

Challenges in Critical Infrastructure Protection

Final Report for the 2006/2007 Sam Nunn Security Program Critical Infrastructure Protection Exercise

2 November 2006

Jan Osburg[†] (jan.osburg@asdl.gatech.edu)

Charles Ume[‡] (charles.ume@me.gatech.edu)

1 Introduction

The 2006/2007 class of fellows of the Sam Nunn Security Program at Georgia Tech was tasked with determining how to best counter natural and man-made threats against the nation's critical infrastructures. The class was divided into eight teams, seven of which analyzed different critical infrastructures and proposed suitable protective measures, with the remaining team compiling the analysis results of the other seven and recommending a consolidated set of measures.

The following critical infrastructures (CIs) were examined as part of this exercise:

- ◆ Civil aviation
- ◆ Border
- ◆ Information and communications technology (ICT)
- ◆ Water management
- ◆ Chemical infrastructure
- ◆ Agriculture
- ◆ Energy

The eighth team, which was referred to as the "National Security Council" (NSC) team, first developed a draft of the evaluation process to be used and communicated it to the CI teams. Then, for each of the CI sectors, the respective teams delivered a 30-minute presentation to the class. Each team also submitted a 12-page paper, containing an overview of the respective infrastructure, the most significant threats facing it, and recommendations of countermeasures addressing those threats. After evaluating the findings of the CI teams, the NSC team presented its preliminary results in a 90-minute discussion with the class, and subsequently generated this final report.

2 Decision-Making Process

The NSC team decision-making process focused on identifying the best countermeasures that addressed the most serious threats to the critical infrastructures. The aim was to strike a balance

[†] Research Engineer II, Georgia Institute of Technology, Atlanta, GA

[‡] Professor, Georgia Institute of Technology, Atlanta, GA

between increased safety and security on one hand, and cost and unintended consequences on the other. This evaluation was based on the input from the CI teams and independent assessment by the NSC team. The following criteria were covered (Figure 1):

- ◆ Likelihood and consequences of a threat
- ◆ Effectiveness of a countermeasure
- ◆ Robustness of a countermeasure
- ◆ Cost of a countermeasure

The effectiveness criterion addressed the direct benefits of a countermeasure, its feasibility, the ease with which it could be circumvented by an opponent, and its complexity. Greater benefits and feasibility were rated as positive, while ease of circumvention and higher complexity were regarded as drawbacks.

Robustness included the flexibility with which a countermeasure could be adapted to changing threats or circumstances, and the broadness of its coverage, i.e. if it addresses a wide range of threats or threat variations. Higher flexibility and broader coverage resulted in a better robustness rating.

For the cost criterion, financial cost, productivity losses, increased wait or transfer times, and

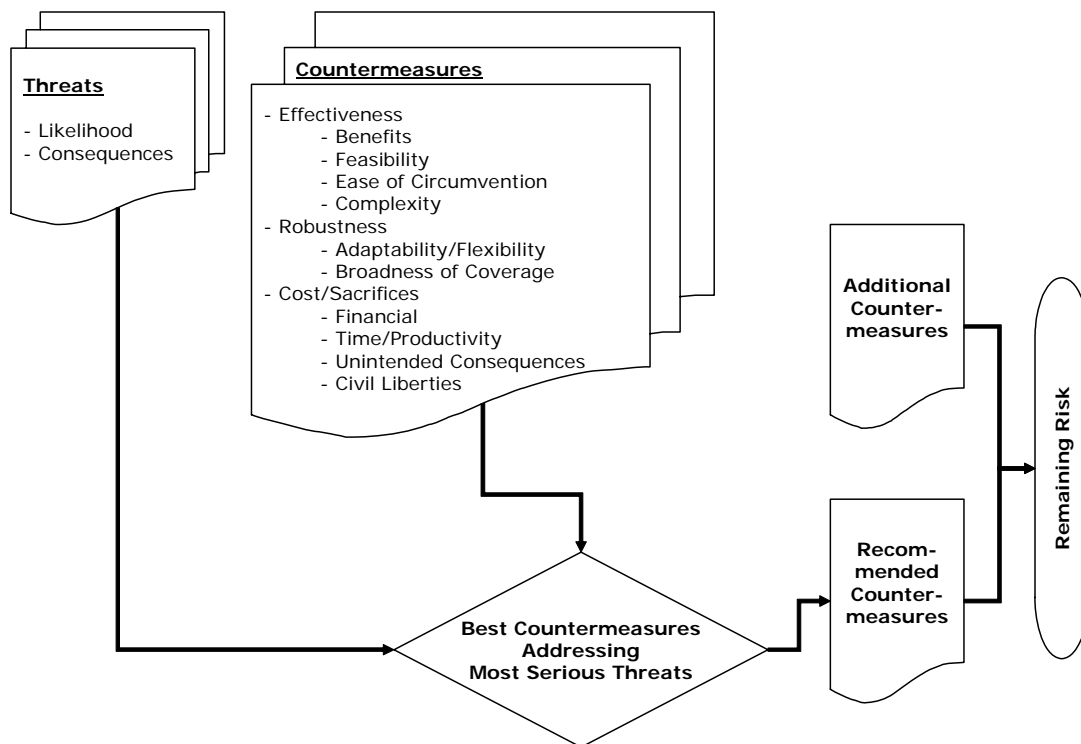


Figure 1: Decision-Making Process

infringements on civil liberties were included. Unintended consequences of a proposed countermeasure were taken into account as well.

For each threat, the NSC team assigned a rating based on a composite of likelihood and consequences. Three rating levels were used: high threat (H), medium threat (M) and low threat (L). Similarly, each proposed countermeasure was rated according to a composite of effectiveness, robustness and cost. Countermeasure rating levels were positive/recommended (+), neutral/conditionally recommended (0), and negative/not recommended (-).

After compiling the final list of recommended countermeasures, the NSC team also generated a set of additional, overarching countermeasures and looked at the remaining overall risk to the nation.

3 Evaluation of Critical Infrastructure Teams Results

The CI teams based their research on a recent report by the National Research Council's Committee on Science and Technology for Countering Terrorism: "Making the Nation Safer: The Role of Science and Technology in Countering Terrorism." [18] Other sources were taken into account as well; they are referenced in the respective CI team reports ([1], [5], [6], [9], [12], [14], [25]).

The following figures show the threats and threat significances as determined by each CI team, and as rated during the NSC team decision-making process (H/M/L symbols, cf. Section 2). They also provide the lists of countermeasures as originally proposed by the CI teams, and the associated NSC team ratings (+/0/- symbols). The figures also illustrate the divergent formats and levels of detail provided by each CI team, which posed a challenge for the evaluation process since most teams did not provide e.g. specific cost and schedule metrics. Due to space constraints, the reader is referred to the original CI team papers for more in-depth information on threats and countermeasures and on the rationales for their inclusion.

Figure 2: Civil Aviation Threats








	Threats	Probability of not intercepting	Cost to America	Risk
	Gun/Grenade attack outside airport	Medium	Low	Medium
	MANPADS attack	Medium	High	High
	Explosives in cargo	High	High	High
	Chemical attack inside aircraft	High	High	High
	High explosives attack inside aircraft	High	High	High
	Liquid explosives attack inside aircraft	High	High	High
	Curbside Car Bomb	High	Medium	High

Figure 3: Civil Aviation Countermeasures

Note: countermeasures that are already implemented were not rated

	Counter Measure	Cost	Delays	Effectiveness
	1 Backscatter X-ray at Entrance	Med	Low	41%
	2 Increased Number of TSA	High	None	38%
	3 Training crew to be adaptive and prepared for unforeseen events	Med	NA	36%
	4 Reducing Congestion through additional security check points	High	None	35%
	5 Profiling Passenger by Autonomous Datamining	High	Low	31%
	6 Backscatter X-ray at Check Points	Low	Med	27%
	7 Increased Number of Federal Marshals	Med	NA	27%
	8 Profiling {of passenger behavior}	Low	Low	27%
	9 Carry-on luggage X-ray	Low	Med	26%
	10 Explosive Residue Testing	High	High	26%
	11 No Fly Lists	Low	Low	25%
	12 Increased Canine units	Med	Low	25%
	13 Increased Canine units {twice?}	Med	Low	25%
	14 Deployment of improved Less-than-lethal weapons	Med	NA	23%
	15 Providing Pilots with handgun	Low	NA	20%
	16 Entrance Metal Detectors	High	High	18%
	17 Entrance Explosive "Sniffers"	High	High	13%
	18 Explosive "Sniffers" {mobile?}	High	Med	13%
	19 Metal Detectors in Security Check Areas	Low	Med	12%
	20 Increasing number of restricted carry-on items	Low	Low	11%
	21 Separate Entrance for Passengers Carrying Weapons (Assuming Metal Detectors at entrances)	Med	Low	10%
	22 Cargo Screening for all Containers	High	High	10%
	23 Checked Luggage Screening	Med	Low	6%
	24 Random Screening	Low	Med	5%
	25 Car Screening			3%
	26 Improved Fire Walls	Low	Na	2%
	27 Outside Terminal Barriers	Low	Low	1%
	28 Random Cargo Screening	Med	Low	1%
	29 Employee Background Checks	Low	NA	1%
	30 Reinforcing Cockpit door	High	NA	1%
	31 Security Cameras and motion in all critical areas of airport	Med	NA	1%

Figure 4: Border Threats










-  → Illegal border crossings
-  → Attack on land border
- Attacks on ships and crews/passengers
-  ✦ Seize control of a ferry or a cruise ship (which can carry large amounts of passengers) and threaten the deaths of passengers if demands are not met
-  ✦ Attack U.S. Navy ships in an attempt to kill U.S. military personnel, damage or destroy a U.S. military asset or cause a radiological release
- Attacks enabled by shipping services
-  ✦ Use of commercial cargo containers to smuggle terrorists, nuclear, chemical or biological weapons, components thereof, or other dangerous materials into the United States
- Attacks using ships as weapons
-  ✦ Seize control of a large commercial cargo ship and use it as a collision weapon for destroying a bridge or waterfront-based refinery
-  ✦ Sink a large commercial cargo ship in a major shipping channel, thereby blocking all traffic to and from the port
-  ✦ Attack an oil tanker in a port or at an offshore discharge facility so as to disrupt the world oil trade and cause large-scale environmental damage
-  ✦ Attack a large ship carrying a volatile fuel (i.e. liquefied natural gas) and detonate the fuel causing a major in-port explosion

Figure 5: Border Countermeasures

















- Land borders:
 -  ✦ Target terrorist funding and travel as suggested in the 911 Commission Report
 -  ✦ Work closely with other governments to prevent the travel and border crossing of illegal persons and goods
 -  ✦ Remove incentives for illegal immigration by implementing a temporary worker program
 -  ✦ Build and install border security infrastructure
 -  ✦ Implement biometric screening systems
 -  ✦ Implement more robust forms of domestic identification
 -  ✦ Link biometric passports to good data systems
 -  ✦ Punish border offenders in a timely and complete manner
 -  ✦ Plan and prepare for possible border attacks
- Maritime borders:
 -  ✦ Make point of origin cargo security a priority
 -  ✦ Engage the international community
 -  ✦ Fund initiatives to develop WMD detection technologies for use at U.S. and foreign ports {and land border ports of entry}
 -  ✦ Fund port security
 -  ✦ Engage private industry's role as a stakeholder in port security
 -  ✦ Continue funding Coast Guard initiatives for maritime security
 -  ✦ Prioritize intelligence sharing

Figure 6: Information and Communications Technology Threats

- Attacks on distributed part of infrastructure
 - ✦ requires little know-how, low-cost (backhoe sufficient)
 - ✦ low/no impact (localized disruption or network self-heals), leaves law enforcement with many clues
 - ✦ examples: cut fiber cable, blow up cell tower
- Attacks on centralized part of infrastructure
 - ✦ requires explosives and infrastructure knowledge, medium-cost
 - ✦ low/medium impact (localized disruption or network fragmentation), many clues
 - ✦ examples: blow up telco central switching station, cut Internet backbone
- Attacks using ICT infrastructure
 - ✦ requires technical expertise, low/zero cost
 - ✦ low-medium impact (service disruptions, typically short), leaves few clues
 - ✦ examples: DoS attacks, viruses, worms, hacking
- Attacks on ICT as amplifier for attacks on non-ICT infrastructure
- ICT as resource for planning attacks and spreading propaganda

Issue	Probability	Consequence	Strategy
Internet DoS	Very High	Low	Response / Recovery
SCADA Takeover	Low	High	Prevention
Classified Information Theft	Medium	Medium/High	Prevention
Distributed Infrastructure	High	Low	Response / Recovery
Centralized Infrastructure	Very Low	Medium	Prevention
Emergency Communications	High	Medium	Prevention
Terrorist Surveillance Failure	High	Medium	Prevention

Figure 7: Information and Communications Technology Countermeasures

- → Eliminate national cyber response coordination group
 - ✦ Increase surge capacity of US-CERT
 - ✦ Federal agencies should have liaisons with US-CERT
- → Promote market solutions by staying uninvolved: eliminate national cyber alert system
- → High-level audit of selected SCADA systems
- → Develop technical EAS solutions for post-convergence landscape: integrate emergency communications with emerging tech
- → Close intelligence/technology gap: fund language translation and data mining tools

Figure 8: Water Management Threats











	System Component	Susceptibility	Impact	Probability
	Age & Deterioration of overall system	Many water systems throughout the nation date to the 19 th century	LOW	HIGH
	Water sources, treatment plants, storage tanks	Very low levels of physical security and insufficient monitoring for contamination	HIGH	HIGH
	Water supply distributions systems	Rarely monitored for contamination Very low levels of physical security	HIGH	HIGH
	Aqueduct structures	Low levels of security or monitoring, systems open for as much as 150 miles	MODERATE	LOW
	Dams	Low levels of security or monitoring	HIGH	LOW
	System treatment chemicals (Cl _{2(g)} , ClH ₂ N, ClO ₂)	Minimal security protecting large stores of treatment chemicals	HIGH	MODERATE
	Supervisory Control and Data Acquisition (SCADA)	Hacking SCADA system through internet or otherwise	MODERATE	LOW
	Sanitary, storm and combined sewers	Subsurface unmonitored systems with easy access	MODERATE to HIGH	HIGH
	Wastewater Treatment Facility	Large areas, sometimes remote, not typically secured by more than a fence	MODERATE to HIGH	HIGH
	Wastewater Pump Stations	Remote and unmanned locations	MODERATE to HIGH	MODERATE

Figure 9: Water Management Countermeasures

- Refocus Monetary Resources
 - ✦ Unrealistic to secure entire water and wastewater infrastructure
 - ✦ Focus on greatest threats
 - ✦ Use current SRFs to enhance security
 - Require all expansions to include monitoring
 - Encourage funds to be used for updates
- Heighten Monitoring
 - ✦ Bring in-line and on-line monitoring to all distribution systems over next 15 years
 - Chlorine level
 - Ph and heat probes
 - Spectral devices (optional but encouraged)
 - ✦ Cost incurred for installation, equipment and upkeep.
- Increase Information Sharing
 - ✦ EPA should work with DHS especially along guidelines of the *2006 National Infrastructure Protection Plan*
 - ✦ Establish channels of communication between various public and private groups
 - ✦ Centralize information resources (e.g. *Wiki Site*)
 - Grant allocation
 - Water quality monitoring systems
 - Personnel training courses
 - Agencies' responsibility outline
 - Relevant links and other resources
- Personnel preparedness and training exercises currently in practice are well funded and should remain an important facet of water security

Figure 10: Chemical Infrastructure Threats
















Threat	Logistics	Terror effect			Other Infrastructures effected						Totals	Total Effect
		death	tactic	Economics	Civil Av.	Water	Border	Energy	AG	Comm.		
Feedstock/product used as a weapon												
 commodity chemicals used as flammables	5	1	1	1	x		x				12	medium
 commodity chemicals used as poisons	4	1	3	1		x	x		x		15	medium
 specialty chemicals as flammables	3	1	1	2	x		x				11	low
 specialty chemicals as poisons	3	1	3	2		x	x		x		15	medium
Feedstock/product used to make a weapon												
 fertilizer as explosive	5	3	2	2	x		x			x	18	high
 developing bioterrorist chemicals	2	2	4	2	x	x	x		x		18	high
 developing WMD	0-1	5	5	5	x	x	x	x	x	x	27	high
Using Transportation of Feedstock/product as a weapon												
 destroying a truck,boat or train w/ flammables	4	1-5	1	1					x		9	low
 destroying a truck,boat or train w/ hazardous chemicals	4	1-5	3	1		x			x		15	medium
 destroying a LNG carrier	4	1	3	3	x		x	x			17	high
 destroying a LNG station	3	5	4	4	x		x	x			22	high
 destroying a pipeline carrying flammables (NG or oil)	3	1-5	4	2	x	x		x			15	medium
Multiple attacks on chemical plants or SCANDA network												
 industry in general	1	2	2	2	x				x		13	medium
 petrochemical industry	3	2	4	4	x	x	x	x		x	23	high
 SCANDA network	2	2	3	3		x		x		x	16	high

Figure 11: Chemical Infrastructure Countermeasures











- Using tools and market incentives to promote safe chemical production and renewable energy to reduce the number and size of attractive targets
 -  ◇ Replacing explosive fertilizers or hazardous solvents with inert alternatives
 -  ◇ Developing chemical process that use non-hazardous feedstocks
 -  ◇ Decentralizing the petrochemical industry and reducing the transporting of fuels
-  → Require all companies to use at least 25% safe chemical processes and 25 % renewable alternative fuels by 2010
- Provide initiatives for research
 -  ◇ List of most hazardous feedstocks/products
 -  ◇ Chemical industry roundtable to determine most dangerous processes
 -  ◇ Government and Industry sponsored grants
 - ◆ Cheaper than in-house research
 -  ◇ Competition for best safe chemical
 - ◆ Winner receives start-up funds, industry pilot plant
 - ◆ University or group receives huge publicity
 -  ◇ Launch "SAFETY STAR"
 - ◆ Building public awareness
 - ◆ Industries are most concerned about customers
-  → Promoting Community Involvement and Education
 - ◇ Environmental regulations are more effective when the community is involved
 - ◇ Knowing what to do in an emergency increases your chances of survival
 - ◇ Reduce cost and impact to emergency response

Figure 12: Agriculture Threats







-  → Spread of exotic disease through global travel & trade
-  → Spread of disease and contamination through modern farming practices
-  → Security breaches at food-related facilities
-  → Poor farm emergency response
-  → Introduction of easy-to-obtain/handle agricultural pathogens
-  → Localized plant and animal disease affecting entire nation

Figure 13: Agriculture Countermeasures














-  → Expand programs to train veterinarians, animal technicians/handlers, and scientists to identify, treat, and study foreign animal disease
-  → Partner with private industry to encourage physical, personnel, and food security measures
-  → Improve coordination between local, state, and federal agencies for agricultural emergency response
-  → Assess ways to improve information sharing between agricultural and intelligence communities
-  → Establish standardized state or federal level programs to compensate farmers for mandatory crop and livestock destruction due to exotic disease or terrorist attack
-  → Support existing and new research focused on animal/crop disease, better methods of carcass disposal, alternatives to mass slaughter
-  → Support existing and new outreach/ educational programs
-  → Increase number and presence of USDA/DHS agricultural inspectors – especially Beagle Brigade and other canine teams – at US points of entry

Figure 14: Energy Threats

	Infrastructures Susceptible to Physical Attacks			Infrastructures Susceptible to Cyber Attacks
	Generation	Transmission	Distribution	Control and Communications
Criticality of Infrastructure	Highly Critical	Highly Critical	Critical	Extremely Critical
Likelihood of Attack	Medium	Medium	Low	High
Consequences of Attack	High	Medium	Low	Extremely High



Figure 15: Energy Countermeasures

	+ 	0 	+ 	+ 	0 
	R1	R2	R3	R4	R5
	Review Regulations	Develop Dynamic Models	Implement MOTES / Sensor Networks	Create E ARPA	Develop & Implement Intelligent SCADA
Cost of Preventative Measure	Low	High	Medium	High	Extremely High
Effectiveness of Preventative Measure	Low	High	Medium	High	High
Likelihood of Unintended Consequences of Preventative Measure	Medium	Medium	Low	Low	Low
Impact of Unintended Consequences of Preventative Measure	Medium	Low	Low	Low	Low

4 Recommended Countermeasures

4.1 Countermeasures Proposed by CI Teams

The evaluation of the risks and countermeasures proposed by the CI teams through the decision-making process outlined in Section 2 resulted in the following set of recommended countermeasures initially proposed by the CI teams:

Civil Aviation

- ◆ Installing backscatter x-ray machines at airport entrances to detect persons carrying weapons and explosives
- ◆ Training flight and cabin crews to be adaptive to potentially threatening situations
- ◆ Reducing congestion at security checkpoints through increasing staffing, streamlining procedures and adding additional lanes
- ◆ Profiling for suspicious passenger behavior at check-in counters and security checkpoints
- ◆ Increasing canine units and using portable sniffers to detect explosives in luggage and on persons
- ◆ Expanding and streamlining the Federal Flight Deck Officer (“armed pilots”) program

Border

- ◆ Improving physical border security (fences, surveillance, response teams)
- ◆ Punishing border offenders in a more timely and thorough manner
- ◆ Prioritizing point-of-origin cargo security through engaging trade partners
- ◆ Funding WMD detection technologies
- ◆ Increasing Coast Guard capabilities
- ◆ Improving intelligence sharing among government agencies and between US and allies

Information and Communication Technology

- ◆ Designating US-CERT as the main response organization for all cyber threats
- ◆ Performing a high-level audit of SCADA systems
- ◆ Developing post-convergence solutions for the emergency alert system
- ◆ Funding automated language translation tools

Water Management

- ◆ Developing and fielding in-line monitoring equipment
- ◆ Refocusing State Revolving Funds on increased security of existing infrastructure (mainly monitoring upgrades), not on general water system expansion
- ◆ Increasing information sharing among water system stakeholders

Chemical Infrastructure

- ◆ Sponsoring roundtables to identify and mitigate the most hazardous chemical products, feed stocks and processes
- ◆ Launching a "Safety Star" consumer safety awareness campaign
- ◆ Promoting community involvement and emergency preparedness education

Agriculture

- ◆ Expanding veterinary training and outreach programs
- ◆ Improving food processing security
- ◆ Improving farmer compensation for crop or livestock destruction
- ◆ Increasing the "Beagle Brigade" at airports

Energy

- ◆ Reviewing regulations that may hinder security improvements
- ◆ Creating an "Energy ARPA" to pursue high-risk high-payoff research and development
- ◆ Improving sensors and networks

4.2 Additional Recommended Countermeasures

While the countermeasures recommended above address specific threats to specific critical infrastructures, a rational approach to threat mitigation and emergency preparedness should also include cross-cutting measures that increase the overall resilience of the nation to a broad spectrum of threats (cf. [18] Ch. 11). The NSC team therefore selected the additional measures listed below due to their predicted relatively low cost and broad impact that will empower communities and citizens to be better prepared for the inevitable next natural or man-made disaster.

General Measures

- ◆ Instituting specific tax breaks for emergency preparedness activities and expenditures (both for businesses and citizens; cf. [8], [30])

- ◆ More actively promoting Citizen Corps programs such as Community Emergency Response Teams [2] and Neighborhood Watch [17], and general preparedness information dissemination ([19], [23])
- ◆ Adding emergency preparedness and related skills to K-12 curricula [28]

Additional Border Protection Measures

- ◆ Increasing investigations and punishment of employers of illegal aliens [3]
- ◆ Encouraging the involvement of border communities (cities, counties, property owners) through instituting tax breaks for property protection measures and mitigating legal liability issues ([20], [27])
- ◆ Reserving government benefits for citizens and legal immigrants/visitors ([10], [15])

Additional Measures for Civil Aviation

- ◆ Subsidizing blast-proof cargo compartments and containers [29]
- ◆ Encouraging passenger awareness and proactive emergency intervention [11]

Additional Information and Communication Technology Measures

- ◆ Promoting the more widespread installation of emergency warning speakers or sirens [7]

Additional Countermeasures for Agriculture

- ◆ Funding research of shelf-stable food and permitting the retail sale of surplus shelf-stable military rations (MREs; [13])
- ◆ Reinstating the national grains reserve [24]

Additional Measures for the Energy Sector

- ◆ Funding additional research of efficient decentralized and emergency power generation ([21], [26])

5 Conclusions

The 2006/2007 Sam Nunn Security Program fellows engaged in a two-phase process to address the most significant threats to the nation's critical infrastructures. The objective was to strike a balance between increased safety and security (through reduced consequences and likelihood of threats), and financial cost, other sacrifices and unintended consequences.

As part of this effort, critical infrastructure protection teams analyzed threats and proposed countermeasures. A "National Security Council" team then compiled the results and, using a qualitative approach, derived an overall set of recommended countermeasures.

5.1 Analyzing Other Critical Infrastructures

In addition to the seven critical infrastructures covered as part of this exercise (cf. Section 3), a recent GAO report lists additional critical infrastructures that warrant similar analysis [4]:

- ◆ Banking and finance
- ◆ Defense industrial base
- ◆ Emergency services (fire, rescue, EMS, law enforcement)
- ◆ Oil and natural gas
- ◆ Continuity of government infrastructure
- ◆ Postal and shipping systems
- ◆ Public health
- ◆ Transportation other than civil aviation (highways, trucks, buses, mass transit, railways, pipelines, ships)

The “Making the Nation Safer” report further mentions areas that go beyond the traditional notion of infrastructure, but the protection of which nevertheless is critical to national prosperity [18]:

- ◆ Cities (Ch. 8)
- ◆ Response of people to terrorism (Ch. 9)
- ◆ Interdependencies among systems (Ch. 10)

Assessing threats and countermeasures for these areas would certainly result in additional recommendations.

5.2 Assessing Remaining Risk

In spite of any countermeasures, it can be assumed that dedicated adversaries will find a way to strike at our society and cause significant temporary disruption. A constitutional republic facilitates attacks by individuals or small groups by enabling the free and mostly anonymous movement of people, goods and information, and by limitations on government powers. The United States’ wealth and power create envy and resentment, which in turn may motivate attackers. In addition, our society’s lifestyle depends on a complex web of interconnected systems, which can be easy to interrupt.

However, these same features – freedom, openness, wealth and power – have also created an unprecedented level of technological capabilities and material assets that provide for a rapid and effective response to crises. Likewise, a large number of citizens are able and willing to take care of themselves, help others, and protect a system of government that has worked well for over two centuries.

In order to maximize robust and cost-effective mitigation and response, while obvious major threats should be addressed directly, additional cross-cutting efforts are needed to address the plethora of unlikely or minor threats that can nevertheless come to pass. Such measures could include general preventive activities like intelligence gathering, and expansion of some of the general-purpose additional measures recommended above (Section 4.2).

5.3 Next Steps

The effort described in this paper encompassed an initial attempt at identifying relevant threats and proposing related countermeasures for the seven critical infrastructures covered by this activity. To complete the set of recommendations outlined above, additional research is needed to analyze threats and countermeasures for those critical infrastructures that were not covered as part of this effort (cf. Section 5.1). In addition, a quantitative assessment of the metrics for threats and countermeasures (cf. Section 2) would enhance the decision-making process described in this report.

6 References

- [1] Balestrini, Santiago; Talley, Diana: "Protecting the Civil Aviation Infrastructure". Sam Nunn School of International Affairs, Georgia Tech, Atlanta, GA, October 2006.
- [2] "Community Emergency Response Teams (CERT)" website. URL: <http://www.citizencorps.gov/cert/>
- [3] "Companies Using Illegal Workers to be Targeted". CNN website, April 2006. URL: <http://www.cnn.com/2006/LAW/04/20/immigration.raids/index.html>
- [4] "Critical Infrastructure Protection – Improving Information Sharing with Infrastructure Sectors". Government Accountability Office report GAO-04-780, July 2004. URL: <http://www.gao.gov/new.items/d04780.pdf>
- [5] Dickherber, Tony; Hill, Elizabeth: "Critical Infrastructure Protection – Water Supply and Waste Water". Sam Nunn School of International Affairs, Georgia Tech, Atlanta, GA, October 2006.
- [6] Draucker, Laura; Klein, Kevin: "Protecting the Chemical Infrastructure". Sam Nunn School of International Affairs, Georgia Tech, Atlanta, GA, October 2006.
- [7] "Federal Warning Systems Modulator Omnidirectional Electronic Siren Series" website. URL: <http://www.federalwarningsystems.com/products.php?prodid=2>
- [8] "Governor Bush Approves 2006 Hurricane Sales Tax Holiday". Press release, 2006. URL: http://www.floridadisaster.org/eoc/eoc_Activations/Wilma05/Reports/GOVERNOR%20BUSH%20APPROVES.pdf
- [9] King, Jeffrey; LaRosa, Chris: "Protecting the ICT Infrastructure". Sam Nunn School of International Affairs, Georgia Tech, Atlanta, GA, October 2006.
- [10] Martin, Philip: "Proposition 187 in California". *International Migration Review*, Vol. 29, No. 1, Special Issue: Diversity and Comparability: International Migrants in Host Countries on Four Continents (Spring, 1995), pp. 255-263. URL: [http://links.jstor.org/sici?sici=0197-9183\(199521\)29%3A1%3C255%3AP1IC%3E2.0.CO%3B2-N](http://links.jstor.org/sici?sici=0197-9183(199521)29%3A1%3C255%3AP1IC%3E2.0.CO%3B2-N)
- [11] McKinnon, Dan: "Safe Air Travel Companion". McGraw-Hill Professional, New York, NY. ISBN 0071399186. 2002. URL: <http://books.mcgraw-hill.com/getbook.php?isbn=0071399186>
- [12] McMichael, Jim; Schmitt, Danika: "Protecting the Energy Infrastructure". Sam Nunn School of International Affairs, Georgia Tech, Atlanta, GA, October 2006.
- [13] "Meal, Ready-to-Eat (MRE)" website. Defense Logistics Agency. URL: <http://www.dscp.dla.mil/subs/rations/programs/mre/mreabt.asp>

- [14] Melonakos, John; Shannon, Michael: "Securing America's Borders – The Key to National Security". Sam Nunn School of International Affairs, Georgia Tech, Atlanta, GA, October 2006.
- [15] "More In-State Tuition for Illegal Immigrants". CNN website, May 2003. URL: <http://www.cnn.com/2003/EDUCATION/05/22/immigrant.tuition.ap/>
- [16] National Infrastructure Advisory Council (NIAC) Homepage. URL: http://www.dhs.gov/xprevprot/committees/editorial_0353.shtm
- [17] "National Neighborhood Watch Program" website. URL: <http://www.usaonwatch.org/>
- [18] National Research Council Committee on Science and Technology for Countering Terrorism: "Making the Nation Safer: The Role of Science and Technology in Countering Terrorism." National Academies Press, ISBN: 0-309-55781-X, 2002. URL: <http://www.nap.edu/catalog/10415.html>
- [19] "pandemicflu.gov" website. URL: <http://www.pandemicflu.gov>
- [20] Pollack, Andrew: "2 Illegal Immigrants Win Arizona Ranch in Court". The New York Times, New York, NY, August 2005. URL: <http://www.nytimes.com/2005/08/19/national/19ranch.html?ei=5088&en=d9c3a3d54e97d931&ex=1282104000&partner=rssnyt&emc=rs&pagewanted=all>
- [21] "Power Anywhere" website. Sky Built Power, 2006. URL: <http://www.skybuilt.com/>
- [22] "Presidential Decision Directive/NSC-63 (PDD-63) Critical Infrastructure Protection". The White House, 1998, URL: <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>
- [23] "ready.gov" website. URL: <http://www.ready.gov>
- [24] Schnittker, John: "Action Proposal: Grain Reserves-Now". *Foreign Policy*, No. 20, 1975. URL:
- [25] Shehan, Erika: "Protecting American Agriculture". Sam Nunn School of International Affairs, Georgia Tech, Atlanta, GA, October 2006.
- [26] "Suntile Residential: Attractive, High-Efficiency Solar Panels Blend Invisibly Into Rooftops". Website, PowerLight, Inc., Berkeley, CA, 2006. URL: <http://www.powerlight.com/products/suntile.php>
- [27] Tarone, L.A.: "Suit Challenges Illegals Crackdown". Standard-Speaker, Hazelton, PA, October 2006. URL: http://www.standardspeaker.com/index.php?option=com_content&task=view&id=3363&Itemid=2
- [28] "Team SAFE-T – Emergency Preparedness Program for Schools K-12" website. URL: <http://www.teamsafe-t.org/>
- [29] "Telair International Delivers First "Blast-Resistant" Aircraft Baggage Containers". Press release, September 2002. URL: <http://www.telair.com/02-01News/02Sept19.html>
- [30] Tran, Van: "Tax-Free Disaster Preparedness". Press release, California State Assembly Republican Caucus Website, April 2006. URL: <http://republican.assembly.ca.gov/members/index.asp?Dist=68&Lang=1&Body=OpinionEditorials&RefID=1448>