

Strategic Approach to Critical Infrastructure Protection

Chris Hornbarger

March 31, 2005

The following discussion focuses on factors states should consider in addressing the critical infrastructure protection (CIP) challenge at the state level. The principles are not substantially different at the federal level.

The CIP Challenge from the State Perspective

What is the bottom line for state political leaders and government officials?

- State has a responsibility to protect critical infrastructure in their state.
- State has a shared responsibility with the federal government, obviously, but cannot rely on the federal government since the federal government looks at the problem from a national perspective, is likely to not move quickly enough from the state's perspective, and since Congressional appropriations will reflect the tug-of-war between competing states.
- The federal government's list of critical infrastructure does not include everything that a state should consider critical infrastructure. Conceptually, the list broadens at the state level, and broadens even further at the local level (e.g. state government offices are critical at the state level but not at the federal level; schools may well be critical at a local level but not a state level).
- Vulnerability assessments of particular targets are essential (e.g. chemical plants in the state), and there's a growing but still insufficient base of "best practices" in particular infrastructure sectors, but vulnerability assessments are not enough – they are only one piece, and not necessarily the most important piece.
- A coordinated, prioritized, rational state-wide approach, though a fairly straightforward problem conceptually, nonetheless takes a lot of analysis. There are many variables, and several of those variables have a much higher degree of uncertainty than most other strategic management problems that states face. Will discuss that in detail momentarily.
- Bottom line: states are unlikely to have the expertise in their current workforce to tackle the critical infrastructure challenge from a strategic management perspective, and there are not a lot of companies or firms that can deliver a coordinated strategy.

How Specifically Can State Governments Tackle the CIP Challenge? A 9-Step Approach

Step 1 - *Inventory* the state's list of potential CIP. Implied task of integrating similar bottom-up inventories conducted at the local level, using a state-wide framework and guidance. Implied task: develop a strategy for including private sector and local stakeholders, earlier in the process rather than later.

Step 2 - *Rate criticality* (choose a set of criteria and metrics to do so -- e.g. casualties, \$ impact, psychological impact).

Step 3 - *Assess and measure interdependence* of infrastructures. Not easy: highly dependent on the specific characteristics of different infrastructures. Moreover, the analytic approaches are not mature. Consider the power outage in the Northeast in 2002 -- big economic effects; result of weakness in how different infrastructures (albeit all in the energy sector) interacted with one another.

Step 4 - *Estimate effects and consequences* of disruption, incorporating the analysis in steps 2 & 3, to the inventory developed in step 1.

Step 5 - *Prioritize* the list based on analysis of steps 1 – 4. A numbered list may be unfeasible, nor entirely necessary -- a tiered breakdown based on categories (e.g. Priority 1, Priority 2, etc.) is probably better, particularly since a numbered list implies that the Commonwealth has a high-degree of objective certainty of what should come 1st, 2nd, 12th and so on -- simply not true as we'll discuss below. Additionally, a numbered list will be a target of critics and sharpshooters who say #20 is more important than #15, and that the Commonwealth screwed it up or is pandering to special interests.

Step 6 - *Develop protective measures* that, among other factors, rest on:

- *Target-specific vulnerability assessments*; and
- *Marginal costs and benefits* of particular measures (straightforward marginal analysis, e.g. every \$1 of investment up to \$1000 yields a 1% improvement in security; after \$1000, benefit drops to 0.2% and keeps dropping – therefore, spending that \$1 elsewhere on other critical targets may more effectively lower the overall risk to the state).
- Note: there is very little data on marginal costs and benefits of particular homeland security measures in general, and in critical infrastructure protection in particular. This is largely because (a) there is not a rich statistical bed of data related to attacks against certain types of targets (thankfully), and (b) there has not been adequate time, resources, and coordination for the Nation to evaluate and measure the effectiveness of security practices implemented after September 11.
- Therefore, the difficulty of performing marginal analysis requires a coherent approach that the state must deliberately manage, continuously adjust and improve over time. The state must periodically reevaluate its assumptions and estimates of marginal cost and benefit, and must systemically capture relevant data, both from the state's experience but also drawing on

available data from the federal government, other states, private sector corporations, and academia. States should consider partnership(s) with institutions of higher learning (e.g. state universities) to advance this research.

Step 7 – *Assess the efficacy of various policy instruments* to implement, encourage, or require the protective measures above. Such instruments could include, but are not limited to:

- legislation
- regulation
- tax incentives
- zoning
- grants
- establishing state, or facilitating the establishment of private sector, boards to certify or rate private sector entities on their infrastructure protection efforts, and/or make public or require that private sector entities make public, those certifications or ratings
- establishing state mechanisms, such as the federal sector-specific Information Sharing and Analysis Centers (ISACs), to share information and best practices
- outreach to private sector
- public education
- insurance and reinsurance

Step 8 - *Integrate the above into a final state plan* that: (1) provides clear guidance on where the state will focus effort and resources, and (2) supports that plan with corresponding programs and budgets, corresponding partnerships with federal, local, and private sector entities, corresponding emergency preparedness plans, and appropriate public communications efforts; and (3) . Again, a tiered approach to classifying the "Priority 1" initiatives and funding priorities, the "Priority 2s" etc is probably the right way to go.

Step 9 - *Implement action, and measure and assess results*. There is inherent difficulty in assessing results: (1) if no attacks occur, which measures helped prevent the attacks?; (2) did we spend too much on those measures?; (3) if attacks occur, clearly the measures were not sufficient and clearly we did not spend enough.

Putting the Plan in Motion

The steps above are logically sequential, but like the Defense Planning, Programming, and Budgeting (PPBS) process, they need to go on simultaneously. It's a loop, not a line.

Cutting across each of these 9 steps is a variable of enormous uncertainty -- the threat. Therefore, as the system continues to function in a cyclical manner, states must constantly evaluate the impact new threat data or threat assessments on each step of the process, make appropriate adjustments to the

process and plan(s), and implement appropriate actions. This is theoretically difficult, but the reality is that either:

- the threat information is very specific and therefore requires a variety of concrete short-term actions that (though potentially significant in terms of effort, resources, scope, and impacts) do not necessarily disrupt the overall set of priorities in a significant way;
- the threat information is based on broad net assessments and therefore is likely to require modest adjustments in each step over a period that's entirely manageable from a program management perspective.

This CIP approach is straightforward, but it requires deliberate management and thoughtfully designed, efficient processes.

Several crucial variables have a high degree of uncertainty – most obviously the threat; but also:

- *Vulnerabilities* - we just don't understand the vulnerability of particular types of targets as well as we need to; it's an immature field;
- *Interdependencies* - ditto;
- *Marginal costs and benefits* - we will never have the rich statistical bed of data that most marginal analysis rests on, and yet marginal analysis is critical to apportioning effort across states and across the Nation.

Therefore, given that the critical infrastructure challenge: (a) is intrinsically complicated by a very high degree of uncertainty, and (b) is non-negotiable given the government's responsibility to protect its citizens, then (c) the key is a coherent plan built upon disciplined and efficient systems that reduce to the practical minimum the uncertainty of each variable.