A Decision Support Tool for a Unified Homeland Security Strategy

Richard White, Aaron Burkhart, Edward Chow, Logan Maynard

Chapter 13

A DECISION SUPPORT TOOL FOR A UNIFIED HOMELAND SECURITY STRATEGY

Richard White, Aaron Burkhart, Edward Chow and Logan Maynard

Abstract This paper describes an asset vulnerability model decision support tool (AVM-DST) that is designed to guide strategic investments in critical infrastructure protection. AVM-DST is predicated on previous research on an alternative risk methodology for assessing the current infrastructure protection status, evaluating future protective improvement measures and justifying national investments. AVM-DST is a web-based application that works within the U.S. Department of Homeland Security Risk Management Framework and enables decision makers to view infrastructure assets risk profiles that highlight various features of interest, select protective improvement measures within a given budget based on defined investment strategies or other criteria, and evaluate protective purchases against varying probabilities of attack over a given period of time. In addition to reviewing the concepts and formulations underlying the application, this paper describes the AVM-DST capabilities, functions, features, architecture and performance.

Keywords: Risk management, asset vulnerability model, decision support tool

1. Introduction

The events of September 11, 2001 and their aftermath exposed the vulnerability of the critical infrastructure to asymmetric domestic attacks. The 2002 Homeland Security Act made critical infrastructure protection a core mission of the Department of Homeland Security (DHS). From the outset, DHS's goal has been to develop a program that would "establish standards and benchmarks for infrastructure protection and provide the means to measure performance" [17]. Quantifiable metrics are not only essential to developing coherent strategy, but they are also the law under the 1993 Government Performance and Results Act. Nevertheless, despite successive attempts over the ensuing years [2–5], a 2010

review of DHS's approach to risk analysis conducted by the National Research Council [16] "did not find any DHS risk analysis capabilities and methods that are as yet adequate for supporting DHS decision making." Arguably, the absence of viable metrics and standards have beset attempts to identify the critical infrastructure [15], assess and analyze risks [10] and allocate resources [14] – all of them basic steps in the Risk Management Framework that underpins the current National Infrastructure Protection Plan [7]. While much research has been conducted on infrastructure [11] and terrorism [13] risk modeling, a cursory analysis of 21 models [9] determined that not one of them satisfied fundamental challenges cited in the National Research Council report [22]. That no effective metrics have been found is indicated by the lack of supporting risk analysis in the 2014 DHS budget request to Congress [6]. Without a viable metric, DHS is unable to assess the current protective status, evaluate future protective improvement measures and justify national investments.

This paper describes a decision support tool based on an asset vulnerability model (AVM) that is designed to lend strategic direction to critical infrastructure protection efforts [21]. AVM-DST is a web-based application that allows decision makers to view infrastructure asset risk profiles that highlight various features of interest, select protective improvement measures within a given budget based on investment strategies or other criteria, and evaluate protective purchases against varying probabilities of attack over a given period of time.

2. AVM Overview

In 2013, an asset vulnerability model (AVM) was developed to overcome the challenges cited in the National Research Council report [16] and provide DHS with a quantitative means to guide strategic investments in critical infrastructure protection [21]. AVM is a risk analysis methodology that works within the DHS Risk Management Framework to provide a baseline analysis, cost-benefit analysis and decision support tools that provide guidance in selecting critical infrastructure protective improvement measures. AVM is predicated on a measure designated as Θ, which represents the attacker's probability of failure. The selection of Θ was informed by the game theoretic research of Sandler and Lapan [18] that evaluates defensive strategies based on an attacker's choice of target. The Θ formulation is constructed from five parameters corresponding to the five phases of emergency management – prevent, protect, mitigate, respond and recover [12]:

$$\Theta = P(dis) \cdot P(def) \cdot P(den) \cdot P(dim) \cdot Pct(dam) \tag{1}$$

where $P(dis)$ is the probability that an attack can be detected or disrupted, $P(def)$ is the probability that an attack can be defeated, $P(den)$ is the probability that a worst case disaster can be averted, $P(dim)$ is the probability that 100% of the survivors can be saved and $Pct(dam)$ is the decrease in economic output times the percentage increase in mortality rate.

$P(dis)$ corresponds to the "prevent" phase of emergency management and is calculated from known intelligence data by dividing the number of thwarted attacks by the number of planned attacks (only planned attacks that were discovered; presumably they were thwarted before execution) and executed attacks culled from available sources such as the Global Terrorism Database (`www.start.umd.edu/gtd`). $P(def)$ corresponds to the "protect" phase of emergency management and is derived from the protective measure index (PMI) assessed by Argonne National Laboratory [10] from data collected in DHS security surveys and vulnerability assessments. $P(den)$ corresponds to the "mitigate" phase of emergency management and may be derived from the resilience index (RI), also calculated by Argonne National Laboratory [9], that assesses failure modes and redundancies. $P(dim)$ corresponds to the "response" phase of emergency management and may be expressed as the percentage of survivors that first responders can rescue and treat within 72 hours of a catastrophe as determined by DHS data collected from the Threat and Hazard Identification and Risk Assessment (THIRA) Program [21]. The $Pct(dam)$ parameter represents both the "recovery" phase of emergency management and the magnitude component of the risk formulation. The parameter is computed as the product of the change in the Gross Domestic Product (GDP) and national homicide rates expected from the loss of a particular asset. According to data from the Bureau of Economic Analysis and the National Center for Health Statistics, the 9/11 attacks registered a 47% decrease in the GDP, down from 6.43% in 2000 to 3.38% in 2001, and a 20% increase in national homicides, up from 5.9 to 7.1 deaths per 100,000 from 2000 to 2001.

The chief criticism leveled by the National Research Council was the inability to produce reliable threat estimates (i.e., "probability of attack") for human-initiated (i.e., "threat-driven") events because of a dearth of data to support robust statistical analysis [16]. AVM overcomes this challenge by adopting an "asset-driven" risk assessment methodology and replacing "threat estimation" with "threat localization." Threat localization realizes that even with a robust set of data, as in the case of natural phenomena, it is still impossible to predict exactly where and when the next natural disaster will occur. The best forecasters can do is localize the problem to justify protective investments. Thus, while earthquakes are national phenomena, their prevalence along the West Coast justifies the more stringent seismic standards imposed in California compared with those imposed in Connecticut. Localization can be similarly achieved for the critical infrastructure without the benefit of a robust data set.

Homeland Security Presidential Directive #7 directs the protection of assets "whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to the use of a weapon of mass destruction... [or] have a debilitating effect on security and economic well-being" [19]. Of the sixteen infrastructure sectors currently categorized by the federal government [20], only the nine sectors listed in Table 1 may be targeted to precipitate mass or debilitating effects.

Table 1. Targeted critical infrastructure sectors.

ID	Infrastructure Sector
1	Chemical Plants
2	Dams
3	Energy
4	Financial Services
5	Food and Agriculture
6	Information Networks
7	Nuclear Reactors, Materials and Waste
8	Transportation Systems
9	Water and Wastewater Systems

According to the National Research Council, a good risk analysis (i) conveys current risk levels; (ii) supports cost-benefit analysis; (iii) demonstrates risk reduction effects across multiple assets at different levels of management; and (iv) measures and tracks investments and improvement in overall system resilience over time [16]. Working within the DHS Risk Management Framework, AVM can convey current risk levels through a baseline analysis of the critical infrastructure sectors identified in Table 1 using the Θ risk formulation in Equation (1). AVM can further facilitate cost-benefit analyses of proposed protective improvement measures using the following formulation:

$$\begin{aligned} \Delta\Theta &= P(\Delta dis) \cdot P(\Delta def) \cdot P(\Delta den) \cdot P(\Delta dim) \cdot Pct(dam) \\ D(\Delta\Theta) &= D(\Delta dis) + D(\Delta def) + D(\Delta den) + D(\Delta dim) \end{aligned}$$

Each proposed measure has an associated $\Delta\Theta$ protective gain and $D(\Delta\Theta)$ implementation cost. Multiple protective improvement measures may be proposed for a given asset, for assets within a region or for assets across the nation. AVM cost-benefit analysis calculates a $\Delta\Theta$ and $D(\Delta\Theta)$ for every combination of proposed improvement measures and identifies the combination that provides the greatest protective gain for the least cost. In this manner, AVM can narrow down a list of candidates to those that offer the best value.

AVM works with and supports the DHS Risk Management Framework. Starting in Step 2 (Identify Infrastructure) of the framework, AVM restricts the problem set to the nine critical infrastructure sectors identified in Table 1, overcoming past problems with developing a definitive National Asset Database, assessed by a DHS Inspector General as containing "many unusual or out-of-place assets whose criticality is not readily apparent, and too few assets in essential areas" [15]. An AVM baseline analysis unifies data collection efforts by the DHS Enhanced Critical Infrastructure Protection (ECIP) Program [10] working inside the perimeter and by the Threat and Hazard Identification and Risk Assessment System working outside the perimeter [8] in Step 3 (Assess and Analyze Risks) of the Risk Management Framework. AVM cost-benefit analy-

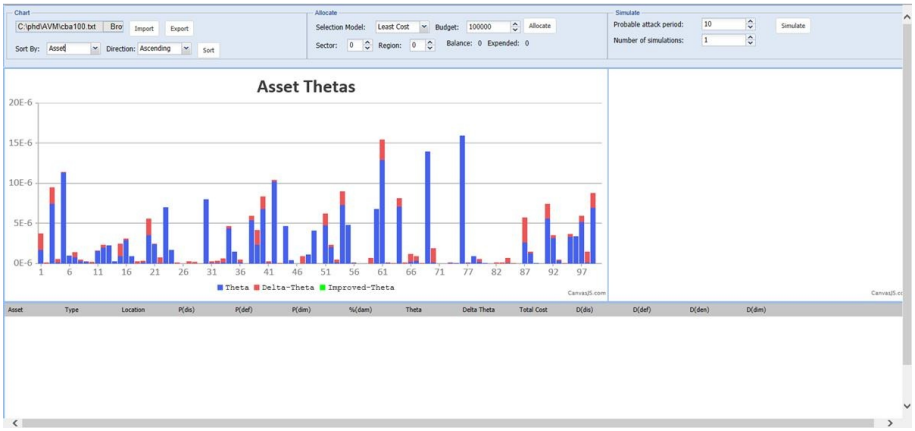

Figure 1. AVM-DST display of 100 simulated assets.

sis, perhaps conducted by the National Infrastructure Simulation and Analysis Center (NISAC), can identify the optimum combination of proposed protective improvements competing for Homeland Security Grant Program (HSGP) funding in Step 4 (Implement Risk Management Activities) of the Risk Management Framework. At every step and at all levels of the Risk Management Framework, AVM-DST can facilitate strategic analysis and decision making as described in this paper.

3. AVM-DST Capabilities and Functions

AVM-DST is a web-based application that allows decision makers to view infrastructure asset risk profiles that highlight various features of interest, select protective improvement measures within a given budget based on defined investment strategies or other criteria, and evaluate protective purchases against varying probabilities of attack over a given period of time.

3.1 Viewing a Risk Profile

Figure 1 shows a critical infrastructure risk profile by asset ID number. Real data is not available because it is protected from disclosure under the 2002 Homeland Security Act, even overriding requests made under the Freedom of Information Act. In the AVM-DST display, the current Θ protective values of assets are represented by blue bars. The current Θ protective values are derived from the AVM baseline analysis. The taller the bar, the better the asset is protected. The notional ID number of an asset is listed on the x-axis. Red bars indicate $\Delta\Theta$, which is the additional protection to be gained by purchasing measures recommended by AVM cost-benefit analysis.

AVM-DST enables decision makers to examine the current critical infrastructure risk profile from a number of different perspectives. For example,

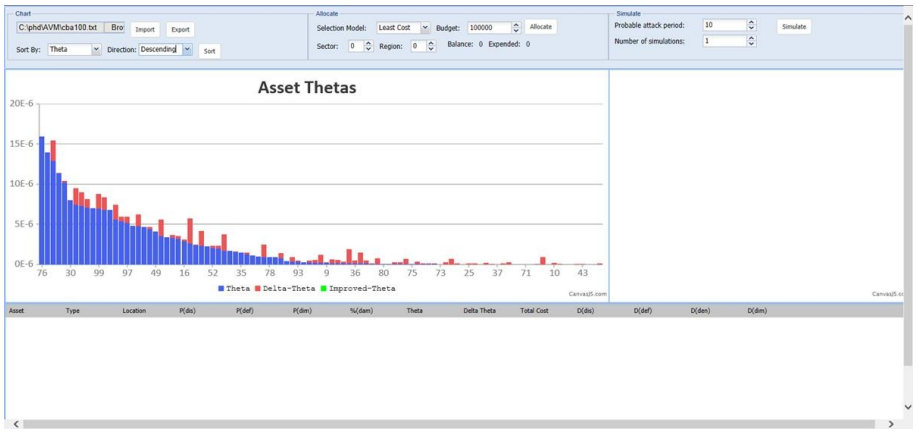

Figure 2. Critical infrastructure risk profile by Θ value.

Figure 2 shows the same assets sorted by Θ, identifying the most protected to the least protected assets. Similarly, the data may be sorted by asset type to display the relative protection of assets in the same sector, or by asset location to depict the relative protection of assets in a given geographic region. Other views may also be generated as desired.

3.2 Selecting Protective Improvements

AVM-DST assists decision makers with selecting protective improvements for purchase. Each protective improvement, indicated by a red bar in Figure 2, has an associated cost value. AVM-DST assists decision makers in selecting protective improvements within the available budgetary constraints. AVM-DST does this by allowing decision makers to select improvements individually or collectively. Individually, the decision maker can select protective improvements by simply clicking on the associated red bars. Collectively, the decision maker can have AVM-DST automatically select protective improvements based on one of seven investment strategies: (i) least cost; (ii) least protected; (iii) region protection; (iv) sector protection; (v) highest $\Delta\Theta$; (vi) highest consequence; or (vii) random protection.

The least cost investment strategy purchases all protective improvement measures based on the lowest cost. Given a fixed budget, this strategy attempts to purchase as many protection measures as possible, regardless of their individual protective gain. The advantage of this strategy is that it affords the purchase of the largest number of protective measures, which may make it politically attractive to "share the wealth" among more congressional districts.

The least protected investment strategy purchases protective improvement measures for the assets that have the least protection as determined by their Θ values. This strategy has the intuitive advantage of allocating resources where they are most needed or at least towards assets that are the most vulnerable.

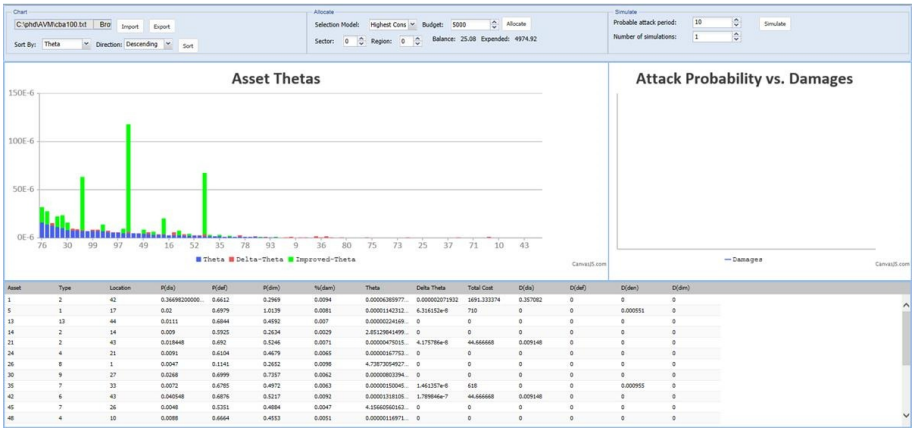

Figure 3. Protective improvement purchase using the highest consequence strategy.

The region protection investment strategy purchases protective improvement measures for regions of the country that are deemed to be more susceptible to attacks than others. This strategy is similar to that used by the Urban Area Security Initiative (UASI) Grant Program administered by DHS.

The sector protection investment strategy allocates funds to a specific sector that is deemed to be more susceptible to attack or whose incapacitation or destruction is considered to have significant damage effects.

The highest $\Delta\Theta$ investment strategy allocates funds to protective improvement measures that provide the highest $\Delta\Theta$ protection gain regardless of cost. This may be considered to be a cost optimization scheme by purchasing protective measures that provide the highest return on investment.

The highest consequence investment strategy allocates funds to assets with the highest magnitude component in terms of national economic and mortality consequences as determined by the product of their $P(dim)$ and $Pct(dam)$ values. Like the least protected investment strategy, this strategy has the intuitive advantage of allocating resources where they are most needed in terms of the damaging effects.

The random protection investment strategy purchases protective improvements without regard to any properties of the measure or asset. This strategy was created to gain insight into the effects of non-systematic purchases, roughly mimicking current practice.

To engage a strategy, the decision maker must select the desired strategy, enter the amount of budgeted funds and click "Allocate." AVM-DST automatically selects the available protective improvements within the given budget amount and uses green bars to indicate their purchase. Additional information regarding each selected improvement is displayed in the detail grid panel as shown in Figure 3. Decision makers may further customize their choices by clicking on asset records in the detail grid panel and deleting them from the selection.

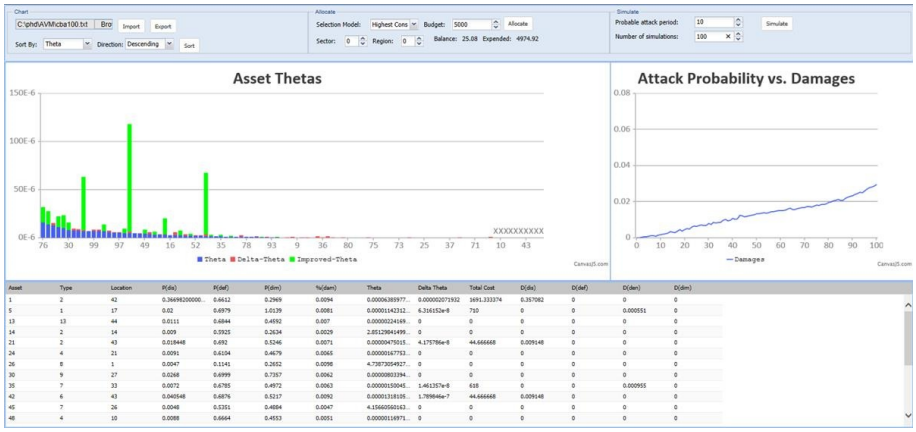

Figure 4. AVM-DST attack simulation and damage estimate.

3.3 Evaluating Protective Improvements

AVM-DST assists decision makers in evaluating their proposed protective improvement purchases through an attack simulator. The attack simulator is engaged by specifying the probable period of attack and number of simulations before clicking the "Simulate" button. The attack simulator graphs the total amount of damage suffered over the probable attack period across a range of attack probabilities as shown in Figure 4. Clauset and Woodard [1] have estimated that there was an 11% to 35% chance of a 9/11-scale terrorist attack in the 40-year period between 1968 and 2007. Moreover, they estimated a 19% to 46% chance of another such attack over the next ten years.

AVM-DST uses the revised Θ values from protective improvement purchases to compute the damage based on the probability of a successful attack. The simulation begins by calculating an annual attack expectancy. The attack expectancy is calculated by dividing the current probability of attack by the probable attack period. So, for example, an estimated 30% probability of attack over ten years has a 3% annual attack expectancy. AVM-DST generates a uniform random number between zero and one that represents the probability of attack during a given year. A probability of attack that is less than the annual attack expectancy indicates that an attack was initiated. Whether or not the attack is successful depends on the target. AVM-DST selects the target with the lowest Θ value in accordance with the position of Sandler and Lapan [18] that attackers will choose targets for which they are the least likely to fail. AVM-DST then generates a uniform random number between zero and one that represents the attacker's probability of success. Next, it calculates a probability of failure as the product of $P(dis)$, $P(def)$ and $P(den)$ for the selected target. These components correspond to the prevent and protect phases of emergency management. If the probability of success is greater than the probability of failure, then the attack is deemed a success and the asset

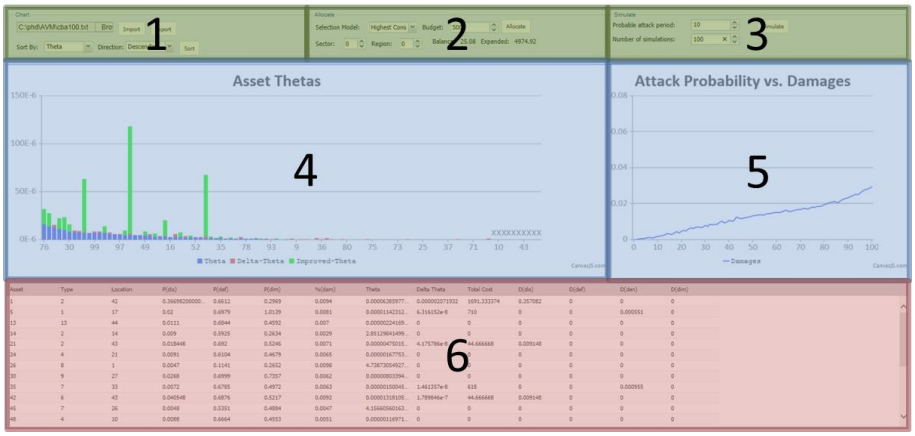

Figure 5. Application user interface.

is removed from further simulation. AVM-DST calculates the damage from a successful attack as the product of $P(dim)$ and $Pct(dam)$ corresponding to the response and recovery phases of emergency management. The collective damage assessments for each attack probability are averaged over the number of specified simulations. More simulations provide finer results, but they also take longer to execute.

4. AVM-DST User Features and Options

The range of AVM-DST robust capabilities and functions are easily accessible from a compact interface that supports a variety of user features and options.

4.1 Compact User Interface

The AVM-DST user interface is differentiated into six display panels presented on a single screen as shown in Figure 5. Each panel facilitates a different application function. The three panels at the top are the control panels, which facilitate user input and control over AVM-DST capabilities. The two panels in the middle are the chart panels: Panel 4 is the main chart that shows assets by their current and improved Θ protective values and Panel 5 is the secondary chart that shows the damage results from attack simulations across a range of probabilities. Both chart panels are fully interactive and support zooming and panning. Panel 6 at the bottom is the asset detail grid panel, which displays detailed record information for each asset selected for protective improvement purchases. This panel is interactive in that records may be added, sorted and deleted from display.

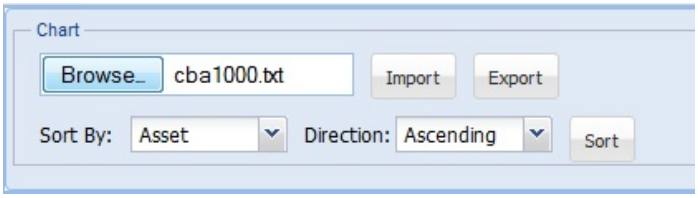

Figure 6. Chart control panel.

4.2 Data Handling and Visualization

AVM-DST provides an extensive set of data handling and visualization capabilities to (i) import assets; (ii) visualize assets; (iii) sort assets; (iv) edit improvements; and (v) export improvements.

- **Import Assets:** AVM-DST imports critical infrastructure asset data from AVM cost-benefit analysis in the comma-separated value (CSV) format. The output file from AVM cost-benefit analysis contains a single record for each asset that identifies its attributes and nominated protective improvements. The following actions must be performed to import an asset file:
  - Click the "Browse" button on the chart control panel (Figure 6).
  - Select the desired asset file to upload.
  - Click "Open" to import the file.

- **Visualize Assets:** Imported assets are automatically displayed in the main chart panel. Each asset is depicted as a bar that represents its current Θ value. The greater the value, the more the asset is protected. The Θ value is updated and displayed as a green bar when protective improvements are selected. The main display also places an "X" below assets that are destroyed in an attack simulation. The damage results from an attack simulation is displayed in the secondary chart panel. The chart shows the calculated damage for different attack probabilities. The following actions must be performed to zoom and pan in each display:
  - Zoom into the chart by clicking and dragging from one point on the chart to another to expand the corresponding subsection of the chart.
  - Pan the chart after it has been zoomed by clicking "Pan" and then click and drag the chart to scroll the chart horizontally. To go back to the zoom mode, click "Zoom."
  - Click "Reset" to restore the chart to maximal zoom.

- **Sort Assets:** AVM-DST also allows users to examine critical infrastructure assets from different perspectives by sorting assets in the main chart panel. The following actions must be performed to sort assets:

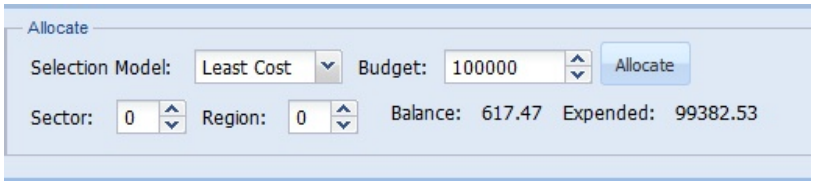

Figure 7. Allocate control panel.

  - Click the "Sort By" box and select the field to use in sorting.
  - Click the "Direction" for sorting and select either ascending or descending.
  - Click "Sort" to update the chart.

- **Edit Improvements:** The record details for assets selected to receive protective improvements are displayed in the asset detail grid panel. AVM-DST allows users to sort this data by clicking the column header associated with the field that is to be sorted. AVM-DST also allows users to remove selected asset improvements by right clicking on the desired record and choosing "Delete."

- **Export Improvements:** Selected improvements may be exported in a CSV file to support implementation efforts. The following actions must be performed to export selected improvements:

  - Click "Export" on the chart control panel (Figure 6).
  - Depending on the browser being used, open the file immediately by selecting the program with which to open it or save the file to the browser-specific download directory.

4.3 Selection of Protective Improvements

As described above, AVM-DST assists decision makers in selecting the desired protective improvements either individually or collectively. To select an improvement individually, a user has only to click on the desired asset indicated by a blue or red bar. The Θ value for the selected asset is updated and is replaced by a green bar. Additionally, the record details associated with the selected asset are displayed in an Excel-like format below the main chart panel. The following actions must be performed to select improvements collectively using one of the predefined investment strategies:

- Click the "Selection Model" dropdown box (Figure 7).

- For the region protection and sector protection models, specify the desired region and sector numbers.

- Enter a dollar amount in the "Budget" field.

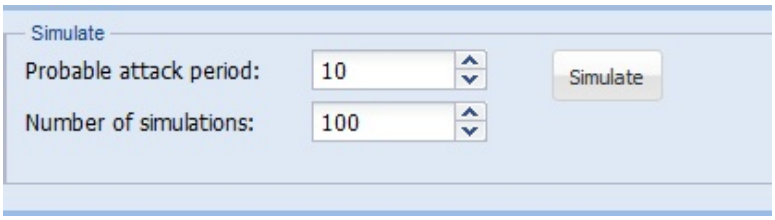

Figure 8. Simulate control panel.

- Click "Allocate."

AVM-DST automatically selects assets based on the user's specifications. The total amount expended and the remaining balance are displayed in the allocate control panel.

4.4 Decision Analysis and Evaluation

As described above, AVM-DST provides a means for a decision maker to assess the effectiveness of an investment strategy by running attack simulations. Each simulation determines if assets are attacked and calculates the total damage due to the attacks over a given period of time. Presumably, the best strategy results in the least amount of damages. The attack simulation results are displayed in the secondary chart panel. The following actions must be performed to run an attack simulation:

- Enter a number of years in the "Probable Attack Period" field in the simulate control panel (Figure 8).

- Enter the number of times to run simulations in the "Number of Simulations" field.

- Click "Simulate."

AVM-DST executes the specified number of simulations and displays the results in the secondary chart, showing the total damage corresponding to each attack probability. The assets that have been destroyed are marked with an "X" on the main chart.

5. AVM-DST Implementation

AVM-DST was constructed in phases using an incremental development process. Phase 1 developed the visualization and data handling capabilities. Phase 2 added the decision support and decision analysis features. AVM-DST is written in JavaScript and utilizes the Ext JS application framework along with the CanvasJS charting plugin. This enables AVM-DST to run with any browser.

5.1 Architecture

AVM-DST is a stand-alone, client-side, browser-oriented web application built using JavaScript and HTML5. It does not currently contain any server side components. It was built using the model-view-controller paradigm, which is recommended, albeit not required, for Ext JS applications. In this paradigm, the model is the representation of the data to be used. The model describes the objects and their fields and specifies object relationships and hierarchies. It also includes the functions used to manipulate the data. Ext JS uses data stores to load, handle and manipulate collections of model instances. A view serves as the visual interface between the user and the application. This includes windows panels and widgets that facilitate input from the user and display output. The controller handles the business logic of the application. It reacts to events and updates the models and views accordingly.

5.2 Development

AVM-DST v1.0 was a proof-of-concept prototype. It included the basic functionality for importing, displaying and sorting asset data. AVM-DST v1.0 used Ext JS built-in charts that did not support zooming and panning. Also, performance issues restricted the number of assets to no more than a few hundred.

AVM-DST v2.0 used CanvasJS to dramatically increase performance and add zooming and panning. This one change enabled AVM-DST to be used to manipulate thousands of assets. It also allowed record details of selected assets to be displayed below the main chart are exported in the CSV format.

AVM-DST v3.0 marked the Phase 2 development by incorporating decision support and analysis tools. It included the control panels, but only the chart and allocate panels were functional. AVM-DST v3.0 did not implement the attack simulation functionality.

AVM-DST v4.0 added the attack simulation functionality. It also added the secondary chart panel to display the results.

AVM-DST v5.0, the current version, fixed the bugs identified in the previous version and optimized the attack simulation algorithm to run faster and accommodate more simulations over longer probable attack periods.

5.3 Performance

AVM-DST was tested on a machine running Windows 7 64-bit with a 3.2 GHz Intel Core i7-4770k CPU and an NVIDIA GeForce GTX 770 GPU. The browser used during testing was Firefox 26.0 and the input test file contained 1,000 records. The least cost investment strategy required the most time to run for this data set, so it was used predominantly during performance testing. Simulation times were recorded using a ten-year probable attack period with ten simulations and 1,000 simulations. The time to run simulations is not always directly proportional to the number of simulations because of a constant

Table 2. Performance of AVM-DST functions.

AVM-DST Function	Time
Import File	65 ms
Render Main Chart	60 ms
Render Secondary Chart	6 ms
Run Allocation Algorithm	174 ms
Render Grid	840 ms
Run 10 Simulations	96 ms
Run 1,000 Simulations	2,287 ms
Sort Data	67 ms

pre-processing time for tasks (e.g., sorting) that are only done once regardless of the number of simulations. Table 2 shows the run times of various functions.

6. Lessons Learned

Performance is always a concern when handling thousands of data records, especially when using web technology. AVM-DST is a stand-alone client-side web application. Because it does not require server-side interaction after it is initially loaded, it does not experience network delays or server-side processing delays that are commonly associated with web applications. AVM-DST was tested using a data file containing 1,000 records and is expected to be able to handle much larger data files.

Initially, the application utilized the built-in Ext JS charts that rely on SVG technology. Because of this, AVM-DST experienced performance problems when handling charts. The browser crashed when the application was tested on the 1,000-record file. Efforts were made to mitigate the problem by implementing paging functionality that loads portions of the data at a time. However, this was not ideal. For this reason, CanvasJS was incorporated because it can quickly and seamlessly handle thousands of data points in the charts.

The asset selection decision support tool must sort the data based on the selection model and then iteratively evaluate each asset for selection. This process is fairly quick so the real performance bottleneck arises when populating the grid with the selected assets.

The performance of the decision analysis tool does not depend on the size of the input file because it only considers the asset that is most likely to be attacked at each iteration. Instead, it is dependent on the probable period of attack and the number of simulations to be performed. Before optimization, this algorithm removes the destroyed assets from the data set during each iteration and then restores and re-sorts them during the next simulation. To prevent the browser from becoming unresponsive, the number of simulations was limited to ten and the probability of attack was incremented in five percent intervals. After optimization, the algorithm sorted only once, then maintained

a counter that referenced the next asset being considered and incremented the counter when it was destroyed. On the next simulation, the counter was then reset to zero. In this manner, a substantial amount of file overhead was eliminated by performing only a single sort and not removing the destroyed asset records. These changes resulted in significant performance improvement. They also afforded greater simulation resolution, allowing the probability of attack to be incremented only one percent at each iteration, but still executing 1,000 simulations in less than three seconds.

7. Conclusions

AVM-DST leverages the AVM risk methodology to enable decision makers to view infrastructure asset risk profiles that highlight various features of interest, select protective improvement measures within a given budget based on seven defined investment strategies and other criteria, and evaluate protective purchases against varying probabilities of attack over a given period of time. Built as a stand-alone, client-side, browser-oriented web application using JavaScript and HTML5, AVM-DST offers a robust range of capabilities and functions that are easily accessible from a compact interface supporting a variety of user features and options. Performance tests show that AVM-DST is capable of handling large data sets with no noticeable delays; it promptly displays simulation results for thousands of assets. Indeed, the AVM-DST research demonstrates that it is possible to guide strategic critical infrastructure protection efforts by assessing the current protection status, evaluating future protective improvement measures and justifying national investments.

Future work related to the AVM-DST web application includes developing additional analytics for the analysis and evaluation component, improved simulation of attack scenarios based on intelligence, support for enhanced trade-offs and extensions for including additional investment strategies. Metrics will be added to the simulations to provide insights into the effectiveness of investment strategies. Additionally, display and visualization enhancements will be implemented, especially optimizing the rendering of the grid panel when the investment allocation tool populates it with the selected assets.

References

[1] A. Clauset and R. Woodard, Estimating the historical and future probabilities of large terrorist events, *Annals of Applied Statistics*, vol. 7(4), pp. 1838–1865, 2013.

[2] Department of Homeland Security, Draft National Infrastructure Protection Plan, Base Plan, Draft NIPP v1.0, Washington, DC, 2005.

[3] Department of Homeland Security, Interim National Preparedness Goal, Homeland Security Presidential Directive 8: National Preparedness, Washington, DC, 2005.

[4] Department of Homeland Security, National Infrastructure Protection Plan, Washington, DC, 2006.

[5] Department of Homeland Security, National Infrastructure Protection Plan, Washington, DC, 2009.

[6] Department of Homeland Security, Budget-in-Brief, Fiscal Year 2014, Washington, DC, 2013.

[7] Department of Homeland Security, NIPP 2013: Partnering for Critical Infrastructure Security and Resilience, Washington, DC, 2013.

[8] Federal Emergency Management Agency, Grant Programs Directorate Information Bulletin, Washington, DC, 2012.

[9] G. Giannopoulos, R. Filippini and M. Schimmer, Risk Assessment Methodologies for Critical Infrastructure Protection, Part I: A State of the Art, JRC Technical Note EUR 25286 EN-2012, Institute for the Protection and Security of the Citizen, European Commission Joint Research Centre, Ispra, Italy, 2012.

[10] Government Accountability Office, Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments, GAO-12-378, Washington, DC, 2012.

[11] T. Lewis, R. Darken, T. Mackin and D. Dudenhoeffer, Model-based risk analysis for critical infrastructures, in *Critical Infrastructure Security*, F. Flammini (Ed.), WIT Press, Southampton, United Kingdom, pp. 3–19, 2012.

[12] M. Lindell, R. Perry, C. Prater and W. Nicholson, *Fundamentals of Emergency Management*, Federal Emergency Management Agency, Washington, DC, 2006.

[13] G. Loo, The evolution of terrorism risk modeling, *Journal of Reinsurance*, vol. 10(3), pp. 1–16, 2003.

[14] T. Masse, S. O'Neil and J. Rollins, The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues and Options for Congress, CRS Report for Congress, Order Code RL33858, Congressional Research Service, Washington, DC, 2007.

[15] J. Moteff, Critical Infrastructure: The National Asset Database, CRS Report for Congress, Order Code RL33648, Congressional Research Service, Washington, DC, 2007.

[16] National Research Council of the National Academies, *Review of the Department of Homeland Security's Approach to Risk Analysis*, National Academies Press, Washington, DC, 2010.

[17] Office of Homeland Security, National Strategy for Homeland Security, Washington, DC, 2002.

[18] T. Sandler and H. Lapan, The calculus of dissent: An analysis of terrorists' choice of targets, *Synthese*, vol. 72(2), pp. 245–261, 1988.

[19] The White House, Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection, Washington, DC, 2003.

[20] The White House, Presidential Policy Directive – Critical Infrastructure Security and Resilience, Presidential Policy Directive/PPD-21, Washington, DC, 2013.

[21] R. White, Towards a Computational Unified Homeland Security Strategy: An Asset Vulnerability Model, Department of Computer Science, University of Colorado at Colorado Springs, Colorado Springs, Colorado, 2013.

[22] R. White, Towards a unified homeland security strategy: An asset vulnerability model, *Homeland Security Affairs*, vol. 10, art. 1, pp. 1-16, 2014.