CRITICAL TRANSPORTATION INFRASTRUCTURE AND SOCIETAL RESILIENCE

A Report by the Center for National Policy

Stephen E. Flynn, Ph.D
Sean P. Burke, JD

Center for National Policy
CNP

CRITICAL TRANSPORTATION INFRASTRUCTURE AND SOCIETAL RESILIENCE

Stephen E. Flynn, Ph.D
Sean P. Burke, JD

March 2012
Center for National Policy

CONTENTS

I. Introduction 1

II. A Counterterrorism Imperative 5

III. Return on Investment 8

IV. Intermodal Transportation System & Supply Chain Security vs. Resiliency 10

V. The Broader Case for Building Infrastructure Resilience 26

VI. A Unifying Imperative 35

VII. Acknowledgements 36

VIII. About the Authors 37

IX. About the Center for National Policy 38

X. Notes 39

I. Introduction

The key to assuring security, safety and prosperity in the 21st Century will be possessing resilience in face of chronic and catastrophic risks. The years ahead will be marked by turbulence, fueled by unconventional conflict, likely changes in climate, and the sheer complexity and interdependencies of modern systems and networks. This places a premium on assuring that individuals, communities, and critical infrastructure have the capacity to withstand, respond, rapidly recover, and adapt to man-made and natural disturbances.

Building resilience requires a broad and sustained engagement of citizens, companies, and communities. For individuals and families, it requires a commitment to a greater degree of self-reliance. At the neighborhood and community level, it requires civic engagement and volunteerism. Businesses must recognize that their ability to operate in good times as well as bad is dependent on the capabilities of the communities that host them. Thus, close collaboration between the private and public sector becomes essential to the success of both.

Resilience building requires creating capabilities from the bottom-up. Concrete policy actions must be shaped by stakeholders from the private and public sectors, drawn primarily from outside the usual Washington, DC policy circles. This will require both a shift in approach and emphasis to the post-9/11 homeland response. The civilian population and private sector will need to be enlisted as full partners in strengthening societal and infrastructure resilience. This effort must be extended beyond the task of

detecting and intercepting terrorists in advance of an attack. In the aftermath of the attacks of September 11, 2001, too little time and energy was assigned to the elements of homeland security most relevant to *resilience—protection*, *response*, and *recovery*. It was largely only due to pressure from Congress that DHS started to pay real attention to critical infrastructure protection. It was not until 2006 that the first "National Infrastructure Protection Plan" was issued – and the plan only established a process for setting priorities and provided a suggested action plan for protection activities.

When President Barack Obama came into office, he made a commitment to recraft the homeland security mission in important ways. First was to explicitly incorporate homeland security into national security; second, to broaden the focus of the homeland security mission to include natural and man-made disasters; and third to identify resilience as strategic element of homeland and national security.

One outcome of broadening the homeland security mission to include natural disasters and placing greater emphasis on resilience is that it has begun the process of recalibrating public expectations about the inherent limits of preventing all catastrophic risks, including the risk of terrorism. The U.S. government is powerless when it comes to preventing a hurricane, earthquake, or tornado. However, American society possesses the means to mitigate the consequences of these events, recover quickly, and adapt. In other words, the actions that are necessary to deal with natural disasters can also support building the kind of resilience that will make man-made threats far less consequential. By

including natural disasters and other catastrophic risks, homeland security generally, and resilience specifically, becomes much more relevant to communities and companies.

To overlook the resilience imperative is to put in peril the future prosperity of the nation. When critical systems such as transportation and logistics do not have the robustness and nimbleness to recover, they present attractive targets for those who are intent on inflicting harm. This is because it offers America's current and potential adversaries a big potential destructive and disruptive bang for their buck. Furthermore, vulnerable systems amplify the deadly and costly consequences that can be wrought by natural disasters. Companies striving to be grow strong and prosperous and then remain so, don't stay in societies that are easy to knock down and slow to get up. These companies know that if they are a part of a supply chain or depend on one that lacks resilient elements, they will wither and die. So they move to safer harbors that can better assure business continuity. And people with the means to do so, will generally select to live in places that demonstrate a capacity to cope with chronic disruptions.

Given the benefits of resilience—and the direct and indirect risks associated with fragile communities and systems—it is very much in the interest of Americans to embrace it. This will require developing policies and incentives that encourage community resilience at the local level, and within and across networks and infrastructure sectors such as transportation at all levels. It also requires acknowledging that safety and security efforts that aim to eliminate risks will always reach a point of diminishing returns. In most cases,

a more prudent and realistic investment is to manage risks by building the skills and capabilities to do three things: (1) maintain continuity of function in the face of chronic disturbances, (2) develop the means for graceful degradation of function when placed under severe stress, and (3) sustain the ability to quickly recover to a desired level of functionality when extreme events overwhelm mitigation measures.

An emphasis on resilience provides a compelling rationale for greater levels of cooperation and collaboration between the public and private sectors. When it comes to assuring the continuity of operations for essential systems and networks, the users, designers, operators, managers, and regulators all have a shared interest in infrastructure resilience and each has an important role to play. There should be no higher priority than engaging and integrating the multiplicity of parties into a common effort that ensures that society's critical foundations such as transportation are resilient.

The simple fact is that there never will be enough professionals at the right place at the right time when terrorists or disasters strike. The United States has vast transportation networks that operate at the local, state, regional, continental, and global levels. Intelligence and technologies are fallible and Mother Nature cannot be deterred. As appealing as it might be to leave security and emergency preparedness and response to professionals, when it comes to detecting and intercepting terrorist activities or dealing with a catastrophic natural event, the first preventers and first responders will almost always be civilians and system operators who by circumstance find themselves unwitting targets of terrorists or in the path of a disaster when it strikes.

II. A Counterterrorism Imperative

The tactical and strategic value of emphasizing resilience as a counterterrorism imperative has been reinforced by a report on "Assessing the Terrorist Threat" that was released on September 10, 2010 by the National Security Preparedness Group. The report highlights how the diversifying nature of the terrorist threat has been motivated in part by a growing recognition by al Qaeda and associated organizations that terrorist attacks on the West and especially the United States do not have to be spectacular or catastrophic to be effective. As the attempted bombing of Northwest Airlines Flight Number 563 on Christmas Day 2009 dramatically illustrated, even near-miss attacks can generate considerable political fallout and a rush to impose expensive and economically disruptive new protective measures. Since relatively small and unsophisticated attacks have the potential to generate such a big-bang for a relatively small investment, the bar can be lowered for recruiting terrorist operatives, including those who belong to the targeted societies.

A succession of recent cases that have come to light within the United States and elsewhere in the West has highlighted that terrorist radicalization and recruitment is indeed growing. The process of training is being facilitated by an increasing diverse array of global bases from which terrorist groups are operating. There seems no longer any clear profile of a terrorist. Moreover, the means through which many of these persons have been radicalized over the Internet, suggests that the ranks will continue to be filled by those who are drawn to radical causes from the privacy of their own homes. Among

the newest operatives drawn from Western countries, the only common denominator appears to be a new found hatred for their native or adopted country; a degree of dangerous malleability; and a religious fervor justifying or legitimizing violence that impels these very impressionable and perhaps easily influenced individuals towards potentially highly lethal acts of violence.

The diversity of this array of recent terrorist recruits presents new challenges for intelligence and law enforcement agencies that are already over-stressed and inundated with information and leads, to run these new threats to ground. Sophisticated attacks such as those carried out on New York and Washington on September 11, 2001 require a larger group of operatives, communications with those overseeing the planning, and time to conduct surveillance and rehearse the attack. Money, identification documents, safe-houses for operatives, and other logistical needs have to be supported. All this effort ends up creating opportunities for detection and interception by intelligence and law enforcement officials.

Less sophisticated attacks on the other hand, particularly those being conducted by homegrown operatives and lone wolves are almost impossible to prevent. In the May 2010 bombing attempt on Times Square it was a sidewalk T-shirt vendor, not the NYPD patrolman sitting in a squad car directly across the street, who sounded the alarm about Faisal Shahzad's explosive-laden SUV. Shahzad was not in any federal or NYPD database that identified him as a suspected terrorist.

The October 2010 air cargo incident involving explosives hidden in ink cartridges shipped from Yemen is consistent with this trend towards smaller attacks, but with the added element of aspiring to create significant economic disruption. The would-be bombers had no way of knowing that the cartridges would end up on a commercial airliner with hundreds of passengers or a dedicated air cargo carrier with a small crew. That was not important since they understood that destroying any plane in midair would trigger U.S. officials and others to undertake an extremely costly and profoundly disruptive response that would undermine the movement of global air cargo.

Given that smaller-scale terrorist attacks are being motivated because they are harder to prevent and can yield a response by the targeted society that is extremely harmful to that society, it follows that there is tactical and strategic value from investing in the means to sustain critical functions and better respond to and rapidly recover from attacks when they occur. If attacks have limited potential to disrupt in any meaningful way critical infrastructure and networks such as transportation systems that support the movement of people and the flow of supply chains, those attacks become less attractive to carry out. In other words, when the United States demonstrates that it has the ability to withstand attacks without inflicting damage on the essential systems that underpin our economy and way of life, terrorism becomes a less attractive weapon for America's adversaries. Alternatively, a lack of resilience that results in unnecessary loss of life, destruction of property, and disruption of key networks and functions is reckless. It is also a strategic vulnerability in an era when non-state actors will continue to elect to wage their battles in the civil and economic space rather than the conventional military space.

III. Return on Investment

Most natural disasters and large-scale accidents are far more routine than people are generally willing to acknowledge. Individuals, community, and corporate leaders often convince themselves that disasters reside in the realm of chance and fate. But the reality is that the risk of disaster is generally predictable. In addition, the overwhelming costs associated with disasters are almost always associated with failures to prepare for them upfront. Losses and damages rise exponentially when risk mitigation measures that assure adequate robustness are not in place, when responses to disasters are poorly planned and executed, and when efforts to speed recovery and implement changes based on lessons learned receive too little attention.

Accordingly, while the danger that disasters will occur is inescapable, boosting resilience will always provide a positive return on investment. On a micro scale, it is far more cost effective to make an upfront investment in safeguards that mitigate risk and consequences, than to pay the price for response and recovery after a foreseeable hazard manifests itself. To illustrate this point, one need look no further than the *Deepwater Horizon* disaster in the Gulf of Mexico in 2010 where inadequate attention to preventative measures and lack of planning for dealing with the aftermath of what was widely viewed as a low probability event ended up leading to a massive ecological disaster and a significant disruption of the offshore drilling industry. The failure of the crucial emergency vents at the Fukushima Daiichi nuclear facility following the March

2011 earthquake and tsunami provides another compelling example. The hydrogen explosions that occurred after the loss of power rendered the vents inoperable triggered not just a local nuclear disaster. It also caused cascading consequences to international transportation networks, global supply chains, and the worldwide investment into new nuclear power plants.

From a macro standpoint, a society's level of resilience will increasingly be a source of its global competitiveness. The one thing that can be safely predicted with confidence is that the 21st century will be marked by major disruptions arising from man-made and natural threats. There is the risk of terrorist attacks, pandemics, earthquakes and volcanoes, and more frequent and destructive storms associated with climate change. In addition, as the world witnessed with the near meltdown of global financial markets in the fall of 2008 and the Japanese earthquake and tsunami in 2011, with increasingly complex and interdependent networks supporting modern global economic activity, problems in one part of the system can quickly have cascading consequences across the entire system. The countries, communities, and systems that are most able to manage these risks and bounce back quickly will be the places where people will want to live, work, and invest. Those that are so brittle that they break instead of bend in the face of familiar and emerging risks will become the national and global backwaters.

IV. Intermodal Transportation System & Supply Chain Security vs. Resilience

When resilience is the overarching strategic imperative, it generates a different assessment of risk, and highlights a wider range of solutions for dealing with that risk. Comparing the current assumptions and policy prescriptions associated with transportation security on the one hand, with the assumptions and optimal policy prescriptions for advancing transportation and supply chain resilience on the other, makes the case. Simply put, the security focus with respect to transportation and cargo can be boiled down to two concerns: (1) how transportation and logistics system might be used as a conduit for smuggling dangerous people and weapons, and (2) how planes, trains, and other conveyances might be targeted to kill and injure passengers, operators, and bystanders. Alternatively, resilience places an emphasis on the core function of transportation; i.e., to provide the mobility our economy and society requires in order to function and prosper. In other words, those who have been looking through a security lens have been largely seeing transportation as something a terrorist might exploit so as to endanger the lives of people. But when we shift to adopting a resilience lens, our focus ends up centering on the fact that transportation is a critical infrastructure whose continuity must be assured in the face of potential threats that would disrupt it.

In the immediate aftermath of the 9/11 attacks, the transportation security response was to ground aviation and divert international flights from U.S. airspace. Maritime traffic into New York and other seaports was halted, and many of the land border crossings were

effectively closed due to the intensive vehicle inspection process immediately put in place. The effect was akin to a self-imposed embargo on the U.S. economy.[1]

There was a straightforward reason for the decision by Washington to throw the equivalent of a transportation "kill-switch" after the 9/11 attacks. Faced with tremendous uncertainty about the nature of the threat and possessing little confidence in the pre-9/11 checks that inspectors routinely used to screen passengers and cargo, the White House had few options. The hijacked passenger airliners were proof-positive that the passenger-screening process had failed and immediately placed that process along with inspection protocols for other transportation conveyances under scrutiny. Those operations and protocols did not hold up to critical review. As a consequence, new requirements were rushed into place, especially at airports, that were costly and disruptive. The added expense in time and resources associated with these new mandates was justified by the assertion that facilitating trade and travel must be "balanced" with the imperative of security.

On its face, the contention seems compelling that there is an inherent tension between advancing the requirements of security and advancing reliable and affordable mobility. Prior to 9/11, the security imperative was largely overlooked, so the scales presumably need to now be tipped in the direction of protecting the transportation system and its users from threats. But advancing both security and the functionality of transportation can and should be complementary. Since an act of sabotage on transportation infrastructure

can mechanically undermine the function of a transportation system and dissuade people from using it, providing adequate security is clearly supportive of the goal of safeguarding the continuity of the mobility. But jeopardizing the purpose of transportation so as to better protect it makes no sense. When a threat to transportation infrastructure leads officials to take actions that are costly and disruptive, it can have the unintended consequence of actually elevating the security threat. This is because the goal of terrorism is to cause a reaction that is harmful to the targeted society. If every terrorist act or near-miss leads to new government measures that make transportation systems more inefficient, then an adversary gets a much bigger dividend than the actual attack could deliver. This fuels the incentive to carry out more of these attacks in the future. In other words, national security and homeland security are ultimately best advanced when primacy is assigned to safeguarding the important service that transportation infrastructure provides should it be attacked or exploited. The emphasis on resilience necessarily incorporates appropriate protection measures, but it does so in order to minimize the risk of disruption. The more resilient transportation systems become, the greater will be the deterrent for an adversary to target those systems.

There are significant policy implications associated with making transportation infrastructure resilience a strategic imperative. To begin with, it should compel a critical examination of current transportation security efforts, centered on three questions: First, are the protective measures unduly disruptive to the function being protected? An extreme example of this would be prohibiting all vehicles from using a bridge in order to

protect the bridge from a potential act of sabotage. Second, will the protective measures be seen as credible following a major breach of security; i.e., will they survive a "morning-after-test" and be judged as reasonable safeguards given what we know about threat, vulnerability, and consequence. Or will they be assessed to be largely cosmetic, ill conceived, or woefully inadequate, leading the public to believe that the risks associated with using the system might outweigh its benefits? Third, should prevention and protection measures fail, are there adequate plans in place to rapidly respond and recover transportation systems in the aftermath of a major security incident?

An objective assessment of the current cargo security measures for the intermodal transportation system leads to three sobering conclusions. First, if these security measures were being fully implemented in strict accordance with current official agency protocols or as the law requires,* global supply chains would face considerable risk of disruption. Second, if put to the test, these measures will not survive the post-mortem assessment of their effectiveness. The public will be justifiably outraged that U.S. officials oversold the limited steps they have been taking while downplaying the ongoing vulnerability of the cargo system to being exploited and targeted by a determined adversary. The resultant collapse in public trust and recriminations will create a toxic political environment that could result in freezing portions or all of the intermodal transportation system until new measures are devised and implemented. Finally, the U.S. government and the other major trade nations still have no plan to respond and recover from a major security incident involving the global intermodal transportation system. As

* The position that Customs Border and Protection (CBP) has taken since the passage of the 2007 9/11 Recommendations Act is to publicly oppose and take little to no action to meet the Act's legislated mandate to have the contents of all U.S.-inbound cargo containers subjected to non-intrusive inspection technology at overseas ports.

a result, there could be a weeks-long period where the international system of trade and logistics grind to a halt with devastating consequences for the global economy.

1. The disruptive risk of the current cargo security regime

The U.S. government's cargo security measures that were put in place after the attacks of September 11, 2001, have had as their primary aim to more effectively police the intermodal transportation system for suspicious cargo. Customs and Border Protection (CBP) has been the lead agency in developing these measures. The U.S. Coast Guard, the Domestic Nuclear Detection Office (DNDO), and the Department of Energy have also been playing an important support role. The underlying approach depends on CBP's ability to assess risk and target containerized cargo for inspection. If a container is determined to pose a higher risk for potential smuggling, it is subjected to closer scrutiny by customs inspectors. If it is deemed to be a low risk, it is allowed to move through the global logistics system with little or no intervention by government officials.

The process for determining risk begins with an analysis of the cargo manifest and other commercial data provided by transportation providers, importers, and companies involved with logistics. The ocean carrier drawing on information it receives from a shipper provides cargo manifest information to CBP at least 24 hours in advance of a shipment being loaded for transport to the United States. Since the container is sealed, neither the marine terminal where the container is stored in advance of loading, nor the

ocean carrier is in position to confirm the veracity of the declarations it receives from its customers. Essentially, it is an honor system.

CBP analyzes the data it receives using rules-based software to identify containers that are at risk of tampering by terrorists. If software triggers an alert, the agency can access a variety of databases to get an impressive array of additional information to help determine whether the contents of a container should be subjected to closer scrutiny. However, except in very rare instances when there is specific intelligence, the software that sounds the alert relies on the truthfulness of the data originally provided by an importer and ocean carrier. This is problematic given that historically, cargo manifest and trade data have been notoriously incomplete and inaccurate.

After the September 11 attacks, CBP instituted the Container Security Initiative (CSI) in 58 ports around the world. Under the CSI protocol, U.S. customs inspectors partner with their overseas counterparts on conducting these examinations using non-intrusive inspection (NII) technology to scan the contents of cargo containers for radiation and to create an x-ray or similar image of what is inside. If these examinations cannot be completed overseas, they are typically undertaken once they arrive at a U.S. port. But this is less desirable from a security standpoint because both the ship and the arriving U.S. port could be placed in jeopardy if the container indeed has a weapon and that weapon is detonated prior to the U.S.-based inspection.

If CBP strictly complied with it own protocol, virtually all U.S.-bound containers determined to present a high risk and warranting an inspection, would have that inspection done at the port of loading. But this rarely happens. Instead, the overwhelming majority of containers that CBP determines to pose a risk are inspected *after* they arrive in a U.S. port. According to congressional testimony provided by a senior CBP official on February 7, 2012, a total of 45,500 containers were examined in the 58 CSI ports in 2011. This represents 0.5% of the 9.5 million manifests CBP reviewed in advance of overseas loading. When 45,500 is divided by the 58 CSI ports and 365 days per year, the result is CSI inspectors are examining with their foreign counterparts on average, just 2.15 containers per loading port per day.[2]

There are practical problems associated with implementing the official protocol of using non-intrusive inspection technology to scan U.S.-bound cargo containers that are targeted as high risk. Cargo containers are typically pre-positioned a few days before shipment in a container yard at a marine terminal in stacks of up to six. If a container is selected for inspection after CBP receives cargo manifest data 24-hours before loading as the agency requires, the container must be located, removed from the stack, and transported to an inspection facility. Performing this labor intensive process often results in the container missing its voyage even if its contents were deemed to be legitimate. This is because the container typically cannot be brought back from the inspection facility with sufficient time to be placed aboard the ship in accordance with a carefully devised loading plan.

According to a simulation conducted by the Wharton Risk Management and Decision Process Center at the University of Pennsylvania, no more than 3 percent of U.S. outbound cargo could be inspected using the CSI protocol at a large marine terminal in South China, without generating a significant backlog. The simulation assumed that local inspectors and cargo scanning equipment would be available to examine U.S.-bound cargo 24-hours per day, 7 days per week. Even under this unlikely circumstance, within 30 days of trying to inspect just 5 percent of U.S. outbound cargo, the accumulated backlog of containers waiting to be examined would fill 2.9 acres, with containers stacked three high. At a 20-percent inspection rate, the backup would fill 31.4 acres.[3] The requirement to inspect more than 3 percent of U.S-bound cargo would not be unrealistic, particularly in the event of an elevated alert level following a terrorist incident or based on intelligence warnings of a likely threat originated from or transiting through a major seaport. In short, CBP's current CSI protocol presents a significant disruptive risk to supply chains. The reason why that risk has not been apparent to date is only because CBP has quietly avoided executing the protocol. This practice exposes the intermodal transportation system to an even greater disruptive risk—the near certainty that container security practices will fail the "morning-after-test."

2. Failing the "Morning After Test"

The test of any security measure is how well it survives an attempt to breach it. Even if it does not successfully foil a determined adversary, it can stilled be judged to be a reasonable

safeguard based on the available information about the threat and the anticipated consequences. But in some instances, bureaucracies succumb to the temptation to adopt cosmetic measures that they believe will reassure an anxious public, even though they know the measures are likely to prove ineffective in stopping or deterring the anticipated threat. For instance, following the detonation by a suicide bomber of a panel-truck full of explosives in a crowded area, having cement barriers placed outside of train stations would likely be reassuring to daily commuters. But if the barriers were not anchored to the ground, which is a costly and time-consuming process, a terrorist at the wheel of an explosive-laden truck would be able to push them aside and drive up to or through the station's entrance. In the aftermath of such a scenario, families of the victims would be rightfully outraged that security officials who should have known better, deployed the barriers without ensuring those barriers could actually stop a truck.

As a stopgap, a case can sometimes be made for taking actions that are more about appearance than substance, given that perceptions play a role in how people—and adversaries--think about risk. But in the end, providing security is a core function of government and preserving public trust is essential to government legitimacy. While the secrecy that surrounds security can help shield an agency from critical review in advance of an incident, after an attack there will be a day of reckoning. If the public concludes that they were deceived into complacency by officials who were aware of the danger but only went through the motions of addressing it, there will be hell to pay.

In short, in order for a security measure to advance versus undermine resilience, it must be able to survive a "morning-after test"; that is, it should be judged as credible if a capable bad guy decides to take it on. If it fails this test, new measures will have to be devised quickly in an atmosphere of heightened anxiety and against a backdrop of damaged public trust. This will substantially slow down the ability to recover after a major security event.

It is extremely unlikely that the current container security regime would survive a security incident involving a weapon of mass destruction. Sadly each of the key elements of that regime poses no meaningful barrier to a determined adversary intent on using a cargo container to ship a dirty bomb or a nuclear device and detonating it within the intermodal transportation and global logistics system. Consider the following hypothetical scenario that is based on a composite of security breaches involving the smuggling of contraband:[4]

A container of athletic footwear for a name brand company is loaded at a manufacturing plant in Surabaya, Indonesia. The container doors are shut and a mechanical seal is put into the door pad-eyes. These designer sneakers are destined for retail stores in malls across America. The container and seal numbers are recorded at the factory. A local truck driver, sympathetic to al Qaeda picks up the container. On the way to the port, he turns into an alleyway and backs up the truck at a nondescript warehouse where a small team of operatives pry loose one of the door hinges to open the container so that they can gain access to the shipment. Some of the sneakers are removed and in their place, the operatives load a dirty bomb wrapped in lead shielding, and they then refasten the door.

The driver takes the container now loaded with a dirty bomb to the port of Surabaya where it is loaded on a coastal feeder ship carrying about 300 containers for the voyage to Jakarta. In Jakarta, the container is transferred to an Inter-Asia ship that typically carry 1200-1500 containers to the port of Singapore or the Port of Hong Kong. In this case, the ships goes to Hong Kong where it is loaded on a super-container ship that carriers 5000-8000 containers for the trans-Pacific voyage. The container is then off-loaded in Vancouver, British Columbia. Because it originates from a trusted-name brand company that has joined the Customs-Trade Partnership Against Terror, the shipment is never identified for inspection by the Container Security Initiative team of U.S. customs inspectors located in Vancouver. Consequently, the container is loaded directly from the ship to a Canadian Pacific railcar where it is shipped to a railyard in Chicago. Because the dirty bomb is shielded in lead, the radiation portals currently deployed along the U.S.-Canadian border do not detect it. When the container reaches a distribution center in the Chicago-area, a triggering device attached to the door sets the bomb off.

There would be four immediate consequence associated with this attack. First, there would be the local deaths and injuries associated with the blast of the conventional explosives. Second, there would be the environmental damage done by the spread of industrial-grade radioactive material. Third, there would be no way to determine where the compromise to security took place so the entire supply chain and all the transportation nodes and providers must be presumed to present a risk of a potential follow-on attack. Fourth—and perhaps most importantly—all the current container and port security initiatives would be compromised by the incident.

In this scenario, the container originated from a one of the thousands of companies that belong to the Customs-Trade Partnership Against Terrorism. It would have transited through multiple

ports—Surabaya, Jakarta, Hong Kong, and Vancouver—that have been certified by their host nation as compliant with the post-9/11 International Ship and Port Facility Security (ISPS) Code that went into effect on 1 July 2004. Because it came from a trusted shipper, it would not have been identified for special screening by the Container Security Initiative team of inspectors in Hong Kong or Vancouver. Nor would it have been identified by the radiation portal. As a consequence, governors, mayors, and the American people would have no faith in the entire risk-management regime erected by the Bush Administration and continued under the Obama Administration. There will be overwhelming political pressure to move from a 0.5 percent inspection rate at overseas ports to a 100-percent inspection rate mandated by the 2007 9/11 Recommendations Act, effectively shutting down the flow of global commerce. The almost certain consequence would be to push the world back into global recession.

Avoiding this sobering scenario requires first a frank admission by the White House, CBP, the Coast Guard, the Department of Energy, and other agencies involved with container security of the shortcomings of the existing measures. Next, it requires aggressive planning to manage a major terrorist incident while new measures are being developed and implemented. Finally, the new measures should be designed to not just protect the intermodal transportation system, but to enhance the capacity to respond surgically and recover the system quickly should the new protective efforts fail.

3. No Plan For Recovery of the Intermodal Transportation System

Immediately following the attacks of September 11, 2001, the White House and the Secretary of Transportation were in direct contact with the top executives of the major airlines. Once commercial aviation was grounded, the challenge was how to get it up and running again. This involved both operational issues as well as convincing the public that it would safe for them to return to the skies. The government had to work closely with the airlines to make this happen and in just three days, the airports began to reopen.

Today, the U.S. government has no contingency plan for managing the aftermath of a major disruption to the global intermodal transportation system. In June 2007, former Secretary of Homeland Security Michael Chertoff rolled out "The Strategy to Enhance International Supply Chain Security" that includes a chapter that outline a response and recovery plan in the aftermath of a major security incident involving a U.S. port. The plan makes no mention of coordination with overseas port authorities and marine terminal operators, ocean carriers, or even America's continental neighbors, Mexico and Canada.[5] In January 2012, the Obama Administration released its National Strategy for Global Supply Chain Security. Three years in the making, the strategy is just under five pages long. It calls for "Fostering a Resilient Supply Chain" by "galvanizing action" and "managing supply chain risk." Given the brevity of the document, not surprisingly, there are few details of how it will achieve these outcomes beyond a commitment "to update our threat and risk assessments; align programs and resources; and engage government,

private sector, and international stakeholders." The stated objective of this engagement is: "to seek specific recommendations to inform and guide our collaborative implementation of the Strategy."[6]

The weakness of these strategy documents points to how underprepared the U.S. government is to deal with the operational aspects of managing a disruption of the global maritime transportation system. For instance, Washington has not established any coordinating mechanisms to work with the four largest global marine terminal operators or the major ocean carriers who move the overwhelming majority of containerized cargo to the United States and elsewhere around the world. Sixty percent of the world's maritime containers are currently at sea. That translates into 10-12 days of shipping traffic underway in the Pacific Ocean and 8-10 days of traffic in the Atlantic Ocean right now. Many of these container ships are post-Panamax which means that they can only be received at the largest seaports and cannot be easily rerouted. A response and recovery plan that identifies no mechanism to directly engage the leaders of the global maritime community is not truly a response and recovery plan.

4. The "Industry-Centric" Inspection Regime: An Alternative Approach for Building Intermodal Transportation System and Supply Chain Resilience

Building more resilient transportation systems and supply chains requires that there be enough transparency to accomplish four things. First, to credibly validate that low-risk

cargo shipments are indeed low risk. Second, to expeditiously resolve whether high-risk cargo shipments actually pose a risk. Third, to support a surgical response to a security breach; i.e., the risk revealed by the incident can be quickly isolated. Fourth, to facilitate a rapid restart of the disrupted portion or portions of the system after a security incident.

The most efficient way to accomplish these four goals is to routinely scan all cargo containers with non-intrusive inspection technology as they enter a marine terminal at the port of loading. This can be accomplished by adapting an "industry-centric" inspection scheme. Such a scheme was assessed by a simulation conducted by the Wharton School using real-world data on container movements in two of the world's busiest ports.[7] The simulation model was informed by experts in terminal operations and experts in fielding and operating container inspection technology within international seaports. The Wharton study concludes that an inspection scheme that integrates non-intrusive inspection technology into the entry gate and as a part of terminal operations is capable of being scaled-up to accomplish nearly universal scrutiny of the contents containerized cargo.

Under the industry-centric scheme, marine terminal operators purchase and install the inspection equipment. That equipment is then maintained and operated by certified third-parties who are overseen by government officials. The equipment and operational costs would be recovered by establishing a universal $15 per-container terminal security fee, much like the security fee included as a part of purchasing a passenger airline ticket. The potential economy and robustness of the industry-centric scheme results from the type and location of the equipment used. The current Container Security Initiative (CSI)

protocol relies on transporting containers to centrally-managed customs facility where the contents are subjected to highly sensitive high-energy x-ray. While the percentage of containers targeted for inspection may be small, the process tends to be time-consuming and disruptive. In contrast, the industry-centric inspection scheme performs a rapid initial scan of 100 percent of inbound traffic as a part of the flow into or within the marine terminal. This is immediately followed, when required, by a secondary inspection using more time-sensitive equipment. The initial and secondary scan can be done using a new passive-detection technology call muon tomography that was originally developed by Los Alamos National Laboratory. Muon tomography can be used to rapidly create three-dimensional images of the objects within cargo containers by using naturally occurring subatomic particles.[8]

The value of routinely obtaining an image of a container's contents as they move through the world's marine terminals is that it can help to immediate validate a low-risk shipment is indeed low-risk. It can also speed up the inspection process associated with shipments that are targeted for examination because they have been determined to be high-risk. Because these images would be available immediate after a container arrives at a marine terminal, concerns can be resolved well before the container is scheduled for loading aboard a container ship. Further, in the event of a security breach, these images can serve as an invaluable forensic tool that will support the rapid isolation of risk. Finally, the these images can support the rapid recovery of the intermodal transportation system in the event of a major security incident, by providing the means to quickly restore trust that in-transit shipments can be double-checked for their safety. In this way cargo can be safely off-loaded at the arrival port.

V. The Broader Case for Building Infrastructure Resilience

Americans know that natural disasters like earthquakes, hurricanes, and tornadoes cannot be prevented. In the nearly ten years that have passed since the attacks on the World Trade Center and the Pentagon, they have also begun to make an uneasy accommodation to the ongoing threat of terrorism as well. The May 1, 2011 killing of Osama bin Laden will not put an end to attacks on innocent civilians and critical infrastructure on U.S. soil.

Even though the risk of terrorism is now a permanent future of 21st Century life, U.S. policy makers and elected officials have generally overlooked the extent to which decisions about infrastructure investment, design, and regulation can play a role in elevating or dampening that risk. As a consequence, they are missing out on both an opportunity to provide a compelling rationale for investing in infrastructure and insuring that when new investments are made, those investments incorporate measures that will mitigate the risk and consequence of attempts to target them.

The case for building more resilient infrastructure should be a compelling one even in the absence of the threat of man-made and natural disasters. Nearly everyday there are media reports that make clear the consequences of deferred maintenance and repair of old and overstressed infrastructure. From bridges collapsing, congested highways, seaports, and airports, to a passenger rail system that is decades behind the rest of the developed world, there is no shortage of evidence that the United States is neglecting a national

transportation system that was once the envy of the world. Add to that a power grid that often cannot handle seasonal rises in temperature, and old pipelines that fail under residential homes and the picture is one of reckless neglect of the essential underpinnings of an advanced society. Modern Americans are acting like grandchildren who are heirs to a mansion that they refuse to maintain. From the street it still looks like a nice house. But as the wiring and plumbing start to fail, the house becomes increasingly unlivable.

Taking infrastructure for granted is not something the United States can afford to do. A new emphasis on building resilience can help change the public's lack of enthusiasm for stepped-up investments in the critical foundations of an advance society. The twin realities that resilience can provide safety and security as well as bolster competitiveness translate into a ripe opportunity for broadening the political base for tackling this important agenda. There is historical precedence for successfully making this kind of case. In creating the interstate highway system, President Dwight Eisenhower made sure to highlight the national defense value that the system could provide by supporting rapid mobilization and urban evacuation.

While emphasizing the role that infrastructure plays in assuring the nation's resilience can strengthen the case for investing in infrastructure, the process of embedding resilience into infrastructure requires specific measures and actions. For the most part, the expertise for developing and the capacity for carrying out those measures and actions

do not lie within the federal government. It is the owners and operators of our country's infrastructure who are best able to identify and mitigate vulnerabilities to the systems they run. Yet the information and intelligence about threats to infrastructure lie almost exclusively within the federal government that is reluctant to share what it knows out of a concern that this knowledge will end up in the wrong hands. The result is that important information and perspectives are not shared, compromising the goal of advancing infrastructure resilience

The federal government is aware that it needs to better cooperate with the private sector. In 2010, the Department of Homeland Security's Office of Infrastructure Protection announced the creation of the "Engagement Working Group" (EWG). The purpose of the EWG is to share classified information with representatives of the private sector in order to better develop strategies to counter threats to infrastructure. While this is a commendable effort, arguably there is a serious flaw with the program. Federal officials will provide security information only to vetted company security officers, who in turn are typically barred from relaying such information to executives and managers who do not hold active security clearances. As a result, investment and operational decisions are often made with little if any attention paid to the potential security stakes – especially for companies where security officers are not a part of the C-suite or where their recommendations are seen as damaging to the bottom-line. Furthermore, without well-tended relationships with decision makers beyond the corporate security office, federal officials will continue to miss out on critically needed insight and perspective of much of the financial and operational expertise of corporate America.

The federal agencies responsible for protecting this country, and their state and local counterparts, still need to do much more work to integrate, fully, the expertise of owners and operators of critical infrastructure and systems. Countering both natural and manmade threats most effectively and efficiently requires both a more open dialogue between federal officials and infrastructure experts and the implementation of truly cooperative, public-private, practitioner-guided programs that build infrastructure resilience.

One promising model for advancing a cooperative, practitioner-guided infrastructure resilience process is the Port Authority of New York and New Jersey's Applied Center of Excellence for Infrastructure Resilience (ACEIR). When the Department of Homeland Security was formed in 2003, it chartered twelve academic Centers of Excellence with the goal of fostering multidisciplinary research in security technologies and processes and providing thought leadership on security policy. This was a good start, but an important next step is to properly test and validate solutions that can function in a demanding operational environment. The White House National Security Strategy released in 2010 recognizes this imperative and calls for employing innovative technology and processes through new, strong and flexible public-private partnerships in order to create next generation, resilient infrastructure. ACEIR is an innovative approach to forging that kind of partnership. The Port Authority, as the nation's largest infrastructure owner and operator, should be applauded for taking the initiative to create an entity dedicated to bridging theory with practical application.

Metropolitan New York offers the ideal environment for developing and testing infrastructure resilience measures. The Port Authority's facilities support the movement of people and goods for one of the world's most densely populated and commercially active regions. The diversity of facilities which include the World Trade Center site and multi-modal transportation systems (tunnels, bridges, bus terminals, airports, maritime facilities, mass transit rail), that cross state borders can test concepts in the environment where they need to be most effective – at the intersection of critical infrastructure interdependencies. And, without addressing the vulnerabilities of critical infrastructure interdependencies, the end game of a more secure society will never be achieved.

As a test-bed, the Port Authority can subject promising technologies and processes to very demanding operational volume and velocity challenges. Those that hold up under the kind of enormous operational stress to which systems in New York are subjected, are likely to fare quite well if adopted nationwide. Infrastructure operators would know that there is little risk that these tools and practices would fail in their urban areas.

In the summer of 2010, the Port Authority stood up ACEIR to facilitate the provision of a real world test-platform for technological applications and processes. Its purpose is to ensure that research projects are vetted at the outset by frontline operators, engineers, and managers. Overtime, ACEIR can also provide a venue for providing industry input into the federal research and development projects. Rather than simply evaluating projects developed by federal agencies, ACEIR could be an excellent source for identifying

new research needs. Though still in its formative stage, ACEIR can and should be replicated for other infrastructure sectors.

Efforts to advance infrastructure resilience must have as a strategic priority ensuring that any new investments made in extending the lifespan of current infrastructure systems, integrate measures that will assure their continuity in the face of disruptive risk. The time for doing so is now. In 2008, the American Society of Civil Engineers evaluated the nation's inventory of infrastructure and gave it a grade of "D." They identified an investment gap of more than $2 trillion to repair U.S. roads, bridges, ports and other critical facilities and systems. That tab cannot be put off indefinitely. When the nation finally begins to attend to its ailing foundations, it will have a historic opportunity to incorporate measures that assure its resilience in the face of man-made and natural disturbances.

The United States is still in the formative stages of crafting the means to secure infrastructure and build resilient infrastructure systems. The most serious challenge to address is the interdependencies among infrastructure sectors. The inescapable reality is that no system operates in isolation. Because these interdependencies are so vast and complicated, the best place to try and understand them is not at the national level, but within regions and communities. This means that developing resilient infrastructure systems must necessarily be from the bottom up as opposed to the top down. But, advancing resilience at the community level requires that the civic and business leaders

of those communities have the tools to do so, that they have a way to measure their progress, and that there be clear benefits for reaching a recognized standard.

One way to tangibly reward communities is to provide them with better bond ratings and lower insurance premiums if they are able to demonstrate that they have adopted measures that both drive down the risk of damages and improve the speed of recovery. But making insurance an ally in dealing with the risk of catastrophic events is challenging for three reasons. First, insurers tend to steer away from things that may involve ruinous losses and insolvency. Second, insurers want to have as broad a pool of policyholders as they can to diversify the risk. Therefore they need to be confident that enough people will elect to buy their insurance product to allow for this diversification. Third, private insurance companies need to be confident that the measures they would be subsidizing by way of reduced premiums do in fact mitigate risk and that their clients are actually adopting these measures.

Federal and state governments can help lower or eliminate each of these barriers for insurers. For instance, government could cap the risk that insurance companies face by effectively becoming a reinsurer. That is, the government can establish a ceiling on the amount of losses a private insurance company would have to pay, and agree to make up the difference to the policyholder if the losses exceed the cap. The government can also help assure an adequate pool of customers for the insurance companies by providing a tax break to the insurers who write new policies or by providing grants to communities to

subsidize the initial premiums. Finally, the government can establish and reinforce the standards against which the insurance incentive is set.

A very promising model for deepening private-public cooperation and aligning financial incentives for building and maintaining preparedness at the local level is the "Community Resilience System Initiative" that has been developed by the Community and Regional Resilience Institute (CARRI) as a project initially based out of Oakridge National Laboratory. CARRI has led an effort to define the parameters of resilience, modeled on the creation of the fire and building codes over a century ago. Drawing on a two-year prototype effort undertaken in Charleston, South Carolina, Gulfport, Mississippi, and Memphis, Tennessee, the initiative set out to identify the policies, practices and capabilities that can increase the ability of communities to maintain essential functions with little disruption or, when disrupted, to recover those functions rapidly and with minimal loss of economic and social value. To accomplish this, the initiative sought to help community stakeholders: (1) understand what characterizes resilience; (2) how to assess resilience; (3) how to prioritize options for improving their resilience; (4) how to objectively measure the impact of the improvements; and (5) how they can be rewarded for their investments.

After two years of field research, CARRI spent an additional eighteen months convening a network of former governors and former and current mayors, emergency planners,

finance and insurance executives, representatives from various government agencies and academics to develop detailed guidelines and comprehensive supporting resources that will allow communities to devise resilience plans. These insights have been embedded into web-enabled tool, that can be quickly modified and upgraded as new lessons are learned. This tool is being tested in eight communities across the United States.

The community resilience system has been designed to provide community leaders the ability to assess their resilience, plan how to make their communities more resilient, implement and sustain those plans, and also evaluate and revise planning as needed. The system includes an emphasis on infrastructure, thereby infusing it with the kind of local knowledge and expertise that will improve the prospects for it to be replicated and quickly adopted by other communities nationwide.

VI. A Unifying Imperative

One final benefit of making resilience a national imperative is that it reinforces what unites a society as opposed to what divides it. Quite simply, it is not possible to build resilience without substantial collaboration and cooperation at all levels within a society. Individuals must develop the means to withstand, rapidly recover from, and adapt to the risks they face at a personal and family level. Companies and communities must look within and beyond themselves to ensure that they are prepared to handle what may come their way as a result of internally and externally generated risks. Finally, at the national, level, the emphasis on resilience highlights the necessity for forging relationships and developing protocols for dealing with shared risks.

In short, a determination to confront ongoing exposure to catastrophic man-made and natural disasters is not an act of pessimism or paranoia. Nor is it something that is inherently a cost center. Resilience is essential for building and maintaining the elements necessary for a productive and competitive economy. It is a mature recognition that things go wrong from time to time, and that in preparing for such times, one is reminded not to take important and critical things for granted.

VII. Acknowledgements

This report could not have been accomplished without the outstanding support provided by the Center for National Policy's Research Assistants, Daniel Glassman and Andrew Lavigne.

Portions of an early draft of this report were published in *TR News*, July-August 2011.

VIII. About the Authors:

Stephen E. Flynn

Dr. Stephen Flynn is a Professor of Political Science and the Founding Co-Director of the George J. Kostas Research Institute for Homeland Security at Northeastern University. Before arriving at Northeastern in November 2011, he served as President of the Center for National Policy and spent a decade as a senior fellow for National Security Studies at the Council on Foreign Relations. Dr. Flynn served in the Coast Guard on active duty for 20 years, including two tours as commanding officer at sea. He is the author of *The Edge of Disaster: Rebuilding a Resilient Nation* (Random House, 2007), and *America the Vulnerable* (HarperCollins 2004). Flynn holds the M.A.L.D. and Ph.D. degrees from the Fletcher School of Law and Diplomacy, Tufts University.

Sean P. Burke

Sean Burke joined Northeastern University's Kostas Research Institute as Associate Director and Research Fellow on November 1, 2011. Immediately prior to coming to Northeastern, Mr. Burke was the Vice President and Senior Fellow at the Center for National Policy in Washington, DC. Mr. Burke has worked as an attorney at the Port Authority of New York and New Jersey, in the Operations Division of the New Jersey Office of Homeland Security and Preparedness and as a policy analyst at the Department of Homeland Security. Mr. Burke is a former U.S. Coast Guard officer. Mr. Burke earned a B.S. in Government from the U.S. Coast Guard Academy and a J.D. from Seton Hall University School of Law.

IX. About the Center for National Policy

The Center for National Policy is an independent think tank dedicated for more than thirty years to advancing the economic and national security of the United States. CNP brings together thought leaders and decision makers who are focused on the revitalization of our economy for the benefit of all Americans and the strengthening of the values of human rights and democracy at home and across the globe.

X. NOTES

---

[1] Stephen Flynn, "American The Vulnerable," *Foreign Affairs* LXXXI: 1 (Jan-Feb. 2002): 60-74

[2] Joint Testimony of David Heyman, Paul Zukunft, and Kevin McAleenan before the Subcommittee on Border and Maritime Security, Committee on Homeland Security, on "Balancing Maritime Security and Trade Facilitation: Protecting Our Ports, Increasing Commerce and Securing the Supply Chain," on Feb 7, 2012; p. 10.

[3] "Estimating the Operational Impact of Container Inspections at International Ports." Nitin Bakshi, Stephen Flynn, Noah Gans, *Management Science*, 57:1 (Jan 2011): 1-20.

[4] Stephen Flynn, "Overcoming the Flaws in the U.S. Government Efforts to Improve Container, Cargo, and Supply Chain Security." Hearing on "Container, Cargo and Supply Chain Security – Challenges and Opportunities" before the Homeland Security Appropriations Subcommittee, Committee on Appropriations, U.S. House of Representatives (April 2, 2008).

[5] "Strategy to Enhance Global Supply Chain Security, U.S. Department of Homeland Security (July 2007)

http://www.dhs.gov/xlibrary/assets/plcy-internationalsupplychainsecuritystrategy.pdf

[6] "National Strategy for Global Supply Chain Security," The White House (Jan 2012). http://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf

[7] "Countering the threat of nuclear terrorism," Nitin Bakshi, Stephen Flynn, Noah Gans, The Wharton School, University of Pennsylvania, Issue Brief (January 2012) http://opim.wharton.upenn.edu/risk/library/WRCib2012a_Port-Security.pdf

[8] Muon tomography scanners are under development by Decision Sciences International Corp. In the interest of disclosure, the principle investigator for this report, Dr. Stephen Flynn, serves on Decision Sciences' advisory council. http://www.decisionsciencescorp.com/solutions_template.aspx?id=34