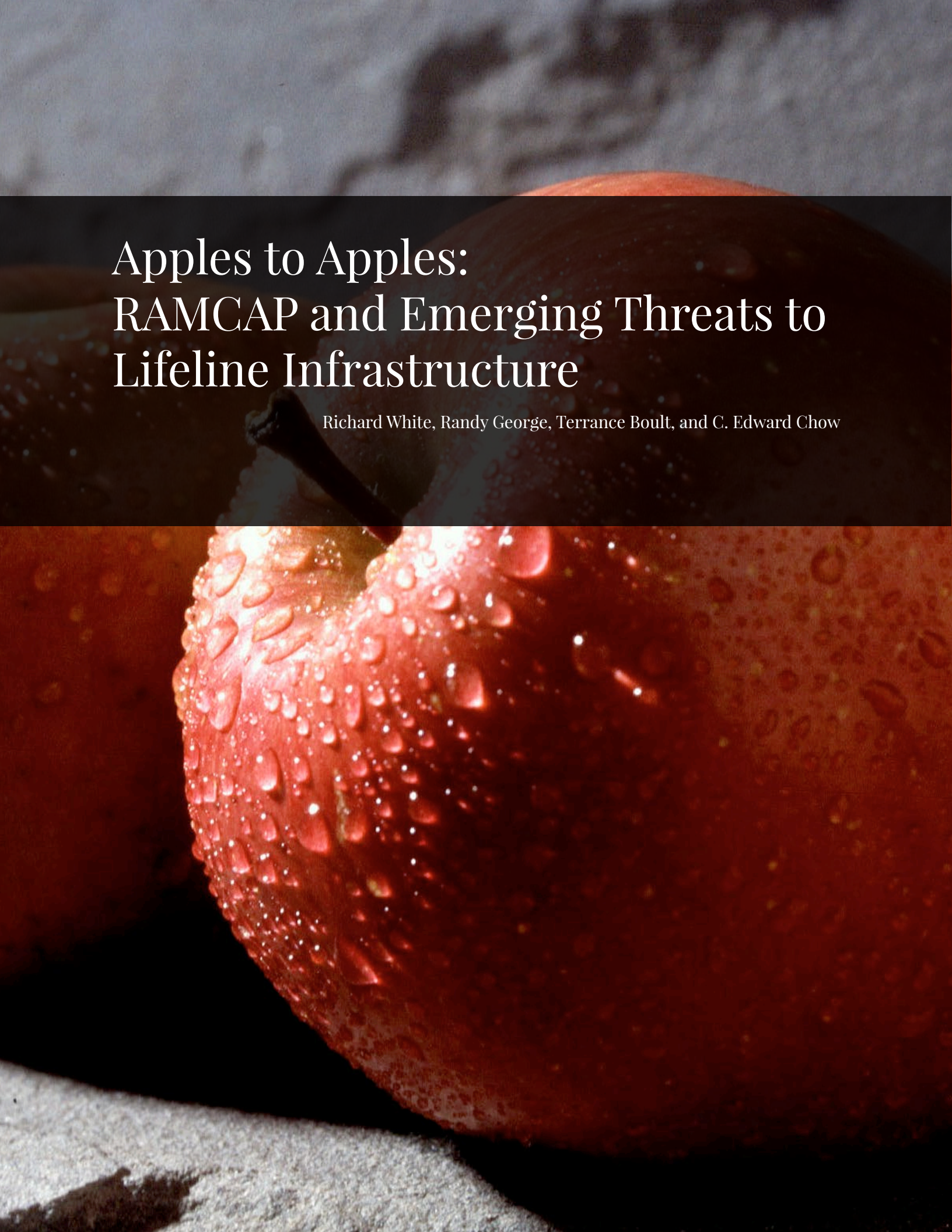

Apples to Apples: RAMCAP and Emerging Threats to Lifeline Infrastructure

Richard White, Randy George, Terrance Boult, and C. Edward Chow

Abstract

The search for a uniform risk analysis for critical infrastructure protection prompted a look at RAMCAP to see if it accommodates emerging threats from climate change, aging infrastructure, and cybersecurity. This article examines the role of Reference Scenarios in guiding RAMCAP estimations of risk, resilience, and countermeasures. It investigates current infrastructure protection practices to identify emerging threats to lifeline infrastructure encompassing the Water, Wastewater, Electricity, Aviation, and Internet subsectors. The investigation found thirty-eight Candidate Scenarios which subsequent analysis filtered down to thirteen Nominee Scenarios. The Nominee Scenarios include new process-based subclasses and types that are unlike current Reference Scenarios. Thus the study found that RAMCAP does not currently address emerging threats to lifeline infrastructure. Those interested in critical infrastructure protection policy and implementation may find the insights from this study useful to their own understanding and research.

Suggested Citation

Richard White, Randy George, Terrance Boult, and C. Edward Chow. "Apples to Apples: RAMCAP and Emerging Threats to Lifeline Infrastructure." Homeland Security Affairs 12, Article 2 (September 2016). https://www.hsaj.org/articles/12012

Introduction

Concern over the water and wastewater infrastructure due to emerging threats from climate change, aging infrastructure, and cyber attack prompted the Department of Homeland Security Science and Technology Directorate (DHS/S&T) to undertake development of a new risk analysis standard to measure risk uniformly across all lifeline infrastructure. According to the 2013 National Infrastructure Protection Plan (NIPP), lifeline infrastructure encompasses Water, Energy, Transportation, and Communications,[1] four of the sixteen sectors identified in Presidential Policy Directive #21 (PPD-21). Uniform risk analysis, comparing "apples to apples" across infrastructure sectors facilitates cost-benefit analysis and strategic planning that are critical to optimizing homeland security investments and safeguarding the nation against catastrophic incidents, both natural and manmade. A uniform risk analysis comparing "apples to apples" can also help the Department of Homeland Security achieve a long-sought goal of measuring current resilience and quantifying the efficacy of countermeasures; or in other words, to inform the President and Congress where we are, where we are going, and at what cost.

The essential importance of a uniform risk analysis for critical infrastructure was recognized by the White House when it recruited the American Society of Mechanical Engineers (ASME) to develop one shortly after 9/11.[2] In 2006 ASME released the final specifications for a Risk Analysis and Management for Critical Asset Protection (RAMCAP). RAMCAP is a seven-step process that assesses risk for a given asset as a product of threat, vulnerability, consequence, resilience, and applied countermeasures. To make RAMCAP uniformly applicable across infrastructure sectors, its creators incorporated a reference set of forty-one threat and hazard scenarios to guide estimations of its terms. The 2006 NIPP recommended RAMCAP

for conducting risk analysis,[3] but was not mentioned in the 2009 and 2013 revisions. No RAMCAP implementations are known to be employed today.[4] RAMCAP, however, continues to serve as the basis for the American Water Works Association (AWWA) J100-10 standard for Risk and Resilience Management of Water and Wastewater Systems.[5]

In October 2014, the University of Colorado, Colorado Springs (UCCS) was engaged by Oak Ridge National Laboratory (ORNL), the program manager for the DHS/S&T project, to conduct a needs assessment of RAMCAP and develop requirements for uniform risk analysis of lifeline infrastructure. The project was divided into three tasks: 1) Analysis of Emerging Threat & Hazard Scenarios, 2) RAMCAP Performance Analysis, and 3) RAMCAP Requirements Analysis. This article presents the results from Task 1 and insights gained into emerging threats from climate change, aging infrastructure, and cybersecurity to the Water, Wastewater, Electricity, Aviation, and Internet subsectors.

Background

RAMCAP is a critical infrastructure risk analysis methodology that calculates risk as a product of consequence, vulnerability, and threat.[6] RAMCAP is comprised of the seven steps listed in Table 1.[7] It is designed to assist infrastructure owners/operators with identifying risk and applying countermeasures to avert or alleviate the "worst reasonable consequences" stemming from disruption or destruction of system assets.[8] Countermeasures beyond the scope of owners/operators to implement could be considered for federal homeland security grants under the NIPP Risk Management Framework.[9] By applying a uniform risk analysis methodology such as RAMCAP, it was possible to rank risk across infrastructure sectors and to conduct cost-benefit analysis to prioritize countermeasures, thus offering the greatest return on homeland security investment.[10]

Table 1. RAMCAP 7-Step Process

Step	Description
1.	Asset Characterization
2.	Threat Characterization
3.	Consequence Analysis
4.	Vulnerability Analysis
5.	Threat Analysis
6.	Risk & Resilience Analysis
7.	Risk & Resilience Management

RAMCAP's uniform analysis capability is predicated on forty-one Reference Scenarios listed in Table 2. The scenarios help guide owners/operators through RAMCAP's seven steps in estimating values for consequence, threat, vulnerability, and resilience. The use of Reference Scenarios helps RAMCAP meet NIPP risk assessment core criteria for documentation, reproducibility, defensibility, and completeness.[11] Our challenge in Task 1 was to determine whether the given forty-one scenarios sufficiently addressed emerging threats to lifeline infrastructure from climate change, aging infrastructure, and cybersecurity.[12]

Table 2. RAMCAP Reference Scenarios (2, p. 55)

#	Class	Subclass	Type	ID
1.	Hazard	Natural	Hurricane	N(H)
2.	Hazard	Natural	Earthquake	N(E)
3.	Hazard	Natural	Tornadoes	N(T)
4.	Hazard	Natural	Floods	N(F)
5.	Hazard	Natural	Wildfire	N(W)
6.	Hazard	Natural	Ice Storms	N(I)
7.	Hazard	Dependency	Loss of Utilities	D(U)
8.	Hazard	Dependency	Loss of Suppliers	D(S)
9.	Hazard	Dependency	Loss of Employees	D(E)
10.	Hazard	Dependency	Loss of Customers	D(C)
11.	Hazard	Dependency	Loss of Transportation	D(T)
12.	Hazard	Dependency	Proximity to Target	D(P)
13.	Threat	Contamination	Chemical	C(C)
14.	Threat	Contamination	Radionuclide	C(R)
15.	Threat	Contamination	Biotoxin	C(B)
16.	Threat	Contamination	Pathogen	C(P)
17.	Threat	Contamination	Weaponization	C(S)
18.	Threat	Sabotage	Physical-Insider	S(PI)
19.	Threat	Sabotage	Physical-Outsider	S(PU)
20.	Threat	Sabotage	Cyber-Insider	S(CI)
21.	Threat	Sabotage	Cyber-Outsider	S(CO)
22.	Threat	Theft	Physical-Insider	T(PI)
23.	Threat	Theft	Physical-Outsider	T(PU)
24.	Threat	Theft	Cyber-Insider	T(CI)
25.	Threat	Theft	Cyber-Outsider	T(CO)
26.	Threat	Attack: Marine	Small Boat	M1
27.	Threat	Attack: Marine	Fast Boat	M2
28.	Threat	Attack: Marine	Barge	M3
29.	Threat	Attack: Marine	Ocean Ship	M4
30.	Threat	Attack: Aircraft	Helicopter	A1
31.	Threat	Attack: Aircraft	Small Plane	A2
32.	Threat	Attack: Aircraft	Regional Jet	A3
33.	Threat	Attack: Aircraft	Long-Flight Jet	A4
34.	Threat	Attack: Vehicle	Car	V1
35.	Threat	Attack: Vehicle	Van	V2
36.	Threat	Attack: Vehicle	Mid-Size Truck	V3

#	Class	Subclass	Type	ID
37.	Threat	Attack: Vehicle	Large Truck	V4
38.	Threat	Attack: Assault	1 Assailant	AT1
39.	Threat	Attack: Assault	2-4 Assailants	AT2
40.	Threat	Attack: Assault	5-8 Assailants	AT3
41.	Threat	Attack: Assault	9-16 Assailants	AT4

Lifeline Infrastructure

Water, Electricity, Transportation, and Communications are considered "lifeline" infrastructure because they are essential to themselves and all other sectors.[13] Lewis classifies them as "Level 1" infrastructure upon which all others depend.[14] The four lifeline infrastructure sectors encompass sixteen subsectors as shown in Table 3. In order to maintain a manageable scope, we restricted Task 1 to the Water, Wastewater, Electricity, Aviation, and Internet subsectors. The Internet is actually a subsector of the Information Technology sector.[15] Task 1 examined the Internet subsector, however, because it underpins a large proportion of the Communications sector.[16]

Table 3. Lifeline Infrastructure Sectors & Subsectors

#	Sector	SSA1	SSA2	CA	Subsector
1.	Water/Wastewater	EPA			Water
2.		EPA			Wastewater
3.	Energy	DOE		FERC	Electricity
4.		DOE		FERC	Natural Gas
5.		DOE			Oil
6.	Transportation	DOT	TSA	FAA	Aviation
7.		DOT	TSA	FHWA	Highway
8.		DOT	TSA	FRA	Freight Rail
9.		DOT	TSA	FTA	Mass Transit
10.		DOT	TSA	PHMSA	Pipeline
11.		DOT	USCG	MARAD	Maritime
12.	Communications	DHS		FCC	Broadcast
13.		DHS		FCC	Cable
14.		DHS		FCC	Satellite
15.		DHS		FCC	Wireless
16.		DHS		FCC	Wireline
SSA = Sector-Specific Agency, CA = Coordinating Agency					

Worst Reasonable Consequences

RAMCAP bases its risk calculation on the "worst reasonable consequence" (WRC) resulting from damage or destruction of critical infrastructure assets.[17] The AWWA J100-10 standard does not define what constitutes a "reasonable" worst case situation except to say it shouldn't combine unlikely coincidences.[18] Step 3 of the RAMCAP process assesses WRC with respect to identified assets independent of any instigating threat or hazard.[19] Various WRC's occupy the concern of the Water, Wastewater, Electricity, Aviation, and Internet subsectors.

Water & Wastewater

Two worst case scenarios specifically concern the drinking water industry: 1) poisoning, and 2) extended service disruption. The first concern stems from the fact that 15% of water utilities service more than 75% of the US population, making it an attractive target. While a valid concern, most experts consider such a possibility highly improbable.[20] The second concern has two components: 1) the ability to procure a safe water source, and 2) the ability to distribute water under appropriate pressure. Even a minor service disruption in a major metropolitan area can cause significant economic damage. A major disruption in a major metropolitan area could have catastrophic economic impact.[21] Whereas disruption to wastewater services could also impact the economy, environment, and public health, such a disruption would be less likely to be considered catastrophic.[22]

Electricity

A primary concern of the electricity subsector is an extended outage across a significant portion of the North American grid. The August 2003 blackout affected 50 million people in the northeastern United States and Canada, causing an estimated $4-$10 billion in economic losses. Though it lasted only a week, the outage resulted in a 0.7% drop in Canada's gross domestic product.[23] A Johns Hopkins study determined that New York City experienced a 122% increase in accidental deaths and 25% increase in disease-related deaths, and that ninety people died as a direct result of the power outage.[24] Project Aurora in 2006, a joint experiment by the Department of Energy and Department of Homeland Security, heightened concern over a large-scale outage by demonstrating how a generator could be remotely commanded over the Internet to physically self-destruct.[25] Physical damage to generators and other critical components on a large scale could result in a prolonged outage as procurement for these components range from months to years.[26]

Aviation

Having already been the instrument of one of the worst catastrophes in US history, the Aviation subsector remains wary of 1) passenger aircraft being targeted en masse, and 2) aircraft again being subverted into guided missiles.[27] In response, the federal government has adopted a layered security strategy to keep terrorists and weapons from boarding aircraft.[28] The reason for increased concern today is that physical security measures are ineffective against cyber intrusion, and that either worst case scenario might be realized by hacking an aircraft's avionics.[29]

Internet

Concerns about the Internet providing an avenue of attack for creating catastrophe may be traced back to the 1996 Commission on Critical Infrastructure Protection.[30] The resulting report is attributed with initiating the post-Cold War concern over critical infrastructure protection. Whereas cybersecurity remains a concern for any device dependent on a computer chip, the more direct concern is the confidentiality, integrity, and availability of the Internet itself. A violation of any of these security conditions at scale would drastically disrupt the Internet and create catastrophe for many critical services that depend on its transport capability.[31] Concerns about breaking the Internet focus on two potential targets: 1) routing services, and 2) Internet Exchange Points.[32] Neither would be easy to break, but doing so would not be impossible.

Risk, Resilience, & Countermeasures

The forty-one Reference Scenarios help guide value estimations for RAMCAP evaluations of risk, resilience, and countermeasures. RAMCAP begins by pairing infrastructure assets against the forty-one threat and hazard scenarios.[33] RAMCAP calculates risk 'R' as the product of consequence, vulnerability, and threat as shown in (1.0).[34] For each threat-asset pair RAMCAP asks: 1) what are the consequence costs of losing this asset to this scenario? 2) what is the probability this asset will be neutralized or destroyed in this scenario? and 3) what is the probability that this asset will experience this scenario?[35] Consequence costs are estimated separately for fatalities, injuries, financial loss to owners, and economic loss to the community. RAMCAP offers conversion tables allowing individual costs to be summed into a single representative value.[36] The maximum value in each table is 13, thus the maximum calculable risk is 52 for any given threat-asset pair with 100% vulnerability and 100% threat occurrence.[37]

$$R = C \times V \times T \qquad (1.0)$$

It would be a simple matter at this point to prioritize threat-asset pairs by their corresponding risk calculation, but the results would be misleading. The RAMCAP risk calculation only accounts for mitigating factors within the owner/operators' control "inside the fence." It does not account for mitigating factors "outside the fence" such as first responders, National Guard, or other capabilities that could further reduce the severity or duration of estimated consequences. This is called "resilience" and must be considered in order to gain a more complete estimate of total risk. Accordingly, resilience 'Rs' amounts to an attenuation of the RAMCAP risk calculation by some mitigating factor percentage as shown in (2.0).[38] The amount of mitigation depends on the scenario, thus estimates are made and resilience calculated for each threat-asset pair.

$$Rs = R \times M \qquad (2.0)$$

It is now reasonable to prioritize threat-asset pairs by their corresponding resilience calculation and evaluate countermeasures to reduce risk among the highest ranks. Countermeasures also amount to an attenuation of risk and may be represented by a mitigating factor 'M-prime' the same as resilience. Risk after applying a countermeasure, 'R-prime' may be calculated as shown in (3.0), and the corresponding resilience, 'Rs-prime' calculated as shown in (3.1). The Gross Benefit (Gb) of implementing a given countermeasure is calculated by taking the

difference in resilience before and after it is applied, as shown in (3.2). The Net Benefit (Nb) is the sum of applying the same countermeasure to all threat-asset pairs (3.3). To select which countermeasure to implement, RAMCAP calculates a Benefit-Cost Ratio (BCR) which divides the Net Benefit by the cost of the countermeasure (3.4). The higher the BCR, the better the return on investment. Of course, the effectiveness and cost of a given countermeasure is greatly affected by the type of scenario.

$$R' = M' \times R \qquad (3.0)$$

$$Rs' = M \times R' \qquad (3.1)$$

$$Gb = Rs - Rs' \qquad (3.2)$$

$$Nb = \Sigma Gb \qquad (3.3)$$

$$BCR = Nb / \$ \qquad (3.4)$$

As can be seen, the Reference Scenarios play an integral role in RAMCAP evaluation of risk, resilience, and countermeasures. The question of whether additional scenarios might be required to account for emerging threats from climate change, aging infrastructure, and cybersecurity could be examined a number of different ways. We chose to examine the question by investigating how these problems are addressed within the current program for critical infrastructure protection.

Critical Infrastructure Protection

Critical infrastructure protection has evolved from the authorities and guidance listed in Table 4. The 2002 Homeland Security Act establishing the Department of Homeland Security prescribes a risk management approach for protecting the nation's critical infrastructure (P.L. 107-296, §201(d)(2)). Accordingly, the 2013 NIPP employs a Risk Management Framework (RMF) to 1) set goals, 2) identify assets, 3) prioritize risk, 4) implement countermeasures, and 5) measure results.[39] The RMF is implemented in voluntary cooperation with industry through Sector Coordinating Councils representing the sixteen infrastructure sectors identified in PPD-21.[40] The Office of Infrastructure Protection (IP) within the DHS National Protection and Programs Directorate (NPPD) is responsible for coordinating RMF implementation across the sixteen sectors and overseeing development of corresponding Sector-Specific Plans (SSPs).[41] Every four years, the Sector-Specific Agency (SSA) federal representative, with support from assigned Coordinating Agencies (CAs), updates the SSP summarizing RMF efforts within their assigned infrastructure sector.[42]

Table 4. CIP Authorities & Guidance

Law	Directives	Strategies	Plans
2002 HSA	1998 PDD-63	2002 NSHS	2005 Interim NIPP
	2003 HSPD-7	2003 CIP Strategy	2005 Draft NIPP
	2013 PPD-21	2007 NSHS	2006 NIPP
		2010 NSS	2009 NIPP
		2015 NSS	**2013 NIPP**

Risk analysis comes into play in Step 3 of the Risk Management Framework. As already mentioned, there are no known implementations of RAMCAP currently employed for RMF risk analysis. However, the Vulnerability Self Assessment Tool employed by the Water and Wastewater sector, is certified by AWWA to be RAMCAP compliant.[43] According to the 2010 SSPs, each lifeline subsector employs a different risk analysis methodology identified in Table 5.

Table 5. Lifeline Infrastructure Risk Analysis Methodologies

Sector/SSP	Subsector	SSA	RA Methodology
Water & WW	Water	EPA	Vulnerability Self Assessment Tool / Security and Environmental Management System
Energy	Electricity	DOE	Site Assistance Visit
Transportation	Aviation	FAA	Aviation Model Risk Assessment
Communications	Internet	DHS	Cyber Assessment Risk Management Approach

Whereas the NIPP/RMF generally addresses all hazards, it does not specifically address climate change, aging infrastructure, or cybersecurity.[44] Climate change and cybersecurity are specifically addressed by executive orders. Aging infrastructure is separately addressed by each subsector.

Climate Change

Issued in October 2009, Executive Order 13514, Federal Leadership in Environmental and Economic Performance, directed all federal agencies to develop a Strategic Sustainability Performance Plan examining, among other things, risk and vulnerabilities stemming from climate change.[45] Executive Order 13653, issued in November 2013, supplemented EO13514 by requiring federal agencies to develop and maintain Agency Adaptation Plans evaluating the most significant climate change-related risks and vulnerabilities.

Aging Infrastructure

With the exception of the Internet, federal regulating agencies have devised programs addressing problems with aging infrastructure in each of their subsectors. In September 2010, the Environmental Protection Agency (EPA) issued a Clean Water and Drinking Water Infrastructure Sustainability Policy to guide investment of State Revolving Funds (SRF) to meet a projected need for $247.5B in water transmission and distribution projects over the next twenty years. [46] In December 2007, President Bush signed into law the Energy Independence and Security Act. Section 1301 established a federal policy to modernize the electric utility transmission and distribution system through research, development, and deployment of Smart Grid technologies.[47] The Smart Grid is a vision for transforming the electric industry from a centralized, producer-controlled network to one that is less centralized and more consumer-interactive.[48] The Department of Energy (DOE) is the lead federal agency responsible for Smart Grid, and has tasked the Federal Energy Regulatory Commission (FERC) with implementing Smart Grid standards developed by the National Institute of Standards and Technology (NIST).[49] Since 2003 the Federal Aviation Administration has been planning

and developing the Next Generation Air Transportation System (NextGen). NextGen[50] is designed to relieve congestion in the Air Traffic Control System, which in 2013 the American Society of Civil Engineers rated a 'D+' in their 2013 Report Card for America's Infrastructure.[51]

Cybersecurity

Issued in February 2013, Executive Order 13636, Improving Critical Infrastructure Cybersecurity, directed NIST to develop a Cybersecurity Framework and tasked federal agencies to evaluate mandating the resulting standards for infrastructure over which they had regulatory authority.[52] In February 2014, NIST released its Framework for Improving Critical Infrastructure Cybersecurity. The Framework is a risk-based approach to managing cybersecurity risk composed of three parts: 1) Framework Core, 2) Implementation Tiers, and 3) Framework Profiles.[53] EPA replied to EO13636 saying there was no need to impose mandatory standards, but that it would work with Water and Wastewater utilities through the DHS Sector Coordinating Council to implement the Cybersecurity Framework as needed.[54] DOE and DHS made similar replies to EO13636 endorsing voluntary cooperation with the Electricity, Aviation, and Internet subsectors. In lieu of the NIST Cybersecurity Framework, DOE recommended continuing with the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), and DHS similarly advocated its own Transportation Sector Working Group (TSWG) Roadmap to Secure Control Systems in the Transportation Sector,[55] and Cyber Assessment Risk Management Approach (CARMA)[56] for the Internet subsector.[57]

Findings

The results of investigating current infrastructure protection programs yielded thirty-eight Candidate Scenarios listed in tables 6-8. Climate Change yielded the most Candidate Scenarios at twenty-seven. These are predicated on adverse incidents similar to the forty-one Reference Scenarios. Most are national in scope, though many are regional, confined to coastal areas. Some are uniquely local, such as melting permafrost in Alaska. One, Geomagnetic Storm, was not identified in any research references, but was considered a sufficient concern to be made a Candidate Scenario. The Climate Change Candidate Scenarios are similar to current RAMCAP Reference Scenarios in that they are predicated on some initiating incident. This is not the case for the Aging Infrastructure and Cybersecurity Candidate Scenarios. Unlike the current Reference Scenarios, they are predicated on progress towards some goal, either a project such as Smart Grid, or a process such as NIST's Cybersecurity Framework. Because the specific threats and hazards are too numerous, these scenarios focus on the vulnerabilities of the asset in question. Though different from current Reference Scenarios, the Candidate Scenarios are still capable of performing in the same capacity of guiding estimations for RAMCAP risk, resilience, and countermeasure evaluations. Table 6 shows the Climate Change Candidate Scenarios, while Table 7 shows the Aging Infrastructure Candidate Scenarios, and Table 8 shows the Cybersecurity Candidate Scenarios.

Table 6. Climate Change Candidate Scenarios

Climate Change (27)

Water & Wastewater

1. Reduced Groundwater Recharge
2. Lower Lake & Reservoir Levels
3. Changes in Seasonal Runoff & Loss of Snowpack
4. Low Flow conditions & Altered Water Quality
5. Saltwater Intrusion into Aquifers
6. Altered Surface Water Quality
7. High Flow Events & Flooding
8. Flooding from Coastal Storm Surges
9. Loss of Coastal Landforms/Wetlands
10. Increased Fire Risk & Altered Vegetation
11. Volume & Temperature Challenges
12. Changes in Agricultural Water Demand
13. Changes in Energy Sector Needs
14. Changes in Energy Needs of Utilities

Electricity

1. Disruption Due to Extreme Weather Events
2. Higher Peak Loads Due to Higher Summer Temperatures
3. Decreased Reliability Due to Climate-Related Regulations
4. Constrained Production Due to Water Availability
5. Disruption Due to Rising Sea Levels
6. Extreme Solar Weather

Aviation

1. Melting Alaskan Permafrost
2. Rising Temperatures and Heat Waves
3. Rising Sea Levels and Storm Surges
4. Extreme Precipitation Events
5. Drought Induced Wildfire

Internet

1. More Severe Storms Due to Rising Temperatures
2. Federal Regulation of Greenhouse Gases

Table 7. Aging Infrastructure Candidate Scenarios

Aging Infrastructure (5)

Water & Wastewater

1. Water Failure Due to Pipe Age & Type
2. Wastewater Failure as Function of Pipe Maintenance and Performance

Electricity

1. Failure as a Function of Progress Towards Smart Grid Implementation

Aviation

1. Failure as a Function of Progress Towards NextGen Implementation

Internet

1. Failure Due to Restricted Capacity of Older Components

Table 8. Cybersecurity Candidate Scenarios

Cybersecurity (6)

Water & Wastewater

1. Cyber Risk as a Function of Process Maturity as Determined by NIST Cybersecurity Framework

Electricity

1. Cyber Risk as a Function of Process Maturity as Determined by NERC Cybersecurity Capability Maturity Model

Aviation

1. Cyber Risk as a Function of Progress Towards TSWG Roadmap Objectives

Internet

1. Breakdown of a Single Interoperable Internet through a Man-made Attack, and Resulting Failure of Governance Policy
2. Large-Scale Man-made Denial-of-Service Attack on the DNS Infrastructure
3. Partial or Complete Loss of Routing Capabilities through a Man-made Deliberate Attack on the Internet Routing Infrastructure

Analysis

We conducted analysis to eliminate redundancies among the Candidate Scenarios. We achieved this by first comparing the thirty-eight Candidate Scenarios against the forty-one Reference Scenarios. We conducted the comparison in stepwise fashion by first determining the Candidate Scenario's class. If the description implied some form of malicious human activity, then it was classified as a threat, otherwise it was classified as a hazard. Next, we determined the Candidate Scenario's subclass by comparing the description to the current subclasses. This was made easier by our previous determination of the Candidate Scenario's class. For instance, if the Candidate Scenario was classified as a "hazard", it only needed to be determined from the description whether the Candidate Scenario best fit the "Natural" or "Dependency/Proximity" subclasses, or neither. If the Candidate Scenario did not fit an existing subclass, then we formulated a new one.. Finally, we attempted to match the Candidate Scenario description with current RAMCAP Reference Scenario Types. If the

Candidate Scenario did not fit an existing type, if there was no match, then we formulated a new scenario type. To preclude an undue proliferation of new subclasses and types, we compared Candidate Scenario descriptions against newly formulated subclasses and types.

Applying the preceding process whittled the thirty-eight Candidate Scenarios down to only thirteen Nominee Scenarios listed in Table 9. Interestingly, Nominee Scenarios #10 and #13 are basically identical, except the process models for #10 are related to hazards (i.e., maintaining capacity), while the process models for #13 are related to threats (i.e., reducing vulnerabilities). Instead of having the same Dependency Subclass as both a hazard and a threat, we decided to create a new Cyber Attack Subclass (CY) under threats. The new Process Maturity Type is inherently different than the Cyber-Insider and Cyber-Outsider Types in the Sabotage Subclass in that the latter encompass the actions of malicious agents, while the former encompasses actions that protect against malicious agents.

The resulting analysis indicates that the current set of RAMCAP Reference Scenarios do not sufficiently account for emerging threats from climate change, aging infrastructure, and cybersecurity. In order to account for these emerging threats to the Water, Wastewater, Electricity, Aviation, and Internet subsectors, RAMCAP should expand its forty-one Reference Scenarios and incorporate the thirteen Nominee Scenarios identified in this study, which are presented in Table 9.

Table 9. RAMCAP Nominee Scenarios

#	Class	Subclass	Type	Identifier
1.	Hazard	Natural	Drought	N(D)
2.	Hazard	Natural	Geomagnetic Storm	N(GS)
3.	Hazard	Natural	Heat Wave	N(HW)
4.	Hazard	Natural	Melting Permafrost	N(MP)
5.	Hazard	Natural	Severe Storms	N(SS)
6.	Hazard	Dependency	Asset Capacity	D(AC)
7.	Hazard	Dependency	Asset Deterioration	D(AD)
8.	Hazard	Dependency	Asset Maintenance	D(AM)
9.	Hazard	Dependency	Governing Regulations	D(GR)
10.	Hazard	Dependency	Process Maturity	D(PM)
11.	Hazard	Dependency	Resource Availability	D(RA)
12.	Hazard	Dependency	Resource Quality	D(RQ)
13.	Threat	Cyber	Process Maturity	CY(PM)

Conclusion

The search for a uniform risk analysis for critical infrastructure protection prompted a look at RAMCAP to see if it accommodated emerging threats from climate change, aging infrastructure, and cybersecurity. RAMCAP uses forty-one Reference Scenarios to help guide estimations of risk, resilience, and countermeasures. The Reference Scenarios help RAMCAP meet NIPP requirements for documentation, reproducibility, defensibility, and completeness. The Reference Scenarios are essential to every step of RAMCAP risk analysis and ultimately determining which countermeasures offer the best Benefit-Cost Ratio on homeland

security investments. We investigated current infrastructure protection practices to identify emerging threats to the Water, Wastewater, Electricity, Aviation, and Internet subsectors. As prescribed by the 2002 Homeland Security Act, the 2013 National Infrastructure Protection Plan employs a Risk Management Framework to systematically identify, prioritize, and mitigate risk across the sixteen sectors identified in PPD-21. Progress is documented every four years in Sector-Specific Plans by federal Sector-Specific Agencies working with industry through Sector Security Councils. Whereas the NIPP/RMF generally addresses all hazards, it does not specifically address climate change, aging infrastructure, or cybersecurity. Climate change and cybersecurity are specifically addressed by executive orders 13514, 13653, and 13636 respectively. Aging infrastructure is separately addressed by various capitalization programs in all but the Internet subsector: Water and Wastewater have the State Revolving Fund; Electricity has Smart Grid; and Aviation has NextGen. Our investigation of current infrastructure protection programs yielded thirty-eight Candidate Scenarios listed in tables 6-8. After comparing against the forty-one Reference Scenarios and eliminating redundancies, we reduced the thirty-eight Candidate Scenarios to thirteen Nominee Scenarios in Table 9. The Climate Change Nominee Scenarios are similar to the current Reference Scenarios in that they are predicated on incidents. The Aging Infrastructure and Cybersecurity Nominee Scenarios are unlike current Reference Scenarios in that they are predicated on progress towards some goal or process. Still, they serve the same purpose as Reference Scenarios by guiding estimations for RAMCAP risk, resilience, and countermeasure evaluations. Thus, this study concludes that RAMCAP, in its current form, does not adequately account for emerging threats from climate change, aging infrastructure, and cybersecurity. Accordingly, this study recommends expanding the forty-one Reference Scenarios to incorporate the thirteen Nominee Scenarios in order to account for emerging threats to the Water, Wastewater, Electricity, Aviation, and the Internet subsectors. Whether or not this will improve RAMCAP performance is a question for Task 2.[58]

About the Authors

Rick White is a Research Assistant Professor at the University of Colorado, Colorado Springs. He is principal investigator for the DHS/S&T RAMCAP Analysis Project. Rick has published textbooks on military strategy, homeland security, and homeland defense. He has a Ph.D. in Security Engineering, Master's Degree in Computer Science, and Bachelor's Degree in History. Rick may be contacted at rwhite2@uccs.edu.

Randy George is a systems manager at US Northern Command and a doctoral student at the University of Colorado, Colorado Springs. Randy is a graduate research assistant on the RAMCAP Analysis Project. Randy has a Master's Degree in Computer Science and a Bachelor's Degree in Computer Science. Randy may be contacted at rgeorge2@uccs.edu.

C. Edward Chow is Professor of Computer Science at the University of Colorado, Colorado Springs. His research focuses on improving the performance, reliability, and security of networked systems. Edward is co-principal investigator on the RAMCAP Analysis Project. He has a Ph.D. in Computer Science, Master's Degree in Computer Science, and a Bachelor's Degree in Electrical Engineering. Edward may be contacted at cchow@uccs.edu.

Terry Boult holds the El Pomar Endowed Chair of Innovation and Security at the University of Colorado, Colorado Springs. He is also co-director of Bachelor of Innovation Programs at UCCS. Terry's research specialty is the design of fast and reliable face recognition algorithms. Terry is co-principal investigator on the RAMCAP Analysis Project. He has a Ph.D. in Computer Science, Master's Degree in Computer Science, and Bachelor's Degree in Applied Mathematics. Terry may be contacted at tboult@vast.uccs.edu.

Acknowledgement

Work funded by the Resilient Systems Division of the Homeland Security Advanced Research Projects Agency. Submitted August 4, 2015.

Notes

1 US Department of Homeland Security, *National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience*, (Washington, DC: , 2013), 17.

2 American Water Works Association, *Risk Analysis and Management for Critical Asset Protection (RAMCAP) Standard for Risk and Resilience Management of Water and Wastewater Systems*, (Washington, DC:, 2010), xiii.

3 *National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience,* 36.

4 Whereas no direct descendant of RAMCAP is known to be in use, both the Vulnerability Self-Assessment Tool (VSAT) and Security Environmental Management System (SEMS) were later made "RAMCAP compliant" based on the AWWA J100-10 standard.

5 *Risk Analysis and Management for Critical Asset Protection (RAMCAP) Standard for Risk and Resilience Management of Water and Wastewater Systems.*

6 Ibid, 1.

7 Ibid, xvii.

8 Ibid, 8

9 *National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience,* 43.

10 Ibid, 4.

11 Ibid, 34.

12 The decision to return to RAMCAP may seem odd given its descent into obscurity. It must be remembered, though, that RAMCAP was the product of the American Society of Mechanical Engineers based on input from more than one hundred industry leaders. No alternatives have such a distinguished pedigree. Thus RAMCAP provided a strong foundation from which to begin this evaluation.

13 *National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience,* 17.

14 Ted G.Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation,* Hoboken, New Jersey: John Wiley & Sons, Inc., 2006, 56-57.

15 US Department of Homeland Security, *Information Technology Sector-Specific Plan,* (Washington, DC, 2010), 7.

16 US Department of Homeland Security, *Communications Sector Specific Plan,* (Washington, DC, 2010), 11.

17 *Risk Analysis and Management for Critical Asset Protection (RAMCAP) Standard for Risk and Resilience Management of Water and Wastewater Systems*, 8.

18 Ibid, 6.

19 Ibid, 9.

20 Claudia Copeland, *Terrorism and Security Issues Facing the Water Infrastructure Sector,* (Washington, DC:Congressional Research Service, 2010), 2.

21 Ibid.

22 Ibid, 4.

23 US-Canada Power System Outage Task Force, *Final Report on the Implementation of Task Force Recommendations,*(Washington DC: U.S. Department of Energy, 2006), 2.

24 Brooke Anderson and Michelle Bell, "Lights Out: Impact of the August 2003 Power Outage on Mortality in New York, NY," *Epidemiology* 23, no. 2 (2012): 189-193.

25 Center for the Study of the Presidency and Congress, *Securing the US Electrical Grid,* (Washington, DC: 2014),21.

26 North American Electric Reliability Corporation, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,* (Washington DC: U.S. Department of Energy, 2010), 12.

27 White House, National Strategy for Aviation Security, (Washington, DC,, 2007), 9-10.

28 Ibid, 18-20.

29 Transportation Sector Working Group, *Roadmap to Secure Control Systems in the Transportation Sector,* (Washington, DC: Department of Homeland Security, 2012), 12.

30 President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures,* (Washington, DC: The White House, 1997), x.

31 US Department of Homeland Security, *Information Technology Sector-Specific Plan,* (Washington, DC, 2010), 25.

32 Ibid, 26.

33 *Risk Analysis and Management for Critical Asset Protection (RAMCAP) Standard for Risk and Resilience Management of Water and Wastewater Systems*, 8.

34 Ibid, 13.

35 Ibid, 9-12.

36 Ibid, 9.

37 Ibid, 36.

38 Ibid, 13-14.

39 US Department of Homeland Security, *National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience,* (Washington, DC 2013), 15.

40 Ibid, 35.

41 US Department of Homeland Security, *Transportation Systems Sector-Specific Plan*, (Washington, DC, 2010), 91.

42 John D. Moteff, *Critical Infrastructures: Background, Policy, and Implementation,* (Washington, DC: Congressional Research Service, 2014), 24.

43 *Risk Analysis and Management for Critical Asset Protection (RAMCAP) Standard for Risk and Resilience Management of Water and Wastewater Systems*, xv.

44 *National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience,* 3.

45 White House, *EO13514: Federal Leadership in Environmental, Energy, and Economic Performance,* (Washington, DC, 2009).

46 US Environmental Protection Agency, *EPA's Clean Water and Drinking Water Infrastructure Sustainability Policy,* (Washington, DC, 2010) ;U.S. Environmental Protection Agency, *Drinking Water Infrastructure Needs Survey and Assessment*, (Washington, DC, 2013), 6.

47 Fred D. Sissine, *Energy Independence and Security Act of 2007: A Summary of Major Provisions*, (Washington, DC: Congressional Research Service, 2008), 22.

48 Litos Strategic Communication, *The Smart Grid: An Introduction,* (Washington, DC: US Department of Energy, 2008), 10.

49 National Institute of Standards and Technology, *NIST Framework and Roadmap for Smart Grid Interoperability Standards*, Release 3.0, (Washington, DC: US Department of Commerce, 2014), 4.

50 Federal Aviation Administration, *NextGen Priorities Joint Implementation Plan,* (Washington, DC: Federal Aviation Administration, 2014), 4.

51 American Society of Civil Engineers, *2013 Report Card for America's Infrastructure,* http://www.infrastructurereportcard.org/a/#p/aviation/overview (accessed May 28, 2015).

52 White House, *EO13636: Improving Critical Infrastructure Cybersecurity*, (Washington DC, 2013).

53 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity,* Washington DC, 2014), 1.

54 U.S. Environmental Protection Agency, *Executive Order 13636, Improving Critical Infrastructure Cybersecurity,* (Washington, DC, 2014).

55 US Department of Energy, *2014 Smart Grid System Report,* (Washington, DC, 2014), 11.

56 Transportation Security Administration, *TSA's Approach to Voluntary Industry Adoption of the NIST Cybersecurity Framework,* (Washington, DC, 2014).

57 US Department of Homeland Security, *DHS Response to the NIST Cybersecurity Framework Request for Information,* (Washington, DC, 2013).

58 To our surprise, Task 2 demonstrated that adding more scenarios to the reference set did not improve RAMCAP performance as measured by the calculated "Net Benefit". For a complete description of the modeling and analysis of RAMCAP, see "Apples to Apples: RAMCAP Revisited", accepted for publication, February 3rd, 2016, by the International Journal for Critical Infrastructure Protection.