interface. Department of Fire Protection Engineering, University of Maryland. (College Park, MD), produced for Fire Protection Research Foundation. Retrieved April 2015 from http://www.nfpa.org/research/fire-protection-research-foundation/reports-and-proceedings/for-emergency-responders/fire-prevention-and-administration/pathways-for-building-fire-spread-at-the-wildland-urban-interface,

[158] Almand, K. (2014, September 3).

newer buildings and furniture have on fires.[159,160] The articles provide some scientific explanations for how fire acts differently in buildings constructed prior to the 1960s (with solid wood) as compared to those built since. While the newer engineered products provide a supposedly stronger structure for less material and money, under the high-heat conditions a fire produces, the structures fail much more rapidly and the fire escalates more quickly and thus the firefighting strategies must be altered depending on the type of building. The articles also suggested there was a lack of consideration for the implications of fire prevention in the construction of these homes. No articles were found that connected new buildings to an increased risk of conflagration, however, urbanization trends in the U.S. – particularly when older homes, which tend to be spaced more closely together than suburban areas, are torn down or gutted and replaced with new materials – may increase the risk of fires with the potential to spread.

Similarly, an NFPA Journal article from January 2015 highlights new research from Fire Science that suggests tactical changes should be made in how firefighters approach fires.[161] Some of this is based on finally having solid scientific data on how structure fires work, but the other reason for the suggested changes are to recognize that the 'fuel sources' in the modern home are extremely different that those fifty years ago when most firefighting tactical standards were developed. One experiment, which can be watched on YouTube, captured the significant difference in how fire behaved in a room with older versus newer furniture. The room filled with legacy furniture takes nearly thirty minutes to reach flashover, but the modern room reaches flashover in just three minutes, 40 seconds. Since the average response time for home structure fires is close to six minutes, it means firefighters are dealing with much more intense fires than their counterparts 50 years ago.

Conclusion

While articles from the past five years appear in agreement that the U.S. does not have a strong or even moderate risk of conflagration from traditional causes, there may be an increasing risk of urban fires caused by other hazards.

Flammable Cities, makes the case that urban fires, even in so-called "first world" countries, may see a resurgence in future years, as people resort to leveraging fire as a political tool. Whether the incidents in France, London, and Ferguson, Missouri are evidence of an emerging trend or an anomaly remains to be seen, and perhaps could be evaluated in future risk assessments.

On the nexus of fires and natural disasters, earthquakes and fires are well-studied due to the 1906 San Francisco Earthquake and associated conflagration[162], however, hurricanes and conflagrations, as Jennings' points out, is less studied. In both cases, firefighters' access to the blaze and access to water for fire suppression appear to be major challenges in keeping a fire from spreading. It should be noted that there was only one scholarly journal found on the topic of

[159] Naum, C. (2015, January). Building Construction for Today's Fire Service: Newer buildings & occupancies present increasing challenges. Firehouse Magazine. P 74.
[160] Earls, A. (2009, July). Lightweight Construction. NFPA Journal. (July-August 2009 Edition). Retrieved March 2015 from http://www.nfpa.org/newsandpublications/nfpa-journal/2009/july-august-2009/features/lightweight-construction,
[161] Roman, Jesse. (2015, January). New Fires, New Tactics. NFPA Journal. January-February 2015. Retrieved April 2015 from http://www.nfpa.org/newsandpublications/nfpa-journal/2015/january-february-2015/features/fire-tactics.
[162] See draft 2011 Risk Summary Sheet on Urban Conflagration.

Superstorm Sandy and the fires.[163,164] The incidents are fairly recent, thus studies may be ongoing and as Thomson and Jennings' articles indicate, there is a need for deeper analysis.

Though the 1989 and 1994 earthquakes did not result in conflagrations, they provided useful insights into the challenges of fighting fires caused by earthquakes. The literature reviewed, however, is limited in providing a useful risk assessment for today's environment due to changes in technology, equipment, and capabilities over the past twenty years. Alternatively, certain factors like climate change, extreme drought, more oil and gas drilling, and more refineries may exacerbate fires. This means that fires that were controllable in 1989 and 1994 may no longer be able to be suppressed.

There is general agreement among experts that "WUI fires will continue to be a serious and costly issue".[165] The NFPA even made it a priority in their current strategic plan. All indications are that the WUI will continue to grow as more and more people move into wildland areas. Current drought conditions in the west, and the potential for climate change to further exacerbate drought and other severe weather will provide more fuel and ignition sources for the fire. Thus the research is focused on mitigation and suppression techniques. This research and the NFPA's updated standards should help reduce the size and consequence of WUI fires, even as the frequency is likely to stay the same or increase.

Finally changes in building materials and furnishings are producing hotter and faster fires, making a structure-to-structure fire spread more likely if outdated firefighting techniques are used. The firefighting community seems to be aware of the need for changes; standards and training are being updated. While the fires may be more intense, there is reason to believe the tactics to mitigate that intensity will be successful.

All of these changes and increased risk factors require urban firefighters to be equipped with the skills necessary to handle the complex challenges of today's fires.

[163] Searches conducted via USFA's online library, NFPA's website and general internet searches, including Google Scholar.

[164] While there were numerous additional trade magazine articles about Superstorm Sandy and the associated fires, only one scholarly journal was found in a search of the USFA's Library catalogue. The article appeared in The Crisis Journal and was solely an interview with Joseph Pfeiffer. It did not contain any references to academic literature. Since Joseph Pfeiffer's article from Fire Engineering magazine had already been reviewed for this Literature Review, it was not included as a separate source for purposes of the Literature Review. Pfeiffer does cite additional lessons learned in the interview. Should further research on this topic be required, this article should be reviewed. Citation for the article: Christo Motz, (2013). How the FDNY responded to Hurricane Sandy. The Crisis Journal (Vol 8 (3)).

[165] Mell, W., Manzello, S. . . . (2010). P 248.

Table 13: Incidents of Fires with 10 or More Fatalities from 1970-2013[166],[167]

Start	End	Location	Name	Killed	Tot. Affected	Est. Dmge (US$ Million)	EM-DAT DisNo	CPI	Dmge. $2011 (US$ Million)
9/6/1970	9/6/1970	Ohio	Nursing Home	31			1970-0011	5.797	
12/1/1970	12/1/1970			28			1970-0130	5.797	
3/2/1971	3/2/1971	Woodbine		25	61		1971-0122	5.554	
6/24/1973	6/24/1973	New Orleans	Nightclubs	30			1973-0064	5.066	
6/30/1974	6/30/1974	New York	Nightclub	24			1974-0067	4.563	
10/24/1976	10/24/1976	Bronx, New York	Nightclub	25			1976-0080	3.953	
10/1/1976	10/1/1976	Fremont (Nebraska)	Nursing Homes	20			1976-0081	3.953	
6/1/1977	6/1/1977			42			1977-0237	3.712	
2/7/1978	2/7/1978	Beverly Hills, Southgate ...	Supper Club Fire	164	100		1978-0248	3.450	
5/28/1978	5/28/1978	Beverly Hills	Beverly Hills Country Club	16			1978-0150	3.450	
1/1/1979	1/1/1979	Sante Fé		28			1979-0120	3.098	
11/21/1980	11/21/1980	Las Vegas	Hotel	84	726		1980-0024	2.730	
12/4/1980	1/1/1981	New York	Hotel 'Stouffers Inn'	26			1981-0020	2.475	
12/24/1989	12/24/1989	Johnson City (Tennessee)	Retirement home	16			1989-0342	1.814	
1/1/1989	1/1/1989	Near Remer (Minnesota)	House	10			1989-0406	1.814	
3/25/1990	3/25/1990	New-York	Night club 'Happy Land'	87			1990-0432	1.721	
4/19/1993	4/19/1993	Waco		78			1993-0449	1.557	
3/16/1993	3/16/1993	Chicago	Hotel	16			1993-0127	1.557	
3/5/1993	3/5/1993	Los Angeles	Apartment complex	10			1993-0152	1.557	
11/21/1996	11/21/1996	San Juan	Building	29	90	12.1	1996-0332	1.434	17.3
3/1/2001	3/1/2001	Oak Orchard (Delaware Sta ...	House	11			2001-0004	1.270	
2/20/2003	2/20/2003	West Warwick (Rhode Isl. ...	Nightclub	100	150		2003-0095	1.222	
2/26/2003	2/26/2003	Hartford (Connecticut)	Nursing home' Greenwood	11	120		2003-0108	1.222	
11/26/2006	11/27/2006	Anderson (Missouri)	Hall for mentally disabled people	10	19		2006-0637	1.116	
7/3/2007	8/3/2007	Bronx (New York)	Home	10			2007-0118	1.085	
3/4/2008	3/4/2008	Pennsylvania	House	10	2		2008-0143	1.045	

[166] EM-DAT: The OFDA/CRED International Disaster Database – www.emdat.be, Université Catholique de Louvain, Brussels (Belgium) [official citation]. EM-DAT is maintained by the Centre for Research on the Epidemiology of Disasters (CRED) at the School of Public Health of the Université Catholique de Louvain located in Brussels, Belgium (http://www.emdat.be/frequently-asked-questions), and is supported by the Office of US Foreign Disaster Assistance (OFDA) of USAID (http://transition.usaid.gov/our_work/humanitarian_assistance/disaster_assistance/).
[167] Accessed March 2015. Verified no further fire incidents available in EM-DAT through 2013.

Migrant Surge / Mass Migration

Synopsis

This survey of recent mass migration surge events and a review of associated research literature indicate there is a strong likelihood of future surges to the U.S. Such surges are caused by complex structural factors that render 'quick solutions' unlikely. This paper provides an overview of the "Why," "Who," and "How" of migration, including the dangers migrants encounter in their journey, an overview of the recent history of migration, examples of recent surges, and a brief overview of the roles and responsibilities of various U.S. Government agencies related to mass migration.

The literature review is grouped into two themes: (1) the 2014 Central American surge of unaccompanied children, and (2) push factors are intensifying and are likely to increase the frequency of surges.

Literature Review – Risk of Mass Migration Likely Increasing

Introduction

Event Description

Mass Migration is defined as a concentrated flow, or surge, of migrants into the United States primarily along maritime and land borders, regardless of method of entry or reason for migrating.[168] This assessment is inclusive of both legal and illegal (undocumented) migration attempts. It is focused on the short-term impacts to the United States in handling a surge of migrants, that is, primarily the increased resources and capabilities needed to manage a surge.[169] It does not attempt to assess the long-term impacts of legal or illegal immigration. This assessment also does not consider repatriation efforts even in events where repatriation and mass migration may be comingled concerns.

Event Background

Why People Migrate

Marc Rosenblum[170] and Kate Brick's 2011 study, *U.S. Immigration Policy and Mexican/Central American Migration Flows: Then and Now*, explains "why people move, who and how many people migrate, and how they choose where to go, depends on a combination of structural factors that are difficult for governments to control and on the policy environment in which migration decision making occurs."[171]

[168] Methods for entry and the reasons/intent for gaining entry are discussed in the event background.
[169] For example, maritime and land-based border patrol and search and rescue services, law enforcement and immigration courts services, and providing shelter, clothing, food, medical treatment, and other health and welfare services.
[170] Marc R. Rosenblum also co-edited the Oxford Handbook of the Politics of International Migration published June 2012. This resource was not reviewed due to its length and the fact that the scope of the book covers more than just migration to the U.S. It is, however, a notable contribution to the literature of Mass Migration.
[171] Rosenblum, Marc R. and Kate Brick. *U.S. Immigration Policy and Mexican/Central Migration Flows: Then and Now. Washington, DC: Migration Policy Institute*. 2011.

The reasons can be categorized into three structural factors:[172]

- Push Factors – Factors in the country of origin that encourage departure. These can include limited economic opportunity, authoritarian or corrupt governments, crime, lack of education, wars, and natural disasters.
- Pull Factors – Factors that attract migrants to a country include availability of jobs and associated economic opportunities for immigrants and families, including safety, limited government, and equality before the law.
- Social networks – The ability to connect migrants to host-state jobs and communities. This occurs through providing funds and information to would-be migrants, assisting with how to relate to public authorities, and integration into the host-state economy. Rosenblum and Brick point out that with 10-20 percent of Mexicans and Central Americans now living in the U.S., social networks are a particularly important factor within this region.

The Current "Wave" of Immigration to the United States

Historically speaking, we are presently in the fourth 'great wave' of immigration. Figure 1 shows that the current immigrant[173] share of the U.S. population, 13.1 percent in 2013, is similar to that of the period of 1860-1920.[174,175] Historians consider that period to include the second and third waves of large-scale immigration. The fourth peak period began in the 1970s and continues today.[176,177,178]

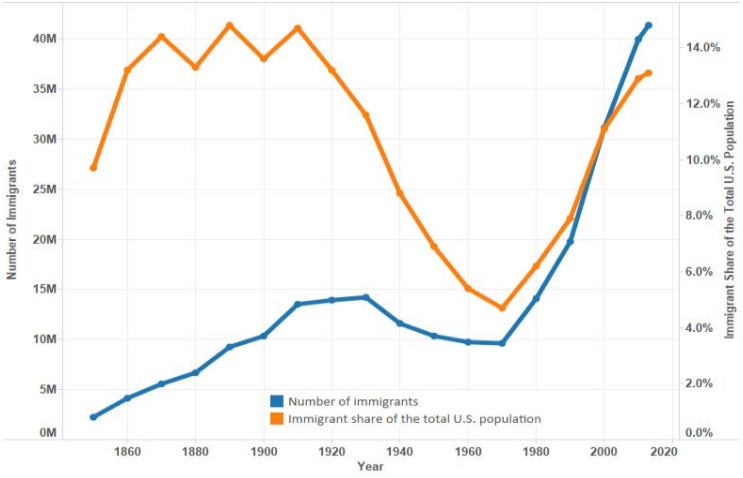


Figure 1: Migration Policy Institute (MPI) - Number of Immigrants and Percentage of the Total U.S. Population, 1850-2013

[172] Adapted from Rosenblum and Brick (2011). P 2. Rosenblum and Brick include the following citation on this list: The classic source on push-and-pull factors, and social networks is Douglas S. Massey, Joaquin Arango, Graeme Hugo, Ali Kouaouci, Adela Pellegrino, and J. Edward Taylor, *Worlds in Motion: Understanding International Migration at the End of the Millennium* (Oxford, UK: Clarendon Press, 1998).

[173] "Foreign born" and "immigrant" are used interchangeably and refer to persons with no U.S. citizenship at birth. This population includes naturalized citizens, lawful permanent residents, refugees and asylees, persons on certain temporary visas, and the unauthorized. Definition from the Migration Policy Institute. Washington, DC. See Zong, J., & Batalova, J. (2015, February 25). Frequently Requested Statistics on Immigrants and Immigration in the United States. Retrieved March 2015, from http://migrationpolicy.org/article/frequently-requested-statistics-immigrants-and-immigration-united-states#Demographic, Educational, and Linguistic

[174] MPI Data Hub. (2013, August 14). U.S. Immigrant Population and Share Over Time, 1850-Present. Retrieved March 2015, from http://www.migrationpolicy.org/programs/data-hub/charts/immigrant-population-over-time?width=1000&height=850&iframe=true MPI tabulation of data from the U.S. Census Bureau's 2010 - 2013 American Community Surveys and 1970, 1990, and 2000 decennial Census data. All other data are from Campbell J. Gibson and Emily Lennon, "Historical Census Statistics on the Foreign-Born Population of the United States: 1850 to 1990" (Working Paper no. 29, U.S. Census Bureau, Washington, DC, 1999).

[175] Grieco, E., Trevelyan, E., Larsen, L., Acosta, Y., Gambino, C., De la Cruz, P., . . . Walters, N. (2012). The Size, Place of Birth, and Geographic Distribution of the Foreign-Born Population in the United States: 1960 to 2010. *Working Paper no. 96, Population Division, U.S. Census Bureau, Washington, DC.*

[176] Hipsman, F., & Meissner, D. (2013, April 16). Immigration in the United States: New Economic, Social, Political Landscapes with Legislative Reform on the Horizon. Retrieved March 2015, from http://www.migrationpolicy.org/article/immigration-united-states-new-economic-social-political-landscapes-legislative-reform

[177] Grieco, E. . . . (2012).

[178] There is some variance by scholars in the segmentation of the immigration "waves". Some group the second and third wave into one wave, while others consider them separate because of different push/pull migration factors. There is also variance in the dating of the beginning of the

In 2007, there was a decline in both legal and illegal immigration, which coincides with the 2007-2009 Great Recession. Figure 2 shows the number of people granted legal permanent residency each year and the decline that began around 2007.[179]

Figure 3 shows the number of illegal immigrants estimated to be in the United States with a slight decline and leveling off around 2007.[180,181]

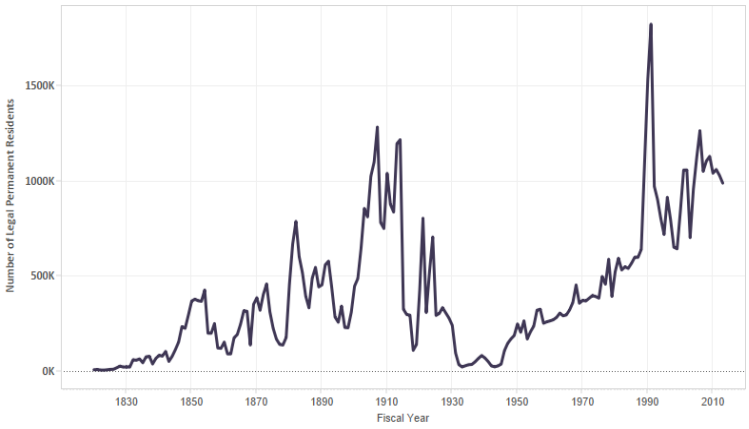


Figure 2: MPI - Annual Number of U.S. Legal Permanent Residents, FY 1820-2013

Hipsman and Meissner assert "illegal immigration is a bellwether of economic conditions, growing substantially in a strong economy with high demand for low-skilled labor (the 1990s and early 2000s), and tapering off with economic contraction (since 2008)." The decline may also be due to "heightened border enforcement, a rise in deportations, and the growing dangers associated with illegal border crossings."[182] As of March 2015, most research reflects data as late as 2013, and the researchers acknowledge it is possible, even likely, that the immigration numbers will increase again as the U.S. economy recovers.

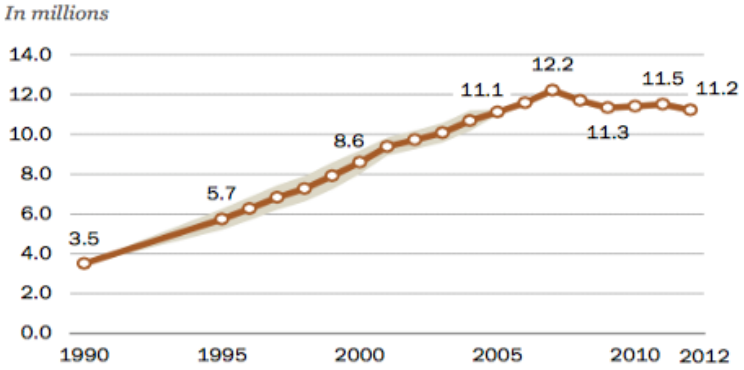


Figure 3: Pew Research Center - Growth in Unauthorized Immigration Has Leveled Off

U.S. Immigrants' Countries of Origin

After the passage of the Immigration and Nationality Act Amendments of 1965, there was a remarkable shift of migratory patterns.

---

fourth wave. Some consider it to start in 1965 at the passage of the Immigration and Nationality Act Amendments of 1965, while others date it to after 1970 when the trend of increased migration occurs.

[179] MPI Data Hub (2013). http://www.migrationpolicy.org/programs/data-hub/charts/Annual-Number-of-US-Legal-Permanent-Residents?width=1000&height=850&iframe=true Migration Policy Institute tabulations of U.S. Department of Homeland Security, Office of Immigration Statistics, Yearbook of Immigration Statistics (various years). Available at http://www.dhs.gov/files/statistics/publications/yearbook.shtm. This chart tracks the number of people who annually are granted legal permanent residence (also known as getting a green card). Green-card holders are permitted to live and work in the country indefinitely, to join the armed forces, and to apply for U.S. citizenship after five years (three if married to a U.S. citizen). As of January 2012, an estimated 13.3 million green-card holders lived in the United States, including an estimated 8.8 million eligible to become U.S. citizens.

[180] Source: Table A1, derived from Pew Research Center estimates for 2005-2012 based on augmented American Community Survey data from Integrated Public Use Microdata Series (IPUMS); for 1995-2004, 2000 and 1995 based on March Supplements of the Current Population Survey. Estimates for 1990 from Warren and Warren (2013).

[181] Note: Shading surrounding line indicates low and high points of the estimated 90 percent confidence interval. Data labels are for 1990, 1995, 2000, 2005, 2007, 2009, 2011 and 2012. The 2009-2012 change is not statistically significant at 90 percent confidence interval.

[182] Passel, J., Cohn, D., & Gonzalez-Barrera, A. (2012, April 23). Net Migration from Mexico Falls to Zero-and Perhaps Less. Retrieved March 29, 2015, from http://www.pewhispanic.org/2012/04/23/net-migration-from-mexico-falls-to-zero-and-perhaps-less/

Prior to 1960, the U.S. immigrant population consisted mostly of European immigrants settling in the U.S. Northeast and Midwest. Beginning in 1970s, it was predominantly Latin American and Asian immigrants settling in the U.S. South and West.[183,184]

In the 1970s there was a sharp rise in the number of Mexican-born immigrants arriving in the U.S. and by 1980, Mexico became the top originating country for U.S. immigrants.[185] In 2013, they accounted for 28 percent of the 41.3 million immigrants in the United States,[186] and they accounted for the largest share of both legal and illegal entries.[187] A Pew Research Center Hispanic Trends study conducted by Jeffrey Passel, D'Vera Cohn, and Ana Gonzalez-Barrera points out that in the history of the U.S., "no country has ever seen as many of its people immigrate to this country as Mexico has in the past four decades."[188,189] Further, the most "distinctive feature" of this wave is the "unprecedented share" (51 percent) of immigrants who have come to the U.S. illegally.[190]

Now after four decades of Mexico leading as the dominant country of migration origin, we may be seeing another significant shift. In 2012, the Pew Research Center's Hispanic Trends project examined census data from the U.S. and Mexico and found that immigration flows from Mexico have declined significantly, and simultaneously that the number of Mexican-born immigrants who left the U.S. for Mexico rose. They asserted that the result is a net migration flow of zero.[191]

Further, in a November 2014 report, the Pew Research Center identified that "as Mexican numbers continued to drop between 2009 and 2012, unauthorized immigrant populations from South America and from a grouping of Europe and Canada held steady," and, migrants from "Asia, the Caribbean, Central America,[192] and the rest of the world grew slightly from 2009 to 2012".[193]

In October 2011, the U.S. Government began

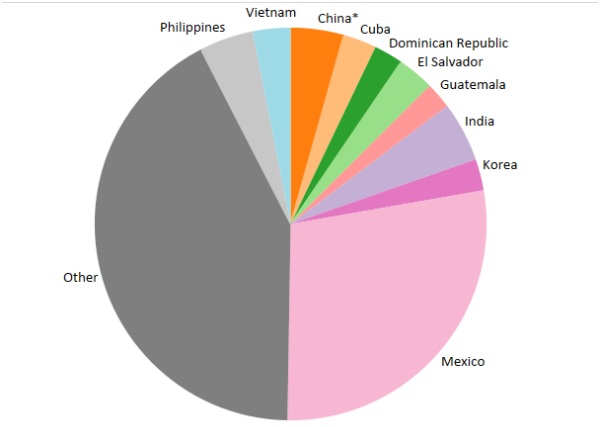


Figure 4: MPI - Top 10 Largest Immigrant Groups (2013)

[183] Zong, J., & Batalova, J. (2015, February 25). Frequently Requested Statistics on Immigrants and Immigration in the United States. Retrieved March 2015, from http://migrationpolicy.org/article/frequently-requested-statistics-immigrants-and-immigration-united-states#Demographic, Educational, and Linguistic

[184] Grieco, E. . . . (2012).

[185] Passel, J., Cohn, D., & Gonzalez-Barrera, A. (2012, April 23). Chapter II. Migration Between the U.S. and Mexico.

[186] Zong, J., & Batalova, J. (2015, February 25).

[187] Hipsman, F., & Meissner, D. (2013, April 16).

[188] Passel, J., Cohn, D., & Gonzalez-Barrera, A. (2012, April 23). Overview.

[189] Passel, J., Cohn, D., & Gonzalez-Barrera, A. point out that when measured as a share of the immigrant population at the time, immigration waves from Germany and Ireland in the late 19th century equaled or exceeded the modern wave from Mexico.

[190] Passel, J., Cohn, D., & Gonzalez-Barrera, A. (2012, April 23). Overview.

[191] Passel, J., Cohn, D., & Gonzalez-Barrera, A. (2012, April 23).

[192] The increase of Central American migration is discussed in more detail in the Literature Review.

[193] Passel, Jeffrey S. and D'Vera Cohn. (2014, November). "Unauthorized Immigrant Totals Rise in 7 States, Fall in 14: Decline in Those From Mexico Fuels Most State Decreases." Washington, D.C. Pew Research Center's Hispanic Trends Project. Retrieved March 2015, http://www.pewhispanic.org/files/2014/11/2014-11-18_unauthorized-immigration.pdf

seeing a dramatic rise in the number of unaccompanied[194] and separated children from El Salvador, Guatemala, and Honduras.[195] Experts believe the surge is related to push factors that have intensified in recent years, including some of the highest homicide rates in the world, increasing crime and violence due to gangs, drug trafficking and organized crime, extreme poverty, and government corruption.[196] In the spring of 2014, a migration surge of unaccompanied minors captured the attention of the American public. This phenomenon is explored in the Literature Review section below, but it is worthwhile to point out that the increase of Central American migrants –adults, family units, and unaccompanied minors – was identified by Border Patrol statistics and recognized by researchers several years prior to 2014.

Figure 4 shows the percentages of the top ten originating countries as of 2013. After Mexico, the top countries of origin are: India, China (including Hong Kong but not Taiwan), Philippines, Vietnam, El Salvador, Cuba, Korea, Dominican Republic and Guatemala.[197]

Examples of Migrant Surges

Along the land border, some would argue the past four decades of Mexican migration have been an ever-growing 'surge' until the decline and leveling-off beginning in 2007. Most of the ebbs and flows of migration on the southern land border have primarily been related to the economic cycles in both Mexico and the U.S. The recent surge of unaccompanied minors will be discussed in the Literature Review.

Along the Southeast maritime border, Haiti and Cuba historically and currently meet the push factors criteria described above and pose a risk for mass migration into the United States.[198] Both countries are geographically near to the U.S. and have had an ongoing flow of undocumented migrants into the U.S. for years.

- Between 1991 and 1995 over 120,000 migrants from 23 countries were interdicted. Haitian migrants began increased departures after a 1991 coup in Haiti.
- In 1994, the U.S. Coast Guard (USCG) responded to three mass migrations almost simultaneously—first from Haiti, then from Cuba, and again from Haiti—rescuing and preventing over 63,000 migrants attempting to illegally entering the U.S.
- The Dominican Republic has historically been a major source country for undocumented migrants attempting to enter the U.S. crossing the Mona Passage (the body of water between

---

[194] The U.S. Department of Health and Human Services' (HHS) Administration for Children and Families (ACF), Office of Refugee Resettlement (ORR)[194] defines an unaccompanied alien child (UAC) as "one who has no lawful immigration status in the United States: has not attained 18 years of age, and with respect to whom: 1) there is no parent or legal guardian in the United States; or 2) no parent or legal guardian in the United States is available to provide care and physical custody. See http://www.acf.hhs.gov/programs/orr/resource/who-we-serve-unaccompained-alien-children

[195] United Nations High Commissioner for Refugees (UNHCR). (2014). Children on the Run: Unaccompanied Children Leaving Central America and Mexico and the Need for International Protection. P 15. Retrieved from http://www.unhcrwashington.org/sites/default/files/UAC_UNHCR_Children on the Run_Full Report.pdf

[196] Gootnick, D. (2015). Central America: Information on Migration of Unaccompanied Children from El Salvador, Guatemala and Honduras. *Government Accountability Office, GAO-15-362*. Retrieved March 1, 2015, from http://www.gao.gov/products/GAO-15-362

[197] MPI Data Hub (2013). http://www.migrationpolicy.org/programs/data-hub/charts/largest-immigrant-groups-over-time Migration Policy Institute tabulation of data from the U.S. Census Bureau's 2010 and 2013 American Community Surveys, and 2000 Decennial Census. Data for 1960 to 1990 are from Campbell J. Gibson and Emily Lennon, "Historical Census Statistics on the Foreign-Born Population of the United States: 1850 to 1990" (Working Paper No. 29, U.S. Census Bureau, Washington, DC, 1999).

[198] Adapted from U.S. Coast Guard (2013, September 19), *Missions: Maritime Security* [electronic resource], at http://www.uscg.mil/top/missions/MaritimeSecurity.asp, and USCG Office of Law Enforcement (2014, October 31), *Alien Migrant Interdiction* [electronic resource], at http://www.uscg.mil/hq/cg5/cg531/AMIO/amio.asp (retrieved March 2015).

the Dominican Republic and Puerto Rico) to enter Puerto Rico. Thousands of people have taken to sea in a variety of vessels, the most common is a homemade fishing vessel known as a Yola. Most of these migrants are smuggled by highly organized gangs. From April 1, 1995 through October 1, 1997, USCG conducted Operation ABLE RESPONSE, with enhanced operations dedicated to interdicting Dominican migrants. Over 9,500 migrants were interdicted or turned back when they sighted a USCG asset.

- Haiti suffered a devastating earthquake on January 12, 2010. Its effects caused roughly 2 million people to become displaced, 3.5 million people requiring humanitarian aid, and $7.8 billion in damages and losses—a figure that was 120 percent of Haiti's gross domestic product. Due to the lack of in-country resources, the stress on traditional United Nations (UN) Office for the Coordination of Humanitarian Affairs (OCHA) response capabilities, political instability, and the desire to reduce the risk of mass migration to the U.S., the U.S., in coordination with UN OCHA and USAID OFDA, deployed 20,000 civilian and military personnel and provided $1 billion in humanitarian funding in part in order to prevent a mass migration into the U.S. In addition to the unstable environmental conditions, issues such as general lawlessness and disease outbreaks continue to prevail. These health, safety, and security factors can trigger a mass exodus to nearby nations, including the U.S.
- In January 2015, the USCG announced[199] there had been a surge of attempted maritime entries by Cubans. (Customs and Border Protection announced a similar surge at land border crossings and airports). The December 2014 announcement that the U.S. and Cuba were seeking to normalize relations spurred rumors and fears that the long-standing Cuban immigration policy, known as "wet foot/dry foot," may change. This misperception prompted an increase of Cubans attempting entry into the U.S. before any changes in policy could occur.[200],[201]

The Dangerous Journey

Migrants often take great risks and endure significant hardships in their attempts to flee their countries and enter the United States. Individuals attempting to gain unauthorized entry into the U.S experience the vast majority of these dangers.

Of the asylum-seeking and unauthorized entries, the United Nations (UN) estimated that 97 percent enter the U.S. clandestinely through the border with Mexico, and maritime interdictions account for only one percent of the total.[202,203] The increased U.S. border enforcement since the terrorist attacks of September 11, 2001, as well as the increased violence and dangers in the route to the border, appears to have deterred independent border crossers.[204] Increasingly, migrants

[199] http://www.uscgnews.com/go/doc/4007/2442054/

[200] The U.S. Government has repeatedly stated no changes in the immigration policy are expected yet, but that has not seemed to quell the concerns and rumors. See USCG Press Release referenced in previous footnote or statement by DHS Secretary Jeh Johnson here: http://tbo.com/ap/new-ties-with-cuba-wont-change-wet-foot-dry-foot-policy-20141218/

[201] Despite U.S. Government (Executive Branch) statements, some legislators and policy experts have suggested it may be time for changes in the policy. For example, see http://www.migrationpolicy.org/article/normalization-relations-cuba-may-portend-changes-us-immigration-policy

[202] United Nations Office on Drugs and Crime (UNODC) (n.d.) Smuggling of migrants: The harsh search for a better life. Retrieved March 2015, from http://www.unodc.org/toc/en/crimes/migrant-smuggling.html#_ednref1

[203] It is assumed the remaining 2 percent arrive by air, but a source could not be found to validate that assumption.

[204] UNODC (2010).The Globalization of Crime: A Transnational Organized Crime Threat Assessment. P. 62. Retrieved March 2015, from https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf

employ smugglers to help them with the journey.[205] Crossing the border is often done in trucks, sometimes on foot, and there have been cases in which the crossing is made by rail, or even through special tunnels.[206] Air travel using fraudulent visas is the preferred route for those who can afford it.[207]

The sophistication of the smugglers range from that of individual and family-run operations to organized criminal groups. For the smugglers, there appears to be little risk of arrest—if they are caught, they often pretend to be migrants themselves and are repatriated rather than apprehended. In 2010, the estimated amount paid to smugglers per migrant varied from $2,000-3,000[208] for a Mexican-born migrant to $10,000 for non-Mexican-born.[209] The UN Office on Drugs and Crime (UNODC) estimates smuggling into the U.S. is a $6.6 billion a year business.[210] Organized crime syndicates that previously focused on narcotics and contraband flows have been attracted by the higher fees and now incorporate humans into their smuggling networks.[211]

The dangers of the journey to unauthorized entry are multi-faceted and somewhat depend on the route and method of crossing:

- Maritime – Travel by sea is precarious as migrant vessels are often nothing more than homemade rafts or boats. They are usually overloaded and unseaworthy, lack basic safety equipment, and are operated by inexperienced mariners. Most of the U.S. Coast Guard's interdictions begin as search and rescue missions.[212] Alternatively, smugglers often use fast boats to avoid interdiction; however, employing smugglers comes with its own risks (see below).
- La Bestia – As many as half a million Central American migrants annually board freight trains colloquially known as "La Bestia," or the beast, on their journey to the United States. The cargo trains, which run along multiple lines, carry products north for export. As there are no passenger railcars, migrants must ride atop the moving trains, facing physical dangers that range from amputation to death if they fall or are pushed. Accidents caused by train derailments and falls because of changes in speed or migrants falling asleep are common.[213] Migrants get off the train prior to reaching the U.S. border and usually cross on foot. The Mexican Government does not have a comprehensive policy to address the La Bestia phenomena and responses of various Mexican authorities have been "disjointed, uncoordinated, and often in reaction to particular events widely covered in the news."[214]

[205] Rosenblum and Brick (2011). P 13. Rosenblum and Brick estimate 70-90 percent of unauthorized Mexicans now rely on a smuggler to cross the border up from 50 perecent in 1986, and 78 percent in 1993.
[206] UNODC (2010). P 62.
[207] UNODC (2010). P 57.
[208] Rosenblum and Brick (2011). P 13.
[209] UNODC (2010). P 67.
[210] UNODC (2010). P 67. UNODC cites the Mexican Migration Project as the source for this data.
[211] Rosenblum and Brick (2011). P 14.
[212] U.S. Coast Guard (2013, September 19), *Missions: Maritime Security* [electronic resource], at http://www.uscg.mil/top/missions/MaritimeSecurity.asp, and USCG Office of Law Enforcement (2014, October 31), *Alien Migrant Interdiction* [electronic resource], at http://www.uscg.mil/hq/cg5/cg531/AMIO/amio.asp (retrieved March 2015).
[213] Villegas, R. (2014, September 10). Central American Migrants and "La Bestia": The Route, Dangers, and Government Responses. Retrieved March 29, 2015, from http://migrationpolicy.org/article/central-american-migrants-and-la-bestia-route-dangers-and-government-responses
[214] Villegas, R. (2014, September 10).

- Lack of Protection from Governmental Authorities – As migrants journey to their destination, they often transit through other countries, the most prominent example being Mexico. In the past, the governments of those countries turn a blind eye to the migrants transiting illegally through their territory because they know they do not intend to stay in their country. Due to increased U.S. pressure to disrupt the flow of migrants, the Mexican Government has made efforts to "implement new security and surveillance measures with U.S. assistance" along the southern border of Mexico.[215] The challenge is that by increasing enforcement, migrants that are victims of crime at the hands of cartels, gangs and organized crime are less likely to report such crime for fear of deportation. Further, "reputable non-governmental organizations including Amnesty International, Sin Fronteras, and Catholic Relief Services, have documented" cases of abuse of power by Mexican authorities.[216] The Migration Policy Institute asserts that the Mexican Government's response demonstrates "the struggle to simultaneously develop policies that tackle border enforcement, increased security, and the protection of human rights."[217]
- Drug Cartels, Gangs and Organized Crime – On the journey from their home country to the U.S. border, migrants are often subject to extortion, kidnapping, violence, sexual assault, serious injury, or death at the hands gangs and organized-crime groups that control the routes into the U.S.[218,219] The National Human Rights Commission (CNDH), an autonomous institution funded by the Mexican government, reported more than 11,000 abductions of migrants between April and September 2010.[220]
- Smugglers – As described above, increasingly, migrants employ smugglers that promise to get them across the borders and help them navigate the dangers of the wilderness. After they receive payment, smugglers have been known to rob, rape, and even kill their "customers." They also often hold the migrants hostage until final payment is received, usually by the migrants' relatives in the country of origin or the U.S.[221]
- Wilderness – Once across the border, migrants must endure long hikes in stretches of desert. In an effort to avoid apprehension by the U.S. Border Patrol, the routes used are difficult and treacherous. The heat, snakes and wild animals, and a lack of water can lead to injuries,

[215] Villegas, R. (2014, September 10).
[216] Villegas, R. (2014, September 10).
[217] Villegas, R. (2014, September 10).
[218] Papademetriou, D., & Hooper, K. (2014, December 15). Top 10 of 2014 - Issue #3: Border Controls under Challenge: A New Chapter Opens. Retrieved March 2015, from http://migrationpolicy.org/article/top-10-2014-issue-3-border-controls-under-challenge-new-chapter-opens
[219] Just one example: In August 2010, the bodies of 72 people attempting to cross the U.S.-Mexico border illegally were discovered on a remote ranch 90 miles from the U.S. border. The drug gang responsible for the kidnapping and murders, Los Zetas, captured its victims as they traveled through Tamaulipas, presumably on their way to cross the border illegally into the United States. When the 72 people refused to work for the gang, they were executed. David Luhnow, "Mexico Killings Show Migrants' Plight," The Wall Street Journal, August 27, 2010, at http://online.wsj.com/article/SB10001424052748704913704575454033356912888.html (May 23, 2011), and "Source: Investigator in Migrants' Massacre Killed," MSNBC, August 27, 2010, at http://www.msnbc.msn.com/id/38883757/ns/world_news-americas/ (May 23, 2011).
[220] Villegas, R. (2014, September 10).
[221] UNODC (2010). P 62.

dehydration, heat stroke, and death.[222,223] For fiscal year 2014, the U.S. Border Patrol conducted 1,457 rescues and reported 307 known deaths in the Southwest border sectors.[224]

U.S. Government Roles and Missions Related to Mass Migration

The U.S. Government's response to mass migration is multifaceted. The Department of Homeland Security (DHS) has the primary responsibility to secure and manage the U.S. borders. Responsibility for the enforcement of immigration law within DHS rests with USCG, U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and U.S. Citizenship and Immigration Services (USCIS).

USCG,[225] as the United States' primary maritime law enforcement agency and tasked with enforcing immigration law at sea, is the lead organization in the DHS for intercepting migrants at sea. The USCG conducts patrols and coordinates with other Federal agencies and foreign countries to interdict undocumented migrants at sea, if appropriate, denying them entry via maritime routes to the United States, its territories, and possessions.

CBP is generally responsible for immigration enforcement at and between the ports of entry, focusing on preventing drugs, weapons, terrorists and other inadmissible persons from entering the country. The CBP's Office of Air and Marine (OAM) also has a maritime law enforcement mission to detect, interdict, and prevent acts of terrorism and the unlawful movement of people, illegal drugs, and other contraband toward or across U.S. borders. OAM is the world's largest aviation and maritime law enforcement organization, and is a critical component of CBP's layered enforcement strategy for border security.[226]

In general, OAM's law enforcement authorities extend to the U.S. customs waters and land/riverine border environments, while the USCG's law enforcement authorities extend from U.S. waterways and marinas outward into international waters. Both operate marine and air assets. Unlike OAM, the USCG can use its Title 10 authority to operate as a member of the armed services under military chain of command.

ICE is generally responsible for interior enforcement, including detention and removal operations. USCIS is generally responsible for the administration of immigration and naturalization functions.[227]

Outside of DHS, other Federal agencies with missions related to immigration are affected by a surge:

---

[222] Rosenblum and Brick (2011). P 14.

[223] Del Bosque, M., & The Guardian U.S. Interactive Team. (2014, August 6). Beyond the border. The Guardian and The Texas Observer. Retrieved March 1, 2015, from http://www.theguardian.com/world/ng-interactive/2014/aug/06/-sp-texas-border-deadliest-state-undocumented-migrants

[224] U.S. Border Patrol Statistics for FY 2014. http://www.cbp.gov/sites/default/files/documents/USBP%20Stats%20FY2014%20sector%20profile.pdf

[225] Unless otherwise noted, Maritime Portions of the Event Background section were adapted from U.S. Coast Guard (2013, September 19), *Missions: Maritime Security* [electronic resource], at http://www.uscg.mil/top/missions/MaritimeSecurity.asp, and USCG Office of Law Enforcement (2014, October 31), *Alien Migrant Interdiction* [electronic resource], at http://www.uscg.mil/hq/cg5/cg531/AMIO/amio.asp (retrieved March 2015).

[226] U.S. Customs and Border Protection Fact Sheet: Office of Air and Marine, (2013). Accessed March 2015: http://www.cbp.gov/sites/default/files/documents/air_marine_6.pdf

[227] Content for this paragraph adapted from the following DHS website accessed in March 2015: http://www.dhs.gov/publication/immigration-enforcement-actions-2013

- The Executive Office for Immigration Review (EOIR), U.S. Department of Justice adjudicates immigration cases and seeks to fairly, expeditiously, and uniformly interpret and administer the Nation's immigration laws. Under delegated authority from the Attorney General, EOIR conducts immigration court proceedings, appellate reviews, and administrative hearings.[228]
- The Department of State's Bureau of Population, Refugees, and Migration's (PRM)[229] mission is to provide protection, ease suffering, and resolve the plight of persecuted and uprooted people around the world on behalf of the American people by providing life-sustaining assistance, working through multilateral systems to build global partnerships, promoting best practices in humanitarian response, and ensuring that humanitarian principles are thoroughly integrated into U.S. foreign and national security policy. PRM administers the refugee admissions program; it works in partnership with USCIS to review refugee and asylum applications.
- The Department of Health and Human Services' (HHS) Administration for Children and Families (ACF), Office of Refugee Resettlement (ORR)[230] provides refugees the social services they need to become self-sufficient as quickly as possible after their arrival in the U.S. ORR provides benefits and services to assist the resettlement and local integration of specific eligible populations, including refugees; asylees; Cuban/Haitian Entrants; Certified Victims of Trafficking; Iraqi or Afghan Special Immigrants; Amerasians; Lawful Permanent Residents (LPRs) who have held one of those statuses in the past, and in most cases, spouses and unmarried children under 21 of those holding such statuses. The ORR Unaccompanied Alien Children Program provides temporary custody and care to unaccompanied alien children who do not have an immigration status.[231]

U.S. Protection and Response-Related Mass Migration Costs

There is limited knowledge on the immediate response-related[232] costs of mass migration to the host country.

The USCG's National Maritime Strategic Risk Assessment (NMSRA) assessed the economic impact per illegal migrant entry via maritime routes to be $33,000. This is an average value over multiple scenarios varying in magnitude and character, and was developed for the purpose of

[228] http://www.justice.gov/eoir/

[229] http://www.state.gov/j/prm/about/index.htm

[230] http://www.acf.hhs.gov/programs/orr

[231] On March 1, 2003, the Homeland Security Act of 2002, Section 462, transferred responsibilities for the care and placement of unaccompanied children from the Commissioner of the Immigration and Naturalization Service to the Director of the Office of Refugee Resettlement (ORR). Since then, ORR has cared for more than 150,000 children, incorporating child welfare values as well as the principles and provisions established by the Flores Agreement in 1997, the Trafficking Victims Protection Act of 2000 and its reauthorization acts, the William Wilberforce Trafficking Victims Protection Reauthorization Act (TVPRA) of 2005 and 2008. Unaccompanied children apprehended by the Department of Homeland Security (DHS) immigration officials are transferred to the care and custody of ORR. ORR makes and implements placement decisions in the best interests of the child to ensure placement in the least restrictive setting possible while in federal custody. ORR takes into consideration the unique nature of each child's situation and incorporates child welfare principles when making placement, clinical, case management, and release decisions that are in the best interest of the child. Source: HHS, ACF, ORR website. Retrieved April 2015: http://www.acf.hhs.gov/programs/orr/programs/ucs/about

[232] This paper is focused on the protection and response-related responsibilities of the U.S. Government in the instance of a mass migration. There is more literature, and a wide-variety of opinion, on the long-term economic effects of immigration—both legal and illegal. Some believe that the costs for absorbing migrants into the U.S. are high as they take advantage of local, state, Federal, and private non-profit resources available (health services, education, welfare, etc.). Others point out that while there may be an initial drain on taxpayer or charitable services, the immigrants contribute to the economy in varying ways as well.

calculating equivalencies across disparate consequences to inform USCG risk assessments for the purpose of long-range strategic planning and long-term capability investment decisions.[233]

In July 2014, the President requested $3.7 billion in emergency supplemental funding to address the surge of children arriving from Central America countries.[234,235] The request[236] included funding for:

- DHS's ICE and CBP to handle increased protective, investigatory, and enforcement costs, as well as transportation and processing costs for the children,
- DOJ's EOIR for hiring more immigration judge teams in order to expedite case processing and legal representation for the children,
- HHS's ACF/ORR for additional capacity to provide temporary care and custody for unaccompanied children in the least restrictive setting while awaiting their immigration court date, and
- Department of State for repatriation and reintegration of migrants to their home countries and for public diplomacy and international information programs.

DHS's 2016 budget request included increased resources for a comprehensive "Southern Border & Approaches Campaign." The request includes funds for:

- The costs associated with apprehension and care of up to 104,000 unaccompanied children. A portion of these funds will be used to prepare facilities for families and unaccompanied children in the event of a surge that exceeds prior year apprehension levels. The request proposes up to $162 million in contingency obligation authority—enabling CBP and ICE to respond effectively in the event migration volume significantly surpasses prior-year levels.[237]

Literature was not found that consolidates and assesses spending requests and actual spending over multiple fiscal years across Federal agencies.

Literature Review Theme 1 - The Central American "Surge" of Unaccompanied Children

In the spring of 2014, the American public was shocked to learn of the flood of unaccompanied minors at the southwest border. This trend began well before that spring however. The total number of CBP apprehensions of unaccompanied and separated children from El Salvador, Honduras, and Guatemala—collectively known as the Northern Triangle—had doubled each year from FY 2011 to FY 2014[238], reaching a peak of nearly 52,000 children. (When children

---

[233] This assessment was based on the 1992-1994 maritime mass migration from Haiti, and as such is likely not valid for estimating the cost of mass migration at the southwest border.

[234] The White House. (2014, July 8). Fact Sheet: Emergency Supplemental Request to Address the Increase in Child and Adult Migration from Central America in the Rio Grande Valley Areas of the Southwest Border. Retrieved March 2015. https://www.whitehouse.gov/the-press-office/2014/07/08/fact-sheet-emergency-supplemental-request-address-increase-child-and-adu

[235] Congress did not approve the funding request. They approved a significantly lesser amount to address the crisis. DHS reported having to reallocate resources from other parts of the Department in order to address the crisis. Information on specific dollar amounts reallocated or actual costs spent to address the surge were not found.

[236] The White House. (2014, July 8). Emergency Supplemental Budget Request. https://www.whitehouse.gov/sites/default/files/omb/assets/budget_amendments/emergency-supplemental-request-to-congress-07082014.pdf

[237] Written testimony of DHS Secretary Jeh Johnson for a House Committee on Appropriations, Subcommittee on Homeland Security hearing on the President's FY 2016 budget request for the Department of Homeland Security. (2015, March 26). Accessed March 2015: http://www.dhs.gov/news/2015/03/26/written-testimony-dhs-secretary-jeh-johnson-house-appropriations-subcommittee

[238] FY 2011: 3,933; FY 2012:10,146; FY 2013: 20,805 and FY 2014: 51,705. Sourced from CBP Statistics – see next footnote.

from Mexico are included, the number reaches over 67,000.) Early indications are that the migration flows may not be as intense as last year, as of March 31, 2015, the FY 2015 statistics show a 45 percent decline when compared to the same time period in FY 2014.[239] However, the rate of migration is still on pace to be at least as high as FY 2012 or 2013. A survey of literature from the past five years on the broad topic of migration to the U.S. found a significant majority of the literature focused on this topic.

In 2014, the UN's High Commissioner for Refugees (UNHCR) released a study entitled "Children on the Run: Unaccompanied Children Leaving Central America and Mexico and the Need for International Protection."[240] Beginning in 2009, UNHCR, the UN agency responsible for receiving asylum requests, began receiving an increased number from El Salvador, Honduras, and Guatemala.[241] From 2008 – 2013, there was a 712 percent increase in asylum requests from these three countries.[242,243] The study was based on in-depth, individual interviews conducted between May and August 2013, with Northern Triangle and Mexican children that began arriving after the October 2011 surge began. Nearly all of the children were interviewed while in the custody of the HHS's ACF/ORR. The report includes compelling narratives collected from the children describing the dangers and hardships from their homeland. It is primarily focused on the causes for attempting entry into the U.S. It does not collect information on the migration journey to the U.S.

Unique to the UNHCR report is a suggestion that there may also be a crisis with Mexican-born unaccompanied minors. Though the increase from the Northern Triangle is more dramatic, the migration of unaccompanied minors from Mexico has occurred over a longer period of time and outpaced the number of children migrating from any one of the Northern Triangle countries until FY 2014. The policy for Mexican-born persons is different than that for other migrants, and they are usually returned to Mexico within a day or two of apprehension. As a result, it was difficult for researchers to determine who the children were and why they were coming to the U.S.[244]

The UNHCR report found that 58 percent of children arriving from the Northern Triangle and Mexico raise potential international protection[245] needs.[246] The primary cause, at 48 percent, was violence by organized armed criminal actors, including drug cartels and gangs or by state actors.[247] The report examines the findings for each country of origin. El Salvador appears to be

---

[239] CBP Statistics on Southwest Border Unaccompanied Alien Children. Accessed April 2015: http://www.cbp.gov/newsroom/stats/southwest-border-unaccompanied-children

[240] United Nations High Commissioner for Refugees (UNHCR). (2014). Children on the Run: Unaccompanied Children Leaving Central America and Mexico and the Need for International Protection. Retrieved from http://www.unhcrwashington.org/sites/default/files/UAC_UNHCR_Children on the Run_Full Report.pdf

[241] UNHCR (2014). P 15.

[242] UNHCR notes that the U.S. receives the majority of the asylum applications, but Mexico, Panama, Nicaragua, Costa Rica, and Belize also received applications.

[243] These statistics come from the UNHCR's webpage for their report, which appears to provide more recent data than included in the report. See http://www.unhcrwashington.org/children

[244] UNHCR (2014). P 5.

[245] The UNHCR report provides a lengthy explanation of International Protection in its Executive Summary (see page 8). More succinctly, the UNHCR defines International Protection as "The actions by the international community on the basis of international law, aimed at protecting the fundamental rights of a specific category of persons outside their countries of origin, who lack the national protection of their own countries." Source – UNHCR Master Glossary of Terms Rev. 1. (2006, June). Retrieved March 2015: http://www.unhcr.org/cgi-bin/texis/vtx/refworld/rwmain/opendocpdf.pdf?docid=42ce7d444

[246] UNHCR (2014). P 6.

[247] UNHCR (2014). P 6.

the most volatile; 72 percent of the migrant children cases raised potential international protection needs.[248,249]

The study demonstrates that the push factors involved in causing the displacement are complex. Notably, most of its recommendations are focused on what the international community, as well as the receiving countries, should do to address not only the emerging displacement of children from Central America, but also the unique needs the children require in the international protection process. It is a quiet acknowledgement that the international community's ability to fix the violence push factor is limited.

The U.S. Conference of Catholic Bishops (USCCB) issued a Report based on a delegation sent to Central America in November 2013.[250] Consistent with the UNHCR Report, they found that "violence and criminal actors have permeated all aspects of life in Central America and are the primary factors driving the migration of children from the region." They also noted that other "push factors include the absence of economic opportunity, the lack of quality education and access to education generally, and the resulting inability for individuals to financially support themselves and their families in their home countries/local communities; and the desire to reunify with family in the United States."[251,252,253]

These in-depth studies indicated children were encouraged by their family members to flee to the U.S. as a way to escape the violence at home. The UNHCR study was limited to a child's perspective on why they were told to leave home. A limit of the study was the inability to ask the child's parents or guardians why they felt that the journey to the U.S. was a more suitable risk than the risk of staying in their home country. Certainly there is a potential that the explanation a parent gives to a child is simplified.

Other potential causes for the surge include the following:

- Attempting to take advantage of how the U.S. immigration process works, particularly for unaccompanied children from non-contiguous countries (countries other than Mexico and Canada):
    - Non-Mexican and non-Canadian children have a lengthier screening process: New provisions added to the Trafficking Victims Protection Reauthorization Act (TVPRA) in 2008, require that all unaccompanied alien children be screened as potential victims of human trafficking. While children from non-contiguous countries are transferred to HHS for trafficking screening, and placed into formal immigration court removal proceedings, Mexican and Canadian children are screened by CBP for trafficking and, if no signs are reported, returned pursuant to negotiated repatriation agreements. The TVPRA in 2008

[248] UNHCR (2014). P 9.
[249] A finding that a migrant has a need for international protection does not necessarily mean they will be granted refugee status. See P 8 of UNHCR report for a deeper explanation.
[250] Mission to Central America: The Flight of Unaccompanied Children to the United States. Report of the Committee on Migration of the United States Conference of Catholic Bishops. (2013, November). Retrieved March 2015, from http://www.unhcrwashington.org/sites/default/files/UAC_1_USCCB_Mission to Central America_November 2013_English.pdf
[251] U.S. Conference of Catholic Bishops (2013, November).
[252] Gootnick, D. (2015). PP 4-7. GAO's report also agrees with these findings.
[253] See U.S. Conference of Catholic Bishops (2013, November). P 10; and UNHCR (2014). P 13.

also ensured that unaccompanied alien children are exempt from certain limitations on asylum (i.e. a one-year filing deadline, and the standard safe third country limitation).[254]

- The process prioritizes and facilitates reunification with the child's parent or other family members in the U.S., even if they are in the U.S. illegally: The TVPRA directs that unaccompanied children must "be promptly placed in the least restrictive setting that is in the best interest of the child."[255] Further, the settlement agreement in Flores v. Reno, which is binding on the U.S. Government, establishes an order of priority for sponsors with whom children should be placed, except in limited circumstances. The first preference for placement would be with a parent of the child. If a parent is not available, the preference is for placement with the child's legal guardian, and then to various adult family members.[256]
- A misunderstanding exists about the U.S. immigration process particularly for unaccompanied children and those seeking asylum.[257,258] There are accounts of smugglers and organized crime perpetuating misinformation about the process.[259,260] One rumor is the belief that U.S. Immigration laws grant permisos (free passes) to unaccompanied children. Another potential source of misinformation is the Deferred Action for Childhood Arrivals (DACA), a 2012 executive order that allowed some undocumented individuals who previously arrived to the U.S. to remain in the U.S. legally. While the order applied only to children arriving prior to 2007, one theory is that the rumors and misinformation may have encouraged the child-migrant wave.
- A stronger, more sophisticated smuggling infrastructure and network.[261,262]

There is no shortage of studies and perspectives on the surge of Central American unaccompanied minors. Multiple Washington, DC based think tanks have issued reports[263,264,265] and there have been numerous Congressional hearings[266,267,268,269] and GAO and CRS Reports[270],[271] to examine both the causes of as well as the actions taken to address the surge.

---

[254] American Immigration Council. (2014, July). Children in Danger: A Guide to the Humanitarian Challenge at the Border. Retrieved April 2015: http://www.immigrationpolicy.org/special-reports/children-danger-guide-humanitarian-challenge-border

[255] See 8 U.S.C. § 1232(c)(2)(A).

[256] HHS, ACF, ORR's website on Unaccompanied Children's Services. Accessed April 2015: http://www.acf.hhs.gov/programs/orr/programs/ucs/about

[257] Chishti, M., & Hipsman, F. (2014, June 13). Dramatic Surge in the Arrival of Unaccompanied Children Has Deep Roots and No Simple Solutions. Retrieved March 2015, from http://migrationpolicy.org/article/dramatic-surge-arrival-unaccompanied-children-has-deep-roots-and-no-simple-solutions

[258] Gootnick, D. (2015). P 6.

[259] A leaked unclassified//law enforcement sensitive intelligence bulletin from the El Paso Intelligence Center (EPIC)'s Criminal Threats Unit, which is jointly run by the U.S. Drug Enforcement Administration and CBP, made national news in July 2014 for attributing misconceptions of U.S. immigration policy as a key driver to the Central American surge. See: http://www.newsweek.com/leaked-intel-report-immigration-crisis-contains-both-iffy-informative-259598

[260] Renwick, D. (2014, September). The U.S. Child Migrant Influx. Council on Foreign Relations, Washington, DC. Retrieved March 2015: http://www.cfr.org/immigration/us-child-migrant-influx/p33380

[261] Chishti, M., & Hipsman, F. (2014, June 13).

[262] Gootnick, D. (2015). P 5.

[263] Migration Policy Institute – Chishti, M., & Hipsman, F. (2014, June 13).

[264] Renwick, D. (2014, September).

[265] Negroponte, D. (2014, July). The Surge in Unaccompanied Children from Central America: A Humanitarian Crisis at Our Border. The Brookings Institution, Washington, DC. Retrieved March 2015: http://www.brookings.edu/blogs/up-front/posts/2014/07/02-unaccompanied-children-central-america-negroponte

[266] For example, Dangerous Passage: The Growing Problem of Unaccompanied Children Crossing the Border: Hearings before the Committee on Homeland Security, House, 113th Cong. (June 24, 2014). Retrieved March 2015: http://homeland.house.gov/hearing/dangerous-passage-growing-problem-unaccompanied-children-crossing-border

The President declared it a humanitarian crisis and some called it a threat to national security because of the drain on CBP resources (focusing on the unaccompanied children and family units left little room for addressing other potential threats).[272] The response by the U.S. Government to the 2014 surge was unprecedented and leveraged capabilities usually reserved for disaster declarations. The President directed the Federal Emergency Management Administration (FEMA) to lead a Government-wide response to the situation, which included the following activities:[273]

- Diplomatic engagement with Central America and Mexico and providing new financial support to address the root push factors;
- Increased enforcement mechanisms to more quickly conduct removal proceedings for those not eligible for asylum—in the hopes that expedited returns will decrease some of the pull factors;
- Communication campaigns to combat rumors that may have been contributing to the pull factors (e.g., DACA eligibility and permisos); and
- Expanding capacity in the HHS/ACF/ORR nationwide shelter network and standing up temporary shelters on Department of Defense sites staffed by trained ORR grantee staff.

There are early hopes that these efforts appear to have worked. By March 2015, CBP reported a 45 percent decline in the number of unaccompanied minors from the Northern Triangle and Mexico. However most experts have indicated that the complicated confluence of pull and push factors will not be fully resolved in the short term.[274,275,276]

A Brookings Institution assessment suggests that the surge from Central America may be a reaction by criminal organizations to the Mexican Government's crackdown on them (i.e., they are seeking "alternative profitable ventures").[277] Similar to successful legal businesses, criminal organizations adapt to their environment. Thus, to the extent the drivers of the surge are the smugglers and other organized criminals, we should expect that as U.S. policy changes, so too will the behavior of these organizations.

---

[267] An Administration Made Disaster: The South Texas Border Surge of Unaccompanied Alien Minors: Hearings before the Judiciary Committee, House, 113th Cong. (June 25, 2014). Retrieved March 2015: http://judiciary.house.gov/index.cfm/2014/6/hearing-an-administration-made-disaster

[268] Field Hearing: Crisis on the Texas Border: Surge of Unaccompanied Minors, House, 113th Cong. (July 3, 2014). Retrieved March 2015: http://homeland.house.gov/hearing/field-hearing-crisis-texas-border-surge-unaccompanied-minors

[269] Securing the Border: Understanding and Addressing the Root Causes of Central American Migration to the United States: Hearings before the Committee on Homeland Security & Governmental Affairs, Senate, 114th Cong. (March 25, 2015). Retrieved March 2015: http://www.hsgac.senate.gov/hearings/securing-the-border-understanding-and-addressing-the-root-causes-of-central-american-migration-to-the-united-states

[270] Gootnick, D. (2015).

[271] Kandel, W., Bruno, A., Meyer, P., Seelke, C., Taft-Morales, M., Wasem, R. (2014, July). *Unaccompanied Alien Children: Potential Factors Contributing to Recent Immigration*. Congressional Research Service, Washington, DC. Retrieved March 2015: http://fas.org/sgp/crs/homesec/R43628.pdf

[272] Renwick, D. (2014, September 1).

[273] Fact Sheet: Unaccompanied Children from Central America. (2014, June 20). The White House. Retrieved March 2015: https://www.whitehouse.gov/the-press-office/2014/06/20/fact-sheet-unaccompanied-children-central-america

[274] Chishti, M., & Hipsman, F. (2014, June 13).

[275] Testimony of Eric L. Olson, Associate Director, Latin America Program, Woodrow Wilson International Center for Scholars to the Committee on Homeland Security and Governmental Affairs, Senate, 113th Cong. Retrieved March 2015: http://www.wilsoncenter.org/sites/default/files/Eric%20L%20Olson%20testimony%20Senate%20Homeland%20Security%20committee.pdf

[276] Negroponte, D. (2014, July).

[277] Negroponte, D. (2014, July).

Some suggest that we are already seeing examples of such adaptability. Papedemetriou and Hooper of the Migration Policy Institute assert that though the U.S. and other European countries have strengthened and take seriously their border security, the system is continually tested by "increasingly creative entry strategies."[278] A relatively new trend is for migrants to make no effort to avoid border patrol; instead they would actually present themselves for apprehension and processing. While some migrants do this because they believe they have a legitimate request for asylum, other migrants without such claims believe that the system will take so long to process them that they will be allowed to stay for at least several years. Because the migration flow is "mixed"—inclusive of asylum seekers as well as economic and family-stream migrants—it is harder for authorities to process and discern which migrants have legitimate claims for asylum. For such a trend to occur, the smugglers must be advising their 'clients' that this is the best approach given the current strength of border security.

Literature Review Theme 2 – Push Factors are Intensifying and are Likely to Increase the Frequency of Surges

Conflict-Related Push Factors

The number of refugees, asylum-seekers and internally displaced people (collectively, forced displacement) worldwide exceeded 50 million people in 2014 – the highest level since the post-World War II era – according to the UNHCR's Global Trends Report for 2013.[279] Half of forcibly displaced people are children, the highest figure in a decade.[280] The war in Syria is the main cause of the massive increase: at the end of 2013, the conflict had led to 2.5 million refugees and rendered 6.5 million internally displaced.[281] In November 2014, the UN High Commissioner for Refugees called it a "mega-crisis".[282] The Migration Policy Institute (MPI) extrapolates that the numbers for 2014 will show an even greater increase due to the rise of the jihadist group Islamic State in Iraq and Syria (ISIS) and the ensuing sectarian violence that forced many Iraqis to flee.[283]

Papademetriou and Hooper reviewed the current state of border security and the challenges posed by migration in a December 2014 assessment that summarized the global trends from the past year. They view the "demand for humanitarian protection" as a significant and growing push factor.[284] The wars and conflicts in Syria, Iraq, Pakistan, Afghanistan, Ukraine, and more recently Yemen, and "a constellation of unstable states in sub-Saharan Africa, and in Central America, have outpaced the ability and political willingness of neighbors in the region and the broader international community to offer meaningful protection to all, let alone resettlement opportunities, pushing many to embark on precarious voyages." Papademetriou and Hooper

[278] Papademetriou, D. and Hooper, K. (2014, December).
[279] World Refugee Day: Global forced displacement tops 50 million for first time in post-World War II era. (2014, June 20). Retrieved March 30, 2015, from http://www.unhcr.org/53a155bc6.html
[280] UNHCR Global Trends 2013: War's Human Cost. (2014, June 1). P 3. Retrieved March 2015, from http://www.unhcr.org/5399a14f9.html
[281] World Refugee Day: Global forced displacement tops 50 million for first time in post-World War II era. (2014, June 20). Retrieved March 30, 2015, from http://www.unhcr.org/53a155bc6.html
[282] http://www.washingtonpost.com/world/national-security/refugee-wave-from-syria-and-iraq-now-a-mega-crisis-un-official-says/2014/11/17/ebc5ee50-6eab-11e4-893f-86bd390a3340_story.html
[283] Esthimer, Marissa. (2014, December). Top 10 of 2014 – Issue #1: World Confronts Largest Humanitarian Crisis since WWII. Migration Policy Institute, Washington, DC. March 2015, from http://migrationpolicy.org/article/top-10-2014-issue-1-world-confronts-largest-humanitarian-crisis-wwii
[284] Papademetriou, D. and Hooper, K. (2014, December).

conclude that the push and pull factors causing mixed migration flows to the United States will not abate.

Globalization, Technology, and Climate Change

Beyond the war and conflict-related push factors, scholars have identified other global trends that are impacting and may increase migration flows. Rey Koslowski's essay, "Economic Globalization, Human Smuggling, and Global Governance" explains that the drivers of globalization—rapidly advancing information, communication and transportation technologies—are "propelling international migration and fostering transnational crime."[285] As noted above, smugglers now facilitate upwards of 90 percent of U.S. border crossings. Local or national crime groups have expanded to become global criminal syndicates.[286] The expansion (much like that of global business except that legal businesses deals in legal commodities) is in response to expanding markets for illegal commodities.[287] For example, the cost of human smuggling across the U.S. border has increased dramatically since border security was strengthened post-9/11, and organized crime and smugglers have tapped into that 'market' to provide a 'service.'

Technology assists another structural factor—social networks. Historically, social networks are those that "connect migrants to host-state jobs and communities of co-nationals typically from the same village and area."[288] Rosenblum and Brick point out that social networks are a particularly important factor for migrants from Mexico and Central America. Other than small references, primarily from interviews of migrants by journalists, it does not appear that the current literature has evaluated the role of technology in facilitating the social network factor. Several news reports covering the Central American surge in 2014, cited instances of migrants leveraging social networking—in the technological variety (e.g., Facebook)—to prepare for the journey. U.S.-based families or the migrant in his country of origin are able to more easily connect with potential smugglers, coordinate the best migration route, and facilitate payment. Additionally, rapid communication capabilities may lead to "sudden" surges. What previously may have taken a few months or years to build as a trend can occur much more quickly.

Finally, there is a growing set of research that asserts that climate change is likely to increase international migrations. In July 2014, Madeline Messick and Claire Bergeron surveyed recent events and unclassified National Intelligence Estimates and determined the demand for Temporary Protected Status (TPS)[289] is likely to grow for reasons beyond war and conflict:

> As the world adjusts to climate change, scientists predict that the number of severe weather events—such as floods, droughts, hurricanes, tornadoes, and wildfires—will increase, forcing more people to migrate. In 2012 alone, an estimated 29 million people

[285] Koslowski, R. (2011). Economic Globalization, Human Smuggling, and Global Governance. P. 60. An essay published as Chapter 2 of "Global Human Smuggling: Comparative Perspective" edited by Kyle, D. and Koslowski, R. JHU Press (2011).
[286] Koslowski, R. (2011). P 63.
[287] Koslowski, R. (2011). P 63.
[288] Rosenblum and Brick. (2011). P 2.
[289] Since 1990, U.S. humanitarian relief has been granted to persons from certain countries suffering from wars, violence or natural disaster in the form of Temporary Protected Status (TPS). It is estimated 340,000 people currently hold TPS status. TPS is not a grant of permanent legal status in the United States. Recipients do not receive lawful permanent residence (a "green card"), nor are they eligible, based on their TPS status, to apply for permanent residence or for U.S. citizenship. Rather, TPS beneficiaries receive provisional protection against deportation and permission to work in the United States for a limited period of time. The United States can end a country's TPS designation once it has recovered from the triggering event. See USCIS' page on TPS at <http://www.uscis.gov/humanitarian/temporary-protected-status-deferred-enforced-departure/temporary-protected-status>. Also, see 8 U.S.C.§1254a. Temporary Protected Status at: <http://www.gpo.gov/fdsys/pkg/USCODE-2011-title8/pdf/USCODE-2011-title8-chap12-subchapII-partV-sec1254a.pdf>

> were displaced by extreme weather events. National intelligence estimates prepared by the U.S. intelligence community have predicted that changing weather patterns could contribute to political instability, disputes over resources, and mass migration.[290]

In a study that explores the methodologies for assessing environment-migration relationships, Fussell, Hunter, and Gray show that scholars and the policy community believe climate change will impact future migration.[291] They assert "most scholars in the field reject the deterministic view that directly links climate change to mass migration," instead recognizing the linkages are complex. The study does not provide any predictions on how climate change may affect migration, but lays out suggested steps that can be taken to further advance the "scientific knowledge of environment-migration relationships and their implications for their future."

Conclusion

The perspectives from which to evaluate the risk of mass migration to the U.S. are numerous and diverse. The volume of potential literature inhibits the ability to gain a completely thorough understanding of the current research from all possible angles and disciplines. In selecting the literature for this review, we attempted to identify common themes and areas most relevant to risk assessment purposes.

This survey of recent surge events and the literature review indicate there is a strong likelihood of future surges to the U.S. Such surges are caused by complex structural factors that render 'quick solutions' unlikely.

Globalization, complete with cheaper access to technology, communication, and travel, will continue to lower the barriers to migration, and enable growth of the human smuggling "business."

Further, the literature reviewed indicated that push factors are increasing, and that "tipping point" incidents—incidents that push the individual to migrate—are likely to increase and be more difficult to contain. Such tipping point incidents may include those caused by climate change, which creates more frequent and severe natural disasters, or by armed conflicts such as the recent coups, civil wars, and terrorist group territorial takeovers.

There were notable limitations in the literature as well. Other than the USCG's National Maritime Strategic Risk Assessment, which was focused solely on maritime mass migrations, publicly available literature did not provide statistics or estimates on the total protection and response-related costs per migrant, or in the case of the Central American surge, per child. More evaluation is needed to understand the economic impact of protection and response actions in a mass migration. Reviewing the most recent Central American surge could provide useful insight into costs. However, it would be applicable only to child migrants, as the processes used for unaccompanied children are different than that of apprehended adults and family units.

---

[290] Messick, M. and Bergeron, C. (2014, July). *Temporary Protected Status in the United States: A Grant of Humanitarian Relief that is Less than Permanent.* Migration Policy Institute, Washington, DC. Retrieved March 2015: http://www.migrationpolicy.org/article/temporary-protected-status-united-states-grant-humanitarian-relief-less-permanent

[291] Fussell, E., Hunter, L., and Gray, H. (2014). *Measuring the Environmental Dimensions of Human Migration: The Demographer's Toolkit*. Global Environmental Change (Impact Factor: 6). 28:182–191.

The literature reviewed did not provide an assessment of the U.S. Government's capabilities and responses to the 2014 surge, perhaps because the events are so recent as to render a complete assessment premature. To the extent the literature assessed the U.S. Government's actions, it tended to focus on policies and steady-state operations, not on the surge response.

One final limitation is that the literature reviewed mentioned, but did not evaluate in-depth, the possibility that the U.S. Government's response to migrants contributes to the mass migration problem. While there are a number of political commentators in recent years that have argued this case, due to bias, they were not considered as part of the literature review. Academic research is needed to evaluate whether the U.S. Government's programmatic service delivery is a potential Pull Factor and if so, how significant of a role does it play in mass migration scenarios.

Until recently, the U.S. Government's experience with migrant surges was primarily related to Haitian and Cuban migrants attempting maritime entries over the past three decades. Lessons learned from the recent Central American surge (2011-2015) should be reviewed. Further research and consideration should be given to how the U.S. Government's capabilities can be made more flexible, resilient, and comprehensive to address what many scholars believe will be a likely increase in U.S. mass migration surges.

References

Chishti, M., & Hipsman, F. (2014, June 13). Dramatic Surge in the Arrival of Unaccompanied Children Has Deep Roots and No Simple Solutions. Retrieved March 2015, from http://migrationpolicy.org/article/dramatic-surge-arrival-unaccompanied-children-has-deep-roots-and-no-simple-solutions

Esthimer, Marissa. (2014, December). Top 10 of 2014 – Issue #1: World Confronts Largest Humanitarian Crisis since WWII. Migration Policy Institute, Washington, DC. March 2015, from http://migrationpolicy.org/article/top-10-2014-issue-1-world-confronts-largest-humanitarian-crisis-wwii

Fussell, E., Hunter, L., and Gray, H. (2014). Measuring the Environmental Dimensions of Human Migration: The Demographer's Toolkit. Global Environmental Change (Impact Factor: 6). 28:182–191.

Gootnick, D. (2015). Central America: Information on Migration of Unaccompanied Children from El Salvador, Guatemala and Honduras. *Government Accountability Office, GAO-15-362*. Retrieved March 1, 2015, from http://www.gao.gov/products/GAO-15-362

Grieco, E., Trevelyan, E., Larsen, L., Acosta, Y., Gambino, C., De la Cruz, P., . . . Walters, N. (2012). The Size, Place of Birth, and Geographic Distribution of the Foreign-Born Population in the United States: 1960 to 2010. *Working Paper no. 96, Population Division, U.S. Census Bureau, Washington, DC.*

Kandel, W., Bruno, A., Meyer, P., Seelke, C., Taft-Morales, M., Wasem, R. (2014, July). *Unaccompanied Alien Children: Potential Factors Contributing to Recent Immigration.* Congressional Research Service, Washington, DC. Retrieved March 2015: http://fas.org/sgp/crs/homesec/R43628.pdf

Koslowski, R. (2011). Economic Globalization, Human Smuggling, and Global Governance. P. 60. An essay published as Chapter 2 of "Global Human Smuggling: Comparative Perspective" edited by Kyle, D. and Koslowski, R. JHU Press (2011).

Messick, M. and Bergeron, C. (2014, July). Temporary Protected Status in the United States: A Grant of Humanitarian Relief that is Less than Permanent. Migration Policy Institute, Washington, DC. Retrieved March 2015:

Negroponte, D. (2014, July). The Surge in Unaccompanied Children from Central America: A Humanitarian Crisis at Our Border. The Brookings Institution, Washington, DC. Retrieved March 2015: http://www.brookings.edu/blogs/up-front/posts/2014/07/02-unaccompanied-children-central-america-negroponte

Papademetriou, D., & Hooper, K. (2014, December 15). *Top 10 of 2014 - Issue #3: Border Controls under Challenge: A New Chapter Opens.* Washington, DC: Migration Policy Institute. Retrieved March 30, 2015, from http://migrationpolicy.org/article/top-10-2014-issue-3-border-controls-under-challenge-new-chapter-opens

Passel, Jeffrey S. and D'Vera Cohn. (2014, November). "Unauthorized Immigrant Totals Rise in 7 States, Fall in 14: Decline in Those From Mexico Fuels Most State Decreases." Washington, D.C. Pew Research Center's Hispanic Trends Project. Retrieved March 2015, http://www.pewhispanic.org/files/2014/11/2014-11-18_unauthorized-immigration.pdf

Renwick, D. (2014, September). The U.S. Child Migrant Influx. Council on Foreign Relations, Washington, DC. Retrieved March 2015: http://www.cfr.org/immigration/us-child-migrant-influx/p33380

Rosenblum, Marc R. and Kate Brick. 2011. *U.S. Immigration Policy and Mexican/Central Migration Flows: Then and Now.* Washington, DC: Migration Policy Institute.

United Nations High Commissioner for Refugees (UNHCR). 2014. *Children on the Run: Unaccompanied Children Leaving Central America and Mexico and the Need for International Protection*. Washington, D.C. Retrieved from http://www.unhcrwashington.org/sites/default/files/UAC_UNHCR_Children on the Run_Full Report.pdf

United States Conference of Catholic Bishops. (2013, November). *Report of the Committee on Migration: Mission to Central America: The Flight of Unaccompanied Children to the United States.* (2013, November). Retrieved March 2015, from http://www.unhcrwashington.org/sites/default/files/UAC_1_USCCB_Mission to Central America_November 2013_English.pdf

Villegas, R. (2014, September 10). Central American Migrants and "La Bestia": The Route, Dangers, and Government Responses. Retrieved March 29, 2015, from http://migrationpolicy.org/article/central-american-migrants-and-la-bestia-route-dangers-and-government-responses

Literature Review: Industrial Accident (Explosion/Fire)

Synopsis

This qualitative risk assessment of the Industrial Accident-Explosion/Fire hazard suggests that the risk of such incidents occurring is likely holding steady. It primarily assesses the risk of an Industrial Accident-Explosion/Fire, of any size, occurring. Accidents that are so catastrophic as to require Federal support in its response are a small percentage of the overall occurrence of an Industrial Accident-Explosion/Fire event. However, new technologies and emerging risks may create more complex disasters that require more complex preventive measures and responses; and we may see an increase in frequency of requests for Federal assistance in response to Industrial Accident-Explosion/Fire incidents.

Within the scientific literature reviewed, new methodologies are being developed to better understand the domino effects of industrial explosions as well as the emerging risk of incidents triggered by natural hazards, which are called by the European Commission NaTech[292] disasters. Such methodologies should allow Federal, state, and local planners to better evaluate risks and enact prevention and protection mechanisms to reduce the risk, or at least the impact, of explosions in the future.

During the review of a draft of this paper, the Department of Labor's Occupational Safety and Health Administration identified additional sources of literature[293] which address the multi-causal nature of major industrial accidents, and provide quantitative and semi-quantitative risk assessment tools. A limitation of this literature review was the inability to access and review these sources within the time constraints of the project. Future iterations of the SNRA should review these sources.

Several recent incident reports were reviewed, and the literature suggests that more needs to be done to reduce the risks of Industrial Accidents-Explosions/Fires. Current efforts in the Executive and Legislative branches may result in significant changes in the regulation landscape for the first time in decades. If proponents are correct, implementation will reduce risks of industrial accidents. It is too early to tell whether such changes will be enacted or what their ultimate effect on risk reduction will be.

Literature Review – Industrial Accident-Explosion/Fire

Introduction

Event Description

Industrial Accident-Explosion/Fire[294] is a technological accident of an industrial nature, involving an industrial site or production facility (e.g., factories), that results in an explosion and/or fire.[295,296,297,298]

---

[292] Natural Hazard Triggering Technological Disasters (NaTech)

[293] The Occupational Safety and Health Administration recommended reviewing publications by the Center for Chemical Process Safety (CCPS), which can be found at http://www.wiley.com/WileyCDA/Section/id-291237.html

[294] This paper was originally developed with a scope of Industrial Accident-Explosion. Based on feedback provided during review of the drafts of this working paper, Fire was added to the scope because there have been many incidents where the investigations could not determine whether

Event Background

Explosions[299]

The National Fire Protection Association (NFPA) asserts that historically the term explosion has been difficult to define precisely.[300] Depending on the focus of the standard, NFPA uses different definitions for an explosion. The broader definition is the sudden conversion of potential energy (chemical or mechanical) into kinetic energy with the production and release of gases under pressure, or the release of gas under pressure. These high-pressure gases then do mechanical work such as moving, changing, or shattering nearby materials.[301,302]

Within that broad definition, there are two major types of explosions: mechanical and chemical.[303] Sub-types of these explosions are differentiated by the source or mechanism by which the blast overpressure is produced.[304]

- Mechanical Explosion: The rupture of a closed container, cylinder, tank, boiler, or similar storage vessel resulting in the release of pressurized gas or vapor. The pressure within the confining container, structure, or vessel is not due to a chemical reaction or change in chemical composition of the substances in the container.[305]
    - The most common sub-type of mechanical explosion is known as a BLEVE—boiling liquid expanding vapor explosion. These are explosions involving vessels that contain liquids under pressure at temperatures above their atmospheric boiling points. The liquid need not be flammable. A BLEVE can occur in vessels as small as disposable lighters or aerosol cans and as large as tank cars or industrial storage tanks. While the initiating event can be caused by vessel failure, the explosion and overpressure associated with a BLEVE is due to expansion of pressurized gas or vapor in the ullage (vapor space) combined with the rapidly boiling liquid liberating vapor.[306]

---

the incident was a flash fire or explosion. Future SNRA iterations on this topic should study the fire aspects of this risk, as most of the literature reviewed for this paper was primarily focused on explosions.

[295] For purposes of coordinating with the Strategic National Risk Assessment's (SNRA) Quantitative Analysis, the categorization of this topic is based on the EM-DAT's categorization and sub-typing. Since a Qualitative Assessment does not require comparison of numbers across the spectrum of potential disasters, the threshold used by the EM-DAT (e.g., 10 or more reported fatalities) is not included in this scope to allow for a more nuanced understanding of the risk posed to the U.S. by Industrial Accidents-Explosion and Fire.

[296] EM-DAT: The OFDA/CRED International Disaster Database – www.emdat.be, Université Catholique de Louvain, Brussels (Belgium) [official citation]. EM-DAT is maintained by the Centre for Research on the Epidemiology of Disasters (CRED) at the School of Public Health of the Université Catholique de Louvain located in Brussels, Belgium (http://www.emdat.be/frequently-asked-questions), and is supported by the Office of US Foreign Disaster Assistance (OFDA) of USAID (http://transition.usaid.gov/our_work/humanitarian_assistance/disaster_assistance/).

[297] The EM-DAT's other types of industrial accidents are chemical spill, collapse, fire, gas leak, poisoning, radiation, and other.

[298] Explosions caused by terrorism attacks, armed assault, nuclear weapons, pipeline failures, and combustible/flammable rail cargo incidents are addressed by separate SNRA topical assessments and are outside the scope of this assessment.

[299] This section is based on the definitions for the various explosions discussed in NFPA Standard 921, 2014, *Guide for Fire and Explosion Investigations.* National Fire Protection Association, Quincy, MA. See Chapter 23 "Explosions". Accessed March 2015: http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=921

[300] NFPA Standard 921, 2014, *Guide for Fire and Explosion Investigations.* National Fire Protection Association, Quincy, MA. P. 921-215. Accessed March 2015: http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=921

[301] A definition for "explosion" was not found in the EM-DAT's glossary.

[302] NFPA. "NFPA Glossary of Terms: 2014 Edition". (2014, September). See "Explosion" Definition for Document 921 (2014). Retrieved March 2015: http://www.nfpa.org/got

[303] NFPA Standard 921 (2014). P. 921-215.

[304] NFPA Standard 921 (2014). P. 921-215.

[305] NFPA Standard 921 (2014). P. 921-215. See section 23.2.1 Mechanical Explosions.

[306] This paragraph is a summary of NFPA Standard 921 (2014). P. 921-215-216. See section 23.2.2 BLEVEs and all sub-sections.

- Chemical Explosion: The generation of overpressure is a result of exothermic reactions wherein the fundamental chemical nature of the fuel is changed. Chemical reactions of the type involved in an explosion usually propagate in a reaction front away from the point of initiation.[307]
    - The most common sub-type of chemical explosion is the combustion explosion, caused by the burning of combustible hydrocarbon fuels, and frequently characterized by the presence of a fuel with air as an oxidizer. A combustion explosion may also involve dusts. In combustion explosions, overpressures are caused by the rapid volume production of heated combustion products as the fuel burns. [308]

Combustion explosions are classified as either deflagrations (sub-sonic blast pressure wave) or detonations (blast pressure wave propagates at a velocity faster than the speed of sound). Several sub-types of combustion explosions can be classified according to the types of fuels involved. The most common are flammable gases, vapors of ignitable liquids, combustible dusts, smoke and flammable products of incomplete combustion (backdraft explosions), and aerosols.[309]

Industries Commonly Affected by Industrial Accident-Explosion/Fire

Industries affected by Industrial Accident-Explosion/Fire are wide and varied, including the following examples:[310]

- Chemical manufacturing
- Oil and gas industry—drilling and refineries
- Grain-handling
- Coal mines
- Lumber and wood products
- Food product
- Metal
- Plastic

Table 14: Table of Large Scale Industrial-Accident Explosions from 1989-2013[311]

Start	Location	Plant Name	Killed	Injured	Cause
10/23/1989[312, 313, 314]	Pasadena, Texas	Phillips 66 Company polyethylene plant	23	314	Instantaneous release of >85,000 lbm of flammable material to the atmosphere that ignited during routine maintenance.

[307] NFPA Standard 921 (2014). P. 921-216. See section 23.2.3 Chemical Explosions.
[308] NFPA Standard 921 (2014). P. 921-216. See section 23.2.3 Chemical Explosions.
[309] This paragraph is a summary of NFPA Standard 921 (2014). P. 921-216. See 23.2.3.1 Combustion Explosions and all sub-sections.
[310] List of industries pulled from The Chemical Safety and Hazard Investigation Board. Combustible Dust Hazard Study. Report No. 2006-H-1 (2006, November). Retrieved March 2015, from http://www.csb.gov/assets/1/19/Dust_Final_Report_Website_11-17-06.pdf.
[311] Incidents were identified from EM-DAT, CSB Reports, and Subject-Matter Experts who reviewed drafts of this paper. This table is not exhaustive. It is intended to provide the reader a broad overview of major events involving explosions at industrial sites over the past 25 years. See footnotes for each event for the specific citations for the details listed for each incident.
[312] U.S. Department of Labor, OSHA, September 24, 1991, Federal Register #56:48133.

Start	Location	Plant Name	Killed	Injured	Cause
07/05/1990[315]	Channelview, Texas	Atlantic Richfield Company (ARCO) petrochemical plant	17		Failed oxygen analyzer allowing excessive oxygen in a vapor space of a wastewater storage tank causing an explosion.
09/03/1991[316]	Hamlet, North Carolina	Imperial Foods processing plant	25	54	Failure in a hydraulic line that powered a conveyor belt supplying the deep fat fryer vat spewing hydraulic fluid onto the vat gas-fired burners. Contributing to the deaths was the locked shut fire doors that prevented workers from escaping the fire.
09/10/1997[317]	Columbus, Ohio	Georgia-Pacific Resin plant	1	4	Explosion may have been triggered by adding all the ingredients to the resin kettle (reactor) at one time instead of sequentially.
09/23/2001[318]	Brookwood, Alabama	Jim Walter Resources #5 Coal Mine, Blue Creek coal seam	13	3	The first explosion most likely caused by a scoop battery that was damaged by a roof fall that short circuited and ignited methane gas. This was followed by a more powerful second explosion 55 min. later.
02/28/2004[319, 320]	50 miles off Virginia coast	MT Bow Mariner, Owner: Odfjell ASA of Bergen, Norway; Operator: Ceres Hellenic Shipping Enterprises Ltd. Of Piraeus, Greece	21	6	Ignition of a fuel/air mixture either on deck or in the cargo tanks, that was within its flammable limits. Ignition source could not be precisely determined.
03/23/2005[321]	Texas City, Texas	British Petroleum Texas City Refinery	15	180	Raffinate splitter tower was overfilled; pressure relief devices opened, resulting in a flammable liquid geyser from a blowdown stack that was not equipped with a flare. This release led to an explosion and fire.
01/02/2006[322]	Tallmansville, West Virginia	Wolf Run Mining Company, Sago Mine	12	1	Lightning strikes observed in the area at the time of the explosion. Lightning most likely ignition source that caused the accumulated methane behind a sealed section of the mine to ignite and explode. All other possible ignition sources discounted.

[313] Explosion and Fire at the Phillips Company Houston Chemical Complex, Pasadena, Texas, Chemical Engineering Department, Texas Tech University, Lubbock, Texas 79409.

[314] U.S. Fire Administration/Technical Report Series, Phillips Petroleum Chemical Plant Explosion and Fire, Pasadena, Texas; USFA-TR-035/October 1989.

[315] ARCO Spells Out Cause of Channelview Blast, Oil& Gas Journal, Vol. 89, Issue 2; January 14, 1991.

[316] U.S. Fire Administration/Technical Report Series, Chicken Processing Plant Fires, Hamlet, North Carolina and North Little Rock, Arkansas; USFA-TR-057/June/September 1991.

[317] The Liaisons, Booth et al. v. Georgia Pacific Resins, Inc.; Final Report of Liaison's Investigation Georgia-Pacific Resins, Inc., Columbus, Ohio; October 2005.

[318] United Mine Workers of America Report: Jim Walter Resources #5 Coal Mine Disaster.

[319] United States Coast Guard Investigation Into The Explosion And Sinking Of The Chemical Tanker Bow Mariner In The Atlantic Ocean On February 28, 2004 With Loss Of Life And Pollution; December 14, 2005.

[320] Tanker carrying ethanol explodes, then sinks off Virginia, claiming 21 lives, six rescued. Professional Mariner, February 2007.

[321] Investigation Report Refinery Explosion and Fire BP Texas City March 23, 2005; U.S. Chemical Safety and Hazard Investigation Board; Report No. 2005-04-I-TX, March 2007.

[322] Report of Investigation Fatal Underground Coal Mine Explosion January 2, 2006, Sago Mine, Wolf Run Mining Company, Tallmansville, Upshur County, West Virginia; U.S. Mine Safety and Health Administration, Coal Mine Safety and Health; ID No. 46-08791, May 9, 2007.

Start	Location	Plant Name	Killed	Injured	Cause
02/07/2008[323]	Port Wentworth, GA	Imperial Sugar Company, Manufacturing Facility and Sugar Refinery	14	38	The recently installed steel cover panels on the belt conveyor allowed explosive concentrations of sugar dust to accumulate inside the enclosure. An unknown source ignited the sugar dust, causing a violent explosion. The explosion lofted sugar dust that had accumulated on the floors and elevated horizontal surfaces, propagating more dust explosions and fires throughout the buildings and fires. The pressure waves from the explosions heaved thick concrete floors and collapsed brick walls, blocking stairwell and other exit routes.
04/20/2010[324]	Mississippi Canyon Block #252, Gulf of Mexico	British Petroleum, Macondo Well, Deepwater Horizon Rig	11	17	Well blowout during the mothballing of the well resulting in hydrocarbon fluid under pressure rising to the drilling platform contacting with an ignition source resulting in an explosion and fire.
04/05/2010[325]	Montcoal, West Virginia	Performance Coal Company/Massey Energy, Upper Big Branch Mine-South	29	2	Accumulated methane ignited by longwall shearer causing a massive coal dust explosion.
1/31/2011[326]	Gallatin, TN	Hoeganaes Corp – produces atomized steel and iron powders	5	3	Two Iron Dust (Combustible Dust) Flash Fires and One Hydrogen Explosion which also resulted in iron dust flash fires.
3/21/2011[327]	Louisville, KY	Carbide Industries – produces calcium carbide	2	2	Electric Arc Furnace Explosion
10/09/2012[328]	East Rutherford, NJ	US Ink	0	7	Combustible Dust Flash Fires and Explosion
04/17/2013[329, 330]	West, TX	West Fertilizer Storage and Distribution Facility[331]	15	~200	Fire in wooden warehouse where approximately 20-30 tons of Ammonium Nitrate were stored. CSB and ATF investigations are still pending, but it is believed that the explosion yield was less than 30 tons.[332] 200 homes damaged or destroyed, nursing home, 2 schools, and an apartment complex were demolished. Estimates that damages are $230 million.

[323] U.S. Chemical Safety and Hazard Investigation Board. "Investigation Report: Sugar Dust Explosion and Fire, Imperial Sugar Company" Report No. 2008-05-I-GA. September 2009. Retrieved May 2015: http://www.csb.gov/assets/1/19/Tanks_Safety_Study_FINAL.pdf.http://www.csb.gov/assets/1/19/Imperial_Sugar_Report_Final_updated.pdf

[324] Investigation Report Volume 1 Explosion and Fire at the Macondo Well Deepwater Horizon Rig, Mississippi Canyon Block #252, Gulf of Mexico, April 20, 2010; U.S. Chemical Safety and Hazard Investigation Board; Report No. 2010-10-I-OS, June 6, 2014.

[325] Report of Investigation Fatal Underground Mine Explosion, April 5, 2010, Upper Big Branch Mine-South, Performance Coal Company, Montcoal, Raleigh County, West Virginia; U.S. Mine Safety and Health Administration, Coal Mine Safety and Health; ID. No. 46-08436.

[326] U.S. Chemical Safety and Hazard Investigation Board. "Case Study: Hoeganaes Corporation: Gallatin, TN Metal Dust Flash Fires and Hydrogen Explosion". Report No. 2011-4-I-TN. December 2011. Accessed April 2015: http://www.csb.gov/assets/1/19/CSB_Case_Study_Hoeganaes_Feb3_300-1.pdf

[327] http://www.csb.gov/assets/1/19/Final_Report_small.pdf.

[328] U.S. Chemical Safety and Hazard Investigation Board. ""Board Voting Copy of Case Study: Ink Dust Explosion and Flash Fires in East Rutherford, New Jersey" Report No. 2013-01-I-NJ. January 2015. Accessed April 2015: http://www.csb.gov/assets/1/19/US_Ink_Case_Study_Draft__Board_Vote_Final_RevI.pdf

[329] Accessed April 2015: http://www.csb.gov/assets/1/19/West_Preliminary_Findings.pdf.

[330] Texas State Fire Marshal's Office. "Firefighter Fatality Investigation: Abbott Volunteer Fire Department, Bruceville-Eddy Volunteer Fire Department . . .". Investigation FFF FY 13-06. May 2014. Accessed May 2015: http://www.tdi.texas.gov/reports/fire/documents/fmloddwest.pdf

[331] http://www.nfpa.org/newsandpublications/nfpa-journal/2014/march-april-2014/features/nfpa-400.

[332] OSHA subject-matter experts.

Start	Location	Plant Name	Killed	Injured	Cause
6/13/2013	Geismar, LA	Williams Olefins Petrochemical Plant Explosion and Fire	2	114[333]	Still under CSB investigation: Equipment Failure. "Catastrophic failure involving a heat exchanger and associated piping which broke loose from a distillation tower."[334]

Federal Government Roles

The **U.S. Chemical Safety Board (CSB)**[335] is an independent Federal agency charged with investigating industrial chemical accidents. Headquartered in Washington, DC, the agency's board members are appointed by the President and confirmed by the Senate. The CSB conducts root cause investigations of chemical accidents at fixed industrial facilities. Root causes are usually deficiencies in safety management systems, but can be any factor that would have prevented the accident if that factor had not occurred. Other accident causes often involve equipment failures, human error, unforeseen chemical reactions, or other hazards. The agency does not issue fines or citations, but does make recommendations to plants, regulatory agencies such as the Occupational Safety and Health Administration (OSHA) and the Environmental Protection Agency (EPA), state and local governments, industry organizations, and labor groups. Congress designed the CSB to be non-regulatory and independent of other agencies so its investigations might, where appropriate, review the effectiveness of regulations and regulatory enforcement.

The **Occupational Safety and Health Administration (OSHA)**, Department of Labor, has the authority to set and enforce safety and health standards, which includes the ability to inspect worksites and levy fines.[336] The Process Safety Management (PSM) standard is the OSHA standard that addresses the management of hazards associated with processes using highly hazardous chemicals. The requirements are addressed in specific standards for general and construction industries.[337,338] OSHA is currently in the process of revising the PSM standard in response to the findings from the CSB and the President's 2013 Executive Order on Improving Chemical Facility Safety and Security (E.O. 13650), which directed OSHA and other Federal agencies to modernize policies and regulations.

The **Environmental Protection Agency's (EPA)** mission is to protect human health and the environment, and they do so by developing and enforcing environmental regulations.[339] Pertaining to this topic, the EPA administers the Risk Management Plan (RMP)[340] rule, which requires facilities that use extremely hazardous substances to develop an RMP. EPA is currently reviewing the chemical hazards covered by the Risk Management Program and determining if it

[333] This number includes those hospitalized due to the subsequent Chemical Spill. See http://www.nola.com/environment/index.ssf/2013/06/geismar_eplosion_and_fire_rele.html.
[334] http://www.csb.gov/testimony-of-rafael-moure-eraso-phd-chairperson-us-chemical-safety-board-before-the-us-senate-committee-on-environment-and-public-works-june-27-2013/.
[335] Adapted from the CSB website. Accessed March 2015: http://www.csb.gov/about-the-csb/.
[336] Adapted from OSHA Website: https://www.osha.gov/about.html.
[337] 29 CFR 1910.119 for General Industry, and 29 CFR 1926.64 for Construction.
[338] See www.osha.gov/SLTC/processsafetymanagement.
[339] http://www2.epa.gov/aboutepa/our-mission-and-what-we-do.
[340] Established by Section 112(r) of the 1990 Clean Air Act.

should be expanded to address additional regulated substances and types of hazards (E.O. 13650).[341]

The **Department of Homeland Security (DHS), National Protection and Programs Directorate, Office of Infrastructure Protection (IP),** coordinates national programs and policies on critical infrastructure security and resilience. The office conducts and facilitates vulnerability and consequence assessments to help critical infrastructure owners and operators and state, local, tribal, and territorial partners understand and address risks to critical infrastructure.[342] **DHS IP's Infrastructure Security Compliance Division** is responsible for implementing the Chemical Facility Anti-Terrorism Standards (CFATS),[343] the Nation's program to regulate security at high-risk chemical facilities and prevent the use of certain chemicals in a terrorist act on the homeland through the systematic regulation, inspection, and enforcement of chemical infrastructure security requirements. Under CFATS, facilities that have been determined by DHS to be high-risk are required to develop and implement Site Security Plans (SSPs) or Alternative Security Programs (ASPs) that meet applicable risk-based performance standards (RBPS).[344]

Theme 1: Scientific and Academic Literature on Risk Methodologies for Industrial Accidents

There are a number of scientific and technological papers devoted to the study of explosions. The vast majority are extremely technical—delving into the physics of explosions and mechanisms that can help prevent, detect, or suppress an explosion—and are targeted at the scientific community, the owners and operators of industrial facilities, or the fire fighters that may have to respond to an explosion (or a fire that might lead to an explosion). Standards and regulations, as discussed below, continue to evolve and be strengthened, which leads to additional literature on the effectiveness of those standards.

A Journal of Risk Analysis and Crisis Response article, "The Assessment of Risk Caused by Fire and Explosion in Chemical Process Industry: A Domino Effect-Based Study" by Farid Kadri, E. Chatelet, and Patrick Lallement, develops a quantitative risk assessment of domino effects[345] caused by heat radiation and overpressure on industrial sites.[346] The Europe-based study notes that accidents caused by domino effects are those that cause the most catastrophic consequences. The quantitative method developed in the study allows for the evaluation of the failure probability for each subsystem. The study defines three areas—zone of certain destruction, zone of possible destruction, and safety zone—that may be useful in the choice of safe distances between industrial equipment. The study concludes with the assertion that more quantitative assessment of risk and damage with probabilistic and deterministic modeling is needed.

---

[341] http://www2.epa.gov/rmp?_ga=1.184772905.122873663.1395699540.

[342] Adapted from the DHS, IP website: http://www.dhs.gov/office-infrastructure-protection.

[343] DHS leads national implementation of the CFATS. In October 2006, Congress passed Section 550 of the DHS Appropriations Act of 2007, Pub. L. 109-295, authorizing and requiring the DHS to regulate security at chemical facilities that DHS determines are high-risk. To implement this authority, DHS issued the CFATS in 2007.

[344] Adapted from the ISCD website: http://www.dhs.gov/iscd.

[345] The authors note that the term "domino effect" does not have a generally accepted definition in the context of accidents in industrial plants. They define it as an accident in which a primary event propagates to nearby equipment (units), triggering one or more secondary events resulting in overall consequences more severe than those of the primary event. (see page 67, section 1.1)

[346] Kadri, Farid, Chatelet, E., Lallement, Patrick. The Assessment of Risk Caused By Fire and Explosion in Chemical Process Industry: A Domino Effect-Based Study. Journal of Risk Analysis and Crisis Response, 2013, 3 (2), pp.66-76.

Kadri, Chatelet, and Lallement cite other recent research including R.M. Darbra, Adriana Palacios, and Joaquim Casal's study, "Domino effect in chemical accidents: Main features and accident sequences" published in the Journal of Hazardous Materials in November 2010,[347,348] which evaluated 225 accidents involving domino effects. The study showed that:

- Storage areas are the most probable starters of a domino effect (35%), followed by process plant (28%);
- The most frequent accident sequences are explosion-fire (27.6%), and fire-explosion (27.5%) and fire-fire (18%);
- The most frequent causes are external events (31%) and mechanical failure (29%);
- Flammable materials were involved in 89 percent of accidents, the most frequent of which was Liquefied Petroleum Gas (LPG).

Another European-based study published in 2011 examines the threat of natural hazards impacting chemical facilities and infrastructures. The authors, Krausmann, Cozzani, Salzono, and Renni, outline the ongoing efforts in the development of new concepts and tools for Natural Hazard Triggering Technological Disasters (NaTech) hazard and vulnerability ranking, risk assessment, risk-based design, and emergency planning and early warning. NaTech accidents are industrial accidents triggered by natural events, such as earthquakes, floods, and lightning.[349,350] Krausmann, Cozzani, Salzono and Renni suggest that NaTech accidents will be exacerbated by climate change and is an emerging risk issue.

The Krausmann study found that a key challenge of NaTech accidents is that standards for industrial accident preventions do not explicitly address NaTech risk, nor do typical methodologies and tools for the assessment of risk. Their study proposes a risk methodology for NaTech. This new methodology for risk appraisal and characterization provide an approach for the ranking and the quantitative assessment of NaTech risk. These capabilities contribute to risk-based design, emergency planning, and early warning.

While there may not be industry standards for NaTech risks, the current U.S. regulations address these risks in part through the PSM standard, which requires process hazards analyses for foreseeable natural disasters such as floods and lightning strikes.

A 2004 study by the European Commission and United Nations, entitled "State of the Art in NaTech Risk Management"[351] examined seven countries' NaTech Risk Management, including the U.S. Though the date of the study, places it out of the time frame for this Literature Review, it is notable for its examples of NaTech incidents in the United States and summary of the U.S.'s mitigation efforts, including describing the roles and responsibilities of various U.S. agencies. The study found that there is "an increasing trend in this type of emergency" in the United States.

---

[347] Darbra, R.M., Palacios, Adriana and Casal, Joaquim. "Domino Effect in Chemical Accidents: Main Features and Accident Sequences." *Journal of Hazardous Materials* 183.1-3 (2010): 565–573. Elsevier. Web. 1 Mar. 2015. http://www.ncbi.nlm.nih.gov/pubmed/20709447.

[348] Full access to this article was not available. Information was obtained from the available abstract.

[349] NaTech risk was acknowledged as an emerging risk in the European 7th Framework Programme Project iNTeg-Risk. See iNTEG-Risk: Early Recognition, Monitoring and Integrated Management of Emerging, New Technology Related, Risks, available at: http://integrisk.eu-vri.eu.

[350] NaTech is a relatively new term. It appears to have gained momentum in the mid-2000's, particularly among European policy and science leadership It is not commonly used in the United States, however, U.S. experts and leaders have participated in dialogues on NaTech.

[351] European Commission, Directorate-General, Joint Research Centre and the United Nations International Strategy for Disaster Reduction. 2004. Report No. EUR 21292 EN. Retrieved May 2015: http://www.unisdr.org/files/2631_FinalNatechStateofthe20Artcorrected.pdf

During the review of a draft of this paper, the Department of Labor's Occupational Safety and Health Administration identified additional sources of literature[352] which address the multi-causal nature of major industrial accidents, and provide quantitative and semi-quantitative risk assessment tools. A limitation of this literature review was the inability to access and review these sources within the time constraints of the project. Future iterations of the SNRA should review these sources.

While the literature indicates NaTech incidents may be increasing most of the accident examples referenced in the literature reviewed did not result in an explosion or fire. [353,354] The lone example from Table 14 above is the West Virginia, Sago Mine explosion in 2006, which is believed to have been caused by a lightning strike.

Theme 2: Recent Investigations and Calls for More Regulations, But Little Regulatory Action Thus Far

Combustible Dust

In 2003, three separate industrial explosions in the U.S. killed a total of 14 workers. The CSB investigations showed a common cause: combustible dust.[355,356] This finding prompted the CSB to conduct a larger study, eventually published in 2006.[357] The objectives of the study were to (1) determine whether combustible dust explosions pose a significant risk in general industry; (2) assess current efforts to manage those risks; and (3) recommend measures that may be necessary to reduce risks.[358]

The CSB identified 281 combustible dust incidents between 1980 and 2005 that killed 119 workers and injured 718, and extensively damaged industrial facilities. The incidents occurred in 44 states, in many different industries, and involved a variety of different materials. The CSB has concluded that combustible dust explosions are a serious hazard in American industry, and that existing efforts inadequately address this hazard.[359]

The study covered various industrial sectors (lumber and wood products, food products, chemical manufacturing) that handle and/or generate combustible dusts. But notably, the CSB excluded incidents involving grain-handling or other facilities currently regulated by the OSHA

---

[352] The Occupational Safety and Health Administration recommended reviewing publications by the Center for Chemical Process Safety (CCPS), which can be found at http://www.wiley.com/WileyCDA/Section/id-291237.html

[353] Cruz, A., Katjitani, Y., and Tatano, H. "Natech Disaster Risk Reduction: Can Integrated Risk Governance Help?" *Risk Governance: The Articulation of Hazard, Politics and Ecology*. Edited by Fra.Paleo, Urbano. Springer, 2014. 441.

[354] Phillips, B., Neal, D., Webb, G. Introduction to Emergency Management. CRC Press, 2011. P.115.

[355] The CSB defines a dust explosion as a fire and/or explosion—fueled by any finely divided solid material—that harms people or property.

[356] The NFPA definition of explosions that are dust-related is the bursting or rupture of an enclosure or a container due to the development of internal pressure from a deflagration. This definition is the common one used for NFPA's for industry or commodity-specific dust explosions: NFPA 61, Prevention of Fires and Dust Explosions in Agricultural and Food Processing Facilities; NFPA 484, Combustible Metals; NFPA 654, Prevention of Fire and Dust Explosions from the Manufacturing, Processing, and Handling of Combustible Particulate Solids; NFPA 655, Prevention of Sulfur Fires and Explosions; and NFPA 664, Prevention of Fires and Explosions in Wood Processing and Woodworking Facilities. See "NFPA Glossary of Terms: 2014 Edition." See "Explosion" definition for documents 61, 484, 654, 655, 664. (2014, September). Retrieved March 2015: http://www.nfpa.org/got.

[357] U.S. Chemical Safety and Hazard Investigation Board (CSB). "Investigation Report: Combustible Dust Hazard Study." Report No. 2006-H-1. November 2006. P1.

[358] CSB. (2006). P6.

[359] This paragraph adapted from the Executive Summary, of the "Combustible Dust Hazard Study." Report 2006-H-1. Published by the U.S. Chemical Safety and Hazard Investigation Board. November 2006. P1.

Grain Handling Facilities Standard; coalmines; non-manufacturing facilities, such as hospitals, military installations, and research institutes; and transportation.

OSHA initiated a combustible dust national emphasis program (DustNEP) in October 2007.[360] The DustNEP conducts focused inspections at facilities that may handle or process combustible dust. Each OSHA Area Office randomly selects four facilities every year in which to conduct combustible dust-related inspections. Since 2007, OSHA conducted over 1,600 inspections in accordance with the DustNEP. Over 1,200 of these inspections resulted in citations and hazard abatement. OSHA considers the DustNEP to be very successful as it creates an enforcement presence in facilities handling and processing combustible dust that, without the NEP, would likely go many years without inspection.

In addition to the DustNEP[361], OSHA has been attempting to publish a comprehensive combustible dust standard since the CSB's report recommended it in 2006.[362]

A survey of literature published since the CSB report shows increased attention to the topic of combustible dust from the scientific and fire communities. Some critics argue, however, that not enough has been done to update regulations and enforcement mechanisms.[363] From 2008 to 2012, the CSB documented 50 combustible dust accidents that led to 29 fatalities and 161 injuries.[364]

Currently, the NFPA is in the process of issuing a new standard—NFPA 652—to be published in the summer of 2015. The NFPA already has five combustible dust standards specific to industries, processes, and dust types. This new, overarching standard will "establish the relationship and hierarchy between it and any of the industry or commodity-specific standards, ensuring that fundamental requirements are addressed consistently across the industries, processes, and dust types."[365]

Deepwater Horizon, New Technologies and the Petrochemical Industry's Safety Culture

On April 20, 2010, an explosion occurred on the Deepwater Horizon Oil Rig. The CSB's final report, prepared in 2014, determined that:

> The blowout preventer (BOP) that was intended to shut off the flow of high-pressure oil and gas from the Macondo well in the Gulf of Mexico during the disaster on the Deepwater Horizon drilling rig on April 20, 2010, failed to seal the well because drill pipe buckled for reasons the offshore drilling industry remains largely unaware… The blowout caused explosions and a fire on the Deepwater Horizon rig, leading to the deaths of 11 personnel onboard and serious injuries to 17 others. Nearly 100 others escaped

[360] The information in this paragraph was provided by OSHA and OSHA's DustNEP website: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=directives&p_id=3830
[361] Combustible Dust National Emphasis Program CPL 03-00-008, 3/11/2008.
[362] An Opinion Editorial by the Chairman of the CSB: Moure-Eraso, Rafael. "The Danger of Combustible Dust." *The New York Times* 22 Aug. 2014. The New York Times Co. Mar. 2015. http://www.nytimes.com/2014/08/23/opinion/the-danger-of-combustible-dust.html?_r=0.
[363] An Opinion Editorial by the Chairman of the CSB: Moure-Eraso, Rafael. "The Danger of Combustible Dust." *The New York Times* 22 Aug. 2014. The New York Times Co. Mar. 2015. http://www.nytimes.com/2014/08/23/opinion/the-danger-of-combustible-dust.html?_r=0.
[364] Ibid.
[365] Colonna, Guy. "Credible Risk." *NFPA Journal*. March 2015. Accessed March 2015: http://www.nfpa.org/newsandpublications/nfpa-journal/2015/march-april-2015/features/dust.

> from the burning rig, which sank two days later, leaving the Macondo well spewing oil and gas into Gulf waters for a total of 87 days…the largest in offshore history.[366]

In a January 2011 Report to the President, the National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling[367] included the following conclusions:

- The explosive loss of the Macondo well could have been prevented.
- The immediate causes of the Macondo well blowout can be traced to a series of identifiable mistakes made by BP, Halliburton, and Transocean that reveal such systematic failures in risk management that they place in doubt the safety culture of the entire industry.
- Deepwater energy exploration and production, particularly at the frontiers of experience, involve risks for which neither industry nor government has been adequately prepared, but for which they can and must be prepared in the future.
- To assure human safety and environmental protection, regulatory oversight of leasing, energy exploration, and production require reforms… Fundamental reform will be needed in both the structure of those in charge of regulatory oversight and their internal decision-making process.
- Because regulatory oversight alone will not be sufficient to ensure adequate safety, the oil and gas industry will need to take its own, unilateral steps to increase dramatically safety throughout the industry, including self-policing mechanisms that supplement governmental enforcement.[368]

The "systematic failures in risk management," lack of "safety culture," and need for regulatory reforms are consistent with findings from the CSB investigations into other industrial accident-explosion/fire events in the refinery and drilling industry. For example, a 2011 CSB study entitled, Public Safety at Oil and Gas Storage Facilities, found 26 explosions and fires from 1983 to 2010, killing 44 members of the public and injuring 25.[369,370] These incidents differ from those traditionally thought-of as "industrial accidents" because they are not occurring at a plant or facility where employees report to work. Rather these oil and gas production and storage facilities tend to be located in rural areas. The CSB report found that children and young adults were the most common to visit, and the primary purpose for visiting without authorization was for recreational purposes such as "socializing, hunting, and driving all-terrain vehicles."[371] Though in most cases, the members of the public would have been aware that they were trespassing, the CSB found they were "unaware of the explosion and fire hazards associated with

---

[366] CSB Press Release, June 5, 2014. "CSB Board Approves Final Report Finding Deepwater Horizon Blowout Preventer Failed…" Retrieved March 2015: http://www.csb.gov/csb-board-approves-final-report-finding-deepwater-horizon-blowout-preventer-failed-due-to-unrecognized-pipe-buckling-phenomenon-during-emergency-well-control-efforts-on-april-20-2010-leading-to-environmental-disaster-in-gulf-of-mexico/.

[367] National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling (Commission). (January 2011). Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling: Report to the President. Retrieved March 2015: http://www.gpo.gov/fdsys/pkg/GPO-OILCOMMISSION/pdf/GPO-OILCOMMISSION.pdf.

[368] See page vii of the Forward. These are direct quotes from Report. There were two other conclusions that are omitted from this list because they are not relevant to this topic.

[369] Note: these explosions did not reach the level of "large scale industrial accident-explosion or fire" included in Table 14. It is referenced to demonstrate the concerns about safety culture challenges within the industry.

[370] U.S. Chemical Safety and Hazard Investigation Board (CSB). "Public Safety at Oil and Gas Storage Facilities" Report No. 2011-H-1. September 2011. Retrieved March 2015: http://www.csb.gov/assets/1/19/Tanks_Safety_Study_FINAL.pdf.

[371] Ibid. Page 21.

the tanks" and "unintentionally introduce[d] ignition sources for the flammable vapor, leading to explosions".[372] CSB found that many of the incidents occurred at unfenced facilities that "did not have clear or legible warning signs as required under OSHA's Hazard Communication Standard, and did not have hatch locks to prevent access to the flammable hydrocarbons inside the tanks."[373] There were other findings and the CSB made six recommendations when it released the study in 2011. None have been implemented.[374]

A separate example of the lack of safety culture comes from an EnergyWire review of federal labor statistics. The oil and gas industry has more deaths from fires and explosions than any other private industry (see Figure 5). It employs less than one percent of the U.S. workforce, but in the past five years it has had more than 10 percent of all workplace fatalities from fires and explosions.[375,376]

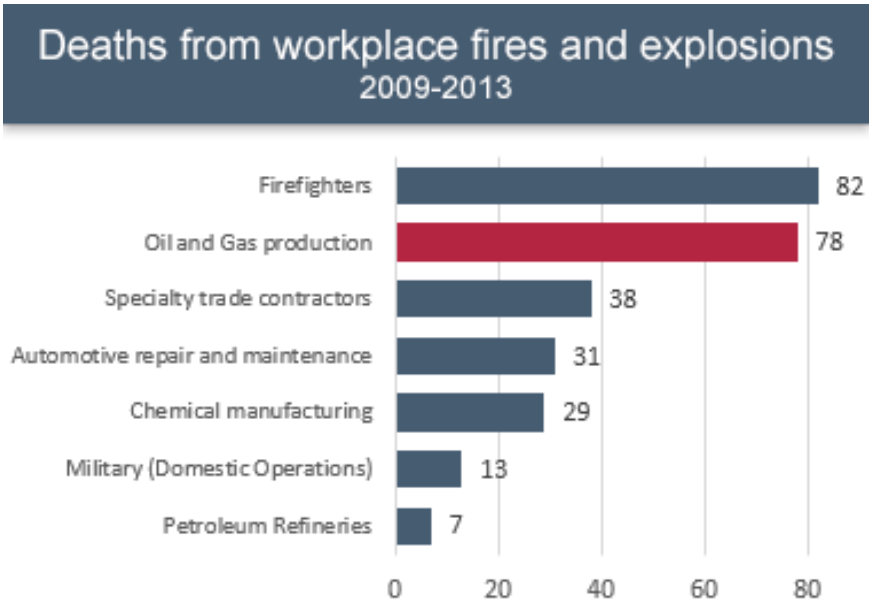


Figure 5: EnergyWire Graphic Based on Bureau of Labor Statistics[377]

Oil and gas production sites are not currently subject to OSHA's Process Safety Management program, and OSHA does not have an industry specific standard for oil and gas, but regulates them under a wide range of standards and their General Duty Clause.[378,379] For example, OSHA frequently cites oil and gas production facilities for 1910 Subpart S - Electrical and for Personal

[372] Ibid. Page 8.
[373] Ibid.
[374] The CSB's investigation webpage shows the number of recommendations made by an investigation report and the number that are "open" and "closed". As of March 2015, the webpage showed all six recommendations remain "open." Retrieved March 2015: http://www.csb.gov/oil-site-safety/.
[375] Soraghan, Mike. "The Drilling Industry's Explosion Problem." *EnergyWire* 20 Oct. 2014. Accessed March 2015: http://www.eenews.net/special_reports/danger_zone/stories/1060007532.
[376] The data collected by the Bureau of Labor Statistics does not offer granularity as to the cause of the fatalities. Explosions are grouped with fire related deaths. Also, while it is likely most of these incidents fall under the industrial accident umbrella, they could be caused by sabotage, work-place violence, terrorism, or other causes that are not within Industrial Accident definition.
[377] Soraghan, M. (2014). Source of data is Bureau of Labor Statistics, Census of Fatal Occupational Injuries.
[378] Soraghan, M. (2014).
[379] Smith, A. (2015).

Protective Equipment (PPE) violations.[380] Likewise, the oil and gas industry receives exemptions from certain aspects of the EPA's regulatory framework.[381] As part of the activities directed by E.O. 13650, OSHA and EPA were to look into strengthening regulations.

New technology at the "frontiers of experience," as the Deepwater Commission framed it, "involve risks for which neither industry nor government has been adequately prepared".[382] While the Commission was referring to the relatively new deepwater drilling technologies, this statement applies to other technologies, for example hydraulic fracturing and directional drilling.

Since 2008, oil production has been on the rise and is now near its 1970 record high.[383] The NFPA Journal reports that the increase is due to the "melding of two advanced drilling techniques that are used to stimulate production of oil and gas wells: hydraulic fracturing, or fracking, and directional drilling".[384] The NFPA asserts that the advanced extraction techniques are not inherently more dangerous than older drilling approaches, but the increase in drilling has increased the number of accidents.[385] Unfortunately, there is no data on the number of fires and explosions at the new drilling sites.

The challenge is that the new drilling sites are often located close to populated communities, and increasingly, communities are moving closer to drilling sites. Not only does this increase the risk of the local community, but also puts local fire fighters in harm's way. Local fire departments are more accustomed to fighting structure fires, and lack the "training, equipment, and tactical approach to handle the fire safely and effectively."[386]

NFPA does not have specific standards for oil and gas drilling sites, but some existing standards would apply. As this is an emerging and growing risk, some have suggested that NFPA write guidelines for fire officials. Separately, the American Petroleum Institute (API) sets safety standards that most states and many Federal agencies have adopted as regulations. In July 2014, the API issued new "Community Engagement Guidelines" for drilling companies.[387] It includes guidelines on engaging with emergency services and first responders.[388] The NFPA Journal article ends with a personal account of how one particular fire department is making an effort to be prepared for the new challenges. It suggests that although the new and increased drilling is increasing the risk of fires and explosions, through proper planning and training and partnering with the drill owners, the risks can be mitigated.

In addition to the drilling hazards, there is also some new evidence that oil from fracking may be more volatile than traditionally drilled oil.[389] Though outside the scope of this assessment, from

---

[380] Information provided by OSHA.
[381] CSB (2011). P. 42.
[382] Commission. (January 2011). Executive Summary.
[383] See U.S. Field Production of Crude Oil Annual, Historical Chart produced by the U.S. Energy Information Administration. Accessed March 2015: http://www.eia.gov/dnav/pet/hist/LeafHandler.ashx?n=PET&s=MCRFPUS1&f=A
[384] Smith, A. "New Frontier". NFPA Journal. March 2, 2015. Retrieved March 2015 http://www.nfpa.org/newsandpublications/nfpa-journal/2015/march-april-2015/features/fracking.
[385] Smith, A. (2015).
[386] Smith, A. (2015).
[387] American Petroleum Institute (API). Community Engagement Guidelines: ANSI/API Bulletin 100-3, First Edition, July 2014. Accessed March 2015: http://www.api.org/~/media/files/policy/exploration/100-3_e1.pdf
[388] API. (2014). P 7.
[389] Sider, A. and Friedman, N. "Oil from U.S. Fracking is More Volatile Than Expected". Wall Street Journal, June 24, 2014. Retrieved March 2015: http://www.wsj.com/articles/oil-from-u-s-fracking-is-more-volatile-than-expected-1403653344

mid-February 2015 to early March, four trains hauling oil derailed in the U.S. and Canada causing spills and explosions.[390] Most were hauling Bakken crude that was extracted by fracking, which some government tests showed is more volatile than other crude oil.[391] Investigations into these incidents are ongoing, and the cause of the explosions are unknown at this time.

More Calls for Updating and Strengthening Regulations

In 2013, an explosion at a fertilizer storage facility in West, Texas, killed 15 people, injured over 200, and damaged or destroyed over 200 homes, two schools, an apartment complex, and a nursing home. West is a small town and the explosion decimated it. Two months after the explosion in West, a fire and explosion occurred at a petrochemical plant in Geismar, Louisiana, that killed two workers and injured over 100 more.

These events renewed attention to the dangers of industrial explosions. In response, the President issued E.O 13650[392] on August 1, 2013, which directed DHS, OSHA, and EPA to perform a number of tasks to improve chemical facility safety and security. Congressional hearings[393,394,395] were held and GAO issued several reports on chemical safety[396] and chemical facilities[397].

One of the tasks from the E.O. was to update chemical safety and security regulations, which have not been updated in decades. This is not an easy undertaking. A 2012 GAO study found that it took an average of seven years to develop and issue safety and health standards.[398]

Some within the chemical industry have stated their support for stronger regulatory oversight, but have less interest in promulgating new regulations.[399] Some of this may be due to what is consistently called the "patchwork" nature of the current regulatory scheme, which is further complicated by multiple agencies (DHS, EPA, and OSHA) having various regulatory responsibilities. While the various positions and nuances of the debate are outside the scope of

---

[390] Lowy, J. "Recent spate of derailments in the US, Canada deepens fear of possible oil train disaster". Associated Press. March 10, 2015. Retrieved March 2015: http://www.usnews.com/news/business/articles/2015/03/10/spate-of-oil-train-derailments-raises-safety-concerns

[391] The API disagrees with this assertion.

[392] https://www.whitehouse.gov/the-press-office/2013/08/01/executive-order-improving-chemical-facility-safety-and-security.

[393] Oversight of Federal Risk Management and Emergency Planning Programs to Prevent and Address Chemical Threats, Including the Events Leading up to the Explosions in West, TX and Geismar, LA: Hearings before the Full Committee on Environment and Public Works, Senate, 113th Cong. (June 27, 2013). Retrieved March 2015: http://www.epw.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=64099921-ffdc-075c-1328-f94f2fb7bae6.

[394] Oversight of the Implementation of the President's Executive Order on Improving Chemical Facility Safety and Security: Joint Committee Hearing of Environment and Public Works, and Health, Education, Labor, and Pensions, Senate, 113th Cong. (December 11, 2014). Retrieved March 2015: http://www.epw.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=b2085dfd-ecb0-3b54-db5e-d2ed8a7730eb.

[395] West Fertilizer, Off the Grid: The Problem of Unidentified Chemical Facilities: Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House, 113th Cong. (August 1, 2013). Retrieved March 2015: https://homeland.house.gov/hearing/subcommittee-hearing-west-fertilizer-grid-problem-unidentified-chemical-facilities.

[396] Moran, R. (2014). Chemical Safety: Action Needed to Improve Federal Oversight of Facilities with Ammonium Nitrate. Government Accountability Office, GAO-14-274. Retrieved March 2015, from http://gao.gov/assets/670/663293.pdf.

[397] Caldwell, S. (2013). DHS Needs to Improve Its Risk Assessments and Outreach for Chemical Facilities. Government Accountability Office, GAO-13-801T. Retrieved March 2015, from http://www.gao.gov/products/GAO-13-801T.

[398] See http://www.gao.gov/products/GAO-12-330

[399] Testimony of Timothy J. Scott, Chief Security Officer and Corporate Director Emergency Services and Security, The Dow Chemical Company, Representing The American Chemistry Council at a hearing on: West Fertilizer, Off the Grid: The Problem of Unidentified Chemical Facilities: Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House, 113th Cong. (August 1, 2013). Retrieved March 2015: http://docs.house.gov/meetings/HM/HM08/20130801/101223/HHRG-113-HM08-Wstate-ScottT-20130801.pdf

this assessment, what is germane is that there is agreement that the current regulatory system needs to be improved.

Finally, relevant to EPA's authorities, U.S. Senators David Vitter (R-La.) and Tom Udall (D-N.M.) introduced new legislation designed to fix the outdated chemical regulatory program managed by the EPA.[400] The Frank R. Lautenberg Chemical Safety for the 21st Century Act[401] would update the 1976 Toxic Substances Control Act (TSCA). It has been in development for several years and included negotiations with the industry, environmentalists, and affected communities. If enacted, it does not appear to affect OSHA or DHS's responsibilities.

It remains to be seen whether the bill will make it through Congress. The initial hearing demonstrated there are strong supporters, but also strong critics of the bill who believe it contains too many compromises.[402]

Conclusion

The Literature Review suggests that more needs to be done to improve the current regulatory scheme in order to further reduce the risks of Industrial Accident-Explosion/Fire. Current efforts in the Executive Branch (related to the implementation of E.O. 13650) and the Legislative Branch (Frank R. Lautenberg Chemical Safety for the 21st Century Act) may result in significant changes for the first time in decades. If proponents are correct, implementation will reduce risk and/or mitigate the consequences of industrial accidents. It is too early to tell whether such changes will be enacted.

Within the scientific literature reviewed, new methodologies are being developed to better understand the domino effects of industrial explosions, as well as the emerging risk of NaTech disasters. Such methodologies should allow Federal, state, and local planners to be able to better evaluate risks and enact prevention and protection mechanisms to reduce the risk or at least the impact of explosions in the future.

The Literature Review highlighted two types of potential emerging risks:

1. NaTech: The European 7th Framework Programme Project iNTeg-Risk believes NaTech is an emerging risk that will likely increase due to climate change. Thus, we may begin to see new or increasing numbers of explosions caused by natural hazards (as compared to historic trends). While explosion as a potential event caused by natural hazards is part of the NaTech definition, existing literature tends to focus on other accidents, such as chemical spills. Currently, the overwhelming majority of industrial accidents resulting in an explosion are unrelated to natural hazards. This may, however, be an area relevant for future study. Additionally, future iterations of the SNRA should review the sources provided by OSHA which address the multi-causal nature of major industrial accidents, and provide quantitative and semi-quantitative risk assessment tools.

---

[400] Press Release: Vitter, Udall Introduce Landmark Legislation to Protect Our Families from Toxic Chemicals. March 10, 2015. Retrieved March 2015: http://www.vitter.senate.gov/newsroom/press/vitter-udall-introduce-landmark-legislation-to-protect-our-families-from-toxic-chemicals

[401] S. 1009 text and current status can be found here: http://www.scribd.com/doc/258283745/The-Frank-R-Lautenberg-Chemical-Safety-for-the-21st-Century-Act

[402] See Transcript of Hearing: Frank R Lautenberg Chemical Safety for the 21st Century Act: Committee on Environment and Public Works, Senate, 114th Cong. March 18, 2015. Retrieved March 2015: http://www.epw.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_id=60d1e265-cdac-7629-3385-2d72dd8fe3eb

2. New technology at the "frontiers of experience," as the Deepwater Commission framed it, "involve risks for which neither industry nor government has been adequately prepared".[403] Techniques such as "fracking" often occur close to suburban and urban communities. Some assert in the literature that the petrochemical industry has a poor record of safety and that the safety culture remains weak. Between the increase in drilling sites, and the potential weak safety culture, an emerging risk could be explosions at fracking sites near populated communities. The literature reviewed focused specifically on the new technology within the petrochemical industry; however, it is reasonable to assume other industries, particularly the chemical industry, are developing and implementing new technologies. It will be a challenge for regulators to keep up with emerging technologies.

This literature review primarily focused on assessing the risk of an Industrial Accident-Explosion/Fire, of any size, occurring. Accidents that are so catastrophic to require Federal support in its response are a small percentage of the overall occurrence of an Industrial Accident-Explosion/Fire event. This assessment leaves frequency calculations to the Quantitative Assessment. However, this qualitative assessment suggests that new technologies and emerging risks may create more complex disasters that require more complex preventive measures and responses. Thus, we may see an increase in frequency of requests for Federal assistance in response to Industrial Accident-Explosion/Fire incidents.

References

Darbra, R.M., Palacios, Adriana and Casal, Joaquim. "Domino Effect in Chemical Accidents: Main Features and Accident Sequences." *Journal of Hazardous Materials* 183.1-3 (2010): 565–573. Elsevier. Web. 1 Mar. 2015. http://www.ncbi.nlm.nih.gov/pubmed/20709447.

Kadri, Farid, Chatelet, E., Lallement, Patrick. The Assessment of Risk Caused By Fire and Explosion in Chemical Process Industry: A Domino Effect-Based Study. Journal of Risk Analysis and Crisis Response, 2013, 3 (2), pp.66-76.

Krausmann, E., Cozzani, V. Salzano, E., and Rennil, E. Industrial Accidents Triggered by Natural Hazards: An Emerging Risk Issue. Natural Hazards and Earth System Sciences, 2011, pp. 921-929.

Moran, R. (2014). Chemical Safety: Action Needed to Improve Federal Oversight of Facilities with Ammonium Nitrate. *Government Accountability Office, GAO-14-274*. Retrieved March 2015, from http://gao.gov/assets/670/663293.pdf

National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling (Commission). Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling: Report to the President. January 2011. Retrieved March 2015: http://www.gpo.gov/fdsys/pkg/GPO-OILCOMMISSION/pdf/GPO-OILCOMMISSION.pdf.

Smith, A. "New Frontier". NFPA Journal. March 2, 2015. Retrieved March 2015: http://www.nfpa.org/newsandpublications/nfpa-journal/2015/march-april-2015/features/fracking.

[403] Commission. (January 2011). Executive Summary.

U.S. Chemical Safety and Hazard Investigation Board (CSB). "Investigation Report: Combustible Dust Hazard Study." Report No. 2006-H-1. November 2006. Retrieved March 2015, from http://www.csb.gov/assets/1/19/Dust_Final_Report_Website_11-17-06.pdf

Plant Disease

Synopsis

This qualitative assessment evaluates the risk of an unintentional plant disease outbreak resulting in a national level event. Three themes were identified from the reviewed literature: (1) globalization and threats from imported pathogens and pests; (2) climate change; and (3) cultural shifts—the impact of the organic and non-genetically modified organism (GMO) movements on plant disease.

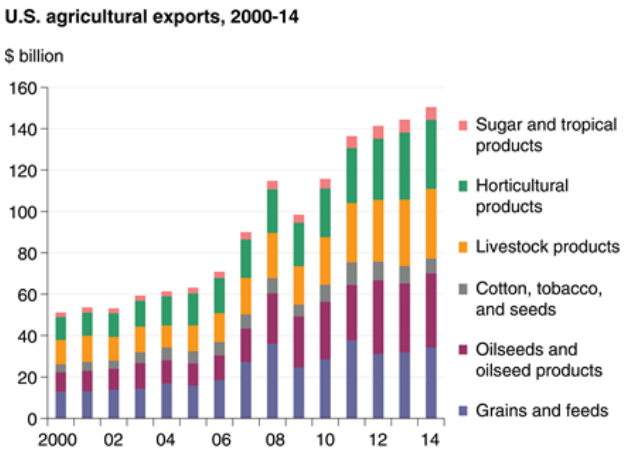
Generally, the literature reflected that there is a constant battle against plant disease. One of the key risk factors about plant disease is its nature to evolve and mutate in order to gain resistance to pesticides and other mitigation techniques. The literature also reflected that the U.S. Government has an established and effective infrastructure to prevent, detect, respond to, and mitigate this evolving threat. The literature encouraged continued research to stay ahead of emerging plant diseases. While the threat is not necessarily increasing, it presents a dynamic landscape that requires close scrutiny.

Literature Review

Introduction

Event Description

For purposes of this assessment, Plant Disease is an outbreak of a plant pathogen or pest that has the potential to reduce or destroy plants so significantly that it results in a national level event. The scope of this assessment is primarily on unintentional outbreaks or accidental releases through commerce or a lab accident.[404] For purposes of this assessment, we are characterizing a national level event to be a plant disease outbreak of such significance that it has the potential to threaten the nation's food supply or cause substantial economic loss (reductions in exports and foodstuffs losses).[405]



Source: USDA, Economic Research Service using data from U.S. Department of Commerce, U.S. Census Bureau, Foreign Trade Database.

Event Background

The Value of Plants

Plants play a vital role in our society.[406] Healthy plant systems are necessary for the health and welfare of our citizens, animals, and economy. Stack and Fletcher argue that the "human, animal, and plant systems are

404 Intentional outbreaks—caused by an adversary intentionally releasing a plant pathogen or pest—are considered an Adversarial Hazard and are addressed by other topics in the SNRA.

405 "More than two-thirds of cropland in the United States is devoted to the production of just four crop species—maize, wheat, soybeans, and cotton" - http://bioscience.oxfordjournals.org/content/59/2/141.short

406 Stack, James P. and Jacqueline Fletcher, "Plant Biosecurity Infrastructure for Disease Surveillance and Diagnostics", pp. 95-105, Global Infectious Disease Surveillance and Detection: Assessing the Challenges-Finding Solutions, National Academy of Sciences Press. (2007).

intricately linked; the intersection of these three systems form the basis of our economy, our culture, and our standard of living."[407] We depend on plants in a number of ways that we often do not think about. Plants generate oxygen, provide food for us and our animals, clothe us through their fibers, shelter us with their timber, and increasingly power our technology through the fuels they provide.[408]

The agriculture sector produces sizeable exports that contribute to the U.S. economy. From 2006 to 2014, U.S. agricultural exports more than doubled. Demand from developing countries, along with higher farm commodity prices, explains recent growth in the value of U.S. exports. Foreign demand for wheat, soybeans, cotton, corn, and their processed products accounts for about half of U.S. export value. U.S. farm exports to developing countries are now more than double what are exported to developed countries. Purchases by developing countries consistently have been greater than developed countries since 1994.[409] In the last century, the U.S. prosperity was due in part to its agriculture providing a "safe, inexpensive, and dependable food supply system."[410]

Plant Diseases

Destructive plant pests and pathogens come from a variety of sources including insect pests and plant pathogens such as fungi, oomycetes, bacteria, viruses, nematodes, protozoa, and parasitic plants. Currently there are several prioritized lists of high consequence plant pathogens and pests.[411] Some of these lists have hundreds of agents. It is difficult to define a set of characteristics that identify which plant pests or pathogens could cause the greatest plant damage to the Nation's ecosystem.[412] Furthermore, many plant pests and pathogens are resilient in the sense that it is not feasible to completely eliminate them from the environment.

The four primary crops grown in the United States are maize, wheat, soybeans, and cotton. Their production takes up more than two-thirds of cropland in the United States. Experts have raised concerns that "homogenization of the American agricultural landscape could facilitate widespread disease and pest outbreaks, compromising the national food supply."[413]

Diseases affecting the major food crops, "cereal grains (wheat, rice, and maize), tubers (potato, cassava, yam, and taro), and vegetable crops (dry beans, peas, lentils and other legumes as well as cabbage and other brassicas)" have the greatest affect on human populations.[414]

---

[407] Stack and Fletcher. (2007).
[408] Stack and Fletcher. (2007).
[409] The chart and this paragraph are from the USDA's Economic Research Service. Retrieved April 2015: http://www.ers.usda.gov/data-products/chart-gallery/detail.aspx?chartId=40077&ref=collection&embed=True&widgetId=39734
[410] Stack and Fletcher. (2007).
[411] Fletcher, Jacqueline, et al., "Emerging Infectious Plant Diseases", Chapter 18, Emerging Infections 9, Ed. W. M. Scheld, 2010, ASM Press, Washington, DC. Retrieved April 2015: http://www.ars.usda.gov/SP2UserFiles/Place/66180000/Fletcher%20et%20al_2010_%20Emerging%20Infectious%20Plant%20Diseases_%20ASM%20Press%20ch18.pdf
412 Fletcher, J. (2010).
[413] Margosian, M., Garrett, K., Hutchinson, S., and With, K. (2009, February). "Connectivity of the American Agricultural Landscape: Assessing the National Risk of Crop Pest and Disease Spread." BioScience Magazine. Vol. 59 No. 2. 141-151. Retrieved April 2015: http://bioscience.oxfordjournals.org/content/59/2/141.full.pdf+html
[414] Fletcher, Jacqueline, et al., "Emerging Infectious Plant Diseases", Chapter 18, Emerging Infections 9, Ed. W. M. Scheld, 2010, ASM Press, Washington, DC. http://webcache.googleusercontent.com/search?q=cache:63DWp_YlflMJ:www.ars.usda.gov/SP2UserFiles/Place/66180000/Fletcher%2520et%2520al_2010_%2520Emerging%2520Infectious%2520Plant%2520Diseases_%2520ASM%2520Press%2520ch18.pdf+&cd=2&hl=en&ct=clnk&gl=us

"Underdeveloped countries lacking infrastructure to detect and mitigate diseases," have the greatest struggle, but diseases of these plants affect U.S. growers as well.

The "disease triangle" that characterizes all plant diseases consists of (1) a susceptible plant, (2) a virulent pathogen, and (3) a conducive environment. Without all three components, disease will not occur.[415] Plant diseases are categorized by symptoms. They can occur in the field or in storage.

U.S. Government Roles and Responsibilities

The United States Department of Agriculture (USDA) is the lead Federal agency tasked with identifying, controlling, and mitigating the effects of plant pests and pathogens.[416] Specific to agriculture health, the USDA has the following responsibilities:[417]

- Developing plant pest and disease exclusion systems and coordinating implementation across the interagency mitigating the risk of introduction of exotic plant pest and disease from foreign countries into the United States (foreign responders, equipment, supplies, and food).
- Developing and maintaining biosurveillance systems to detect exotic plant pests and disease and coordinating surveillance activities with local, state, tribal, and territorial governments.
- Identifying and confirming the presence of newly detected exotic plant pests and disease in the United States.
- Coordinating emergency response to newly detected plant pests and disease of economic or environmental significance with local, state, tribal, and territorial governments.
- Mitigating the interstate movement and potential spread of exotic plant pest and disease in the United States (applies to equipment and supplies moving in and out of quarantine zones, debris removal, and movement of agricultural commodities or soils).

A large infrastructure exists in the U.S. consisting of Federal and state agencies and related research laboratories responsible for surveillance, prevention, detection, and recovery from destructive plant pests and pathogens. This infrastructure regularly demonstrates that it can control and mitigate the effects of plant pests and pathogens in the environment.

Preventing and Interdicting Pests

The Department of Homeland Security assists, supports and enforces USDA regulations within the designated areas of responsibility such as the ports of entry. To mitigate the effects of destructive plant agents in the U.S., the USDA, through the Animal and Plant Health Inspection Service Plant Protection and Quarantine (APHIS PPQ), and the DHS, through Customs and Border Protection (CBP), share responsibility for preventing the introduction of new plant pathogens and pests into the U.S.

---

[415] Fletcher, J. (2010).

[416] In addition to their statutory responsibilities, the USDA is also the lead for Emergency Support Function (ESF) #11 – Agriculture and Natural Resources Annex. http://www.fema.gov/media-library-data/20130726-1914-25045-2457/final_esf_11_ag_and_natural_resources_20130501.pdf

[417] This only a portion of USDA's plant health related responsibilities. This list is from ESF #11.

Detecting Outbreaks

The National Plant Diagnostic Network (NPDN) under the USDA provides infrastructure for the detection and diagnoses of destructive plant agent outbreaks. The NPDN collaborates with the National Institute for Food and Agriculture (NIFA) (formerly the Cooperative State Research, Education, and Education Service [CSREES]), APHIS, and other organizations to detect outbreaks.

Responding to Outbreaks

To respond to a destructive plant agent, the U.S. set up the National Plant Disease Recovery System (NPDRS) within the USDA's Agriculture Research Service (ARS). NPDRS has the responsibility of responding to high consequence plant pests and pathogens with pest control measures and the use of disease resistant seeds. NPDRS gets seeds from the U.S. National Plant Germplasm System. NPDRS involves APHIS, NIFA, and state departments of agriculture.

Research

As of 2002, USDA and APHIS, were spending more than $1 billion annually in research, risk assessment, and emergency response plans to outbreaks.[418] USDA's ARS and the U.S. Forest Service conduct in-house research and support basic and applied plant pathology research through formal (NIFA) and informal (APHIS) extramural grant programs. The National Science Foundation and other funding sources also fund basic research on plant-microbe interactions. Individual states fund plant pathology research at land grant universities (LGUs) in various academic departments (plant pathology, microbiology, horticulture, and agronomy, etc.). In addition, Cooperative Extension Service (CES) personnel conduct applied field research and provide advice directly to producers and serve as first responders to pathogen outbreaks.

Research is also sponsored and conducted by state agencies and private sector organizations. State Department of Agriculture (SDA) laboratories often addresses diseases and pathogens specific to the state's climate and commodities. Several large commodity groups, representing the agricultural production sector, collect "checkoff" funds from growers to support research on pathogens attacking that commodity, and seed companies monitor and conduct research on plant pathogens emerging in the U.S., as well as in countries where offshore nurseries are used to generate seed for subsequent planting in the U.S.[419]

Literature Review

Globalization and threats from imported pathogens and pests

Plant disease outbreaks are not solely natural occurrences. Human actions are extensively implicated in the spread and outbreak of disease, thus making it difficult to determine the precise drivers, impacts, and regulations of the disease.[420] Human-induced globalization is increasing the spread of plant disease; organisms are transported more easily as a result of extended trading

[418] Margosian 2009
[419] Fletcher, J. (2010).
[420] Wilkinson, K., Grant, W., Green, L., Hunter, S., etc. (2011, May). "Infectious diseases of animals and plants: an interdisciplinary approach". Philosophical Transactions of the Royal Society. Vol. 366, 1933-1942. Retrieved April 2015: http://classic.rstb.royalsocietypublishing.org/content/366/1573/1933.full

systems.[421] There are 10 new types of insects or pathogens introduced to American farms each year.[422]

Imported pathogens are considered an existing as well as an emerging threat to the U.S. agricultural scene. The threat of foreign pathogens to native vegetation has been recognized internationally and steps are in place to control this threat to an extent. Lessons learned have pointed to trends in diseases and their "ability to coevolve with new hosts and to rapidly exploit the environments with which they come into contact…" posing "…both a scientific and management challenge."[423] While recognized and actively mitigated, it was widely agreed that further research is necessary for continued management as new, exotic, and resistant pathogens emerge.[424]

Concerns were put forth not only for pathogens and pests brought in through food bearing plants, but also in recreational plants. As discussed below, any type of foreign agriculture can introduce diseases into the food supply.

> Huge markets exist for international trade of live ornamental plants. Flowers and other ornamentals include a wide variety of plant species that host a multitude of diseases. The movement of commercial ornamental propagation activities to tropical offshore facilities has generated new pathways for movement of exotic plant diseases into the United States. For example, Ralstonia solanacearum race 3 biovar 2, a serious pathogen of potato and tomato designated a "select agent," was introduced into the United States in 2003 on propagated geranium plants from Central America and again in 2004 from West Africa, causing growers to destroy their inventories. Because plant pathologists and regulatory authorities were concerned that the pathogen would threaten U.S. potato and tomato production if it escaped from nursery facilities, geranium growers who had received infested shipments were directed to destroy their inventories.[425]

Another concern with imports is the reintroduction of previously mitigated risks to plant health. The U.S. and most developed countries have encountered basic pathogens and have either wiped out the cause, or have developed plants that are resistant to common forms of the disease. In 1999, the developing nation of Uganda unwittingly re-introduced a strain of wheat stem rust, which was thought to have been eradicated. This instance provided "a humbling example of the capacity of pathogens to mutate in response to selective pressure, acquiring new virulence traits and overcoming resistance genes."[426]

Climate Change

Climate change is another issue impacting the spread of diseases. Disease organisms may find more favorable conditions for reproduction and transmission as a consequence of global

---

[421] Wilkinson, K. etc. (2011, May).
[422] Margosian. (2009).
[423] Potter, C., Harwood, T., Knight, J, and Tomlinson, I. (2011). "Learning from history, predicting the future: the UK Dutch elm disease outbreak in relation to contemporary tree disease threats." Philosophical Transactions of the Royal Society. Vol. 306. 1966-1974 Retrieved April 2015: http://classic.rstb.royalsocietypublishing.org/content/366/1573/1966.short
[424] Magarey, Roger D., et al., "Plant Biosecurity in the United States: Roles, Responsibilities, and Information Needs", pp. 875-884, Bioscience, Vol.59, No 10, November 2009. Retrieved April 2015: http://bioscience.oxfordjournals.org/content/59/10/875.short
[425] Fletcher, J. (2010).
[426] Fletcher, J. (2010).

warming. "Climate change affects disease transmission at three levels: firstly, it acts directly on the biology and reproduction of pathogens, hosts or vectors; secondly, it affects the habitats present in a region, the community of hosts that can live in them, and the lifecycles, or lifestyles, of those hosts; and thirdly, climate change induces social and economic responses, including adaptive and mitigating measures, which alter land use, transport patterns, human population movements, and the use and availability of natural resources."[427]

It was found that even small changes to the ecosystem could "have large impacts on the incidence of infection in a population, as pathogens more successfully jump species."[428] There is a cyclical impact: increased agricultural production leads to increased greenhouse gases, which further exacerbates climate change, leading to further issues with plant disease.[429]

Cultural Shifts: The Impact of the Organic and Non-GMO Movements on Plant Disease

Consumers' preference for food grown with minimal chemical pesticides has led to the presentation of GMOs into the agricultural scene. Due to the rise of pesticide-resistant pathogens and the introduction of foreign pests, "…chemical pesticide [use] continues to rise."[430] This rising incidence of plant diseases created a need for continued research in the area of biopesticides and other alternative strategies such as GMOs. However, consumer wariness of the use of these GMOs in food products makes the use of this as an alternative to pesticides difficult. More research should be done on the impact this has on the ecosystem and on end use products.

Some experts[431] have suggested the increased demand[432] for organically grown food and non-GMO food products may have an inadvertent negative affect on pests and diseases. The theory is that as more organic agriculture productions are stood up, it creates reservoirs for pests to thrive and provides time for pests to adapt to the pest-resistant GMO plants at a neighboring farm. No literature was discovered on this topic during the review. It is currently unknown what impact the increase of organic and non-GMO agriculture will have in the ecosystem.[433]

Conclusion

At this time, pathogen and disease concerns from developing countries do not directly affect our country but they have in the past. As the technology, crop productions, and import/export laws change, however, we will need to be vigilant in our methods of detection to ensure safety from new, or the reintroduction of eradicated, diseases that could impact agricultural supplies.

Generally, the literature reflected that there is a constant battle against the plant disease threat. One of the key risk factors about plant disease is its nature to evolve and change. The literature also reflected that the U.S. Government has an established and effective infrastructure to prevent, detect, respond, and mitigate this evolving threat. For a plant disease event to occur at such a

[427] Wilkinson, K. etc. (2011, May). P. 1934.
[428] Wilkinson, K. etc. (2011, May).
[429] There is extensive information on this topic in the literature, however Climate Change is addressed as a separate SNRA topic, thus it is treated in a limited way in this assessment.
[430] Wilkinson, K. etc. (2011, May).
[431] USDA Official
[432] The demand for organic food has seen double-digit increases each year for the past few years. USDA, Economic Research Service. http://www.ers.usda.gov/topics/natural-resources-environment/organic-agriculture/organic-market-overview.aspx
[433] We were unable to procure additional information on the topic of the impact of GMOs on the evolution of pests versus organic methods that do not employ pesticides.

level that it meets the criteria for a national level event it would likely be intentional (i.e., bioterrorism) or the cascading affect of some other disaster. Climate change may be an example of the latter.

The literature reviewed included discussions on biowarfare, and the potential for the deliberate introduction of pathogens within our country by state-sponsored threat actors. However, the main takeaway is that the country needs to increase awareness and research into detection, mitigation, and response for "deliberate use of plant pathogens to inflict harm on a person, company, industry, or nation."[434] While additional information is available on this topic, it is not within the scope of the topic for this assessment.[435]

Though the U.S. Government's approach to plant disease is well organized and effective, the literature encouraged continued research to stay ahead of existing plant disease as it continually evolves and mutates based on exposure to new resistant strains. The threat is not necessarily increasing, but it presents a dynamic landscape that requires close scrutiny.

[434] Fletcher, J. (2010).

[435] Intentional outbreaks—caused by an adversary intentionally releasing a plant pathogen or pest—are considered an Adversarial Hazard and are addressed by other topics in the SNRA.

Antibiotic Resistant Strains

Summary

Antibiotic-resistant pathogens, or "superbugs," are natural or man-made induced mutations created by the acquisition of new genes in disease causing bacteria resulting in the reduction or elimination of the effectiveness of antibiotics. Such resistant bacterium is presently a major public health threat and, if unresolved, threatens to evolve into a health security crisis. The Centers for Disease Control and Prevention (CDC) reported two million Americans acquire serious infections to one or more strains of antibiotic-resistant pathogens annually resulting in 23,000 deaths with many more dying from other medical conditions complicated by such infections.[436] In addition to their direct role in combating infectious diseases, the prophylactic use of antibiotics is essential for a wide range of basic to complex surgical and medical procedures. As antibiotic-resistance grows, so does the possibility of losing such surgical and other therapeutic interventions due to an unacceptable high risk of postoperative or procedural infections. Additionally, the public health risk of endemic bacterial contagious diseases will increase proportionately with antibiotic resistance (e.g. Group A Streptococcus (GAS) or “strep;” pneumococcal pneumonia; bacterial meningitis; multidrug-resistant tuberculosis [MDR-TB]; etc.). There is also the added risk that the public confidence in scientific evidence based medical therapies could eventually be undermined causing patients to seek unproven and hazardous alternatives cures.

Antibiotic-resistant pathogens are a direct threat to the resiliency of the nation. This would include increased morbidity and mortality rates related to trauma and contagious diseases impacting: U.S. military personnel, public safety officers and health-care workers. Moreover, services provided by critical health infrastructures such as tertiary care centers, nursing homes, dialysis centers, etc. could be dramatically impaired due to healthcare-acquired (or nosocomial) antibiotic-resistant pathogens. Antibiotic-resistant pathogens increases the strain on limited medical and public health resources at all levels of government as well as carry significant future risk to domestic and international economies.[437] This issue also presents an increased risk to a rapidly aging U.S. population who are more susceptible and vulnerable to infectious diseases. Current intercontinental commerce and travel provides ready opportunities for antibiotic-resistant pathogens to spread globally, severely limiting the ability of any one country to successfully tackle this issue in isolation. International cooperation will be required to avoid a post-antibiotics world.

Discussion

In recognition of the risk posed to the nation by antibiotic-resistant pathogens, the *National Strategy for Combating Antibiotic-Resistant Bacteria* was released by the White House in

[436] Centers for Disease Control and Prevention, *Antibiotic Resistance Threats in the United States, 2013* (Washington, DC: US Department of Health and Human Services, 2013), p. 11.

[437] British High Commission- Chaired by Jim O’Neill (December 2014) *Antimicrobial Resistance: Tackling a crisis for the health and wealth of nations,”* United Kingdom. http://amr-review.org/sites/default/files/AMR%20Review%20Paper%20-%20Tackling%20a%20crisis%20for%20the%20health%20and%20wealth%20of%20nations_1.pdf

September 2014.[438] This national strategy initiative was in direct response to CDC's findings that an estimated 2 million people annually in the U.S. acquire serious bacterial infections resistant to one or more of the antibiotics, resulting in approximately 23,000 deaths.[439] These numbers do not include those who die from other conditions that were complicated by an antibiotic-resistant infection. Antibiotic-Resistant is defined in this National Strategy as "…resistance results from mutations or acquisition of new genes in bacteria that reduce or eliminate the effectiveness of antibiotics."

Simply stated, antibiotic-resistant pathogens are able to adapt, multiply, and cause diseases unimpeded by the use of one or more antibiotic therapies. Antibiotic-resistant pathogens result in increased severity of infection with greatly limited and more expensive treatment protocols – if treatment is available at all. Over usage of antibiotics is the primary cause for the increase in antibiotic resistance as select bacteria survives by developing mutant genes against which antibiotics have decreased effectiveness. Through reproduction and/or the exchange of genetic material between different bacteria such resistance may spread rapidly and unpredictably, potentially causing a wide scope of resistant infections. As antibiotics often belong to similar classes of medicines, specific resistance to one agent can result in resistance to an entire related class of antibiotics. In addition to circulating in human and animal populations, resistant bacteria can be also found in the human consumption food-chain.

As the risk of antibiotic-resistant pathogens grows, so will the associated morbidity and mortality rates, resulting in longer hospitalization stays, increasing the risk of compromising protection of surgical patients and others undergoing a wide-range of medical and dental procedures as well as an accompanying increase health care costs. The CDC has estimated annual excess direct health care cost of antibiotic-resistant pathogens to the U.S. economy at $20-35 billion, including approximately 8 million additional days of hospitalization, with an annual lost productivity cost of $35 billion.[440]

Inappropriate and overuse of antibiotics can exacerbate the selection resistant microorganisms to such an extent that "[t]he extensive use of antimicrobial drugs has resulted in drug resistance that threatens to reverse the medical advances of the last seventy years."[441] This problem is compounded in hospitals, nursing homes, etc., where the widespread use of antibiotics, along with the close proximity among the sick, provides a fertile environment for developing and transmitting antibiotic-resistant pathogens, also known as nosocomial infections. This becomes a more pressing concern given the increased risk presented by a rapidly aging U.S. population that is more susceptible and vulnerable to infectious diseases while concurrently placing greater

[438] The White House (September 2014) *The National Strategy for Combating Antibiotic-Resistant Bacteria*, Washington, D.C. https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_carb_report_sept2014.pdf

[439] Centers for Disease Control and Prevention, *Antibiotic Resistance Threats in the United States, 2013* (Washington, DC: US Department of Health and Human Services, 2013), p. 11

[440] Roberts, RR, Hota, B, Ahmad, I, et al. *"Hospital and Societal Costs of Antimicrobial-resistant Infections in a Chicago Teaching Hospital: Implications for Antibiotic Stewardship,"* Oxford Journal of Clinical Infectious Disease, 49(8): 1175-1184, 2009. www.tufts.edu/med/apua/consumers/personal_home_5_1451036133.pdf.

[441] Interagency Task Force on Antimicrobial Resistance, 2012. *A Public Health Action Plan to Combat Antimicrobial Resistance* - page 5. Washington, D.C. http://www.cdc.gov/drugresistance/pdf/actionplan-2012.pdf

utilization demand on such health-care facilities. The U.S. population aged 65 and over, currently at approximately 43.1 million, is projected to grow to 83.7 million in 2050.[442]

There is also the concern that antibiotic-resistant pathogens are being accelerated through the commercial practice of adding antibiotics to agricultural feed products to stimulate growth and/or for disease control in animals confined in crowded and unsanitary conditions, especially given that "approximately 80 percent of the antibiotics sold in the United States are used in meat and poultry production."[443] To illustrate in 2011, "ground beef from the Hannaford grocery store chain in New England was linked to 19 infections and at least seven hospitalizations, all caused by a strain of Salmonella resistant to multiple antibiotics, including amoxicillin/clavulanic acid, ampicillin, ceftriaxone, cefoxitin, kanamycin, streptomycin, and sulfisoxazole."[444] CDC has presently identified "carbapenem-resistant, *Enterobacteriaceae* (CRE), ceftriaxone-resistant *Neisseria gonorrhoeae* and *Clostridium difficile*," within its highest or "urgent" threats.[445]

The following are included in the CDC's second highest or "serious" threats category:

> Multidrug-resistant *Acinetobacter*, Drug-resistant *Campylobacter*, Extended spectrum *β-lactamase* producing *Enterobacteriaceae* (ESBLs), Vancomycin-resistant *Enterococcus* (VRE), Multidrug-resistant *Pseudomonas aeruginosa*, methicillin-resistant *Staphylococcus aureus* (MRSA), Drug-resistant *Non-typhoidal Salmonella*, Drug-resistant *Salmonella Typhi*, Drug-resistant *Shigella*, Drug-resistant *Streptococcus Pneumonia* and Drug-resistant *Tuberculosis*.[446]

The third level, labeled "concerning" threats include:

> *Vancomycin-resistant Staphylococcus aureus (VRSA), Erythromycin-resistant Group A Streptococcus*, and *Clindamycin-resistant Group B Streptococcus*. CDC has also indicated that "Among all of the bacterial resistance problems, gram-negative pathogens are particularly worrisome, because they are becoming resistant to nearly all drugs that would be considered for treatment."[447]

The U.S. Department of Health and Human Services (HHS) is the lead federal agency responsible for addressing and coordinating the whole of government response to this issue. The scale of antibiotic-resistant pathogens needs to be acknowledged as a global risk within the context articulated in the U.S. Department of Health and Human Services' (HHS) *National Health Security Strategy 2015-2018*. "The health of the American people and that of the people around the world are more closely linked than ever before. Greater movement of people, animals, and goods across international borders increases the risk of exposure to health threats

---

[442] Jennifer M. Ortman, Victoria A. Velkoff, and Howard Hogan, U.S. Census Bureau, *An Aging Nation: The Older Population in the United States*, May 2014, Report Number: P25-1140. http://www.census.gov/content/dam/Census/library/publications/2014/demo/p25-1140.pdf

[443] Congresswomen Slaughter Louise M. U.S. House of Representatives. "*Confirmed: 80 Percent of all antibacterial drugs used on animals, endangering human health.* http://louise.house.gov/press-releases/confirmed-80-percent-of-all-antibacterial-drugs-used-on-animals-endangering-human-health/

[444] CDC. 2012. "*Investigation Update: Multistate Outbreak of Human Salmonella Typhimurium infections Linked to Ground Beef.* www.cdc.gov/salmonella/typhimurium-groundbeef/010512/index.html

[445] The White House (September 2015) *The National Strategy for Combating Antibiotic-Resistant Bacteria*, Washington, D.C. https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_carb_report_sept2014.pdf

[446] Centers for Disease Control and Prevention, *Antibiotic Resistance Threats in the United States, 2013* (Washington, DC: US Department of Health and Human Services, 2013), p. 7 & 22.

[447] Ibid

originating outside one's own country."[448] To underscore how wide-spread this issue is, the European Centre for Disease Prevention and Control (ECDC) and European Medicines Agency (EMEA) in 2007, estimated 25,000 deaths attributable to infections due to selected antibiotic-resistant pathogens in the European Union, Iceland and Norway.[449] And "In a study of resistance patterns of several common bacteria in China in 1999 and 2001, the mean prevalence of resistance among hospital-acquired infections was as high as 41%, and that among community-acquired infections was 26%.[450]

In an age of globalization, no country can on its own ensure the public health of its population from this risk. Every country is directly or indirectly vulnerable by forces driving international social, economic, and political interdependences such as immigration, travel, commerce, etc. Additionally, foreseen and unforeseen consequences may occur driven by natural and geopolitical crises (e.g. global climate change, conflict, mass refugee displacement, breakdown of other nation critical health infrastructure, etc.) which reduce the global resiliency to antibiotic-resistant pathogens.

In conclusion the U.S. Department of Health and Human Services (HHS) provides the leadership for ensuring that the "actions the United States takes domestically must be complemented by coordinated international action in order to ensure that resistant strains that arise in one part of the world are rapidly detected, diagnosed, and contained at the source of emergence. The United States and international partners must work to promote innovations in drug and diagnostics development, enhance stewardship of existing antibiotics in human and agricultural settings, and strengthen systems for detecting, diagnosing, and monitoring resistance so that reporting is timely, accurate, and transparent."[451]

[448] U.S. Department of Health and Human Services (HHS). (2015, February) *The National Health Security Strategy 2015-2018 (NHSS)*. Page 29, Washington, D.C. http://www.phe.gov/Preparedness/planning/authority/nhss/strategy/Documents/nhss-final.pdf

[449] European Centre for Disease Prevention and Control ECDC/ European Medicines Agency: *EMEA Joint Technical Report: The Bacterial Challenge: Time to React***.** ECDC, Stockholm Sweden; 2009.

[450] Heddini A, Cars O, Qiang S, Tomson G., *Antibiotic Resistance in China--a Major Future Challenge*. Lancet. 2009 Jan 3;373 (9657):30. doi:10. 1016/S0140-6736(08)61956-X. http://www.thelancet.com/pdfs/journals/lancet/PIIS0140-6736(08)61956-X.pdf

[451] The White House (September 2015) *"The National Strategy for Combating Antibiotic-Resistant Bacteria"*, page 20. Washington, D.C. https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_carb_report_sept2014.pdf

Emerging Infectious Diseases Other Than Influenza

Summary

Emerging Infectious Diseases (EIDs) with pandemic potential represents a major worldwide risk to global health security. Though there is no single universally agreed upon definition, EIDs can be understood either as new recognized diseases or "re-emerging" or "resurgent diseases" which are known and may have been previously controlled but are now reappearing with increasing occurrence, or threaten to increase over previously endemic or new population or geographic area. This also includes pathogens that have developed new attributes such as increase resistance or virulence. Of most concern are EIDs which have possible global pandemic risk where limited or no readily available therapeutic counter-measures are available. Leaving governments to rely on enhanced mass public health infection control practices such as protective travel and commercial restrictions, closing schools, or in worst case scenarios enforced quarantine for the affected population. If it is scientifically proven that a particular EID resulted from an accidental or deliberate release, then it could be anticipated that the U.S. government, private critical health care infrastructure stakeholders, as well as foreign governments will take countermeasures commensurate with the nature and scope of such a threat. Such a scenario may result in additional and unforeseen geopolitical consequences depending on the scale and scope of the event or incident.

Not including influenza outbreaks such as H1N1, examples of recent notable EIDs have included: Ebola; Severe Acute Respiratory Syndrome (SARS); Middle East Respiratory Syndrome (MERS). Combined, these EIDs resulted in the loss of millions of lives and billions of dollars. Causal factors include: microbial adaptation and evolution; demographic migration; new technology and industry; increased economic development and changing land use; greater contact between people and animals; international travel and trade; and the lack of adequate global public health infrastructure to carry out surveillance and control measures. Added to this list is the potential for bio-engineered EIDs resulting from future military conflict or terrorism. In addition to the human and economic toll, the Ebola epidemic in West Africa is very instructive of the risk that EIDs have to destabilize governance processes, ferment social unrest, overstress critical national health infrastructures, and restrict international commerce and travel.

Discussion

An emerging infectious diseases (EIDs) is defined as "infectious disease that is newly recognized as occurring in humans; one that has been recognized before but is newly appearing in a different population or geographic area than previously affected; one that is newly affecting many more individuals; and/or one that has developed new attributes."[452] New and naturally occurring attributes can include changes in mode of transmission, incubation periods, severity of morbidity and mortality rates, etc. Additionally, there is the risk of man-made bio-engineering to be

[452] Institute of Medicine IOM, *Microbial Threats to Health: Emergence, Detection and Response*, 2003; and Fineberg and Wilson, "Emerging Infectious Diseases," International Risk Governance Council (IRGC), 2010.

deliberately or inadvertently misused to create new or change existing pathogen characteristics sufficient to result in the direct or indirect endangerment of humanity.[453]

According to the Centers for Disease Control and Prevention (CDC) "approximately 75% of recently emerging infectious diseases affecting humans are diseases of animal origin; approximately 60% of all human pathogens are zoonotic."[454]

Causes involved in the emergence of infectious diseases can be broadly categorized as "(1) genetic and biological aspects; (2) physical environmental factors; (3) ecological factors; and (4) social, political, and economic factors".[455] These complex and interdependent categorizations can be further defined into the following thirteen points:

1. Microbial adaptation and change
2. Human susceptibility to infection
3. Climate and weather
4. Changing ecosystems
5. Human demographics and behavior
6. Economic development and land use
7. International travel and commerce
8. Technology and industry
9. Breakdown of public health measures
10. Poverty and social inequality
11. War and famine
12. Lack of political will
13. Intent to harm[456]

The National Institute of Allergy and Infectious Diseases (NIAID), under the U.S. National Institutes of Health (NIH), defines EIDs as infectious diseases that have newly appeared in a population or existed but are rapidly increasing in incidence or geographic range, or that are caused by one of the NIAID Category A, B, and C Priority Pathogens. Category A pathogens are those organisms/biological agents that pose the highest risk to national security and public health because they:

- Can be easily disseminated or transmitted from person to person
- Result in high mortality rates and have the potential for major public health impact

---

[453] BioMed Central/Genome Biology. "On The Trail Of Rogue Genetically Modified Pathogens." Science Daily. , 18 March 2008. www.sciencedaily.com/releases/2008/03/080317191441.htm

[454] Centers for Disease Control and Prevention - National Center for Emerging and Zoonotic Infectious Diseases *"Emerging and Zoonotic Diseases — At a Glance"* at http://www.cdc.gov/ncezid/

[455] Institute of Medicine IOM, Mark S. Smolinski, Margaret A. Hamburg, and Joshua Lederberg, editor(s);"*Microbial Threats to Health: Emergence, Detection and Response*," pages 53-54, 2003. Committee on Emerging Microbial Threats to Health in the 21st Century, Board on Global Health. National Academy of Sciences

[456] Ibid

- Might cause public panic and social disruption
- Require special action for public health preparedness[457]

Examples include: *Bacillus anthracis* (Anthrax); *Clostridium botulinum toxin* (Botulism); *Yersinia pestis* (Plague); *Variola major* (Smallpox) and other related pox viruses; *Francisella tularensis* (Tularemia); Viral hemorrhagic fevers (Arenaviruses, Bunyavirus, Flaviruses, Filoviruses-Ebola); etc.[458]

Category B pathogens are the second highest priority organisms/biological agents because they are:

- Moderately easy to disseminate
- Result in moderate morbidity rates and low mortality rates
- Require specific enhancements for diagnostic capacity and enhanced disease surveillance[459]

Examples include: *Burkholderia pseudomallei* (Melioidosis); *Coxiella burnetii* (Q fever); Brucella species (Brucellosis); *Burkholderia mallei* (Glanders); *Chlamydia psittaci* (Psittacosis); *Ricinus communis* (Ricin toxin); *Clostridium perfringens* (Epsilon toxin); Staphylococcus enterotoxin B (SEB); *Rickettsia prowazekii* (Typhus fever); etc.[460]

Category C pathogens are the third highest priority and include emerging pathogens that could be engineered for mass dissemination in the future because of:

- Availability
- Ease of production and dissemination
- Potential for high morbidity and mortality rates and major health impact[461]

Examples include: Nipah and Hendra viruses; Tickborne hemorrhagic fever viruses; Tickborne encephalitis complex flaviviruses; Yellow fever virus; Tuberculosis, including drug-resistant TB; Influenza virus; Other Rickettsias; Rabies virus; Prions; etc.[462]

Emerging Infectious Diseases is an evolving and constant risk. However, the ability to significantly mitigate this risk is also progressing through the leadership provided by the Department of Health and Human Services in spearheading U.S. efforts in meeting the global challenges related to public health surveillance and detection, critical health care capabilities for timely and effective and response. This includes sufficient resources and training to develop efficient information-sharing and research leading to the advancement of new diagnostics, vaccines, and pharmaceuticals which to address EID.

In conclusion, "The health of the American people and that of the people around the world are more closely linked than ever before. In such an interconnected environment, the best way for a country to protect its population is to prevent a health threat from emerging and spreading in the

---

[457] National Institute of Allergy and Infectious Diseases (NIAID) - "*Biodefense and Emerging Infectious Diseases - NIAID Category A, B, and C Priority Pathogens"*- February 2015. http://www.niaid.nih.gov/topics/BiodefenseRelated/Biodefense/Pages/CatA.aspx
[458] Ibid
[459] National Institute of Allergy and Infectious Diseases (NIAID) - "*Biodefense and Emerging Infectious Diseases - NIAID Category A, B, and C Priority Pathogens"*- February 2015. http://www.niaid.nih.gov/topics/BiodefenseRelated/Biodefense/Pages/CatA.aspx
[460] Ibid
[461] Ibid
[462] Ibid

first place. This means addressing threats early and at their source, before they spread more widely within and across borders; it also means that other countries, including the United States, should prepare for the arrival of such trans-national threats within their own borders."[463]

[463] U.S. Department of Health and Human Services (HHS)-Assistant Secretary for Preparedness and Response, *"National Health Security Strategy and Implementation Plan 2015-2018"* - February 2015. http://www.phe.gov/Preparedness/planning/authority/nhss/Documents/nhss-ip.pdf

Threat and Hazard Identification and Risk Assessment: Capability Target Visualizations

Introduction

The SNRA provides a strategic view of risk to support the collective understanding of the full range of threats, hazards, and challenges facing the Nation. With this in mind, the SNRA project team analyzed the Threat and Hazard Identification and Risk Assessments (THIRA) received from jurisdictional partners to gain a better understanding of what capabilities requirements jurisdictions have identified and for which they are currently planning. The SNRA project team intends on comparing the effects identified across a broad range of risks from the SNRA, against the capabilities requirements identified in the jurisdictional THIRAs, to identify any correlations between national-level risk assessment and reported jurisdictional requirements. The following depicts the outputs from the THIRA analysis. The crosswalk between effects identified in the SNRA and jurisdictional capability requirements was not accomplished during the 2015 SNRA project and should be considered for future iterations of the SNRA.

Background

The THIRA is a four-step common risk assessment process that helps the whole community understand its risks and estimate capability requirements. FEMA) Regions and jurisdictions identify risks in Step 1 of the THIRA process and map their risks to core capabilities to develop capability targets which define success. Capability targets provide a glimpse of the impacts regions and jurisdictions are preparing for across the Nation.

Analysis

The following graphs depict representative targets* in terms of absolute capability for selected core capabilities. Each core capability graph depicts a sample subset of capability targets on a logarithmic scale and incorporates isoclines to show increasing levels of absolute capability requirements. Taken together, these graphs demonstrate the range of jurisdictional planning to deliver core capabilities across a wide range of threats and hazards.

**Representative targets depict a sample subset of submitted 2013 THIRA targets, as not all targets included comparable elements for analysis.*

Fatality Management Services

Figure 7 represents the range of 2013 THIRA targets that focused on initiating fatality management services within a set period of time. While the number of fatalities varied widely, most jurisdictions defined their success as initiating fatality management within 24 to 72 hours. Figure 1 shows a majority of the represented targets included impacts of 10,000 fatalities or fewer, while a smaller subset suggested potential impacts of higher magnitudes. Several of

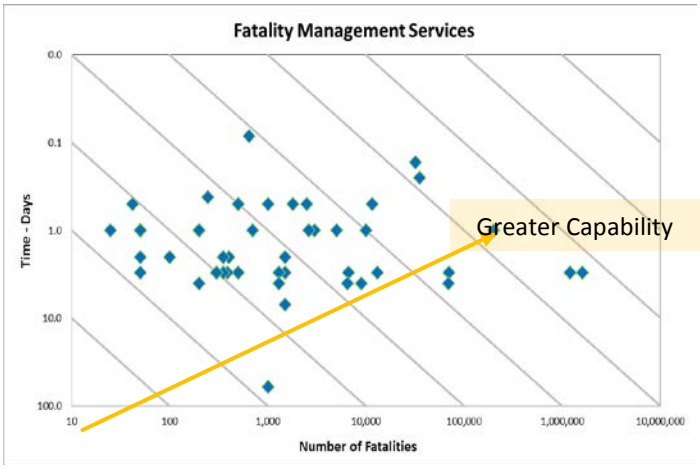


Figure 7: Fatality Management Services

the targets with higher fatality impacts also identified time frames of 24 to 72 hours, indicating that these targets require greater capability to be successful.

Mass Care Services

A majority of Mass Care Services targets indicated jurisdictions' desires to achieve their targets within 72 hours or fewer; however, a third of representative capability targets included a range of 5 days to 8 weeks as sheltering objectives can vary widely depending on requirements. Likewise, the range of people requiring sheltering services ranged from several dozen to several million, indicating that jurisdictions are planning for a wide scale of impacts. The variation in Mass Care Services targets is likely due to the wide range of sheltering impacts identified in Step 3 of the THIRA process, as impacts are linked to the size and complexity of threat and hazard scenarios identified in Step1 of the THIRA process.

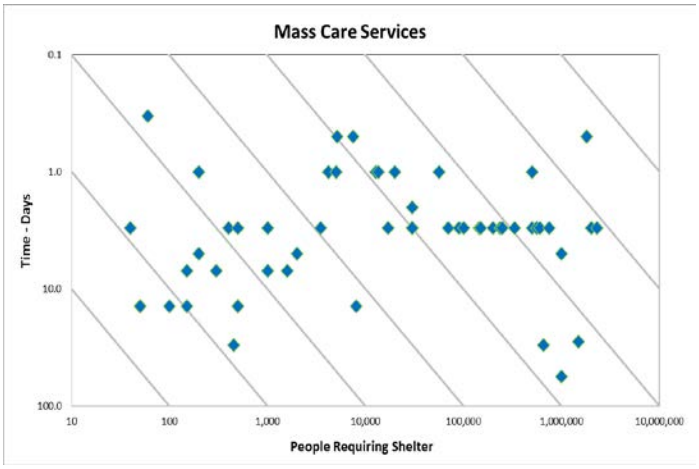


Figure 8: Mass Care Services

Public Health and Medical Services

Figure 9 shows that approximately half of the represented Public Health and Medical Services targets included impacts of 10,000 to 100,000 people requiring treatment. The Public Health and Medical Services targets are correlated to time parameters, as they depict that the time required to achieve success increases with the number of people requiring treatment. Several targets requiring the most capability to be successful included longer-term actions, such as providing prophylaxis and treatment for an epidemic.

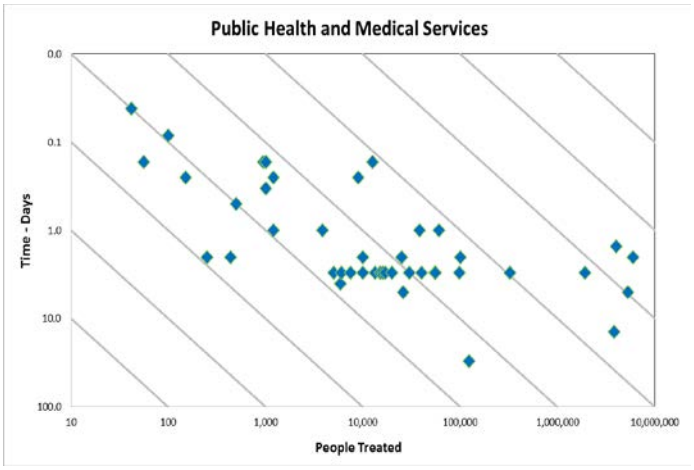


Figure 9: Public Health and Medical Services

Housing

Similar to the wide range of targets to deliver Mass Care Services, Figure 4 depicts a wide variation in Housing targets to meet long-term housing

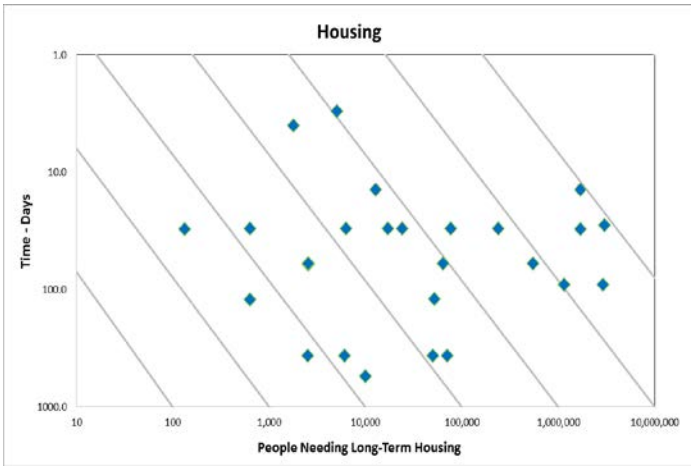


Figure 10: Housing

requirements. People needing long-term housing varied widely from less than a thousand to several million, while time constraints ranged from 3 days to 4 years due to the nature of the Recovery mission area and Housing core capability. The wide variation in Housing targets is likely due to the size and complexity of threat and hazard scenarios selected by jurisdictions in Step 1 of the THIRA process and the unique displaced populations identified as potential impacts in Step 3.

Cyber-Risk Scoping Study for the Strategic National Risk Assessment

Summary

The Office of Cyber and Infrastructure Analysis (OCIA) in the National Protection and Programs Directorate (NPPD) has worked with partners in NPPD to identify, scope, and provide preliminary assessments of the leading categories of risk from cybersecurity incidents, from 2015 and 2020.[464] While, this analysis is not definitive, it provides the first known assessment of such risks that is entirely unclassified and is not focused on vulnerabilities or threat actors, but on the consequences of such incidents on the victims of the attacks and the United States. This study will inform the update of the Strategic National Risk Assessment that is being refreshed as part of the National Preparedness Goal led by the Federal Emergency Management Agency (FEMA).

The February 2015 Worldwide Threat Assessment by the Office of the Director of National Intelligence (ODNI) summarizes the current state of affairs from a strategic perspective:

> Cyber-threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact. The ranges of cyber-threat actors, methods of attack, targeted systems, and victims are also expanding. Overall, the unclassified information and communication technology (ICT) networks that support U.S. Government, military, commercial, and social activities remain vulnerable to espionage and/or disruption. However, the likelihood of a catastrophic attack from any particular actor is remote at this time. Rather than a "Cyber-Armageddon" scenario that debilitates the entire U.S. infrastructure, we envision something different. We foresee an ongoing series of low-to-moderate level cyberattacks from a variety of sources over time, which will impose cumulative costs on U.S. economic competitiveness and national security. [465]

Both the ODNI and NPPD's assessments reveal that within the last few years there have been significant changes to the availability and transparency of information about cybersecurity concerns in the United States (U.S.) This development allows us to create an analytic product which provides qualitative assessments with quantitative details that illustrate the trends of increasing risks. The consequence-focus of this analysis shows that, while some scenarios create significant direct burdens on individual organizations, the overwhelming majority of the consequences are experienced broadly throughout the U.S. by individuals, companies, not-for-profit organizations, and government authorities at all levels. While some scenarios can be clearly associated with financial losses, other scenarios may have greater risk. Much of this risk-burden comes from the high degree of uncertainty.

---

[464] OCIA thanks U.S. Computer Emergency Readiness Team (US-CERT), Industrial Control Systems-Computer Emergency Readiness Team (ICS-CERT), the Office of Infrastructure Protection, private sector partners, and the NPPD Front Office for their contributions, as well as the many Whole of Community contributors to the SNRA.

[465] Clapper, James, Statement for the Record, Worldwide Threat Assessment of the Intelligence Community, http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf , accessed March 24, 2015

Background

The body of evidence available to the public regarding cybersecurity incidents and their consequences is notoriously limited; information is revealed, rather than observed, and these revelations give us an incomplete view. Despite this challenge, NPPD believes that there is greater knowledge about cybersecurity risks today than there was when the first Strategic National Risk Assessment was conducted in 2011 to inform the National Preparedness Goal.

The distribution of this knowledge is inconsistent; it does not reflect the risk itself, so much as the degree to which victims of cybersecurity challenges have been forthcoming. We consider this analysis a scoping study, as it provides insights into size, depth, cost and frequency of various aspects of the risk space, without meeting a requirement to put forward comparable measures of expected loss for different types of scenarios. Furthermore, a scoping study also allows the use of inferred resources, which have greater uncertainty associated with them.

The selection of scenarios should help analysts and planners recognize general categories of risk in cyberspace and understand specific examples of how these incidents have developed. We hope that the readers who use this assessment will include those focused on:

- Proactive investments in improved information security,
- Proactive investments in operational alternatives that make an organization less vulnerable in the event of a cybersecurity incident,
- Preparations for responding to an incident that affects the data and operations of the organization, and
- Discussions and decisions about how to engage effectively in the public-private partnership necessary to understand and manage security and resilience risks.

These scenarios also allow the reader to gain insights into what is observed by NPPD, without having to delve into classified information or distorting our view of the cyber-risk landscape. The assessments for the scenario types may reflect publicly reported examples, insights from NPPD's Industrial Control Systems Computer Emergency Response Team (ICS-CERT), analogy, or the results of simulations and analysis. The scenarios themselves reflect concerns identified by different stakeholders, including:

- State and local inputs in the Threat and Hazard Identification and Risk Assessment (THIRA), which showed a high level of concern with the uncertainty and poor preparedness for cybersecurity incidents. The raw data for the THIRA sometimes reflected inconsistencies or infeasibilities that we allowed in this study as a reflection of how unclear this threat space is, and we adjusted to generalized scenarios of types that allowed a productive assessment.
- Research of publically available reporting of incidents. Often, such research discovers instances of reported breaches or hints of problems that are not publically discussed. Not all data is presented consistently or disaggregated sufficiently so that one can discern the characteristics of individual cybersecurity incidents. Such research clearly reveals the degree to which there is little consensus for how to assess the consequences of such events.
- Reporting in the ICS-CERT Monitor. These scenarios reflect anonymized reporting by partners and may provide a clear basis for why stakeholders are so concerned about cybersecurity risks that have not really fully materialized.

- Scenarios developed for exercises by the National Cybersecurity and Communications Integration Center (NCCIC) that represent shared concerns among key partners. Exercises allowed them to discuss how partners would deal with a challenge as it emerges. Unlike the state and local-generated scenarios, the information and data available to the NCCIC reflects a much clearer understanding of cybersecurity professionals about how such incidents might unfold. They also reflected a general lack of understanding of how to assess the consequences.
- Office of Cyber and Infrastructure Analysis (OCIA)-identified scenarios. Such scenarios were developed when we found a category of cybersecurity incident that was sufficiently well defined that analysis could improve the body of knowledge and understanding about the potential risks. In some cases, OCIA used simple logic models to clarify how the results of an as yet unseen cyberattack would be analogous to the effects of another type of event. It is certain that the societal and economic consequences could be greater than most of the consequence assessments presented here. But it is helpful for planners and analysts to think through the logic of how such events unfold.

This study focuses on the types of victims, what it costs them, and whether or not we as a nation should expect these losses to increase. Analysts in the cybersecurity environment may wish to study this and other referenced cybersecurity annual reports to gain better insights into how to prepare for such incidents, and hopefully, how to avoid them. This study should help all readers understand why we should manage these risks.

The summary of these scenarios includes the general category of the scenario type, some distinct manifestations that affect the risk, and NPPD's view of the risk trend from 2015-2020. The risk trend is a reflection of the combination of:

- frequency of incidents;
- strength, speed, virulence, of attacks; and
- value or scope of expected consequences – or both.

In scoping expected consequences we considered the pattern of vulnerabilities, the information and communications technology effects, the infrastructure functional effects (if they exist), and whatever organizational and societal consequences can be described.

It is extremely difficult to parse out the perception of the risk from the real risk in cybersecurity incidents. Our investments in cybersecurity pay off in increasing awareness. The increasing willingness of victims to report what is going on is believed to be an accurate reflection of real increasing risk. Some of these incidents, however, are discoveries that have been at risk for some time, but did not know it.

Those areas of the cyber-risk landscape that seem most uncertain may be prioritized to develop new analytic capabilities, improve information sharing, and to improve risk management and emergency response. The areas that seem to have more compelling evidence may be priorities for connecting the dots between the cybersecurity source of the risk, the operational activities that are impacted, and the executive decisions to manage risk across the enterprise.

Table 15 summarizes different categories of scenarios considered in this analysis, providing a qualitative assessment of the risk trend. These scenario types are described more fully in the pages that follow.

Category	Scenario	Risk Trend
National Security	Insider threat takes advantage of information security assumptions to facilitate a compromise of U.S. National Security Information and international standing	High, Increasing Slightly
	Sensitive but unclassified information is extracted by an adversary and used for intelligence	Moderate, Increasing Significantly
	Cyberattack interferes with availability of traffic flowing from a civil-purpose data source to a national-defense user	Unclear
	Supply chain corruptions result in hardware or software that has imbedded exploits to be triggered by time or a change in conditions	Unclear
Financial Services	Systemically important bank is subjected smokescreen DDoS campaigns and the extraction of customer PII and financial data	High, Increasing Significantly
	Payment system infrastructure is hacked, enabling criminals to increase the value of payments and create fraudulent means to receive payments	Moderate-High, Increasing Slightly
	Criminal hackers install malware in payment card systems for national retailer, extracting PII and financial information for customers over the course of several months. The information is sold on the black market	Moderate
Other data breach	Data breach extracts PII and other information from a government entity or not-for-profit	Moderate, Increasing Significantly
	Data breach extracts PII, financial information and personal health information from hospital or insurer	Moderate-High, Increasing Significantly
	Data breach extracts intellectual property from innovative businesses or R&D center	High, Increasing Significantly
Just DDoS	DDoS attack campaign that just impedes access	Low, Increasing Slightly
Attacks on ICS	Distributed campaign of attacks on natural gas pipeline system ICSs, timed to maximize the impacts on energy assurance	Unclear
	Cyberattack on ICSs in a drinking water systems result in contaminated water supply	Unclear
	Distributed and coordinated attack on ICSs used in drinking water system results in contaminated water supply and broken infrastructure	Unclear
	Complex coordinated attack on the grid is conducted so as to maximize physical damage and power outage	Unclear
Cyber-9/11[466]	Complex coordinated attack on significant infrastructure resulting in catastrophic outcomes	Unclear for utilities, High, Increasing for Financial Services
	Cyberattack leaves malware inserted in the control systems of many key infrastructures without further activation, such as is observed with an advanced, persistent threat	Unclear

Table 15: Summary of Cyber-Risk Scenarios

[466] In most cases, when someone refers to a cyber-9/11 they are not connecting this to terrorism, but to the concept of a large-scale attack that has a broadly felt negative impact on the Nation and compels a change in the way that governments and individuals go about their business. Other references to this game-changing cataclysmic event have included "cyber-Pearl Harbor" and "cyber-Armageddon".

National Security Scenarios

Introduction

It is very difficult to estimate risk for national security scenarios. There are intangible but sometimes existential values involved, such as national sovereignty, our ability to defend our homeland and interests in the event of hostility, the confidence of our people – and other nations – in our Government and our economy.

The question of risk is commonly determined for natural hazards, accidents, and random criminal acts as a function of likelihood and consequence. The frequency for such incidents is typically easy to discern based on observation of past incidents. However, for national security incidents there is a potentially large and unmeasurable gap between what is actually going on, and what is observed. Efforts to estimate such frequencies by observation will undoubtedly undervalue the risk dramatically. Efforts to estimate the real frequency of such incidents will be speculation.

This challenge is exasperated by the ambiguity of how to define the scope of an information-security-centric national security incident. It may be a single act of unlawfully collecting classified information or transferring it to a foreign national. Should it be the prolonged efforts over an entire career of acting in the clandestine service of a foreign government? Do we define it as the discovery or legal resolution of an espionage case in which the use of information technology (IT) was a primary means? Is it carrying out any intelligence operation through information and communications technology which once demanded human intelligence agents? Are some cyberattacks by nation-states an attempt to divert attention from some more subtle actions? Do sophisticated threat actors prepare complex overwhelming cyberattacks with physical system effects to obscure our ability to detect and defend against a physical attack? Do they use such attacks to remind other nations of their power to retaliate if they are not given full rein in other spheres of international influence?

In defining the impact of a national security incident, the primary measure may be a change of vulnerability. Our exposure as a nation is greater. There is also a cost. How do we account for the loss of the value of significant investments made to protect our nation?

What about nation-states' use of large volumes of sensitive-but-unclassified data to develop intelligence about the U.S.? The U.S. legal system and the Information Security Oversight Office recognize the responsibility of the U.S. Government to protect aggregated unclassified information with a classification in some cases. This is the recommended action in cases where the aggregate produces insights that warrant greater safeguarding of national security information. There is no mechanism to classify such information before it becomes aggregated, yet the use of modern cybersecurity exploits and Big Data analytic tools clearly enable foreign nations to develop the insights that our legal system expects us to protect as classified.

The lines between national security incidents and criminal acts become very blurred in cyberspace. When one considers the role of the foreign intelligence agents placed in the U.S. with false identities to function as spies and potential saboteurs during the Cold War, their assignments included tasks such as collecting information and preparing to disable the

Washington, D.C. electric grid and poison the public drinking water in the event of a superpower crisis.[467] The alignment of their tasks with the pattern of sophisticated cyberattacks on critical infrastructure-type targets suggests that the cyberattacks may be serving some of the same purposes as the sleeper cells of the Cold War. Like sleeper cells, advanced persistent threats (APTs) and sophisticated threat actors have historically been associated with highly resourced nation-states. They are able to gain access to computer systems and stay in these systems without detection for long periods of time. In some cases we have observed these types of attacks being brought to conclusion with extraordinary complexity in short periods of time. This is believed to be the result of the attackers' patient preparation of malware and exploits and readiness to wait for the timing to fulfill the objective of the attacker. The association of particular threats to any given nation is rarely publicly made. The ODNI reported that:

> Politically motivated attacks are now a growing reality with foreign actors reconnoitering and developing access to U.S. critical infrastructure systems which might be quickly exploited for disruption if the adversary's intent became hostile. In addition, those conducting cyber-espionage are targeting U.S Government, military, and commercial networks on a daily basis. These threats come from a range of actors, including: (1) nation states with highly sophisticated cyber programs (such as Russia or China), (2) nations with lesser technical capabilities but possibly more disruptive intent (such as Iran or North Korea), (3) profit-motivated criminals, and (4) ideologically motivated hackers or extremists. Distinguishing between state and non-state actors within the same country is often difficult—especially when those varied actors actively collaborate, tacitly cooperate, condone criminal activity that only harms foreign victims, or utilize similar cyber-tools. [468]

This connection was made by the U.S. Department of Justice recently, in the indictment of a team of Chinese military hackers, and again when the Federal Bureau of Investigation (FBI) attributes the November 2014 Sony attack to North Korea. In the Worldwide Threat Assessment the ODNI highlights the growing number of computer forensic studies by industry experts that strongly suggest that several nations – including Iran and North Korea – have undertaken offensive cyber-operations against private sector targets to support their economic and foreign policy objectives, at times concurrent with political crises.[469] Despite these recent cases of attribution, it is generally very hard to make the connection between any particular attack and a particular nation-state or threat actor with great confidence.

Complicating this analysis is the fact that increasingly the nation-state actors and the criminal element are using the same methods and tools. The threat of destroying data or damaging infrastructure was used in the past by criminals to extort payment from owners and operators of critical infrastructure. The majority of infrastructure-focused incidents can be traced back to advanced, persistent threats or sophisticated threat actors and are not accompanied by demands for money. The perpetrators are simply in our systems…waiting, sometimes for years before

---

[467] Kalugin, Oleg, former KGB general, interviewed by Josh Rogin, for Foreignpolicy.com, *Ex-KGB general: Soviet sleeper agents were tasked with blowing up DC power grid; poisoning water supply,* http://foreignpolicy.com/2010/07/12/ex-kgb-general-soviet-sleeper-agents-were-tasked-with-blowing-up-dc-power-grid-poisoning-water-supply/ accessed March 4, 2015.
[468] Clapper, James, Worldwide Threat Assessment Report.
[469] Ibid.

they are discovered. Some national security-focused analysts give this a benign interpretation, seeing it as a present-day application of the theory of mutually assured destruction, which serves as a disincentive to nation-states to use powerful weapons and risk retaliation. Other analysts see this as a modern-day version of the Soviet illegals program[470]. Its secretive nature makes it less a disincentive, since it is not obvious, and more a contingency plan. The ODNI falls into this category, reporting that "Politically motivated cyberattacks are now a growing reality, and foreign actors are reconnoitering and developing access to U.S. critical infrastructure systems, which might be quickly exploited for disruption if an adversary's intent became hostile.[471]

While the motivations of the individual nation-state intelligence services may be unknown, cyberattacks are affecting the civilian U.S. Government entities and the private sector and having a national security impact. Attacks that diminish the U.S. foundations of rule of law, respect for the privacy of the individual, intellectual property and economic security have the effect of degrading our national security. In most cases this is an indirect effect, thus, it is more subtle. This subtle erosion of our national values is difficult to manage because the victims cannot account for the idea that they are victims of well-planned foreign cyberattacks. We also have a hard time anticipating all of the systemic interdependencies among infrastructure sectors.[472]

Below is a small sample of the scenario space, each with a scoping assessment of the risk for the focus of the scenario. They are highly aggregated, limited by being completely unclassified, and by a lack of consensus for how to identify and measure the consequences. Scoping and contextualizing these risks is the first step to enable analysts to develop needed capabilities, for planners to begin to discern what response capabilities they lack, and to enable conversations about the value proposition for improving cybersecurity. Table 16 provides a more focused summary of the consequences, vulnerabilities and threats associated scenario 1. Subsequent tables will precede each scenario for the reader's convenience.

[470] The term "illegals" is used for intelligence staff officers who are recruited and trained to operate under deep cover in their target country. Unlike "legals" – intelligence officers who are given official diplomatic cover assignments and thus are protected by diplomatic immunity if discovered – illegals live and work seemingly ordinary lives, typically as immigrants with fake pasts. Illegals were expected to be ready to fulfill all manner of intelligence tasks when needed, from intelligence gathering to assassinations or sabotage, in the event of the outbreak of hostilities. For an article about this real, but rarely discussed practice, please see the Vanity Fair article, From Tradecraft to Sexpionage, Cold War K.G. B and U.S. Spies Concur: *The Americans* Actually Happened., http://www.vanityfair.com/hollywood/2014/05/the-americans-real accessed April 13, 2015

[471] Clapper, James, Worldwide Threat Assessment Report.

[472] Ibid. This point is made by the ODNI for some members of the private sector. NPPD believes this problem is more widespread.

Scenario	Consequences	Vulnerabilities	Threats
Insider threat takes advantage of information security assumptions to facilitate a compromise of U.S. National Security Information and international standing	The direct effects of these types of scenarios are the uncontrolled loss of classified information. The consequences, in peacetime include loss of value of intelligence sources and methods, loss of public trust, loss of international standing, competitive advantage to adversaries, and more. During a time of conflict these consequences could lead to unnecessary casualties, economic losses, and the risk of impaired national sovereignty.	Ineffective screening of personnel. Overly connected and unmonitored access to data within protected systems. Ability to use portable devices to collect records and to remove portable devices undetected.	Foreign intelligence agencies Unstable personnel in the cohort with unfettered access Disingenuous or corrupted individuals with unfettered access

Table 16: National Security Scenario Type 1

As information systems have become the core of the knowledge management and information sharing capability of the U.S. intelligence community, insider threats have increasingly used them as tools for collection and espionage. Since the year 2000, of the seventeen cases where a U.S. insider was accused or convicted of espionage in connection with their unlawful release of national security information, nine of those cases appear to have been facilitated by the use of computer systems in the furtherance of their crimes.

Some of these acts, most notably by Edward Snowden and Private Bradley Manning, took advantage of significant access to classified information systems to gather a broad range of information and used portable media to extract the data from its authorized location.[473]

A comparatively low consequence profile for such an incident would result from smaller amounts of less critical information being provided to a single adversary without a strong competitive advantage against the U.S. In cases where more information was carefully analyzed and prioritized for a highly capable foreign adversary's use, the consequences are much higher. Cases where individuals may have worked on behalf of Russia (or the former Soviet Union), accepted the protection of Russia, or who have pursued disclosure policies that benefit Russia are good examples of instances where there is greater harm. Examples of higher consequence cases that have harmed U.S. interests and international standing include the efforts of Robert Hanssen, Manning, and Snowden.[474]

The minimum economic consequences of such attacks are the exposure of significant U.S. sources and methods that cost at least tens of billions of U.S. dollars to develop and maintain.

[473] Edward Snowden was a contract computer professional who collected classified documents from the National Security Agency using his privileged access and then released portions of these documents publicly. Bradley Manning was an enlisted intelligence analyst in the U.S. Army who similarly collected classified documents and released them to the public through a website. Manning later underwent a gender transition and began using the name Chelsea.

[474] Robert Hanssen was an FBI agent who spied for the Russian Intelligence Services.

Exposing our sources and methods enables adversaries to develop ways to avoid being monitored, significantly reducing the value of the national investment. In the event of actual hostilities the strategic and operational value of this information is inestimable.

Analytic judgments of this situation, not guided by classified information, suggest that it is reasonable to project that such risks are increasing. From 2015 to 2020, given that current international tensions are becoming more acute and economic competition in the international marketplace plays an increasing role the past pattern of incidents is likely to continue. Individuals with authorized access are increasing the sophistication of their abuse of this access. The consequences of the public release or unauthorized transmittal to foreign agents of classified information may reasonably be greater, as the balance of power is shifting and tense. As our culture becomes increasingly fragmented and some in society view this type of activity as heroic, we might expect this to increase in frequency. However, this increase in motivated individuals may be counterbalanced by increasingly vigilant information security and counterintelligence.

Scenario	Consequences	Vulnerabilities	Threats
Sensitive but unclassified information is extracted by an adversary	Foreign intelligence services have large bodies of data useful for pattern analysis and future targeting. Often this is data about individuals with access to sensitive information.	Technical vulnerabilities vary. Management vulnerabilities include maintaining more PII, employment data, and other sensitive information than may be essential.	Foreign intelligence services conducting data breach attacks typically over the Internet

Table 17: National Security Scenario Type 2

Chinese intelligence efforts appear to take advantage of Big Data approaches to gathering unclassified information about individuals with access to classified information. Public reporting of the Anthem Blue Cross health insurance data breach attack revealed that there are strong indications the incident was perpetrated by Chinese hackers. Some have speculated about the value of the data on the large number of defense contractors at Northrup Grumman and Boeing whose personally identifiable information (PII) were gathered in the Anthem attack. [475] This attack will have serious economic repercussions on Anthem, and, if it is found to have exposed personal health information, it could theoretically cost the company over $800 billion, mostly in fines – which is likely to be an existential penalty. Limited regulatory tools meant to incentivize private companies to do all they can to safeguard individuals' data may also drive a wedge between the public and private sector in just such an area where collaboration is the only path to success. The more likely national security consequences of this attack may be that Chinese intelligence has large datasets that help them identify likely targets for further intelligence gathering.

Security researchers in Kaspersky Lab reported discovering a cyber-espionage campaign called "Careto", or "The Mask", which in February 2014 had been active in 31 countries for 7 years. The campaign appears to have been authored by Spanish attackers, and targets primarily

[475] Riley, Michael; Robertson, Jordan, Chinese State-Sponsored Hackers Suspected in Anthem Attack, http://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack, accessed March 3, 2015

government institutions, diplomatic offices and embassies, energy, oil and gas companies, research organizations and activists. Victims were in the Middle East and Europe to Africa and the Americas. [476]

It is possible that these attacks have a further destabilizing impact in the U.S. by creating incredible challenges for victim companies, who may believe they are using best known practices but are still successfully attacked. The 2015 Verizon Data Breach Investigations Report notes that "…the reality is that if a determined, state-sponsored adversary wants your data, they're going to get it unless another state-sponsored entity helps you defend it."[477] And yet, a political climate of distrust of companies and fear of new legislation or regulation establishes obstacles in the public-private partnership that must be engaged improve cybersecurity.

Attacks such as these that make use of large amounts of unclassified but sensitive data are likely to grow in frequency and sophistication over the next 5 years. The consequences of such attacks are likely to increase in two ways: the costs will increase for the direct victims (those experiencing the cybersecurity incidents), and the indirect victims (those whose personal information is being collected), and the U.S. will suffer a national security loss as adversaries gain valuable insights through the aggregation and abuse of sensitive but unclassified data.

Scenario	Consequences	Vulnerabilities	Threats
Cyberattack interferes with availability of traffic flowing from a civil-purpose source to a national-defense user	National defense utilizers of civil data become blind to a normal data input. In peacetime this may conceal an individual incident. During a time of conflict this may significantly empower an adversary.	Technical vulnerabilities vary, but are decreasing through proactive management.	Most likely foreign military intelligence services in support of tactical operations.

Table 18: National Security Scenario Type 3

Still other cyber-attacks can be designed to interfere with the normal movement of data that keeps our national defense authorities informed of the lawful movement of accepted civilian traffic, such as the Automated Identification System used by maritime vessels. This is a route-injection or route hijacking attack. A route injection or hijacking occurs when a threat actor gains access to routers running Border Gateway Protocol (BGP) and alters or injects their own route. Physical access is not necessary to exploit a vulnerability if the router can be found on the Internet. Filters are used to identify alternate data routes, but can be avoided by a savvy attacker. An incident such as this may obscure the situational awareness of defense authorities. Once detected, if the information flow is not restored, the detrimental outcomes are difficult to work around. It is not possible to replace a real-time data stream with snapshots and reporting by other

[476] Kaspersky Lab, Kaspersky Lab Uncovers "The Mask": One of the Most Advanced Global Cyberespionage Operations to Date Due to the Complexity of the Toolset Used by the Attackers, http://www.kaspersky.com/about/news/virus/2014/Kaspersky-Lab-Uncovers-The-Mask-One-of-the-Most-Advanced-Global-Cyber-espionage-Operations-to-Date-Due-to-the-Complexity-of-the-Toolset-Used-by-the-Attackers accessed March 17, 2015

[477] 2015 Data Breach Investigations Report, downloadable at http://www.verizonenterprise.com/DBIR/2015/?&keyword=p6922139254&gclid=CKb03ZXLisUCFbLm7AodFWQAqA, accessed April 22, 2015.

means, such as email and phone calls. During a time of peace, such a cybersecurity incident may be an impedance or nuisance, but it may provide a significant tactical advantage during hostility. A recent risk assessment completed in a coordinated effort between DHS and the Information Technology Sector, outlines more detail on risks to Domain Name Servers (DNS) and Internet routing. Specific to this scenario, they have identified areas of vulnerability targeted by threat actors and offer potential mitigations and recommendations with regards to risk management.

While the risk and the risk trends for scenarios such as this are unclear in this discussion, government analysts systematically try to discern scenarios that are effective for planning and proactive vulnerability management. The consequences of an attack such as this would likely be minor during peacetime, but significant during a time of crisis. They would be less for some types of civil-purposes, and greater for others. There is no basis to assess the frequency of attacks such as these, nor is frequency very relevant to the risk. In cases such as this, proactive management of the vulnerabilities is the commonly accepted approach.

Scenario	Consequences	Vulnerabilities	Threats
Supply chain corruptions result in hardware or software that has imbedded exploits to be triggered by time or a change in conditions	National defense agencies or defense contractors relying on software or hardware in sensitive systems lose access to reliable services when an exploit is triggered to execute an operation outside of the control of the system managers. During peacetime this may be mitigated by regular back-ups. During a time of conflict the loss of services may be timed to stress U.S. capacities just when they are needed.	Components or software manufactured or shipped through the control of adversaries	Foreign intelligence services controlling the operations or corrupt businesses seeking to profit by manufacturing counterfeit products without addressing known vulnerabilities.

Table 19: National Security Scenario Type 4

Analysts are concerned about the risks associated with supply chains. This includes the possibility that hardware or software may have originated in adversarial countries, or passed through adversary controls and now are corrupted with malware that may be activated at a later date. According to the CISCO 2014 Annual Security Report, "Malicious actors will seek out and exploit any security weakness in the technology supply chain. Vulnerabilities and intentional backdoors in technology products can ultimately provide them with access to the "full house." Backdoors have long been a security issue and should be a concern for organizations, because they exist solely to help facilitate surreptitious or criminal activity."[478] Even in networks that may have an excellent perimeter security, with no connectivity to the Internet, the possibility that data could be corrupted or destroyed within the network should remain a significant concern.

This concern has led to long collaboration among the Department of Homeland Security (DHS), the Department of Defense (DOD), and the Defense Industrial Base Sector. Proactive action has resulted in a pilot program to mitigate supply chain risk for the defense industrial base, recognizing that it is typically their acquisitions that are tainted, rather than their production. This

[478] CISCO 2014 Annual Security Report http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf Accessed March 11, 2015

pilot is meant to deal with "the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system."[479] The DOD pilot program will continue through FY 2017. It is not yet clear whether this pilot program will succeed in identifying and mitigating risks closer to the beginning of supply chains, or how successful it may be in light of the problem of counterfeit products entering the supply chain.

While this type of attack does not require a great deal of tactical sophistication to accomplish a great deal of harm, it does require knowledge of vulnerabilities along with logical or physical access, or both. When corrupted software or hardware makes its way to systems that connect to the Internet, it is possible that backdoors could be used later to trigger whatever harmful outcome is intended by an adversary. In systems without backdoors, adversaries could use a "set it and forget it" approach, which results in data destruction, or sabotage of a system when certain system parameters are reached. This latter scenario type, while feasible, is likely to be less appealing to adversaries as it removes so much active control. Supply chain vulnerabilities are greater in countries where manufacturing of counterfeit products is more common, or where governments legally require the collaboration of the private sector. Under such circumstances the challenges of coordination may be less of an obstacle than subject matter experts in the IT Sector assessed in the 2009 IT Sector Baseline Risk Assessment.[480] Their assessment that such attacks may be less frequent than other types of cyberattacks may be true, but the risks associated with tainted supply chains was sufficient for DHS's Office of Cybersecurity and Communications to establish an IT Supply Chain Risk Management program focused on addressing this challenge.

The effects of such attacks are simply that the adversary has accomplished a change of vulnerability. Instead of outside the fence, he is inside. The exploit that is triggered by any malware or further actions by an adversary is what would result in consequences, so they would greatly vary. The frequency of such attacks is unclear, but likely be less than common Internet-based attacks. This is a risk in which substantial efforts are now invested in controlling, and there are surprising discoveries of known vulnerabilities in newly acquired software. The efforts face greater challenges, however, in that it is difficult to find an unknown threat or vulnerability.

Financial Information and Other Data Breaches

Introduction

Financial-information-related cyberattacks have great value to both criminals as well as other adversaries. The increasing use of exploits that allow criminals to gather individuals' personal identity information (PII) and their financial information has demonstrated that this is a growing industry. This information can be sold on the black market or turned around by a multidisciplinary criminal organization to create counterfeit credit or debit cards and used as quickly as possible, to get as much cash as they can before the fraud is discovered. This endeavor easily brings in millions of dollars a year to individual criminal groups, with relatively low risk.

---

[479] Defense Federal Acquisition Regulation Supplement: Requirements Relating to Supply Chain Risk (DFARS Case 2012-D050) https://www.federalregister.gov/articles/2013/11/18/2013-27311/defense-federal-acquisition-regulation-supplement-requirements-relating-to-supply-chain-risk-dfars, accessed March 11, 2015

[480] IT Sector Baseline Risk Assessment, https://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf , accessed April 24, 2015

Data breaches that result in the loss of financial information are not unique to the Financial Services Sector. In fact, financial institutions are probably best equipped to deal with the losses, as they can recover their costs through their lines of business and their practice of covering the fraud losses of their customers has resulted in this being a fairly managed risk, from the perspective of the Sector. Nevertheless, identity theft remains the highest consumer complaint, according to the Federal Trade Commission, and harm from the exposure of an individual's PII is difficult to calculate.

The actual fraud loss going to the criminals is just one type of cost, as noted, typically covered by the financial institution if an institution is involved. In cases where retailers are also involved, the retailers themselves pay for services to protect their customers for a period of time as well. Other types of organizations also maintain individuals' PII and financial information, and it is much less clear what sort of resources they can use to provide comparable protections to individuals whose identities and financial information are compromised.

Furthermore, organizations may be fined, depending on what regulations apply to them, and their tolerance for absorbing these penalties may vary. Another source of loss is the direct costs of responding to cybersecurity incidents, which are going up as the complexity of attacks goes up and the level of defensive resources are invested in an attempt match it.

When one considers these as campaigns of recurring, high-frequency attacks, some with real direct fraud losses, fines, and most with increases in operational demand on defenders' information security and data centers, the costs of these attacks are becoming increasingly burdensome. In many cases the requirement for public notice is established by the State where the victims are found. A requirement to notify all whose identity is exposed results in significant additional costs for the victim organization, as the very act of dealing with the notification process is expensive, let alone the additional consequences the institution may take from the perspective of public confidence in the institution. Surveys by cybersecurity companies produce results too aggregated to assist in understanding risks for scenarios, but they do indicate that the costs of responding to cyberattacks is increasing dramatically, in part due to the increasing prevalence of using a distributed denial of service (DDoS) attack as a smokescreen to distract the cybersecurity staff while the criminals extract large volumes of data that they can then capitalize on. Forty percent of one survey's respondents reported losing more than $1 million a day from these sophisticated combination attacks.[481]

The concern about the level of cyberattacks against the U.S. financial services industry has increased significantly in the past few years. Information security threats prompted the Financial Stability Oversight Council in 2013 and 2014 to highlight operational risk, and information security in particular, as worthy of heightened risk management and supervisory attention.[482] In its 2014 annual report, the Council stated that mitigating evolving information security threats, effectively managing incidents, and promoting recovery efforts are critical to maintaining public confidence and reducing financial risk.

---

[481] Neustar, 2014 The Danger Deepens, Neustar Annual DDoS Attacks and Impact Report, http://www.neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf , accessed March 4, 2015

[482]The Financial Stability Oversight Council (FSOC) was established to identify risks to the financial stability of the United States, promote market discipline, and respond to emerging threats to the stability of the financial system. FSOC consists of 15 members, including the heads of the Department of the Treasury, the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, National Credit Union Administration, and Securities and Exchange Commission.

The protection of critical infrastructure (which includes banking and financial institutions) from cyber threats is a high national priority, but different understandings of the Financial Services Sector leads to varied priorities among the different stakeholders. While the individual customer may be greatly concerned about identity theft and the possibility of becoming a victim of fraud, the institutions may view this risk as managed through their absorption of the fraud losses. National Sector leaders have a global view, informed by the comparison of the retail payment system, through which passes approximately $160 billion a day, to the wholesale payment system, through which passes $16 trillion a day. They encourage the institutions' effective management of these observed cybersecurity risks, while trying to assure the continued prevention of more catastrophic attacks against the Financial Services Sector infrastructure or those Communications Sector and Information Technology Sector infrastructures that they depend upon.

At least one important state regulator is concerned about the potential that banks may be unable to manage them, and, as a result, there may be cascading systemic risk that spills from one bank to affect others, and that this may in turn affect the larger economy. In a February 25, 2015 speech at Columbia Law School, Ben Lawsky, the Superintendent of New York's Department of Financial Services stated that he is concerned that there will be an attack on Wall Street firms that could "spill over into the broader economy." "We are concerned that within the next decade, or perhaps sooner, we will experience an Armageddon-type cyber event that causes a significant disruption in the financial system for a period of time," calling such an event a "cyber 9/11." If the changes that the New York Department of Financial Services proposes are put in place it will create new requirements for all of the Wall Street banks and insurers.[483] Since the majority of major financial institutions in the U.S. have a New York presence, this is significant.

There are many financial regulators at the Federal and state levels. In recent years as the global economy has become even more interdependent, the consensus guidance of international bodies of financial regulators has increased. Ultimately, the confusion and burden of many regulators creates an environment of distrust and a fear of being noncompliant. Compliance risk sometimes distracts organizations from other important risk management.

Simply reducing regulation is not necessarily the answer. Governments started regulating the financial services industry because of both criminal abuses and the realization that there are risks that emerge within markets or financial systems that propagate throughout the system of systems and into the larger economy. While activities that are highly regulated tend to be less profitable, which creates an incentive to innovate with new products, new payment platforms, etc., innovation is a mark of American strength. Today, within the financial services industry, much of these new innovations bring increasing exposure from cybersecurity risks.

Below are two scenarios which provide samples of this risk space. One highlights the potential for sudden and unexpected transitions to serious economic problems, the other highlights a risk that is becoming commonplace, expensive, and not always reported. There are many other scenarios that deserve assessment, but the potential consequences of these attacks can be so complex, and so fast moving that it is difficult to define and the available information for an assessment such as this is insufficient to provide value to planners. Such attacks may include

[483] Kaja Whitehouse, USA Today, Regulator warns of "Armageddon" cyber attacks on banks http://www.usatoday.com/story/money/business/2015/02/25/lawsky-goldman-sachs-banks/23995979/ accessed March 6, 2015

coordinated attacks on financial market utilities, securities or futures exchanges, etc. These scenarios may include attacks on the financial services infrastructure itself. The complexity of this sector, its increasing globalization, and its interconnection with current world events and individual perceptions make it difficult to develop a clear view of financial systemic risks.

Scenario	Consequences	Vulnerabilities	Threats
U.S. Systemically Important Bank is subjected to smokescreen DDoS campaigns and the extraction of customer personal identity information and financial data	Bank will absorb costs related to individual customers' initial credit monitoring and actual fraud, and costly incident management and notification activities. Additional soft costs relate to reputational risks for the bank, and substantial risk and time on the part of the customer, participating in the close monitoring of their credit and charges to their accounts, legal actions, and other uncovered expenses. If risks become intolerable and the public begins to distrust banks, problems for systemically important banks could have a destabilizing impact on the system of systems.	Interconnected systems allowing threat actors to infiltrate through smaller, less secure systems. Lack of oversight or management within organizations over newly installed technology and employees supporting.	Globally systemically important banks would logically be more likely targeted by criminals, terrorist groups, or agents of nation-states who are not well-integrated in the global economy. Risk of destabilizing the global economy is a disincentive to actors whose investments depend on financial stability.

Table 20: Data Breach Scenario Type 1

Systemically important banks (SIBs)are those banks that have met some threshold for heightened supervision based on the amount of assets they manage. Regulators are concerned that the role of these banks in the overarching financial system of systems is so great, that if some overwhelming stress impacts them and causes them to fail, the exposure of many other institutions to this failure could trigger another financial systemic risk event and potentially another global economic crisis such as was seen beginning in 2007. By requiring heightened supervision, related stress tests, greater capital reserves, and other risk management efforts to help them recover from their own incidents, rather than have a failure extend to others who are exposed to their problems, it is expected that the dominance of any one of these institutions will not lead to systemic reactions in the event that they experience shocks.

The international financial regulatory body, the Financial Stability Board, monitors and makes recommendations about the global financial system. The Board was responsible for identifying which banks fit into the category of Global Systemically Important Bank (G-SIB). Many, but not all of these banks are headquartered in the U.S. There is no evidence that cyber threats target these banks in an attempt to destabilize the global economy, just that their health is important to the global economy. The following G-SIBs are headquartered in the U.S.:

Global Systemically Important Banks Headquartered in the U.S.	
Bank of America	JP Morgan Chase
Bank of New York Mellon	Morgan Stanley
Citigroup	State Street
Goldman Sachs	Wells Fargo

An additional 24 G-SIBs are not headquartered in the U.S., though, by definition, the stability of these other banks is vital to the interests of the U.S. economy.

The Dodd-Frank Act established a threshold for any banks or bank holding companies that imposes heighted supervision standards. Any such institution with a balance sheet of greater than $50 billion is perceived in the international financial community as the equivalent of a U.S. domestically systemically important bank. Like the G-SIBs, there is no evidence that cyber threats are striving to destabilize the national or global economies through attacks on these banks. They are simply determined by legislated threshold to be of greater concern to avoid the potential that their failure may affect the larger economy.

U.S. Domestic Systemically Important Banks	
Ally Financial	KeyCorp
American Express	M&T Bank
BB&T	Northern Trust
BVA Compass	PNC Financial Services
BMO Financial Corp	RBS Citizens Financial Group
Capital One Financial	Regions Financial
Comerica	Santander Holdings USA
Discover Financial Services	Sun Trust Banks
Fifth Third Bank	U.S. Bancorp
HSBC North America Holdings	UnionBanCal
Huntington Bancshares	Zions

In a scenario of this type the target is a more capable defender, as it is one of the largest U.S. banks. The financial institution is hit with multiple campaigns of repeated DDoS attacks that serve as a smokescreen for data breach, which extracts customer financial information and PII. It is not uncommon that these attacks are so frequent that the victim bank has lost count; they are more than weekly. Some last for hours, others for several days. The institution must cover the losses of their customers, which they can recoup in part through fees and possibly insurance. They are very concerned about the hidden costs, such as the reputational risks, the churn of current customers going to other institutions and the potential that new customers would be put off from using their services in the future.

The Financial Stability Oversight Council's 2014 Annual Report contained at least six recommendations to stakeholders ranging from institutions to Congress for reducing cybersecurity risks. These recommendations include a demand for coordinated and collaborative Government-wide commitment and partnership with the private sector to promote infrastructure security and resilience, increased accountability through financial regulators of institutions' efforts to assess cyber-related vulnerabilities and to address gaps in oversight, increased engagement between institutions and private sector infrastructure cybersecurity providers, improved information sharing, and removal of legal barriers.

Banks have increased their investments in cybersecurity attempting to manage these risks yet they continue to experience them and incur additional costs. Occasionally, they have had to cover $5M-$10M real financial losses for customers who have become victims of fraud. They have observed that their shareholder value dips, but not for more than a few weeks. JP Morgan Chase announced plans, after experiencing the 2012 to 2013 DDoS attacks on the U.S. Financial

Services Sector, to increase their annual cybersecurity expenditures to $250 million by the end of 2014. After they suffered a hacking intrusion in 2014, JPMorgan's CEO said he would probably double JPMorgan's annual computer security budget within the next five years.[484]

The sophistication of these attacks is increasing, not just in terms of the combinations of cyber threats used in perpetrating the attacks, but with organization of teams of people ready to promptly make use of stolen financial information. The consequences are increasing as the sophistication increases, but there are additional risks that may emerge if a systemic reaction is triggered. The frequency of such attacks for individual institutions is expected to increase between 2015 and 2020 and the number of institutions affected is also likely to increase. We have no expectation that an adversary would attempt to induce a larger systemic risk that would impact the global economy, but there are often unintended consequences in highly complex interdependent systems, and the risk of systemic responses remains a concern.

Scenario	Consequences	Vulnerabilities	Threats
Retail Payment Service Provider is Hacked, Enabling Criminals to Increase the Value of Payments and Create Fraudulent Means to Receive Payments	Owners and operators of payment system infrastructure are apt to cover fraudulent payments and monitor the credit of impacted parties. Additional soft costs relate to reputational risk for the service provider, substantial risk and time on the part of customers and payees, participating in the close monitoring of charges to their accounts, evidence of identity fraud, legal actions, some of which is not covered by the payment service provider.	Lack of system awareness and understanding.	Criminal groups are most likely to attack payment service providers in an attempt to quickly siphon large amounts of funds.

Table 21: Data Breach Scenario Type 2

Payment infrastructure is complex and diverse, and innovations in how payments are made are sometimes better understood by international criminals than they are by many in the U.S. The feasibility of computer-enabled interference or manipulation of many of these systems is unclear. It is clear that some criminal hackers have figured out how to manipulate at least small portions of and turn it into a profitable criminal endeavor.

In one international hacking event that has been successfully prosecuted, a criminal group used sophisticated techniques to compromise the data encryption that was used by Royal Bank of Scotland's RBS WorldPay to protect customer data on payroll debit cards. Payroll debit cards are used by various companies to pay their employees. By using a payroll debit card, employees are able to withdraw their regular salaries from an ATM. Once in, the criminals raised the account limits on compromised accounts, and then provided a network of cashers with 44 counterfeit payroll debit cards, which were used to withdraw more than $9 million from over 2,100 ATMs in at least 280 cities worldwide, including cities in the U.S., Russia, Ukraine, Estonia, Italy, Hong Kong, Japan and Canada. The $9 million loss occurred within a span of less than 12 hours.[485]

[484] Clapper, James, Worldwide Threat Assessment

[485] 2008 attack through payment infrastructure, with international collaboration. http://www.justice.gov/usao/gan/press/2014/10-24-14.html

Financial infrastructure systems are complex. This payment card system is not common in the U.S. In addition to understanding how to successfully execute a cyberattack, this criminal enterprise had to identify infrastructure elements that operate in the background, figure out how to manipulate them, and develop and manage teams around the world to quickly complete the crime. The sophistication of attacks on portions of the retail payment infrastructure is multidisciplinary, challenging, but likely to increase. It was remarkable that RBS WorldPay and international authorities were able to respond as well as they did. Criminal groups are likely to be working on new attacks. The consequences of such attacks are also likely to increase as the motives for improving the criminal endeavor is to get away with more money. The frequency of such attacks is likely to increase as well, as the incentives to do them are significant.

Scenario	Consequences	Vulnerabilities	Threats
Criminal Hackers Install Malware in Retail Payment Card Readers at a National Retail Chain	Here the costs are both economic and societal. Financial institutions and victims of identity theft shoulder the burdens with fines and recovery payments, along with the steps needed to rebuild and maintain credit.	Interconnected systems allowing threat actors to infiltrate through smaller, less secure systems. Lack of monitoring activities over legacy and newly installed technology.	Criminal hackers are the most likely threat actors.

Table 22: Data Breach Scenario Type 3

This portion of the retail payment system is part financial services and part commercial retail industry. Cybersecurity attacks here affect the card issuers, the retail chain, and of course, the customer. In this scenario type, criminal hackers install malware in retail payment card reader systems at a national chain, extracting PII and financial information for customers over the course of several months. The information is sold on the black market, and retailers and card issuers incur significant costs to compensate the affected customers, though the long-term impact for many customers remains significant. For some customers this impact is unnoticed or delayed; some criminals hold the stolen PII until the incident appears to have faded from public notice. Despite the fact that there are increasing notifications of these events, it is suspected that these events are now occurring without notice, as they are yet to be identified. Typically these crimes are discovered, by either actual fraudulent use of the customers' account details in online or telephone purchases that are challenged, or by the discovery of large amounts of customer PII and financial information for sale on the black market. A smaller percentage of these cyberattacks result in the quick manufacture of counterfeit physical payment cards.

There has been such an intense and broad set of cyberattacks against retailers in recent times that a multi-agency Government task force looked into these attacks to determine if there was evidence that they were a coordinated campaign designed to adversely affect the U.S. economy. In their two page report, the National Cyber Investigative Joint Task Force stated that they have not found evidence of overarching responsibility behind all of the attacks, but they underscored

that the global implications of the retail attacks and the economic impacts to private business and individuals cannot be overstated.[486]

Numerous efforts have been made to account for the costs associated with such events. In addition to the costs that are reported in cybersecurity industry surveys about dealing with the expense of responding to cybersecurity incidents (too aggregated to be used here), the U.S. Sentencing Guidelines provides a useful estimate of the minimal costs associated with the loss of personal financial data that is sufficient to commit fraud. The intention behind the sentencing guidelines is not to estimate the actual financial losses that any individual company or affected customer experiences from the crime, but to provide a defensible approximation of the average combined costs for all stakeholders. Recent studies have suggested that any fixed cost per record is apt to produce an erroneous result.[487]

What are these costs? The company itself suddenly has to turn to corporate emergency response mode to address the incident, pay fines, fees, hire consultants, possibly notify victims, etc. It is the reputational costs, the opportunity costs of work that did not get done because of this attack, as well as churn that results as their customers go to competitors. In addition to these costs, many of the criminals turn around and use stolen identity information to file for tax refunds. The Internal Revenue Service (IRS) reported that, while they estimate that they prevented $24.2 billion in fraudulent identity refunds in 2013, they still paid out $5.8 billion in fraudulent refunds—and that is just what they know about.[488]

To a degree, individuals bear similar costs when they become victims of identity theft. Even if no actual fraud takes place, the victim often has to invest time and resources to address his or her risk. They may cancel cards and increase monitoring of their financial information. If the data is used and an individual becomes the victim of identity fraud, the individual may suffer much greater losses. While financial institutions bear the burden for those fraud losses that may be promptly realized, it is not hard to see that once someone's PII and financial information is out in the domain of criminals, the possibility of long lasting harm is quite real. The Federal Trade Commission estimated that identity theft takes an average of 200 hours of work and six months to recover. Most of this work involves keeping track of creditors, correspondence and phone calls, working with law enforcement and working with credit bureaus. These efforts are needed to prevent the victim from being liable for the debts the imposter created in their name, if actual fraud occurs. Additional work is needed in the fight to recover an accurate credit score. Since credit scores are used to establish the interest rates one is charged and whether or not credit will be offered, without this investment the victim will continue to pay for years. In some cases, victims of identity fraud lose out on job opportunities because they appear to be unreliable. Victims of identity theft choose to do all this work to restore the true record of their credit. It may be a better alternative to being held responsible for these debts, but it is a real cost to the individual. And yet, once individuals do most of the work to set up their own monitoring, the actual effort is not likely to increase much if their identity is stolen a second time. Thus, the

[486] Associated Press, U.S. retail cyberattacks not coordinated, shows government report, http://m.tech.firstpost.com/news-analysis/us-retail-cyberattacks-not-coordinated-shows-government-report-217998.html accessed March 17, 2014

[487] Verizon 2015 Data Breach Investigation Report, downloadable at http://www.verizonenterprise.com/DBIR/2015/ , accessed April 24, 2015

[488] Robert. W. Wood, IRS Paid $5.8 Billion in Fraudulent Refunds, Identity Theft Efforts Need Work, http://www.forbes.com/sites/robertwood/2015/02/19/irs-paid-5-8-billion-in-fraudulent-refunds-identity-theft-efforts-need-work/ accessed March 18, 2015

costs per record would logically go down for the individual, who may actually pass on lower costs per record to the institution that lost their data. How many credit monitoring efforts are needed?

The difference between identity theft and identity fraud is that a victim of identity theft may not experience the actual losses associated with the criminal using their data to commit fraud. Unfortunately, this distinction is not always clear in research and reporting on the topic; but this appears to be an important distinction. It reveals that the extraordinary work that both industry and individuals take on after identity theft occurs appears to be paying off. After a trend of increasing numbers of U.S. fraud cases from 2010 to 2013, the 2014 number of cases dropped 3 percent to 12.7 from 13.1 million cases in 2013. The total fraud losses dropped 11 percent to $16 billion, from $18 billion in 2013.[489] As both the number of cases drops and the total lost through fraud is calculated, however, it is important that to recognize that the amount of time and money spent by companies and individuals to prevent these losses is not included in the estimates. It remains a big problem.

In view of the information above, it is clear that these losses are not all borne by the retailers or the card issuers, nor can they easily be accounted for. There is some additional societal cost and individual harm. But it is not reasonable to just directly utilize these Sentencing Guidelines as a proxy for losses. They are explicitly about unauthorized telecommunication access devices, and, while it is clear that payment card skimming devices fall within the guidelines, it is not clear how the Sentencing Guidelines would apply to hacks that did not use a card skimmer. The Sentencing Guidelines have no clear reference to the number of victims or number of records of an incident. The financial estimates that refer to these Guidelines seem to interpret the illegal extraction of the electronic record as an instance of the use of an unauthorized access device, which this analysis can neither endorse nor dispute.

While those that argue against the use of the Sentencing Guidelines suggest that it inflates the cost, it could be argued that the Sentencing Guidelines may undervalue the losses. As written, if the unauthorized access device is unused (i.e. only identity theft), the minimal potential loss is $100 per affected account. If the data is used (i.e. unauthorized charges take place), the minimal potential loss goes up to $500 per affected account.[490] Thus, in addition to the costs accrued by the retailers and the card issuers for dealing with the cybersecurity incident itself, the minimal costs associated with the impact on the individual may be what is reflected in these loss estimates that refer to these Guidelines. If the Federal Trade Commission analysis is correct, the $100 for the average American's 200 hours of work to clear up identity theft is clearly underestimating the harm.

The 2015 Verizon Data Breach Investigation Report has probably produced the most authoritative and understandable estimates of the insured costs for data breaches, through contributions from NetDiligence, which partners with cyber-insurance carriers to aggregate data on cyber liability insurance claims and produces its own *Cyber Liability and Data Breach Insurance Claims* study. Through this collaboration, Verizon was able to improve their loss

[489] Javelin Strategy and Research, https://www.javelinstrategy.com/news/1556/92/16-Billion-Stolen-from-12-7-Million-Identity-Fraud-Victims-in-2014-According-to-Javelin-Strategy-Research/d,pressRoomDetail, accessed March 18, 2015

[490] U.S. Sentencing Guidelines Manual, http://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2014/2B1.1.pdf, accessed February 24, 2015

estimation models and they realized that the cost of a data breach with a small number of records loss had a much higher per-record cost, whereas those breaches where an organization lost millions of records, had a much lower per-record cost. The evidence shows that the range of forecasted average costs for the same number of records still remains wide, typically more than an order of magnitude for the same number of records lost.

The Verizon model forecast that the average loss for a breach of 1,000 records would be between $52,000 and $87,000, with 95 percent confidence. The breach affecting 10 million records has an average loss forecasted between $2.1 million and $5.2 million. The confidence interval widens as the number of records increases to account for growing uncertainty. This means that the cost per record goes down as the number of records goes up, and the amount of uncertainty goes up as the number of records goes up.

This recent reporting reveals why it is wrong to try to rely on a single point estimate per record. Verizon concludes that the improvements to understanding this variation would probably be tied to collecting more and different data in order to make better models.[491] Some of the data that may explain the wide variations might include information about the cost as it relates to the organizations past experience with data breaches. If this is the first or the fifteenth data breach, we might expect that the institutional costs associated with dealing with the problem would reduce over time. Many other factors (type of organization, regulatory framework, etc.) may have an impact on costs beyond just the number of records.

In retail point-of-sale attacks that took place between 2013 and 2014 there were a number that made the news. On the lower end of the large data breach attacks, was the attack on Sally Beauty Supply, which affected just 282,000 customer cards. There were two attacks that affected less than a half million cards reported in 2014, and an additional three comparably sized retailers who did not report the number of cards affected.

There were two reported incidents in 2013–2014 where between a half million and a million customer records were affected. For example, the September 2014 Goodwill Industries attack exposed 868 thousand customers.

More alarming were the attacks on Harbor Freight (a tool vendor with 445 stores and nearly 200 million customers), Home Depot and Target. The number of compromised records for Harbor Freight is still unclear. Home Depot reported attacks that affected 56 million customers; they estimated their cost of the breach to be $62 million.

It is reasonable to expect that as the value of these attacks goes up for the criminals, they will become an attack vector of choice and more sophisticated. We would expect that, unchecked, these attacks will continue to increase significantly in scale and scope, consequences and frequency during the next 5 years. This estimate of increasing risk may need to be moderated, however. Recent efforts of retailers and card issuers to reduce the possibility of such attacks have lead them to become more adept at discovering these incidents quickly, thus stopping the losses sooner and reducing the number of customers exposed. Efforts to clearly notify customers whose identity has been stolen also help keep them from becoming the victims of fraud as well.

[491] Verizon 2015 Data Breach Investigations Report; downloadable at http://www.verizonenterprise.com/DBIR/2015/ accessed April 24, 2015

Data Breaches Complicated by Other Factors

Introduction

Outside of financial institutions and retail businesses there are other types of data breach scenarios that have discernibly different outcomes and consequences. Many state and local governments, universities, utilities, healthcare organizations and other entities use online customer service systems or maintain databases with personal and financial information to allow automatic billing and telephone or online payments. All of these organizations hold PII and financial information, but may not be expected (or able) to cover the losses of individuals who become the victims of identity theft or fraud to the same degree as financial institutions or retailers may be. Just as the requirement to notify victims varies among states, the responsibilities of different types of organizations vary greatly as well.

Scenario	Consequences	Vulnerabilities	Threats
Data breach extracts PII and other information from a government entity or not-for-profit, or health care entity	Consequences range from loss of PII to consumer confidence, not to mention the economic losses incurred by both the organization and the public.	Lack of adequate system protection, monitoring activities, and training of employees.	Criminal hackers are the most likely threat actors.

Table 23: Data Breach Scenario Type 5

When a commercial entity suffers from attacks that steal customers' PII and financial information they have some recourse and established processes to recoup these losses through fees and increases in prices. When a not-for-profit or government agency is subjected to the same attack, it is disproportionately painful. Summarizing the big victims in 2014, Advisen's Cyberrisk Network reported the U.S. Office of Personnel Management suffered such an attack in 2014, losing 5 million records, the U.S. Postal Service lost 3.7 million, and the Texas Health and Human Services Commission lost 2 million. By cost, the U.S. Marshals Service was found to have lost $18 million, the Oregon Department of Employment lost $16 million, and Miami-Dade county $3.3 million. The University of Maryland lost $2.6 million.[492] Goodwill Industries, noted earlier as a retailer subjected to a point-of-sale hack, as a not-for-profit has nowhere near the capability to absorb such losses as an ordinary retailer might.

In early 2015, the news of a significant attack on Anthem Blue Cross rolled out in pieces as the scope of the incident unfolded. At the time of this writing, Anthem reports that no individuals' personal health information has been compromised, but approximately 80 million current and former customers and employees of Anthem and other Blue Cross affiliates have had their PII and financial information stolen by the perpetrators.[493],[494] Anthem is offering the same

[492] Josh Bradford, 2014 by the Numbers, Record-Setting Cyber Breaches, http://www.cyberrisknetwork.com/2014/12/31/2014-year-cyber-breaches/, accessed March 5, 2015

[493] http://www.cyberrisknetwork.com/2014/12/31/2014-year-cyber-breaches/

[494] Kaiser Health News, FBI Closing in on Culprits Behind Massive Cyberattack on Anthem's Database, http://kaiserhealthnews.org/morning-breakout/fbi-closing-in-on-culprits-behind-massive-cyberattack-on-anthems-database/ accessed March 5, 2015

protections of credit monitoring that retailers might under such circumstances. However, some analysts differ as to whether or not personal health information was compromised. If it is discovered that the data that was extracted included protected health information, in addition to the costs that Anthem is paying to deal with the incident, they will be required to pay penalties ranging from $100 – $50,000 for each violation up to $1,500,000 in a calendar year.[495] It is not yet clear how many calendar years may be in question.

While this scenario is very similar to other data breach scenarios, it is important to realize that the penalties for exposing personal health information are different and additional. The consequences of nearly the same incident seem to be greater when in involves healthcare information. The Symantec Internet Security Threat Report 2014 reported that Healthcare, Education and the Public Sector were ranked highest for the number of data breach incidents in 2013, accounting for 58 percent of all data breaches. However, these three sectors lagged way behind when viewed from the perspective of the numbers of identities exposed. The most lucrative way to steal identities is targeting retail, computer software, and financial institutions accounting for 77 percent of the identities exposed, compared to only 2.1 percent of the identities exposed through attacks on Healthcare, Education and the Public Sector.

Such data breaches experienced by the health care industry, not-for-profits, and government agencies may be increasing in scope, but not necessarily in sophistication. The outcomes of these attacks are not as obviously lucrative to the attacker. It is clearly more valuable to a criminal to target retailers or financial institutions, but the consequences of these attacks are different in many ways. Government agencies, education and not-for-profits are less able to invest in system protections, but even much less able to provide the same types of identity monitoring protections to individuals whose identities are exposed. Individuals may lose confidence these institutions, and not-for-profits may suffer greatly in consequence to such a loss. Agencies may also suffer from the loss of public trust, but it is not existential to them. Individuals cannot easily shift to a different agency because one of them failed to meet their expectations. Thus, while it may be more costly and difficult for a company to manage the consequences of a similar event and compensate the affected customers, it is possibly worse for individuals to feel helplessly dependent on an agency to protect their information and have no recourse when the protections fail.

[495] Ellen Tucker, Anthem Cyber Attack, The Importance of Data Security, http://blog.capital.org/anthem-cyber-attack-the-importance-of-data-security/ , accessed March 5, 2015

Scenario	Consequences	Vulnerabilities	Threats
Data breach extracts intellectual property from innovative businesses or research and development center	The theft and/or destruction of intellectual property can set research and development within an organization back in their production, undermining pricing strategy and investment costs or takes them out of business.	Integrated systems that can be breached through lesser protected businesses. Lack of security (physical and/or logical), monitoring activities, and training of employees.	Criminal hackers, corporate espionage, and nation states interested in the intellectual property are the most likely threat actors.

Table 24: Data Breach Scenario Type 6

There are several examples of data breaches, including instances where intellectual property appear to be the target. There is no clear and commonly held method of evaluating the value of the loss of intellectual property. It is difficult to establish because there are so many competing issues involved. When someone steals a copy of intellectual property, the rightful owner still retains the use of this data. It still has some value to its rightful owner. Its value is greatly decreased if the theft results in a cheaper knock-off of their own product that undermines their pricing strategy in the market place. It could be even worse if every instance of the data in the rightful owners' databases is completely destroyed. When someone steals intellectual property, they do so because the thief recognizes that they will benefit from the results of the innovative research and development (R&D) that the victim has invested, potentially years' worth of work and in some industries, billions of dollars of effort. The pharmaceutical industry, for example, is noteworthy for having the legal right to have no other manufacturers use their formulation to produce generic drugs for twenty years, so that they can recoup their investments in R&D. In developing innovations, it is not just the time, effort and expense of creating something that works, but the cost associated with discovering what doesn't work that must be considered.

Assessments in this scenario type cannot have high confidence, because it is not common for victims to advertise their losses or for law enforcement to successfully identify and prosecute perpetrators of intellectual property theft. There have been numerous citations of large figures associated with the theft of intellectual property, most notably the 2013 estimate of over $300 billion dollars a year – the value of the U.S. exports to Asia.[496] But these estimates reflect an admittedly weak valuation capability, and they ultimately are tied back to the loss of all intellectual property in the U.S., including the manufacture of bootleg CDs, DVDs, designer purses and the like. Perhaps a more compelling consideration is the fact that, as cyberattacks by competitors or by foreign governments who provide the stolen data to their national industries continues, this loss of the value of their investment puts companies at risk of going out of business and costs the victim national economy significantly. As economic and political adversaries grow more sophisticated and confident in their ability to operate with impunity in U.S. networks, they are likely to recognize cyberattacks as a more efficient and effective way to

[496] The Report of the Commission on the Theft of American Intellectual Property, http://www.ipcommission.org/report/ip_commission_report_052213.pdf, accessed March 5, 2015.

get what they are after. Cyberattacks have become the dominant focus of experts in field of intellectual property theft.

This problem is greater now than it ever has been, in part due to the interconnectedness of our economic world. This is reflected in global supply chains, multinational corporations and the heavy reliance on the Internet. These factors make it easier to access the intellectual property of a competitor, without the cost involved in a corporate espionage effort.

According to a figure cited in the President's 2006 Economic Report to Congress, 70 percent of the value of publicly traded corporations is estimated to be in "intangible assets," that is, intellectual property. A 2012 study by the Department of Commerce found that protection and enforcement of intellectual property rights around the globe directly affects an estimated 27 million American jobs in intellectual-property-intensive industries, which is roughly 19 percent of the U.S. workforce, producing over one-third of America's GDP. [497]

The Commission on the Theft of American Intellectual Property noted that in addition to the direct losses felt by victims, if American intellectual property rights were respected overseas as they are here, the U.S. economy would add millions of jobs and restore incentives for innovation and investment, resulting in a significant growth to the U.S. gross domestic product. The U.S. Trade Representative's "2012 Special 301 Report" points out that while Ukraine, Russia and India contribute significantly to the volume of intellectual property theft from the U.S., 50–80 percent of our loss is to China.[498]

Both Verizon, a broadband and telecommunications company, and Mandiant, a cybersecurity firm have conducted studies that point to overwhelming responsibility for cyberattacks aimed at economic espionage being attributed to state-affiliated actors in the People's Republic of China (PRC). These assertions were endorsed by the U.S. DOD in its 2013 report to Congress on Chinese military developments. Reinforcing the findings from the Mandiant Corporation, their report notes that the PRC "is using its computer network exploitation (CNE) capability to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs." It asserts that "the information targeted could potentially be used to benefit China's defense industry, high technology industries, [and] policymaker interest in U.S. leadership thinking on key China issues," among other things.[499]

It is because there is such strong consensus that there is a significant, under-discovered, under-reported and unmeasured risk associated with the loss of intellectual property through cyberattacks that the examples serve as exceptionally weak representations of the risks. Except in cases where victim organizations come forward publically to help prosecute criminals or draw attention to the issue, much of this is reported only confidentially, if at all.

Some cases help to clarify the scale of these losses, however. A single attack against RSA in 2011, the maker of the widely used SecurID tokens, which was traced back to China, resulted in

---

[497] U.S. Department of Commerce, "Intellectual Property and the U.S. Economy: Industries in Focus," March 2012.

[498] Office of the U.S. Trade Representative (USTR), "2012 Special 301 Report," April 2012, http://www.ustr.gov/sites/default/files/2012%20Special%20301%20Report_0.pdf; and Office of the USTR, "2013 Special 301 Report," May 2013, http://www.ustr.gov/sites/default/files/05012013%202013%20Special%20301%20Report.pdf.

[499] Office of the Secretary of Defense, Department of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013," prepared for Congress, Washington, D.C., 2013, 36, http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf.

the compromise of at least three major defense contractors.[500] The same attack compromised security at an estimated 720 companies, including 20% of the Fortune 100.[501] Through another series of attacks, dubbed operation Shady RAT, it was discovered that petabytes of highly proprietary information, including sensitive military and infrastructure data, had been siphoned off from the U.S. Government and its allies, supranational organizations such as the United Nations, and many other sovereign nations and independent organizations over a period of more than five years.[502] Former General Keith Alexander, then the commander of the U.S. military's Cyber Command, said that one U.S. company alone lost $1 billion worth of intellectual property over the course of a couple of days.[503]

The onslaught of such attacks has been so significant that in May of 2014 a Federal grand jury indicted five Chinese military hackers, who for all intents and purposes appeared to be working to advance the ability of Chinese state-owned enterprises when they were negotiating with U.S. firms or unions. They are alleged to have stolen trade secrets and other sensitive business information, using cyber espionage for economic advantage.[504] The Chinese were after Westinghouse Electric, U.S. subsidiaries of SolarWorld AG, U.S. Steel, Allegheny Technologies and Alcoa. [505]

Smaller cases are most likely to reach indictments and prosecutions. In one case, international hackers were charged with breaking into computer networks of prominent technology companies and the U.S. Army and stealing more than $100 million in intellectual property and other proprietary data. The alleged cyber theft included software and data related to the Xbox One gaming console and Xbox Live online gaming system; popular games such as "Call of Duty: Modern Warfare 3" and "Gears of War 3"; and proprietary software used to train military helicopter pilots.[506]

The New York Times, the Wall Street Journal, and the Washington Post all disclosed that they believe their networks were compromised by intrusions that originated in China. A reasonable motive for targeting media is to identify reporters' sources for reporting that the Chinese government may not condone.

In another case, in August of 2014 a Federal grand jury indicted a Chinese national on five felony offenses stemming from a computer hacking scheme that involved the theft of trade secrets from American defense contractors, including The Boeing Company, which manufactures the C-17 military transport aircraft. The indictment alleges that the indicted Chinese national worked with two unindicted co-conspirators based in China to infiltrate computer systems and obtain confidential information about military programs, including the C-

[500] Zeljka Zorj, "RSA Admits SecurID Tokens Have Been Compromised," Help Net Security, June 7, 2011, http://www.net-security.org/secworld.php?id=11122.
[501] Brian Krebs, "Who Else Was Hit by the RSA Attackers?" Krebs on Security, web log, October 2011, http://krebsonsecurity.com/2011/10/who-else-was-hit-by-the-rsa-attackers.
[502] Peter Bright, "Operation Shady Rat: Five-Year Attack Hit 14 Countries," Ars Technica, August 3, 2011, http://arstechnica.com/security/news/2011/08/operation-shady-rat-five-year-hack-attack-hit-14-countries.ars; and "Massive Global Cyberattack Targeting U.S., U.N. Discovered; Experts Blame China," Fox News, August 3, 2011, available at http://www.foxnews.com/scitech/2011/08/03/massive-global-cyberattack-targeting-us-un-discovered-experts-blame-china.
[503] Ellen Nakashima, "In a World of Cybertheft, U.S. Names China, Russia as Main Culprits," *Washington Post*, November 3, 2011.
[504] http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor
[505] Pete Williams, U.S. Charges China with Cyber-Spying on American Firms, http://www.nbcnews.com/news/us-news/u-s-charges-china-cyber-spying-american-firms-n108706, accessed March 19, 2015
[506] http://www.justice.gov/opa/pr/four-members-international-computer-hacking-ring-indicted-stealing-gaming-technology-apache

17 transport aircraft, the F-22 fighter jet, and the F-35 fighter jet.[507] It is not yet known what the economic value of the loss of this intellectual property is, but it is clear that it provides a significant advantage to Chinese military aircraft producers.

The NextGov.com article on Federal agencies' capacity to bounce back from cyberattacks that wipe out data reported that those Federal agencies that protect intellectual property as part of their business invest to protect it. In a recent budget, the Department of Energy devoted $218 million; the Pentagon—$7 billion; NASA—$86 million; and the tiny National Science Foundation—$150 million for cybersecurity.[508]

It is reasonable to expect the frequency of such attacks to continue to increase between 2015 and 2020. It is likely that there will be an even greater increase in the following industries, based on their alignment with the Chinese 12th 5-Year Plan for National Strategic Emerging Industries:

- New energy auto industry
- Energy-efficient industry
- Advanced environmental protection industry
- Resource recycling industry
- Next generation information network industry
- Fundamental industry of core electronics
- High-end software and new information service industry
- Bio-pharmaceutical industry
- Bio-medical engineering industry
- Bio-breeding industry
- Bio-manufacturing industry
- Aviation equipment industry
- Satellite and its application industry
- Rail transportation equipment industry
- Marine engineering equipment industry
- Intelligent equipment-manufacturing industry
- Nuclear energy technology industry
- Wind energy industry
- Solar energy industry
- Biomass industry

[507] Edvard Pettersson, Chinese Man Charged in Plot to Steal U.S. Military Data http://www.bloomberg.com/news/articles/2014-07-11/chinese-citizen-charged-with-hacking-boeing-computer-in-u-s- accessed March 5, 2015

[508] Alia Sternstein, NextGov.com, Most Federal Agencies Wouldn't be able to Bounce Back From a Sony Hack http://www.nextgov.com/cybersecurity/2014/12/most-agencies-wouldnt-be-able-bounce-back-sony-hack/101658/ accessed March 5, 2015

- New functional material industry
- Advanced structural material industry
- High-performance composite material industry[509]

Cyber Extortion or Terrorism

Introduction

In recent years, we have seen attacks where the perpetrator was using their attack to influence others. This has been seen as a form of extortion by criminals, as a politically-motivated prank by terrorist groups, and as a threatening exercise of powers by nation-states displeased with the actions of companies in the U.S. While each of these manifestations has different direct effects, the indirect effect of a culture of supersized cyberbullying is a common result.

Scenario	Consequences	Vulnerabilities	Threats
Victim's data is destroyed, encrypted, or the victim is extorted with the threat of loss of access to their data	The theft and/or destruction of data leading to economic losses to recover from threat actors or to rebuild what was lost.	Inadequate malware or virus detection. Lack of logical security, monitoring activities, data back-up, and training of employees.	Criminal hackers are the most likely threat actors, and, in some cases, those with political motivations.

Table 25: Cyber Extortion or Terrorism Scenario Type 1

There are many alternate approaches to conducting an attack like this. Sometimes the result is significant and existential to the organization that was attacked. In other cases it is a small incident in the history of an organization. Unfortunately, the easiest way out is often to pay the ransom.

In a smaller impact attack, a virus called Cryptowall managed to bypass spam filters and firewalls and infected the police-department computer system in Durham, New Hampshire, when an officer opened an infected attachment on an email. By the next morning, they had widespread problems on the computer systems. This type of attack uses software that encrypts a user's hard drive, restricting them from accessing their own data. It holds it with a timer and a threat of destruction, until they pay a ransom. The town refused to pay the ransom, and the manager of the IT systems took the department's computer system offline, dealt with the problem, and reloaded their system with the backup files. [510] Their success in managing through this incident was largely attributable to the way they backed up their files.

Another more sophisticated and actively managed attack had a much more devastating impact on its victim. The code-hosting company Code Spaces was hit by a DDoS attack and then extorted

[509] Yao Lu, http://www.china-briefing.com/news/2012/07/25/china-releases-12th-five-year-plan-for-national-strategic-emerging-industries.html#sthash.dqWt0NAX.dpuf, accessed March 10, 2015

[510] Virus Infects Police Computer System In Durham NH, http://boston.cbslocal.com/2014/06/06/virus-infects-police-computer-system-in-durham-nh/ accessed March 20, 2015

by a hacker who had gained control of the firm's Amazon EC2 control panel, hoping to get paid in exchange for returning control of operations to Code Spaces. Code Spaces refused to comply, and quickly regained control of the account by changing password. The hacker recognized what was happening, used back-up logins that he had created, and started deleting files. Code Spaces revealed that "most of our data, backups, machine configurations and offsite backups were either partially or completely deleted." They were put out of business.[511]

The case of the Sony Pictures Entertainment hack where large amounts of intellectual property PII and other sensitive information was stolen was more complex. Recent evidence suggests that the intrusion that prepared for this attack began more than a year prior to its discovery in November 2014.[512] Director of National Intelligence James Clapper, speaking at conference at Fordham University, said the North Korean military's Reconnaissance General Bureau was responsible for "overseeing" the attack against Sony.[513] If this is true, it suggests that North Korea was watching for potentially offensive movies and began preparing to punish Sony well before they were ready to release the film.

In the case of the Sony attack, several exploits were used. The hackers extracted confidential data and then installed malware to erase data from the servers.[514] In the days following this hack, the perpetrators began leaking yet-unreleased films and started to release portions of the confidential data to attract the attention of social media sites, although they did not specify what they wanted in return.

Sony Pictures set aside $15 million to deal with ongoing damages from the hack.[515] While Sony made substantial additional investments in cybersecurity after this attack, according to Assistant Director Joseph M. Demarest, Jr., the head of the FBI's Cyber Division, an attack like this would have "slipped and gotten past 90 percent of the net defenses that are out there today in private industry."[516]

In such a data-destruction case, Government agencies would be in a particular trouble. As reported byNextGov.com, "a file-wiping attack such as the Sony Pictures Entertainment hack could bring major Federal departments to their knees, because most have no data-loss contingency plans, according to the latest figures on compliance with government cybersecurity laws. Further, unplugging systems to contain damage, as Sony did, would impair an agency's ability to carry out constitutional duties, some former Federal cyber-leaders say."[517] It is likely that targeted organizations will all have to learn how to operate in the trade-space between different types of risk.

---

[511] 6 Recent Real-Life Cyber Extortion Scams http://www.darkreading.com/attacks-breaches/6-recent-real-life-cyber-extortion-scams/d/d-id/1278774, accessed March 20, 2015

[512] Zetter, Kim (December 3, 2014). "Sony Got Hacked Hard: What We Know and Don't Know So Far". *Wired*. Accessed January 4, 2015

[513] FBI head details evidence that North Korea was behind Sony hack, http://touch.latimes.com/#section/-1/article/p2p-82479451/ accessed March 20, 2015

[514] Palilery, Jose (December 24, 2014). "What caused Sony hack: What we know now". CNN Money. Retrieved January 4, 2015.

[515] Frizell, Sam (February 4, 2015). "Sony Is Spending $15 Million to Deal With the Big Hack". *Time*. Retrieved February 4, 2015.

[516] House Homeland Security Chairman Michael McCaul, "Preventing a 'cyber Pearl Harbor': The Hollywood hack attack revealed the need to upgrade cybersecurity," *The Washington Times*, January 8, 2015, http://homeland.house.gov/news/mccaul-op-ed-preventing-cyber-pearl-harbor-washington-times.

[517] Alia Sternstein, NextGov.com, Most Federal Agencies Wouldn't be able to Bounce Back From a Sony Hack http://www.nextgov.com/cybersecurity/2014/12/most-agencies-wouldnt-be-able-bounce-back-sony-hack/101658/ accessed March 5, 2015

While the sophistication of these attacks varies and simpler individual attacks might be less consequential, in aggregate, a simple ransomware like Cryptolocker has affected at least 250,000 victims. Profits made from people complying with the demands can produce several million dollars per day.

The trend towards increasing complexity is likely to continue. The real consequences of these attacks vary by the organization, but as American work is commonly built on information and data, attacks that threaten to keep our data from us can be devastating. The ability of an organization to manage through such an attack and have a backup that cannot be affected by the same incident is critical to controlling its consequences.

Scenario	Consequences	Vulnerabilities	Threats
Victim's web-enabled communications are hijacked by the attacker, who uses it to convey their own message for political purposes, or just to embarrass authorities	The consequences of these attacks are costs borne by the victim for regaining control and dealing with the bad publicity.	Lack of security (physical and/or logical), monitoring activities, data back-up, and training of employees.	Criminal hackers are the most likely threat actors.

Table 26: Cyber Extortion or Terrorism Scenario Type 2

In January 2015, Twitter accounts for WBOC, a Salisbury, Maryland-based television station, and the Albuquerque News Journal in New Mexico were both hijacked by a hacker claiming to be sympathetic to terrorist group Islamic State of Iraq and the Levant, or ISIL. The hacker named "CyberCaliphate" used the Twitter accounts to post pictures and tweets throughout the day claiming to have classified information from Federal investigations into terrorist groups. The station's website was also hacked, with the top story being changed to one posted by "CyberCaliphate" before the station took it down. The station recovered control of its website on its own but had difficulty regaining control of its Twitter account.[518] A similar bout of attacks by ISIS sympathizers took place in March 2015 as well.

Other takes on this type of scenario have included taking over electronic highway messaging systems, modifying organizational intranets, and other efforts to pull pranks, embarrass or annoy the victims.

These types of attacks are not necessarily sophisticated but they are increasing in scope, with multiple organizations being attacked *en masse*. The consequences of these attacks are costs borne by the victim for regaining control and dealing with the bad publicity. However, the indirect consequences are not significant, except possibly to further the social divide between people who suspect others of being radical Islamists and those who are apt to be suspected.

In January 2015, Twitter accounts for WBOC, a Salisbury, Maryland-based television station, and the Albuquerque News Journal in New Mexico were both hijacked by a hacker claiming to be sympathetic to terrorist group Islamic State of Iraq and the Levant, or ISIL. The hacker named "CyberCaliphate" used the Twitter accounts to post pictures and tweets throughout the day

[518] Delmarva Now, WBOC Twitter, website hacked by ISIL supporters,http://www.delmarvanow.com/story/news/local/maryland/2015/01/06/wboc-twitter-hacked/21341645/ accessed March 21, 2015

claiming to have classified information from Federal investigations into terrorist groups. The station's website was also hacked, with the top story being changed to one posted by "CyberCaliphate" before the station took it down. The station recovered control of its website on its own but had difficulty regaining control of its Twitter account.[519] A similar bout of attacks by ISIS sympathizers took place in March 2015 as well.

Other takes on this type of scenario have included taking over electronic highway messaging systems, modifying organizational intranets, and other efforts to pull pranks, embarrass or annoy the victims.

These types of attacks are not necessarily sophisticated but they are increasing in scope, with multiple organizations being attacked *en masse*. The consequences of these attacks are costs borne by the victim for regaining control and dealing with the bad publicity. However, the indirect consequences are not significant, except possibly to further the social divide between people who suspect others of being radical Islamists and those who are apt to be suspected.

Scenario	Consequences	Vulnerabilities	Threats
Distributed Denial of Service Attack (DDoS) alone	The consequences of these attacks vary based on the goals of the attacker and range from data and economic loss to a loss of public confidence.	Lack of security (physical and/or logical), monitoring activities, or redundancy.	Given the varied reasons for a DDoS attack, the threat could come from any number of actors.

Table 27: Cyber Extortion or Terrorism Scenario Type 3

In the recent past, many offered the opinion that a DDoS was unsophisticated and likely to decline as a source of cybersecurity concerns. It is true that many of the very powerful DDoS attacks experienced in recent years have served as a smokescreen that distracted the cybersecurity staff while sophisticated break-ins and data extractions took place. However, DDoS alone remains a useful tool for adversaries who simply want to punish their victim. The exploit gives an adversary the ability to deny a victim of the normal commerce that would take place over their website or to embarrass them in the eyes of the general public. For many adversaries this is either sufficient, or at least good enough for the time being.

In 2014, DDoS attacks increased in size and power. Incapsula, a security company that specializes in protecting company websites, reports that such attacks more than tripled from December through February over the same period a year earlier. Incapsula labels DDoS "the weapon of choice" for hackers these days, in part because technology is making it increasingly convenient and powerful.[520] According to Verizon's most recent Data Breach Investigations Report, an attacker can rent a botnet for only $10 an hour. [521] But a botnet is just one element in a successful, large-scale DDoS attack. A popular method of increasing the size and power of DDoS attacks is to use a domain name system (DNS) amplification attack to take advantage of

[519] Delmarva Now, WBOC Twitter, website hacked by ISIL supporters,http://www.delmarvanow.com/story/news/local/maryland/2015/01/06/wboc-twitter-hacked/21341645/ accessed March 21, 2015
[520] Downloadable PDF, http://lp.incapsula.com/ddos-report-2014.html accessed March 5, 2015
[521] Downloadable PDF, http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf , accessed March 5, 2015

open recursive or authoritative servers to flood a target with DNS-responsive traffic. This works by amplifying the responses, at a rate of approximately 70:1. [522]An attacker can design his attack using a variety of contributing tools in an effort to exhaust the targets' resources.

Recent examples include the Sony DDoS Sony's PlayStation Network and Sony Entertainment Network in August 2014. An attack of this sort does not just cost the company the resources necessary to defend against the attack. When their customers try to access their sites and are frustrated, they often move on. Gaming service providers are very concerned about churn, with their regular customers' moving to competitors [523] Two different groups laid claim to the August Sony attacks, adding a tweeted bomb threat against an executive's flight in one of these claims.

Another retaliatory strike was experienced by the St. Louis County, Missouri police department, when their website and email servers were brought down in apparent protests over the shooting of Michael Brown. [524] A review of the Threat and Hazard Risk Identification and Assessment (THIRA) results provided to the Federal Emergency Management Agency reveals that state and local emergency planners look at incidents such as this as an indication of the potential use of this exploit as a way to complicate their responses in emergencies, such as the response to a natural disaster.

Other examples of DDoS attacks reported by Verizon include the 2012 and 2013 DDoS attacks on financial institutions claimed by the Izz ad-Din al-Qassam Cyber Fighters. This group appears to have been protesting an offensive film trailer hosted on YouTube. CNN reported, however, that it may be that the group was simply jumping on the attacks to promote their protest, noting that Sen. Joe Lieberman placed the blame on Iran. The goals of the threat actors may not be as relevant as the impact of the incidents on the targets. The resources of major financial institutions make them better equipped to fight against such onslaughts, but the cost of these attacks was still significant.

Attacks on Industrial Control Systems

Introduction

Industrial control systems (ICS) support the efficient and safe operation of large complex interconnected physical systems, such as those in major manufacturing plants, water purification and distribution systems, pipelines transporting petroleum products or natural gas, systems operating the electrical transmission and distribution grid, etc. For much of this infrastructure, ICS integration is decades old, incorporated with the primary purpose of increasing system reliability, and focused on infrastructure operating requirements. At that time, cybersecurity risks associated with this internet-based technology was not foreseen as a measurable business risk – assessed as low risk or not well understood. Owners and operators also range in their corporate risk tolerance, which can be based on a multitude of factors that vary across industrial sectors and across individual companies. Fast forward to the present day, we now find the concerns over cybersecurity risks are leading topics of discussion on corporate Board agendas.

---

[522] Anatomy of a DNS DDoS Amplification Attack. https://www.watchguard.com/infocenter/editorial/41649.asp, accessed April 27. 2015

[523]Charlie Osborne, Sony PlayStation Network struck by DDoS attack, bomb threat grounds executive http://www.zdnet.com/article/sony-playstation-network-struck-by-ddos-attack-bomb-threat-grounds-executive/

[524] Dara Kerr, Ferguson, Mo., police site hit with DDoS attack, http://www.cnet.com/news/st-louis-police-website-suffers-ddos-attack/ accessed March 5, 2015

It is noteworthy that the ICS-CERT FY 2014 Incident Response statistics showed that 55% of the incidents reported to them involved advanced persistent threats (APT) or sophisticated actors. Other actor types included hactivists, insider threats and criminals.[525] Attack types include attempts to exfiltrate ICS information. There are several key factors that influence the consequences associated with cyberattacks on ICS: the speed of the operations of the infrastructure under attack, the role of humans in the decision making processes for the operation of the infrastructure, and the number of opportunities to mitigate the direct effects of an attack before the full range of possible consequences materialize. Such adversaries are typically associated with a high degree of uncertainty and risk, as they often will expend a great deal of resources establishing themselves within a control system without a direct economic or short-term political motive.

Over the past few years, tools such as SHODAN, Google, and other search engines have enabled researchers, and really, the general public, to discover and identify a variety of ICS devices that were not intended to be Internet facing. Adding to the threat landscape is the continued scanning and cataloguing of devices known to be susceptible to emerging vulnerabilities. The increasing body of public knowledge about ICS, coupled with these tools, lowers the level of expertise necessary to successfully locate Internet-facing control system. Many of these devices have not been configured with adequate authentication mechanisms, making it easy to directly access the systems by both opportunists and sophisticated threat actors. As tools and adversary capabilities advance, we expect that exposed systems will be more effectively discovered and targeted by adversaries. Clearly, it has become more important for asset owners and operators to audit their network configurations and properly install their ICS devices behind patched VPNs or firewalls, and yet surprisingly few do, until they discover a problem and seek help.

Owners and operators vary in the clarity with which they focus on this problem. Some systems have been hacked, but with no apparent outcome, suggesting this is not a real problem. Some owners and operators respond to this discovery with little concern, because nothing happened. Others respond defensively and take action, concerned about the reality of sophisticated threat actors possibly having an ability to sabotage their systems in ways they have not yet imagined. The ODNI reports that:

> Russia's Ministry of Defense is establishing its own cyber command, which—according to senior Russian military officials—will be responsible for conducting offensive cyber activities, including propaganda operations and inserting malware into enemy command and control systems. Russia's armed forces are also establishing a specialized branch for computer network operations[526].

The Worldwide Threat Assessment goes on to refer to private sector "computer security studies which assert that unspecified Russian cyber actors are developing means to access industrial control systems remotely. These systems manage critical infrastructures such as electric power grids, urban mass-transit systems, air-traffic control, and oil and gas distribution networks. These unspecified Russian actors have successfully compromised the product supply chains of three

[525] ICS-CERT Monitor September 2014-February 2015
[526] Clapper, James, Worldwide Threat Assessment

ICS vendors so that customers download exploitative malware directly from the vendors' websites along with routine software updates."[527]

If this undiscovered presence in their control system was used maliciously, the outcomes would vary tremendously based on the system, infrastructure subsector, the conditions surrounding the actual manipulation of the control system and more. Sometimes the adverse outcomes for the equipment and materials may be risks that may prove costly, but have low potential for life and safety impacts. Some sectors have such tight operating margins, that any costly errors are unacceptable. Other sectors have the margins available to exchange profits for safety and do so without concern that they could not make up the losses. Thus, owners and operators can range between highly risk-averse to accepting some forms of loss as a trade for avoiding others.

ICS-CERT conducts risk mitigation activities and incident response for critical infrastructure owners and operators. In FY 2014 Incident Response statistics reported that 55 percent of the incidents reported to them involved advanced persistent threats or sophisticated threat actors. Other actor types included hactivists, insider threats, and criminals.[528][529] When an organization is attacked by a sophisticated threat actor the organization is left with a high degree of uncertainty and incalculable risk. It is unclear to the victims what the adversary's motivations were. They doubt the explanations of computer security consultants and the Government. They wonder why these adversaries expend such a great amount of resources establishing themselves within this control system, without a direct economic or short-term political motive. Many find this type of uncertainty immobilizing. It is easier to deal with known problems than to try support decisions about such uncertain risks.

Illustrative of Government efforts to help clarify these risks, ICS-CERT and the FBI teamed up in 2014 to respond to sophisticated cyber-exploitation campaigns against U.S. infrastructure ICS. These campaigns involved different sets of malware, both of which used tactics to target and gain access to control systems environments. One of them, BlackEnergy, has been discovered within the controls that operate many infrastructure sectors. The BlackEnergy hacking campaign had been ongoing since 2011, but there is no evidence of any attempt to activate the malware to damage, modify, or otherwise disrupt affected systems. Havex, the other malware, also called Dragon Fly, has also been found in ICS. According to Joel Langill, security consultant and author of the *SCADAhacker* blog, "A lot of malware impacts control systems, like Conficker or Slammer," referring to two computer worms that caused headaches for tens of thousands of people using Microsoft. "Those have consequences on industrial environments, but ... Stuxnet, Dragonfly and now Black Energy have specific ICS payload components; they are targeting specifically industrial control systems. This is very disturbing."[530]

The Energy Sector led all others again in 2014 with the most reported incidents. ICS-CERT's continuing partnership with the Energy Sector provides many opportunities to share information and collaborate on incident response efforts. Also noteworthy in 2014 were the incidents reported by the Critical Manufacturing Sector, some of which were from control systems

[527] Clapper, James, Worldwide Threat Assessment
[528] ICS-CERT Monitor September 2014-February 2015
[529] An insider threat is one or more individuals with access or insider knowledge of an enterprise that allows them to exploit vulnerabilities, resulting in harm to the enterprise
[530] SECURITY: Secret meetings tackle back-to-back energy-sector cyberthreats, http://www.eenews.net/stories/1060008193, accessed March 24, 2015

equipment manufacturers. The ICS vendor community may be a target for sophisticated threat actors for a variety of reasons, including economic espionage and reconnaissance.[531]

The scenarios considered in this scoping assessment reflect a sample from the Energy Sector, based on the predominance of voluntarily reported incidents of this type to ICS-CERT. Owners and operators in the Energy Sector have noted the measurable value they receive in return for their partnership with ICS-CERT. In addition there is a scenario for the Water and Wastewater Sector. While water-system attacks are less commonly reported, state and local authorities have a high level of concern with them as is evidenced by their contributions to THIRA. There is no evidence that these types of attacks have been completed; which is to say, the results of ICS-CERT investigations into incidents of these types typically conclude that detection and mitigation mechanisms effectively employed prevented adversaries from fully executing intended attacks. The analysis below provides insights into the how the management of the targeted infrastructure may or may not provide a limiting effect on attacks of this type. It is likely that whatever alternate management controls owners and operators may have on the operation of their infrastructure would be severely stressed if there were coordinated complex attacks, as these alternate controls all rely more heavily on human operators.

In clarifying the potential impacts of cyberattacks on ICS, we have used a simple logic model and validated conclusions with representatives of the owner and operator community. This logic model focuses on identifying a series of related, but normally obscure conditions and effects, including:

- The role of information and communications technology in managing or monitoring the infrastructure's equipment;
- The direct effects of lost confidentiality (data breaches), integrity (altered data or co-opted control), and availability (destroyed data or denial of service) on the various infrastructure systems;
- The availability and limitations of alternatives, such as human operators or back up mechanical devices, to perform the functions that the ICS normally controls;
- The potential infrastructure functional impacts that may result;
- The availability and limitations of infrastructure management alternatives that may address the infrastructure functional impacts.

[531] ICS-CERT Monitor, September 2014-February 2015

Scenario	Consequences	Vulnerabilities	Threats
Distributed campaign of attacks on natural gas pipeline system industrial control systems (ICS), timed to maximize the impacts on energy assurance	While an individual attack on a pipeline system can be adequately managed, a distributed attack could lead to shortages and customer outages. This would create a loss of revenue for the utility company and could adversely affect consumers.	Distributed nature of pipeline control systems. Integrated nature of systems allowing less secure devices that are directly connected to the Internet to be breached, thereby granting access to the more secure ICS.	Criminal hactivists, terrorist organizations, and nation states are the most likely threat actors.

Table 28: ICS Scenario Type 1

Natural gas transmission systems are those that deliver natural gas from the processers to local distribution companies, also known as the utility. They may be likened to a system that keeps the warehouses stocked. Because they ship large volumes that get split to different distribution networks, the pipelines have a large capacity. They are typically located away from populated areas and require compressors every 50–100 miles to keep the gas moving at the required rate. If a few of the compressors are damaged or not functioning as required, the movement of the gas may slow or stop. Transmission pipeline operators stop the movement of gas if there has been an accident with the pipeline in order to make the repairs. Typically, customers are unaffected by these shutdowns because of the resiliency of the pipeline systems to work around an incident area and to deliver product through back-up alternatives. Similarly, cyber-disruptions impacting the movement of gas through a pipeline may reduce the amount of gas that can be delivered. However, this can be mitigated in the short-term by stored reserves or alternative gas delivery paths.[532]

Local distribution systems have many localized branches, with reduced pressure and capacity as the system gets closer to the customer. The features of the distribution system make it very unlikely that a single disruption in a pipeline would affect all of their customers. Most service disruptions would more than likely impact smaller customer sets, if at all, which may be isolated for response and recovery.

Since the management of natural gas demands a strong safety culture, the industry is well versed in emergency controls that can be applied across many situations. These mandated controls may be used to mitigate the direct physical effects of cybersecurity incidents as well. There are also natural limits on what might happen on a single pipeline. For example, if a pipeline ruptures, a single release could lower system pressure, thus reducing the potential for further physical damage. In most cases, if control systems are found to be corrupted, pipelines can also be operated manually without these digital controls, though at a diminished rate.

Some areas of the country are much more dependent on natural gas. The demand for natural gas for heating and power generation during a harsh winter may be sufficient to cause shortages when combined with an unexpected incident. When a shortage occurs, it is sometimes possible to move gas from areas with more stored capacity to areas with a shortfall by diverting flow from other pipelines. Similarly, major natural gas users usually have contractual agreements to switch

[532] Office of Cyber and Infrastructure Analysis, Natural Gas Cyberdependencies, February 3, 2015

from natural gas to another fuel supply in the event of shortage, and smaller customers can reduce their use through conservation. Natural gas utilities place a very high priority on avoiding any service disruptions and use all of the options available to them to keep customers supplied and prevent natural gas appliance lights from extinguishing.

Pipeline operators recognize that despite the robustness of the pipeline system and the standard practices for managing many types of emergencies, the impacts of a broad-scale attack on their systems must be taken seriously. Operators were confronted with this challenge when an active series of cyber-intrusions targeting natural gas pipeline sector companies occurred in 2011–2012. This single campaign from an unknown source was identified by ICS-CERT through the proactivity of owners and operators' reporting and effective information sharing. The campaign, which started in December 2011 with sophisticated, targeted spearfishing and continued for months, extracted data that could facilitate remote unauthorized operations.[533]

Since ICS are in place to facilitate reliable and efficient operation of pipeline systems that span long distances, they have the effect of reducing the number of operators needed onsite at compressor stations to control compressors. As a result the standard risk management techniques associated with onsite personnel and effective for individual events may become much more challenging given a coordinated and distributed cyberattack. Responding to such an attack would be much more stressful for the industry, testing the usefulness of mutual aid agreements within the industry if owners and operators perceive themselves simultaneously under the same attacks. There are limits to mechanisms that bring in reserve workforce and emergency responders with equipment. Response may be based on the availability of these assets. Some emergency response planners have noted that the challenges of dealing with declining budgets have resulted in decisions to reduce back-up resources and increasingly depend on mutual-aid agreements. These agreements have limitations, especially when considering the possibility of large-scale attacks that may affect multiple jurisdictions.[534]

Repeated and persistent efforts are being made to create an undetected presence of malware within natural gas pipeline systems. The scale and sophistication of these attacks appear to be increasing. The consequences of such attacks, if they were to result in active exploitation of the ICS and affected the operation of the pipelines, would be very challenging to the owners and operators. Most of these impacts are felt within the natural gas industry. It would be unlikely that such an attack would result in outages that affected the customers, unless the scale of attacks was so great that it overwhelmed the combined capabilities of the human operators. If there were a significant regional gas outage, especially if it were timed to maximize the negative impact on the population, the normal procedures would be to provide warming centers for those who are affected and then systematically manage the problem. Boulder County, Colorado experienced this problem in December 2103, when temperatures were in the single digits. Their experience, which affected 7,200 customers, provides a useful example.

The Red Cross opened warming centers to help those who could not manage the temperature drop in their homes. The utility called in extra resources from elsewhere in Colorado, and from

[533] ICS-CERT Monthly Monitor, June/July, Gas Pipeline Cyber Intrusion Campaign-Update; http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jun-Jul2012.pdf.

[534] Deborah Strasheim, Mutual Aid a concern for region's fire departments, http://www.theday.com/article/20140628/NWS01/306289976 , accessed March 6, 2015

four other states. The crews visited all customers and, turned off affected gas lines so the pressure in the lines could be restored. They were told they could not relight appliances themselves, as they would risk damaging the appliances or equipment, as well as placing themselves and their families in danger.

In summary, cyberattacks on natural gas pipeline systems continue. Data from ICS-CERT demonstrate the scale and scope of these attacks are increasing, though none of these have resulted in sabotage of the system. Nevertheless, the types of exploits observed reflect an evolving capacity to do so. The consequences of attacks that have physical effects are not likely to be devastating or have long-term impacts on customers. Natural gas pipeline systems must comply with the U.S. Department of Transportation pipeline safety regulations which are intended to prevent or minimize natural gas pipeline incidents. Owners and operators, government authorities and not-for-profits have demonstrated the capacity to manage gas delivery and reliability even during stressful periods. Attacks that combine cyber and physical tactics are much more likely to cause significant damage. Such attacks require more resources from perpetrators to understand pipeline operations, to assess pipeline infrastructure vulnerabilities and to gain access to the ICS.

Scenario	Consequences	Vulnerabilities	Threats
Cyberattack on ICS in a drinking-water system results in contaminated water	The consequences of an attack on the water system would be minimal to the public given the amount of manual and system checks currently in place. However, any type of communicated risk can have an adverse effect on public confidence in the quality of the product and the organization providing it. The greatest impact would be to the water utility in an increased need for additional cybersecurity technology.	Distributed nature of pipeline control systems. Lack of monitoring or systems, logons, and third party vendors. Integrated nature of systems allowing less secure devices that are directly connected to the Internet to be breached, thereby granting access to the more secure ICS.	Criminal hactivists, terrorist organizations, and nation states are the most likely threat actors.

Table 29: ICS Scenario Type 2

Drinking-water systems often use ICS for storage, treatment, and distribution systems. These ICS are involved in monitoring the operations of the equipment, monitoring the quality of water, and controlling different functions to execute the operations of the system. Many water utilities have ICS that are isolated from general IT enterprise systems, but trends of increasing connectivity and automation are increasing cybersecurity risks. Water utility IT services may be remotely operated by external entities which could result in unsecure remote access leaving utilities unable to detect or prevent unauthorized access.[535] Furthermore, it is not uncommon for utilities to maintain their electronic records solely for the purpose of operating safely and efficiently. They do not always consider the forensic value of recording logon events, assuring

[535] Office of Cyber and Infrastructure Analysis, Critical Infrastructure Security and Resilience Note: Water and Wastewater Systems Sector Cyberdependencies, August 22, 2014

individual usernames, or maintaining network monitoring systems and operating system records for later use.[536]

A cyberattack may cause a brief interruption or degradation within the drinking water and wastewater services. However, water infrastructure can be operated manually in the event of an incident, preventing prolonged inoperability. There is little risk of regional or national impact to public health and the economy from a single cyberattack against a water or wastewater system. A cyberattack that compromises control systems in a drinking water system is unlikely to have an immediate effect on customers, due to the existing water supply within the system.[537]

The effect of overtreatment is not toxic. The water will have chemical odors and taste, but it is not harmful to the public. The effect of under-treatment could result in pathogens being found in the water, but this still does not mean that the public will be impacted. The time delays between a gallon of water undergoing treatment and when it actually comes out of a faucet can be measured in hours or even days. This gives operators a chance to correct undertreated water while it is still in the transmission and distribution system. Even if all of the backstops fail, and undertreated water reaches the faucet, the outcome is comparable to other incidents, such as water-main breaks, electrical outages, which may force boil-water notices, or some other advisory not to use the water until the conditions have been cleared.

Risk perception is often a matter of perspective. National authorities may view boil-water or Do-Not-Use notices as a routine and appropriate action for water system operators who have operational problems. Many of the owner-operators, however, experience these problems infrequently and are more risk averse. Furthermore, they believe that the public would respond differently if the same notice went out because of a cyberattack.

Managing these risks are problematic as well. Sometimes they do not have as much control over their own IT systems as other infrastructure operators. The IT or cybersecurity staff at a water system may be limited in their authority. They are often part of a larger municipal enterprise with shared IT systems. This creates a layer of bureaucracy that may make it harder to execute needed changes within the enterprise architecture. The costs of cybersecurity are significant for a water utility. They do not have the authority to simply charge more for water to cover these expenses. Any rate hikes must be approved by an oversight authority, such as a planning commission. Finally, water systems often contract with third parties to manage and update their control systems. This model of operations may seem less costly, but it typically results in their devices being exposed to the Internet, leaving them uncertain about who is accessing these systems.

There have been instances where cyberattacks have had physical consequences in the Water and Wastewater Systems Sector. In one instance, the system that controlled a vital operating function was hacked by a foreign national, who used it as his own distribution system for email or pirated software. The unauthorized traffic used so much of the system's capacity that operations were impacted, but the facility was able to manage and the water quality was not impacted.[538] In a more removed example, in 2000, at a sewage treatment plant in Queensland, Australia, a former employee of a software company hacked into the SCADA system releasing over 264,000 gallons

[536] ICS-CERT Monitor, Water Treatment Facility Control System Anomalies, May-August 2014
[537] CISR Note: Water and Wastewater Systems Sector Cyberdependencies
[538] Jerome, Sara. *Water Sector Eyes Federal Cybersecurity Efforts*. Water Online. July 31, 2013, http://www.wateronline.com/doc/water-sector-eyes-federal-cybersecurity-efforts-0001, accessed March 6, 2015

of raw sewage into the surrounding environment. The situation in Queensland is a noteworthy example as this vulnerability may be found in U.S. water and wastewater systems that have not taken extra measures to prevent it.

Also, cyberattacks could potentially result in breakage of pipes, treatment equipment, pumps, etc. If an attack were to result in breakage, the consequences would go up. Some state and local planners want to prepare for scenarios with distributed and coordinated cyber-attacks on ICS that result in water treatment failures and broken infrastructure. Such attacks have not been reported, but may be feasible. The concerns about water contamination are noted above. Broken infrastructure would add significantly to costs, and increase the stress on a sector with very tight operating margins. Concerted public and private collaboration has considered the possibility of such physically destructive attacks. The safety-engineering designs seem likely to intervene to protect pumps and valves. There is a low level of confidence that significant physical destruction is even feasible through attacks on the water infrastructure.

The costs of replacing broken equipment within a drinking water system will vary. As a rough planning guide, equipment that is concealed below the surface, delaying the recognition of the problem and requiring excavation to address it, will be more costly and disruptive to replace than comparable equipment closer to the plant. The costs and disruption increase significantly if this is in a highly trafficked area. This considers just the costs to the utility. If water service was lost in an area, the local and regional economic losses would be far greater. If there were a widespread outage, the time to repair and replace the damaged infrastructure could be significant.

It is important to maintain flow in water distribution systems. If pipes become empty, the external pressure on the pipes is not balanced by an interior pressure. This may result in seepage into the pipes and contamination of the water, which would be mitigated by a boil water notice. Some consider it is also feasible there might be fractures in older or more fragile pipes, and repairs, replacements and environmental impacts can be very costly.[539]

There have been no observed incidents of drinking water equipment breakage. Comparable equipment has been attacked with relatively minor consequences. In 2007, in Willows, California, a failure of physical security allowed a former employee to gain access to a SCADA system and install unauthorized software which damaged the SCADA system itself, but not the irrigation system it was managing.[540]Another example of the potential harm that may stem from an information security problem was the 2005 failure of the Taum Sauk Dam in Missouri. This dam did not contain a drinking water reservoir, but rather a reservoir built on top of a mountain to facilitate hydro-generation. It was an earthen embankment dam that operated by releasing water during peak electrical demand hours, and then pumping the water back up during off-peak hours. There was a difference between the data reported by gauges at the dam and gauges at a remote monitoring system which led to water continuing to be pumped, even though the reservoir was already at maximum capacity. The resulting overflow led to a catastrophic

[539] Office of Cyber and Infrastructure Analysis, Critical Infrastructure Security and Resilience Note: Water and Wastewater Systems Sector Cyberdependencies, August 22, 2014

[540] U.S. Government Accountability Office, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain*, GAO-08-119T, October 17, 2007. Page 7.

release.[541] It may be rare for drinking water reservoirs to be situated this way, or for the status of drinking water reservoir to be monitored less closely. While this type of loss seems a plausible example of significant physical damage that could occur, Environmental Protection Agency (EPA) subject matter experts maintain that the peculiarities of the hydroelectric reservoir involve conditions that cannot be found in water systems.

Individual cybersecurity incidents in the Water and Wastewater Systems Sector typically do not have offsite consequences, but when they do, the consequences are unlikely to be greater than those that arise occasionally from other causes, such as equipment malfunctions or flooding. All infrastructure sectors depend on drinking water and wastewater systems to some degree, and would not be able to function for extended periods of time without these systems. Any suggestion that there are likely to be cascading infrastructure consequences from individual cybersecurity incidents at water or wastewater infrastructure would be misleading and overstated, because a cybersecurity incident is unlikely to result in a significant denial of water or wastewater services. The potential for a temporary loss of water or wastewater services to have a cascading effect in another sector is small and localized, but could be significantly greater if coordinated distributed attacks impacted many parts of an individual large system, or affected many systems.

Cyberattacks on water and wastewater systems continue, with sophisticated actors often the perpetrators. It is not clear if the scale and scope of these attacks is increasing; if so, they are not increasing significantly. The consequences of isolated attacks that are actually able to contaminate the water system through under-or over-treatment are not likely to have a devastating effect. Water moves slowly enough through a system that there are opportunities to discover, through additional monitoring, that the water quality is incorrect and to intervene and flush the water before it is released. Attacks that result in physical damage or those that combine cyber- and physical tactics are much more likely to cause significant damage and costly consequences. Water system information security incidents continue to increase in frequency, though very few to date have had actual physical consequences. These, however, are not the type of scenarios where sophisticated actors have invested in developing the presence and capacity to sabotage the system. It is unclear if these exploits are actually increasing, or if it is just due to owners and operators revealing them at a greater rate. In either case, the sophisticated and coordinated attacks that result in devastating outcomes have not occurred.

[541] National Weather Service Weather Forecast Office, December 14, 2005 Taum Sauk Dam Failure at Johnson's Shut-In Park in Southeast Missouri. http://www.crh.noaa.gov/lsx/?n=12_14_2005.

Scenario	Consequences	Vulnerabilities	Threats
Complex coordinated attack on the grid is conducted so as to maximize physical damage and power outage	The most serious consequences of a successful cyberattack on the grid would be associated with attacks that succeeded in destabilizing the grid by removing a large proportion of either generation or load resulting in rolling blackouts.	Distributed nature of electricity substations. Lack of monitoring or systems, logons, and third party vendors. Integrated nature of systems allowing less secure devices that are directly connected to the Internet to be breached, thereby granting access to the more secure ICS.	Criminal hactivists, terrorist organizations, and nation states are the most likely threat actors.

Table 30: ICS Scenario Type 3

In November 2014, Admiral Michael Rogers, the Director of the National Security Agency and Commander of the U.S. Cyber Command testified before the House (Select) Intelligence Committee that sophisticated attacks from nation-states had the potential to "shut down the entire U.S. power grid."[542] Concern about cyberattacks on the electrical grid is reflected in a large number of the scenarios identified from a review of THIRAs.

Electric power networks are required to be resilient to the loss of any single component (including generation units, high-voltage transmission lines, and transformers) under the reliability standards developed and enforced by the North American Electric Reliability Corporation (NERC), which oversees eight regional reliability entities and encompasses all of the interconnected power systems of the contiguous United States, Canada and a portion of Baja California in Mexico. Each of these regional entities is also required to maintain an "operating reserve margin" of available generation capacity that can be called up within minutes to mitigate the loss of generation sources due to an unplanned outage.

The most serious consequences of a successful cyberattack on the grid would be associated with attacks that succeeded in destabilizing the grid by removing a large proportion of either generation or load. A cyberattack could theoretically be designed to disrupt power generation directly through its control system or by causing a precipitous drop in demand. This drop in demand could be achieved by disconnecting portions of the transmission network, which could cause generation plants to trip offline to avoid damaging the turbines. The consequences of an attack will depend on two factors: the amount of generation capacity taken out of service and whether the equipment is physically damaged. If a sufficient amount of generation is taken offline, low voltage and outage conditions could result. If equipment is physically damaged, restoration will take far longer than if it has only been disconnected. Even if equipment is not damaged, operators would still need time to investigate the causes, assess operability, and restart generators.

[542] National Security Agency Hearing of the House (Select) Intelligence Committee; Subject: "Cybersecurity Threats: The Way Forward," transcript at www.nsa.gov/public_info/_files/speeches_testimonies/ADM.ROGERS.Hill.20.Nov.pdf, accessed March 5, 2015.

Transmission networks combine cyber-dependent control systems and the potential for high consequences from outage. The high-voltage transformers used in electric power transmission, in particular, would be expensive and difficult to replace if damaged. However, it is not clear that a cyberattack would be able to physically damage multiple transformers, because this equipment is protected by multiple protection layers, including some protection layers built into the transformers, specifically designed to minimize the damage to transformers.543 Replacing damaged extra-high voltage transformers would be expensive and logistically difficult as replacements can take up to 18 months to manufacture.

If enough generation is lost that the operating reserve margin is exhausted, the regional operators could call for utilities to shed load through voluntary conservation, exercising interruptible contracts, or implementing rolling blackouts as needed. Rolling blackouts are likely to be the worst-case consequence for the disruption of a small number of generation plants.

An attack on transmission network or generation equipment that disrupts a large number of assets on the network could have high consequences, perhaps similar to the 2003 Northeast Blackout, which affected an estimated 10 million people in Ontario and 45 million people in eight states in the U.S.544 This would likely require a very well-planned and sophisticated attack, because even though multiple systems may use the same control system protocols, the protocols can be implemented differently; each time a system operator sets up the control system, there should be a unique set of access controls (e.g., passwords). Disconnecting or damaging a sufficiently large amount of generation could cause widespread blackouts and "islanding" of portions of the grid still operating. In addition to the time needed for assessment, operators would need to restore power gradually to maintain the stability of the grid as more generation returned to service. In the event of a complete regional blackout, certain generation stations capable of starting up without using offsite power would be the first to be restored, so that they could provide the offsite power needed to bring other sites back online.

Although the system is resilient to unplanned outages of one or two assets, such as may occur in the normal course of operation, it is not designed to cope with an intentional attack on many assets. Outages of this length obviously pose health and safety concerns, would incur business disruption costs, and stress the backup power provisions for critical infrastructure. There is also the potential for added psychological impact associated with the fact that the outage was caused by a cyberattack. This will likely shake the public's confidence in critical infrastructure security and perhaps infrastructure regulators.

Modeling and simulation of electric power is well-developed and is used for the daily operation of electric power networks, planning for future network conditions, predicting the impacts of

---

[543] See for example GE Digital Energy, "Transformer Protection Principles," www.gedigitalenergy.com/smartgrid/Mar07/article5.pdf , accessed March 9, 2015.

[544] Although advances in reliability standards make such an event unlikely today, this is an example of a cascade set off by a software bug in a control room alarm system. At the peak of summer demands for electric power, a transmission line sagged into an unpruned tree. This cascaded into an outage that affected an estimated 10 million people in Ontario and 45 million people in eight states in the U.S. because control room operators did not receive the alarm and respond in time. The fluctuating power on the network caused more than 508 generating units at 265 power plants to trip offline. Secondary impacts were felt to communications (including 911 services), water infrastructure, and electric rail transportation. See U.S.-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," April, 2004, at http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf, accessed March 3, 2015.

impending or hypothetical hazards, and optimizing network restoration. In addition to utilities and their authorities, numerous National Laboratories, universities, Government entities and others use commercially-available models, sometimes tailored to answer particular questions.[545] Thus, there is a wealth of information (historical data and modeling results) about how the electric grid might behave under various contingencies. Nonetheless, it is impossible to predict the outcome of any scenario with complete certainty. This is partly because the instantaneous conditions on the network can affect the outcome, and partly because it is impossible to know all the factors that will influence the decisions made by the people actually managing the grid.

Similarly, there is a wealth of information about cybersecurity and a strong motivation to protect the information and communications networks on which the electric grid increasingly relies. What is missing is a good understanding of how vulnerabilities in cyber infrastructure might play out in an attack scenario. This is likely to be a very thorny problem, as the answers will vary from region to region and perhaps, utility to utility, depending on the exact configuration of existing physical and virtual infrastructure.

For example, it is not clear to what degree a cyberattack could physically damage infrastructure. If damage is minimal, the impacts could be orders of magnitude less than the worst-case scenarios involving damaged high-voltage transformers. Even as widespread, disruptive, and costly as the 2003 Northeast Blackout was, most customers had power restored within 2 days. In contrast, although Superstorm Sandy affected a smaller number of customers, restoration required repairing or replacing a huge amount of equipment damaged by winds and flooding, and took much longer to complete. Still, the rate of restoration after Sandy was similar to that required for other strong, damaging storms; it took about 10 to 14 days to restore power to 95% of customers.[546] Clearly, the degree of physical damage to the system will be a key driver in the duration of an outage and therefore the human, economic, and social impacts.

For this reason, scenarios that combine cyber and physical attacks are likely to have the greatest potential consequences. For example, a cyberattack could make a physical attack more difficult to detect and mitigate, while physical damage could delay restoration and thereby magnify the impacts of a cyberattack. Combined attacks may be cyber-enabled physical attacks (in which cyber means are used to get access to enable a physical attack) or a physical-enabled cyberattack (in which physical means are used to access a control system, thereby allowing the system to be maliciously altered). Either type could have serious consequences.

Cyberattacks on the grid continue, with sophisticated actors often the perpetrators. The scale and scope of these attacks may be increasing, but if so, not significantly. The consequences of attacks that are only able to impact individual generators, or which do not cause significant physical damage are unlikely to have a devastating effect. Attacks that combine cyber- and physical tactics are much more likely to cause significant damage and costly consequences, and it is unclear if such attacks are being planned. Electric grid cybersecurity incidents continue to increase in frequency, including attacks by sophisticated actors appearing to establish the

[545] One example is the electric power analysis performed by DHS for hypothetical disaster scenarios or in response to real-world events. DHS is supported by the National Infrastructure Simulation and Analysis Center, a joint endeavor of Los Alamos and Sandia National Laboratories. For more information, see www.dhs.gov/office-cyber-infrastructure-analysis.

[546] Fahey, Jonathan, Associated Press, "Power Outages After Hurricane Sandy Weren't Unusually Long After All," November 16, 2012, at www.dailyfinance.com/2012/11/16/power-outages-after-hurricane-sandy-werent-unusually-long-after/, accessed March 3, 2015.

capability to sabotage the grid. The actual acts of sabotage are not attempted, however, and it is unclear if the risk of coordinated and effective sabotage of the grid through cyberattacks will happen.

Cyber 9/11

Introduction

There are quite a number of sources that have postulated that massive distributed attacks against infrastructure are expected, which would have massive debilitating effects on the U.S.. Starting back in 1991, when Winn Schwartau, then Director of the International Partnership against Computer Terrorism, warned against an electronic Pearl Harbor in his testimony before the House Subcommittee on Technology and Competitiveness of the Committee on Science, Space and Technology of the U.S. House of Representatives.[547] Members of the 9/11 Commission called attention to the threat in "Reflections on the Tenth Anniversary of the 9/11 Commission Report.[548] Homeland Security Secretary Janet Napolitano warned in January 2013 speech at the Wilson Center that a "cyber 9/11" could happen imminently. If it were to occur, it could cripple the country, taking down the power grid, water infrastructure, transportation networks and financial networks."[549]

The most recent assessment of the U.S. Intelligence community reduces the expectation for such a scenario. In his February 26, 2015 testimony before the Senate Armed Services Committee James Clapper, Director of National Intelligence stated that, "Rather than a 'cyber-Armageddon' scenario that debilitates the entire U.S. infrastructure, we envision something different," …"We foresee an ongoing series of low-to-moderate level cyber-attacks from a variety of sources over time, which will impose cumulative costs on U.S. economic competitiveness and national security."

Coincidentally, this speech followed a day after New York financial regulator Ben Lawsky predicted that a cyber-Armageddon would occur within the Financial Services Sector in the next decade. This reflects the importance of the viewpoint of those who are interpreting what is going on.

> Complex coordinated attack on significant infrastructure resulting in catastrophic outcomes …Interpreting the data

The Internet and American Life project conducted by the Pew research firm on the subject released its findings in Digital Life magazine in 2015.[550] Their survey of 1,642 experts in the field found that 61percent believe that by 2025, there will a major cyberattack that has caused widespread harm to a Nation's security and capacity to defend itself and its people. (By

---

[547] The record of the proceedings http://babel.hathitrust.org/cgi/pt?id=pst.000018472172;view=1up;seq=14#view=1up;seq=1 , accessed March 6, 2015

[548] Adam Goldman, 9/11 commission members warn of cyber attack threats, http://www.washingtonpost.com/world/national-security/911-commission-report-authors-warn-nation-of-cyberattack-threats/2014/07/21/82d0fb84-10e5-11e4-98ee-daea85133bc9_story.html accessed March 6, 2015

[549] Reuters, U.S. homeland chief: cyber 9/11 could happen "imminently", http://www.reuters.com/article/2013/01/24/us-usa-cyber-threat-idUSBRE90N1A320130124?feedType=RSS&feedName=technologyNews&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+reuters%2FtechnologyNews+%28Reuters+Technology+News%29 accessed March 6, 2015

[550] http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/

"widespread harm," they specified significant loss of life or property losses/damage/theft at the levels of tens of billions of dollars.) Survey respondents provided the basis for their judgment, which the Pew researchers organized into four themes:

- Internet-connected systems are inviting targets. The Internet is a critical infrastructure for national defense activities, energy resources, banking/finance, transportation, and essential daily-life pursuits for billions of people. The tools already exist to mount cyberattacks now and they will improve in coming years—but countermeasures will improve, too.
- Security is generally not the first concern in the design of Internet applications. It seems as if the world will only wake up to these vulnerabilities after catastrophe occurs
- Major cyberattacks have already happened, for instance the Stuxnet worm and attacks in nations where mass opposition to a regime has taken to the streets. Similar or worse attacks are a given.
- Cyberattacks are a looming challenge for businesses and individuals. Certain sectors, such as finance and power systems, are the most vulnerable. There are noteworthy divides between the prepared and the unprepared.

The other 39 percent of the respondents believed that there would not be such a major attack by the year 2025. The justifications for their responses were grouped into the following lines of thought:

- There is steady progress in security fixes. Despite the Internet's vulnerabilities, a distributed network structure will help thwart the worst attacks. Security standards will be upgraded. The good guys will still be winning the cybersecurity arms race by 2025.
- Deterrence works, the threat of retaliation will keep bad actors in check, and some bad actors are satisfied with making only small dents in the system so they can keep mining a preferred vulnerability and not have it closed off.
- Hype over cyber-attacks is an exaggeration of real dangers fostered by the individuals and organizations that will gain the most from creating an atmosphere of fear.

Perhaps the most interesting outcome of this research is insight into how individuals who seem to be experts in a field, maintain inconsistent knowledge of current events in their area of expertise, how they synthesize the large amount of information on the topic, and the potential role of biases in their responses. Regardless of anyone's perceptions of what is actually happening and whether it will continue, decrease or increase, the fact is that vulnerabilities are constantly being discovered by both those who wish to take advantage of them and those who would like to see them managed. The time advantage goes to the offense, however, who may root undetected for months planning and laying the foundation for an exploit, where the defense must respond quickly and decisively, typically after a loss has occurred.

Insights gained over the last few years from cybersecurity specialists also reveal a disturbing blurring-of-the-lines between the capabilities of sophisticated state actors and cybercriminals who seek financial gain. Some of these commonalities include increasingly insightful use of spear-phishing emails, custom malware tools, crimeware that has been available for years,

persistent presence for years and attempted return after being kicked out, and a common and growing interest in collecting PII.[551]

It is noteworthy that none of the respondents considered the ingenuity of infrastructure operators, normal emergency responses, the logical limitations of the how to combine interdependent outages of different infrastructures in their assessment. They also clearly segregated the Armageddon cyberattack from those attacks that are occurring and may yet occur within our Financial Services Sector.

The nearly coincidental dismissal of the threat of a cyber-Armageddon by the Director of National Intelligence and the prediction of an impending cyber-Armageddon by a financial regulator may ironically both be true, since so few recognize the financial services industry as an infrastructure sector, nor understand the concept and causes of systemic financial risks. Just as a few people demanding their funds from a bank may not be problem, but many of them doing so created runs on banks in the past, and just as a loss of confidence can spin out of control into a crisis of confidence, financial regulators must concern themselves with these sudden amplifications of problems within the financial services industry. They recognize the possibility that operational risks such as cybersecurity could lead to unexpected exposures or crises of confidence that institutions had not prepared for. It is this type of risk that may be most likely to lead to a cyber-Armageddon.

Scenario	Consequences	Vulnerabilities	Threats
Cyberattack leaves malware inserted in the control systems of many key infrastructures without further activation	The costs of constant scanning, cleanup and removal of malware that has not yet been used is significant but minor compared to the costs of dealing with the consequences of an actual attack that affects the operation of infrastructure. The consequences envisioned by a massive attack on key critical infrastructure are catastrophic, however, there is currently no evidence to suggest this is an imminent possibility.	Distributed nature of critical infrastructure ICS. Lack of monitoring or systems, logons, and third party vendors among utilities. Integrated nature of systems allowing less secure devices that are directly connected to the Internet to be breached, thereby granting access to the more secure ICS.	Criminal hactivists, terrorist organizations, and nation states are the most likely threat actors.

Table 31: Cyber 9/11 Scenario Type 16

The concern continues that some catastrophic attack that exploits vulnerabilities in much of U.S. physical infrastructure in a coordinated and felling strike. The reason for this continued concern is that it is common to discover that sophisticated adversaries have planted malware in systems and then just left, with a back-door to ease their access at a later date. An example of such

[551] Mandiant, M-Trends 2015: A view from the front lines, downloadable PDF at: https://www.fireeye.com/current-threats/threat-intelligence-reports.html, accessed March 17, 2015

evidence is the recent discovery that the Sony data breach and wipe, while enacted suddenly, was found to have been started a year prior.

The scale, scope, and complexity of attacks on infrastructure may be increasing, or may simply being discovered at a greater rate. The lack of clarity between the rate of occurrence and the rate of discovery is an obstacle to understanding the frequency of such attacks as well. The costs of constant scanning, cleanup and removal of malware that has not yet been used is significant but minor compared to the costs of dealing with the consequences of an actual attack that affects the operation of infrastructure. But perhaps the greatest burden associated with this "partial attack" is the realization that an adversary has invested time and resources to be ready at a moment's notice to deliver a decisive attack. The adversary has radically changed the game, the defender has already lost, and no one really knows what may yet be discovered.

Conclusion

The risks associated with cybersecurity incidents in the U.S. are better understood today than ever before. This is a result of improved reporting and increased analytic foundations for understanding consequences. The increased transparency has provided better insight into a larger portion of a risk landscape, though it remains comparatively unclear to risk managers and planners who may try to compare these challenges to more obvious and predictable hazards, such as natural hazards, accidents, and routine crime.

Unlike natural hazards, cyberthreats do not have a geospatial aspect that makes it easier to determine the likelihood, character, or the strength of incidents. Like accidents, many cybersecurity incidents are the result of human reliability failures. Unlike accidents, cyberattacks have malicious individuals attempting to lure victims into compromising themselves.

Like routine crime, many cybersecurity incidents are all about the money. Organized crime and major drug cartels have demonstrated that having intelligent managers of a major criminal endeavor can make it all the more lucrative. This may be even more so for cybercriminal groups. Cybercriminal groups provide the opportunity to unscrupulous people who could clearly make a very respectable income in the real economy to gamble for a much more extravagant return with fairly low risk. While the prosecution of cybercrimes is increasing, the cases are so complicated, often with so many different jurisdictions involved, that it would be unreasonable to suggest that the fear of prosecution is a substantial deterrent. Like other crimes where individual's privacy and personal autonomy is violated, there is a culture of blame and shame for the victims of cybercrime that has created a substantial incentive for victims to hide, to try to deal with these attacks privately or with the assistance of cybersecurity consultants. The degree to which this incentivizes improved security, or to which improving security can sufficiently protect an organization is unclear.

Like terrorism and Nation-state competition, failures of cybersecurity give an adversary power. This power may be in the ability to control a message, silence free speech, or deny an organization the right to do its lawful business. It may be in the ability to systematically establish and maintain a presence in our networks that allows the adversary to extract the hard-earned value of intellectual property, and turn it over to their own enterprises, so they do not have to compete on a level field. It may make it easy to figure out who works in sensitive positions and what their personal challenges are, so that intelligence agents can focus their attention on subjects most likely to become useful spies. It may be the systematic mining of the computer systems that we use to manage and operate our complex infrastructures and industrial plants with

computer exploits which can be triggered at the convenience of the adversary, giving him an effective and distracting attack that may enhance some other activity. Like physical attacks by terrorists or nation-states, these politically and militarily driven cyberattacks lead to a loss of confidence in Government.

Given the diversity adversaries, their intentions, the known and unknown dangers, and the persistence of the American public in moving so much of their lives and work into cyberspace, the comparison that may be most apt is the analogy of the westward expansion of the U.S. President Barack Obama made this analogy on February 13th, 2015. He cautioned against the expectation that the U.S. could expect the Federal Government to fill the role of the sheriff in this new frontier, and he encouraged broad collaboration and cooperation across government and industry in this challenging cybersecurity space.[552]

In addition to these efforts to help stem the attacks, owners and operators of systems may be able to find ways to decouple the cause and effect of cybersecurity incidents and the harms they currently produce. Planners may be positioned to make the case for cybersecurity investments in redundancies, backups, and quick-response capabilities. Researchers in the fields of human reliability may be able to identify ways to reduce the likelihood of human errors resulting in cybersecurity compromises. Agencies may systematically identify and evaluate networks where their information is exposed, and how the exposed information could benefit adversaries, as part of their enterprise risk management. Legislators and regulators may consider how to maximize the incentives for public/private partnership on the defense of government and industry systems and services; and encourage the growth of a cybersecure workforce and public. These distributed contributions reinforce the idea that a whole-of-community approach will improve the safety and security of U.S. interests in cyberspace.

[552] National Public Radio, Obama: Cyberspace is the New 'Wild West', http://www.npr.org/blogs/thetwo-way/2015/02/13/385960693/obama-to-urge-companies-to-share-data-on-cyber-threats, accessed March 23, 2015.